Державна служба
спеціального зв'язку
та захисту інформації
України

Російські кібероперації

Аналітика
за II півріччя 2023 року

ЗМІСТ

Євгенія Волівник,
керівниця Урядової команди реагування на комп'ютерні надзвичайні події України CERT-UA

Ці два роки повномасштабного вторгнення стали каталізатором прискорення і без того стрімкої еволюції кіберспроможностей ворога та зробили його команди значно досвідченішими. Російські хакери та їхні аналітичні центри постійно шукають нові шляхи застосування кіберможливостей для отримання розвідувальної інформації та підсилення ефекту наземних військових кінетичних та психологічних операцій.

Ми спостерігаємо чіткі зміни у поведінці та цілях хакерських угруповань. З початку другого півріччя 2023 року активність відомих нам військових хакерських груп значно зменшилася, натомість з'явилися нові, раніше невідомі угруповання, які використовують нові методи та процедури. Їх походження та склад учасників ще належить з'ясувати, проте є підстави вважати, що вони так само фінансуються та координуються з російських державних центрів управління. Здобуті під час протистояння цим угрупованням знання та навички не менш цінні, ніж ті, якими ми вже ділимося з нашими партнерами.

Водночас варто звернути увагу на реалізацію тих прогнозів, які ми робили раніше. Кількість та сфокусованість атак зростає, і ключові з них стають дедалі складнішими з технічної точки зору. Все це вимагає подальшого нарощування нашої кіберстійкості, залучення більше ресурсів, а також посилення кооперації та обміну інформацією та технологіями з партнерами, адже Україна продовжує залишатися полігоном для апробації найсучасніших підходів застосування кіберскладової для військових дій.

Попередні звіти:

[II півріччя 2022]

[I півріччя 2023]

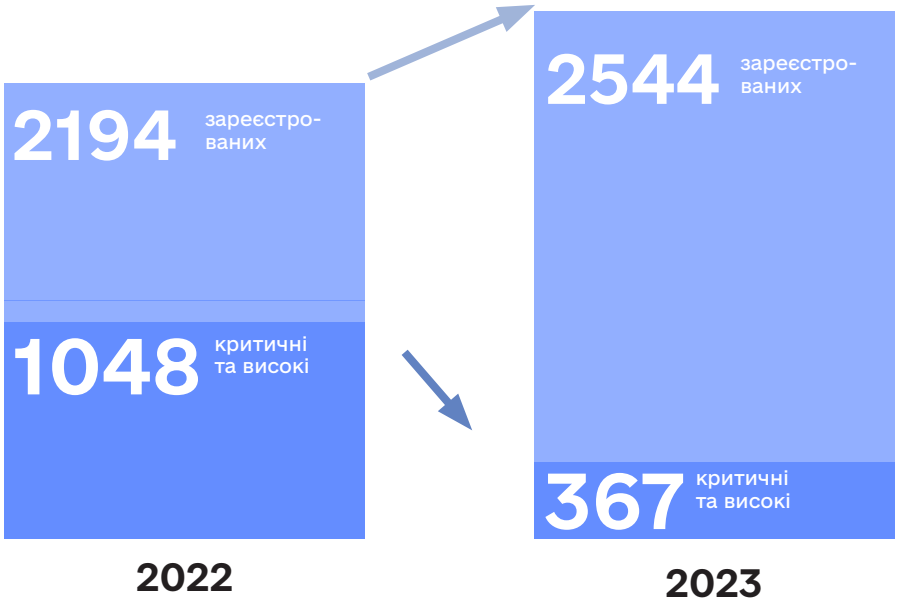
Як ми зазначали у своїх попередніх звітах, всі успішні напрацювання російських кіберпідрозділів із часом починають застосовуватися і проти інших демократичних країн. Це той факт, який всім доведеться взяти до уваги — кіберпростір єдиний, він не має кордонів і потребує оновлення вже застарілих доктрин до захисту. Те, що вас не атаковано, свідчить лише про те, що до вас не дійшла черга, або ви не маєте необхідної телеметрії щодо присутності ворожих хакерських груп вже у ваших системах.

В цілому у 2023 кількість зареєстрованих кіберінцидентів була більша, ніж у 2022. Але треба зазначити позитивну тенденцію — кількість кібератак, які мали критичні наслідки, вдалося суттєво зменшити. Все це стало можливим завдяки покращенню злагодження в діяльності основних суб'єктів забезпечення кібербезпеки України та налагодженню каналів комунікацій з потенційними цілями хакерів, що дозволило швидше реагувати на виклики та попереджати реалізації зловмисних задумів противника.

Пропонуємо вашій увазі аналітичний звіт на основі інформації про російські кібероперації, які були зафіксовані та проаналізовані у другій половині 2023 року. Ми ретельно проаналізували зміни тактик, методик і процедур ворожих хакерів, виокремили ключові підходи, які дадуть можливість прогнозувати подальшу поведінку російських кіберугруповань.

КЛЮЧОВІ ВИСНОВКИ ТА ІНСАЙТИ

КІЛЬКІСТЬ, ІНТЕНСИВНІСТЬ ТА СКЛАДНІСТЬ ІНЦИДЕНТІВ, ОБРОБЛЕНИХ КОМАНДОЮ CERT-UA



У 2023 році кількість кіберінцидентів критичного та високого рівня вдалося зменшити на

65%

У першому півріччі 2023 року в українському кіберпросторі було зафіксоване активне застосування дорогих експлойтів нульового дня*. Угруповання ГРУ отримувало важливі розвіддані, використовуючи популярні клієнтські ПЗ (наприклад, Microsoft Outlook).

У другому півріччі до цього додалися масовані атаки проти телекомунікаційних компаній. Водночас хакери частіше застосовували на N-day експлойти** та збільшили частоту застосування мобільних імплантів.

Суттєві зміни полягають у домінувані серед розслідуваних нами інцидентів саме нових угруповань, кримінальних і хакерських груп, активність яких фахівці не фіксували у попередні періоди. Злами українських телекомунікаційних компаній, які, при цьому, мають широкий арсенал захисних систем, достатні бюджети та кваліфіковані кадри, продемонстрували, що ніхто не може вважати себе захищеним. Атака — це лише питання часу та наполегливості зловмисника. Як зазначалося в попередньому звіті, показовим є тренд на прискорення процесів отримання контролю над ключовими IT-системами через автоматизацію*.

*0-day — вразливість програмного забезпечення, яка ще не відома користувачам чи розробникам та проти якої ще не розроблені механізми захисту

**на N-day експлойт — відома вразливість, яку розробники вже виправили оновленням, проте його ще не встигли всі встановити

*Прикладом тут є діяльність угруповання APT28

КЛЮЧОВІ ІНСАЙТИ ІІ ПІВРІЧЧЯ 2023:

ТЕЛЕКОМ — КЛЮЧОВИЙ НАПРЯМ

Цілеспрямована кампанія з боку російських хакерів, спрямована на провайдерів телекомунікацій.

АКТИВНЕ ЗАСТОСУВАННЯ НАЙСВІЖІШИХ ЕКСПЛОЙТІВ ЯК КІБЕРЗБРОЇ

Активніше застосування найсвіжіших вразливостей в клієнтському програмному забезпеченні (client-side attacks) з метою прихованого доступу та імплантації.

ДОМІНУВАННЯ НОВИХ ГРУП В ЗАГАЛЬНІЙ СТАТИСТИЦІ

Рейтинг найактивніших акторів очолили групи, що наразі не асоційовані зі спецслужбами країни-агресора (хоча вони діють в інтересах російської влади). Вони відзначилися використанням добре продуманих фішингових атак, основною ціллю яких є розповсюдження шкідливого програмного забезпечення для віддаленого керування (RemcosRAT, RemoteUtilities) або програм для викрадення даних (LumaStealer, MeduzaStealer).

ШВИДКА ЕКСПЛУАТАЦІЯ АКТУАЛЬНИХ ТЕМАТИК

Спостерігається висока оперативність розповсюдження вірусів з використанням актуальних інформаційних приводів, наприклад щодо членства України в Організації Північноатлантичного договору чи набору до ЦАХАЛ (на початку військового конфлікту в Ізраїлі).

ЦІЛЬОВІ КІБЕРОПЕРАЦІЇ, СПРЯМОВАНІ ПРОТИ СИЛ ОБОРОНИ, З МЕТОЮ ШПИГУНСТВА

Атаки з метою доступу, контролю та зняття розвідувальної інформації зі спеціалізованих систем контролю поля бою — стратегічна військова ціль противника. Щоб мати доступ до таких систем і до чатів військових та отримати компрометацію облікових даних, хакери створювали і розповсюджували підроблені версії програмного забезпечення, здійснювали атаки, спрямовані на компрометацію мессенджерів, якими активно користуються військові.

ЗРОСТАННЯ АКТИВНОСТІ З БОКУ ФІНАНСОВО СФОКУСОВАНИХ КІБЕРУГРУПОВАНЬ

Ми спостерігаємо активізацію фінансово мотивованих хакерських груп проти українського бізнесу й організацій. У другому півріччі 2023 року фактично 40% зареєстрованих інцидентів були пов’язані саме з викраденням коштів. До прикладу, угрупування UAC-0006 відновило свою діяльність у травні 2023 року, і вже в другому півріччі кількість індидентів, асоційованих з їх діяльністю, зросла до 200.

Це можна вважати новим витком війни — певною ескалацією у спробах утримати ініціативу та присутність на українських об’єктах інформаційної інфраструктури, які становлять інтерес у російських хакерів.

ТЕНДЕНЦІЇ ТА НОВІ ВИКЛИКИ

Disclaimer: цей набір даних зібрано на основі аналітики інцидентів, наданої Урядовою командою реагування на комп'ютерні надзвичайні події України CERT-UA, без урахування випадків, зареєстрованих SOC Державного центру кіберзахисту Держспецзв'язку та інших кіберцентрів*.

ДИНАМІКА ІНЦИДЕНТІВ У ДРУГОМУ ПІВРІЧЧІ 2023

ЗАРЕЄСТРОВАНІ ІНЦИДЕНТИ

+36%

ЗРОСТАННЯ КІЛЬКОСТІ ЗАРЕЄСТРОВАНИХ ІНЦИДЕНТІВ У II ПІВРІЧЧІ 2023 Р.
(окрім інцидентів SOC)

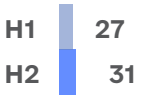
У СЕРЕДНЬОМУ НА МІСЯЦЬ

У СЕРЕДНЬОМУ НА ДОБУ

+15%

КРИТИЧНИХ ІНЦИДЕНТІВ

КРИТИЧНІ ІНЦИДЕНТИ



+33%**

СПРОБ КОМПРОМЕТАЦІЇ ЧЕРЕЗ ШПЗ ЕЛЕКТРОННОЮ ПОШТОЮ

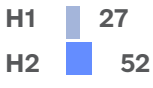
ВИПАДКИ, ДЕ ПЕРЕВАЖАЛО ШПЗ

ВИПАДКИ ЗА РАХУНОК ВИКРАДЕНИХ ПАРОЛІВ

+92%

НОВИХ АТАК НА ЕНЕРГЕТИЧНИЙ СЕКТОР І ЗМЕНШЕННЯ КІЛЬКОСТІ КРИТИЧНИХ ІНЦИДЕНТІВ НА 50%

ІНЦИДЕНТИ В ЕНЕРГЕТИЧНОМУ СЕКТОРІ



*Звіт Державного центру кіберзахисту

**Варто відзначити, що у II півріччі 2023 року ворожі кіберугруповання різко наростили використання такого інструменту, як розсилання шкідливого програмного забезпечення через електронну пошту.

Кількість спроб компрометації таким способом зросла порівняно з першим півріччям 2023 року на 33%. Якщо на H1 було зафіксовано 285 випадків з переважним використанням фішингових атак, то у другому півріччі було зафіксовано 380, значна кількість яких здійснювалась зі скомпрометованих скриньок, що стало можливим через відсутність двофакторної автентифікації.

ДЕ І ЧОМУ

СЕКТОРИ, ЯКІ ЗАЗНАЛИ ЦІЛЕСПРЯМОВАНИХ АТАК

ПІРАМІДА ЗАЛЕЖНОСТІ НАПРЯМУ І ВПЛИВУ КІБЕРАТАК УГРУПОВАННЯ SANDWORM

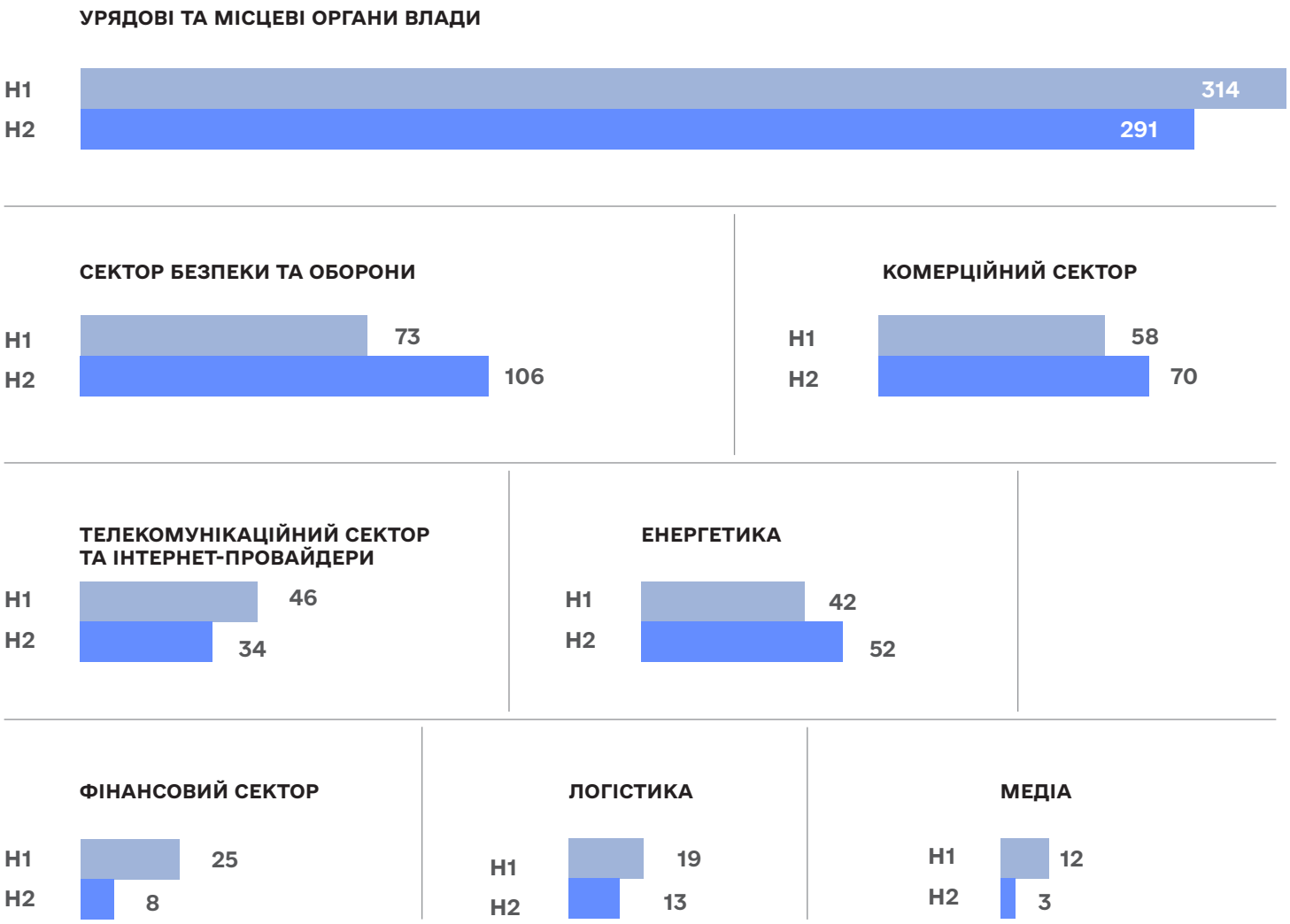
Угруповання динамічно змінюють сектори та цілі для кібератак, що ми спробували відобразити у піраміді.

У 2023 році угруповання UAC-0082 (також відоме як Sandworm, що є військовим підрозділом ГУ ГШ МО РФ) реалізувало 68 атак, з яких 10 були скеровані проти провайдерів телекомунікацій України з використанням технічних вразливостей та

людського фактору. Кібератака на «Київстар» є повноцінною складовою цієї гібридної війни. Кількість спроб здійснити такі атаки зростатиме, а їх успішність залежатиме від готовності організацій протистояти ворогу в кіберпросторі.

Також ми спостерігаємо активну роботу кримінальних груп, які сфокусовані на отриманні доступу до акаунтів поштових сервісів та криптовалютних бірж і викраденні коштів у великих обсягах із застосуванням вірусів та програмного забезпечення для віддаленого доступу «Remote Access Trojan». На підставі аналізу випадків, до дослідження яких були залучені фахівці Держспецзв'язку, презентуємо розподіл інцидентів за секторами.

ОСНОВНІ ЦІЛІ ЗЛОВМИСНИКІВ



РОЗПОДІЛ ІНЦИДЕНТІВ ЗА РІВНЕМ КРИТИЧНОСТІ

Для більш детального розуміння зміни тактик з 2022 та протягом 2023 року, рекомендуємо ознайомитися зі змістом попереднього звіту за І півріччя 2023

CRITICAL SEVERITY INCIDENTS

HIGH-SEVERITY INCIDENTS

MEDIUM-SEVERITY INCIDENTS

LOW-SEVERITY INCIDENTS

ХТО І ЯК

ТОП-5 ВІЙСЬКОВИХ ХАКЕРСЬКИХ ГРУП

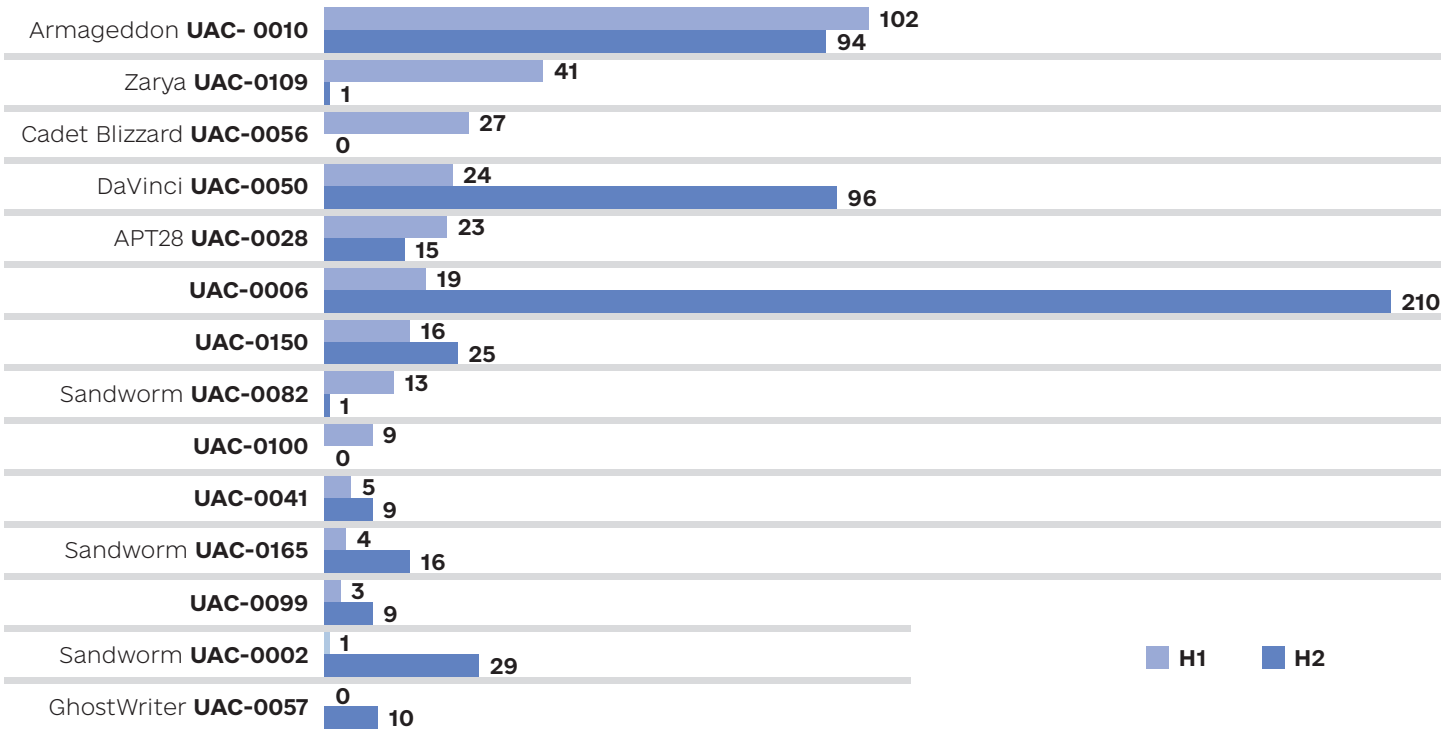
- UAC-0010 (Armageddon) — ФСБ
- UAC-0002 (Sandworm) — ГРУ
- UAC-0028 (APT28) — ГРУ
- UAC-0056 (Cadet Blizzard) — ГРУ
- UAC-0057 (GhostWriter) — Міноборони Білорусі

КОЖНА ДЕСЯТА

кібератака на Україну здійснюється військовими хакерами ворога!

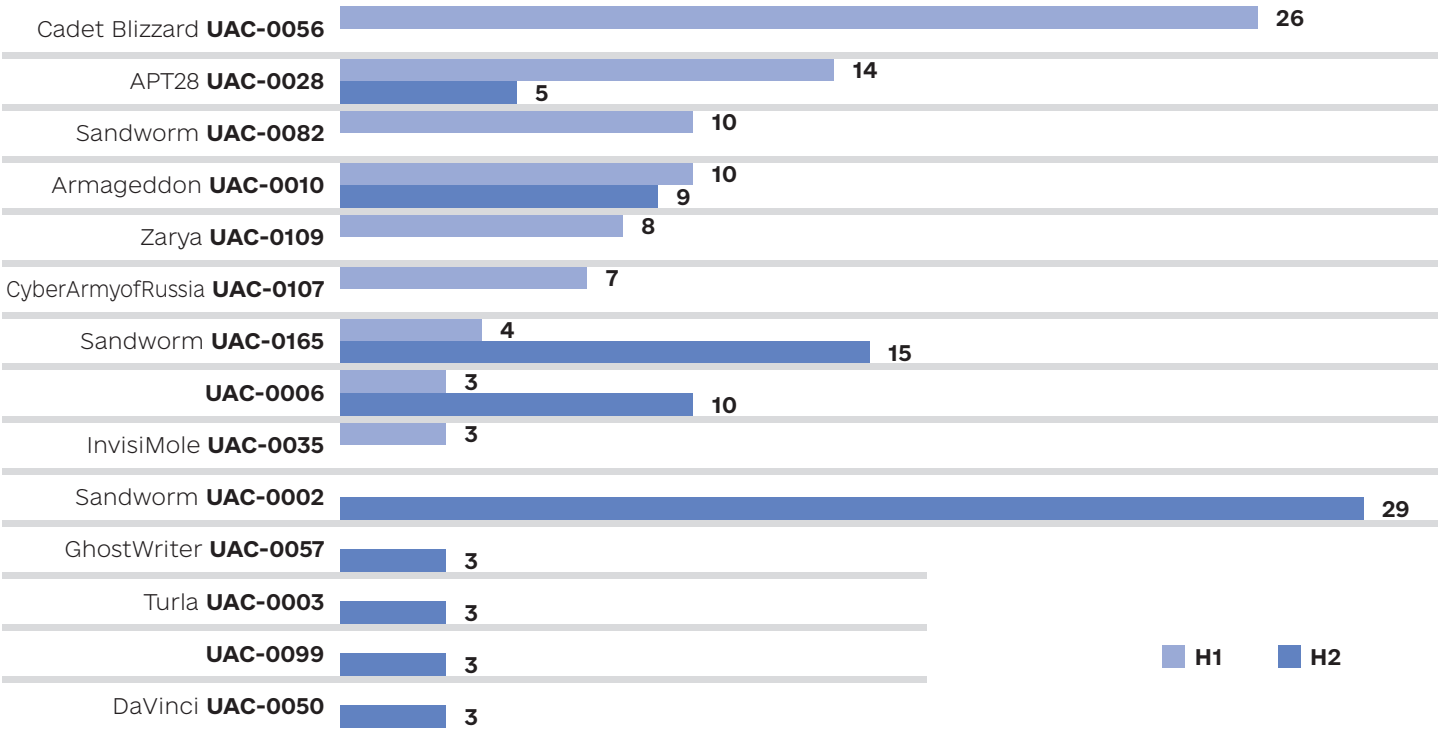
Загальна статистика може не відображати всієї картини. Серед активних гравців є багато тих, хто генерує максимальну кількість інцидентів. І є ті, хто своїми атаками завдає значної шкоди і проводить серйозні кібероперації. На ілюстрації нижче відображено загальний розподіл активних угруповань.

НАЙАКТИВНІШІ УГРУПОВАННЯ



Для повноти картини треба розуміти, хто саме завдавав реальної шкоди та здійснює всі ці кібероперації.

НАЙАКТИВНІШІ УГРУПОВАННЯ, ПОВ'ЯЗАНІ З ІНЦИДЕНТАМИ ВИСОКОГО ТА КРИТИЧНОГО РІВНІВ У 2023 РОЦІ



Серед 80 кейсів з критичним і високим рівнями загрози та відомою атрибуцією (+45 кейсів без атрибуції) у II півріччі 2023 домінують військові угруповання ГУ ГШ МО РФ (ГРУ) — як давно відомі, так і новостворені. Не спостерігається домінування протягом тривалого періоду тої чи іншої групи, що свідчить про підхід до роботи малими угрупованнями. Це, на переконання аналітиків CERT-UA, може свідчити про змагальність хакерських груп рф у реалізації операцій впливу.

КЕЙСИ

Атаки на провайдерів телекомунікацій та інтернет-послуг

З кінця весни 2023 року цілями хакерів (наприклад, Sandworm) з ГУ ГШ МО РФ (ГРУ) стали телекомунікаційні та інтернет-компанії України.

Від 11 травня до 29 вересня 2023 року хакерське угруповання, що відстежується за ідентифікатором UAC-0165, також втрутилося в інформаційно-комунікаційні системи не менше ніж 11 провайдерів. Це призвело до перебоїв у наданні послуг доступу до мережі інтернет, хостингу та електронної пошти*. Вже тоді було видно ознаки цілеспрямованої кампанії, про яку фахівці CERT-UA попереджали телекомунікаційні компанії та провайдерів. Після детального аналізу кіберінцидентів вдалося встановити зв'язок цього кластера загроз з угрупованням Sandworm.

При цьому Росія не відмовляється від практики нанесення гібридних атак, які поєднують кібер-складову та ракетні удари.

Ми можемо з високою ймовірністю віднести до гібридних атак кібератаку на найбільшого українського оператора мобільного зв'язку – компанію «Київстар», яка обслуговує 25 млн абонентів. Ця атака в часовому вимірі відбувалася разом з ракетними ударами в грудні, які відновилися після тривалого затишшя.

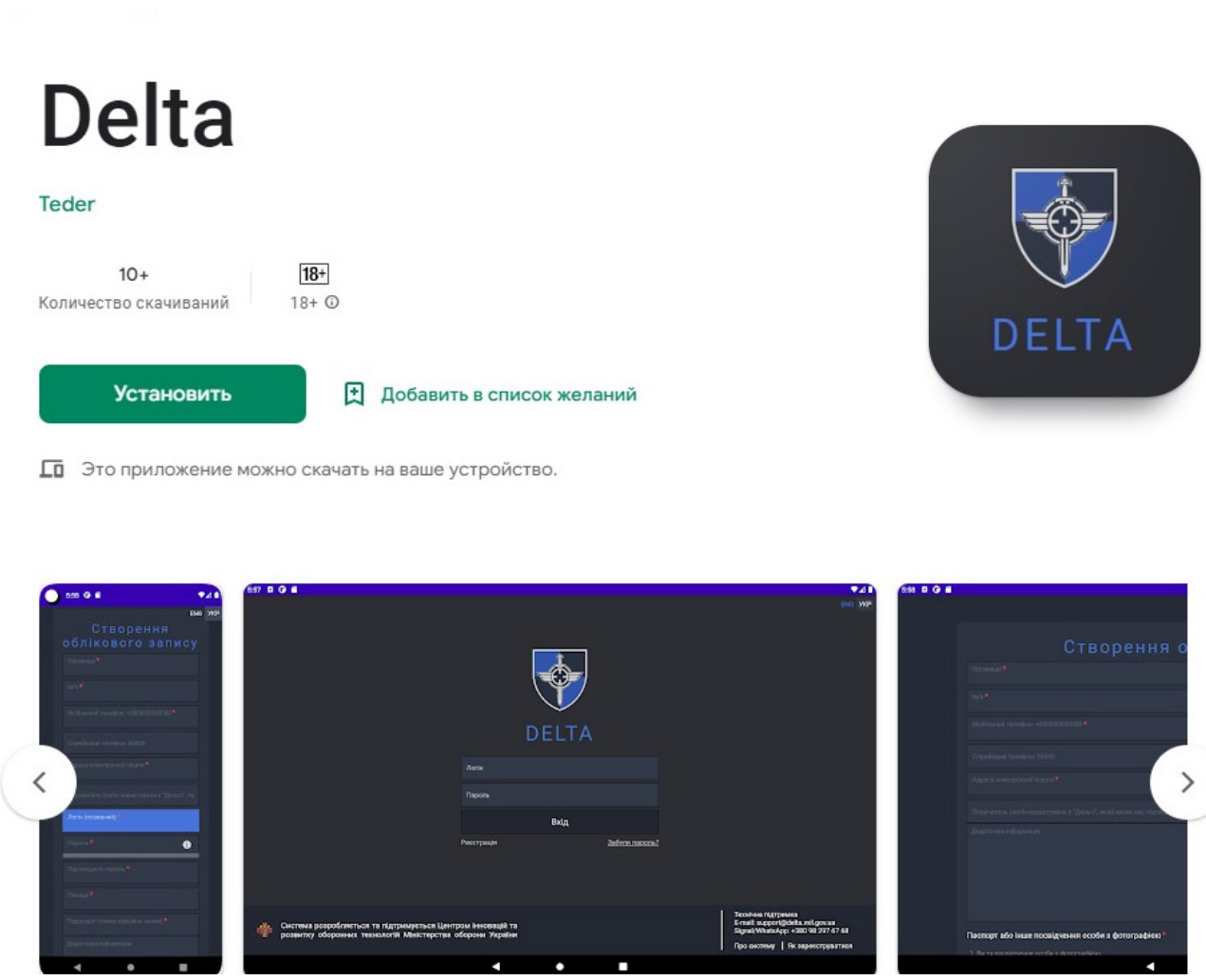
UAC-0082 (також відомі як Sandworm) — група, яка працює проти українських організацій з 2014 року. Вона відома за атаками на українські енергорозподільчі компанії у 2015 році, які стали першою в історії хвилею атак на енергетичний сектор країни, а також атакою NotPetya 2017 року. Кількість зафіксованих кібератак Sandworm у другому півріччі 2023 року збільшилась в 2,5 рази (18 атак у першій половині 2023 року проти 48 атак у другій).

* Детальний опис, технічна інформація

Атаки на військові системи

Серед атак у другому півріччі 2023 року важливо відзначити численні спроби злому військових систем, зокрема національної військової системи ситуаційної обізнаності Delta, яку використовують Сили безпеки і оборони України. Атаки на мобільні пристрої та ланцюги постачання використовуються значно менше, хоча їх кількість у 2023 році суттєво зросла.

Особливо цікавим є кейс, коли група хакерів ГУ ГШ МО РФ (ГРУ) розробила мобільний додаток, який імітував додаток Delta для військових, та опублікувала в Google Play, офіційній платформі для операційної системи Android.

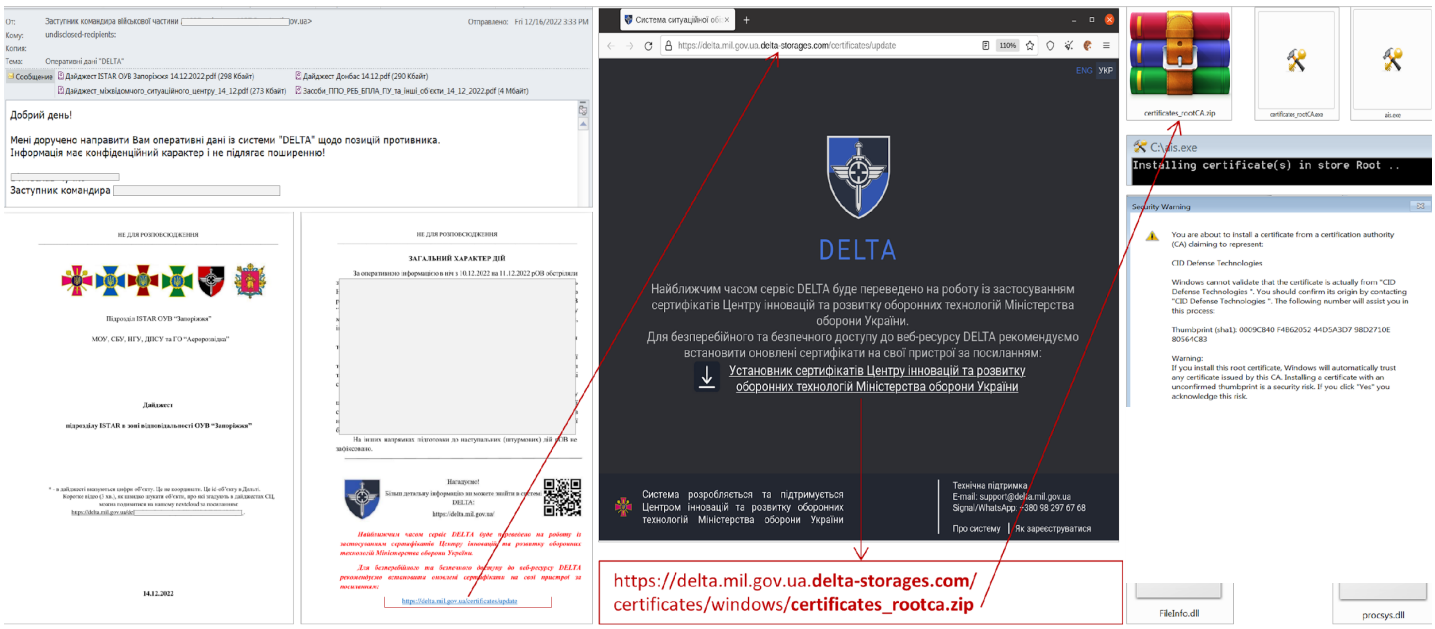


При цьому хакери ГРУ навіть випередили публікацію справжнього мобільного додатку від розробників Міністерства оборони України. Російські хакери заохочували завантажувати додаток на телефони військовослужбовців та старших офіцерів.

Для реалізації таких операцій військовим хакерам необхідно мати значний запас вільних ресурсів, які можна спрямувати на розроблення та розповсюдження мобільних додатків, та мати інформацію про плани військових щодо реалізації застосунка. Тож, очевидно, що ГРУ має суттєвий пул розробників та активно залучає їх для різних операцій імплантації та присутності. Раніше ми також спостерігали розповсюдження електронною поштою повідомлення про необхідність оновити сертифікати в системі «DELTA». Для цього використовували скомпрометовану електронну адресу одного зі співробітників оборонного відомства і месенджери. При цьому долучені до повідомлення PDF-документи, які містять посилання на шкідливий ZIP-архів, імітують легітимні дайджести підрозділу ISTAR ОУВ «Запоріжжя», які містять посилання на шкідливий ZIP-архів.

Зловмисники використовують домени з довгими іменами і фішинг-сайти для того, щоб здійснити інфікування пристроїв військових, хоча посилання при наведенні на нього курсора виглядало легітимним:

hXXps://delta.mil.gov.ua.delta-storages[.]com/certificates/update



Атаки на користувачів мобільних пристроїв

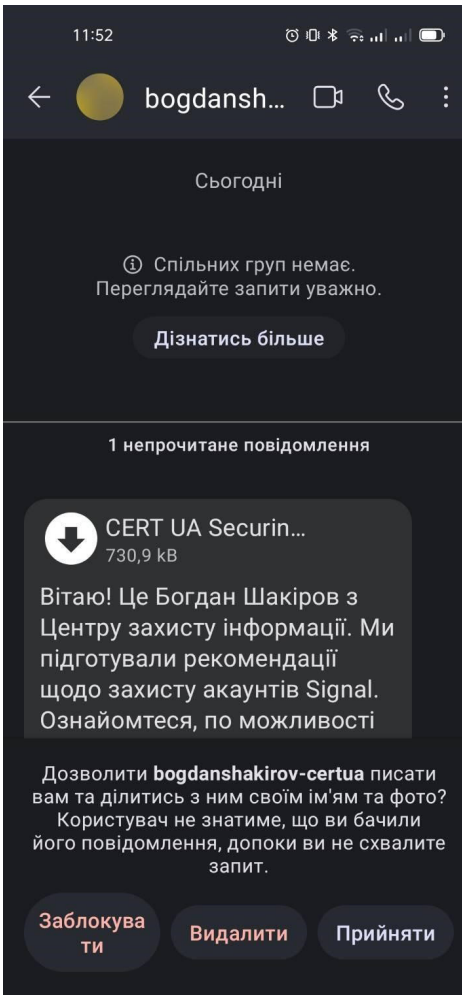
Увага російських хакерів до атак на мобільні пристрої впевнено зростає. Це насамперед пов’язано зі зручністю месенджерів для швидкого обміну інформацією і їх популярністю, зокрема й серед військових. Противник залучає дедалі більше фахівців для розробки інструментів віддаленого отримання інформації з мобільних пристроїв.

Це складна робота, яка вимагає особливого підходу до потенційної жертви, тому нерідко ми спостерігаємо випадки зв’язування спеціалізованого ШПЗ з легітимними продуктами.

У одному з кейсів другої половини 2023 року військові ГУ ГШ МО РФ (ГРУ) замаскували відкритий код шпигунської програми для Android – SPYNOTE (SpyMax) — під інсталятор системи ситуаційної обізнаності «Кропива». На жаль, маємо констатувати, що основним каналом доставки поза Google Play, який блокує ШПЗ, залишається соціальна інженерія під час спілкування через Signal та Telegram. У серпні 2023 року Держспецзв’язку підготувала та опублікувала матеріал щодо налаштувань захисту Signal*. Тому закликаємо ще раз ознайомитися з нею* та відключити автоматичне скачування файлів на комп’ютер.

Цю ж інструкцію почали активно поширювати через месенджер Signal між представниками сил безпеки та оборони у вигляді PDF-документу, оскільки вона містила важливу для безпеки інформацію. Противник вирішив використати цей матеріал для реалізації своєї кампанії із соціальної інженерії. Вже через 13 годин зловмисники почали розповсюджувати шкідливе програмне забезпечення, нібито від імені CERT-UA, під виглядом цієї ж інструкції.

* Чи зламали Signal, та як убезпечити себе від ризиків?



Швидкість реакції та експлуатації нового вектора зараження, фішингу і соціальної інженерії дійсно вражає. Це також підтверджує гіпотезу про наявність великої кількості доступних людських ресурсів для реалізації таких кампаній «на ходу», оскільки, як правило, планування та реалізація таких атак займають значно більше часу.

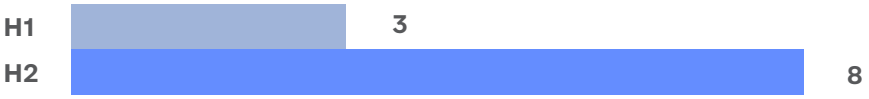
Практично всі таргетовані атаки через месенджери мають на меті розповсюдження ШПЗ для операційної системи Windows, адже для спілкування в месенджерах часто використовуються їх комп'ютерні чи веб- версії. Були зафіксовані випадки, коли зловмисники підготували і запакували підроблене ПЗ як оновлення до спеціалізованого комплексу ситуаційної обізнаності на полі бою. Часто файли-приманки розповсюджують у вигляді Zip чи Rar архівів. Зокрема, ми фіксували розповсюдження шкідливого програмного забезпечення для віддаленого керування комп'ютером, що містилось в архіві, що експлує вразливість WinRAR.

ЗАГАЛЬНІ СПОСТЕРЕЖЕННЯ ЗА ЗМІНОЮ ЛАНДШАФТУ ЗАГРОЗ

ЗМІНИ В ЕНЕРГЕТИЧНОМУ СЕГМЕНТІ, 2023 Р.

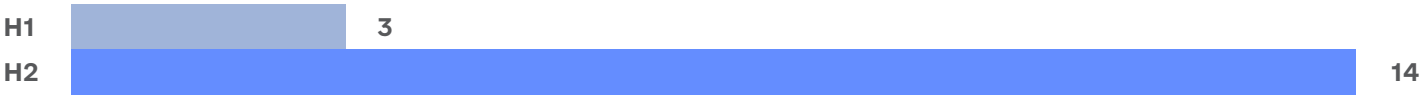
СПРОБА ЕКСПЛУАТАЦІЇ ВРАЗЛИВОСТІ

ФІШИНГ



DOS/DDOS

РОЗПОВСЮДЖЕННЯ ШПЗ

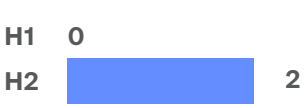


КОМПРОМЕТАЦІЯ СИСТЕМИ

КОМПРОМЕТАЦІЯ ОБЛІКОВОГО ЗАПИСУ

ВРАЗЛИВІСТЬ

СПРОБИ АВТОРИЗАЦІЇ/ ВХОДУ В СИСТЕМУ



Якщо в першому півріччі 2023 року домінувала спроба експлуатації вразливості та компрометації облікових записів, то в другому півріччі ми спостерігаємо перехід до фішингових атак і спроб інфікування ШПЗ. Це відбувається у зв'язку зі значним зниженням присутності противника в мережах, зачищенням імплантів, встановленням та підключенням сенсорів і якісним аналізом телеметрії.

З-поміж розслідуваних Держспецзв'язку зламів, які мали критичний і високий рівні, переважало проникнення через публічно доступні вебресурси. У багатьох кейсах, де не були встановлені технології для моніторингу підозрілої активності, це призводило до подальшої компрометації внутрішніх систем.

Спроби експлуатації вразливостей, пошук нових точок входу та намагання повернутися на раніше атаковані енергетичні об'єкти є постійними, тож загальнодоступні веб- та інші ресурси будуть постійною загрозою. Саме тому значна кількість організацій в енергетичному сегменті має докладати максимум зусиль для мінімізації своєї поверхні атаки* Attack Surface Reduction (ASR) та захисту публічних ресурсів.

* Поверхня атаки в програмному середовищі - це сукупність точок доступу (векторів атаки), де несанкціонований користувач (зловмисник) може намагатися отримати, ввести або контролювати дані або критичне програмне забезпечення.

Розмір поверхні атаки може змінюватися з часом через додавання або видалення IT-активів, таких як веб-сайти, хости, хмарні та мобільні програми.

Основний принцип безпеки - зменшення поверхні атаки.

ВИСНОВКИ ТА ПРОГНОЗИ

ЗБІЛЬШЕННЯ ФОКУСУ НА ТОЧКОВІ ПРИХОВАНІ РОЗВІДУВАЛЬНІ КІБЕРОПЕРАЦІЇ

Інформаційні ресурси організацій сектору безпеки і оборони, як і окремі комп'ютери та гаджети працівників/службовців таких структур, будуть ціллю номер один в 2024 році. Таргетована соціальна інженерія стає все більш дієвим способом доставки шкідливих програм на кінцеві пристрої.

ОБ'ЄКТИ ЕНЕРГЕТИКИ ТА КРИТИЧНОЇ ІНФРАСТРУКТУРИ ЗНОВУ БУДУТЬ В ЦЕНТРІ УВАГИ ХАКЕРІВ

Зі збільшенням кінетичних ударів по об'єктах критичної інфраструктури буде збільшуватись зловмисна активність афілійованих організацій в кіберпросторі для отримання зворотного зв'язку щодо результатів та наслідків. Хакерські угруповання будуть шукати нові способи проникнення в мережі ОКІ, зокрема методом компрометації компаній, які є постачальниками послуг для ОКІ. Особлива увага до розробників програмного забезпечення.

КІЛЬКІСТЬ ТА СКЛАДНІСТЬ КІБЕРАТАК ФІНАНСОВО МОТИВОВАНИХ ГРУП БУДЕ РОСТИ

Прогнозується збільшення кібератак, які будуть спрямовані на викрадення коштів. Такі кібератаки будуть націлені на комерційний сектор. Реалізація таких атак буде передбачати два напрямки:

1) зараження та проникнення в мережі компаній з метою отримання доступу до банківських облікових записів;

2) використання вірусів-шифрувальників (ransomware) з подальшим вимаганням викупу за розшифровку даних.

ІГНОРУВАННЯ ВИМОГ КІБЕРЗАХИСТУ ТА РЕКОМЕНДАЦІЙ ДЕРЖСПЕЦЗВ'ЯЗКУ - ОСНОВНА ПРИЧИНА УСПІХУ РЕАЛІЗАЦІЇ КІБЕРАТАК

Успішній реалізації зловмисного задуму сприяє ігнорування типових вимог кіберзахисту, які є актуальними для ландшафту кіберзагроз протягом останніх 7 років. Так, найбільш розповсюдженими векторами первинної компрометації є:

- Відомі вразливості (PHP, MS Exchange, FortiGate, Zimbra)
- Скомпрометовані облікові записи (→ VPN → LAN)
- Спір-фішинг
- Самоінфікування (встановлення операційних систем та програмного забезпечення, які завантажені з неофіційних джерел та трекерів)

РЕКОМЕНДАЦІЇ

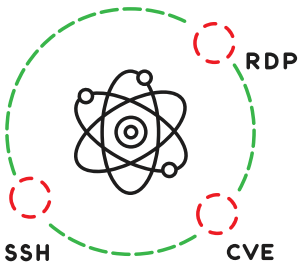
ПІДКЛЮЧИТИСЯ ДО ДЕРЖАВНОГО ЦЕНТРУ КІБЕРЗАХИСТУ ДЕРЖСПЕЦЗВ'ЯЗКУ

Кіберцентр Держспецзв'язку має фахівців і технічні спроможності забезпечити кіберзахист та моніторинг критичних для України організацій шляхом встановлення та налаштування захисту кінцевих точок, підключення мережних сенсорів, аналізу телеметрії та сигналів атак, вчасного реагування на компрометацію. Ми закликаємо організації скористатися професійною допомогою, застосувати наявні ресурси, пропоновані державою для забезпечення захисту під час дії воєнного стану.

ЗМЕНШЕННЯ «ПОВЕРХНІ АТАКИ»

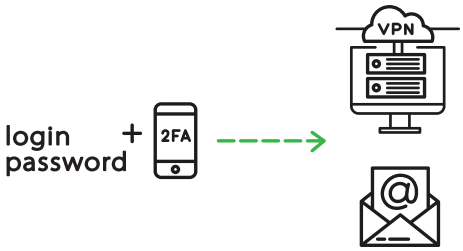
Зменшення кількості інформаційних систем та сервісів («відкритих мережевих портів»), що доступні з мережі Інтернет, підвищує захищеність периметра. Скористайтеся інструментами censys.io, shodan.io, Nmap та перевірте свою поверхню атаки або зверніться за допомогою

https://cert.gov.ua/article/1751036



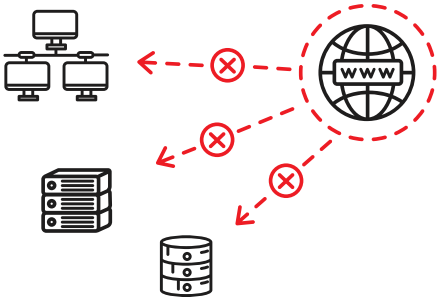
БАГАТОФАКТОРНА АВТЕНТИФІКАЦІЯ — НЕОБХІДНА ВСЮДИ (MFA)

Наш досвід показав необхідність застосування MFA на всіх корпоративних ресурсах. Особливо VPN та MAIL повинні передбачати використання двофакторної автентифікації за тимчасовим одноразовим кодом (TOTP). Інакше компрометація логіна-пароля або сертифікату доступу гарантуватиме отримання несанкціонованого доступу до пошти і/або локальної мережі.

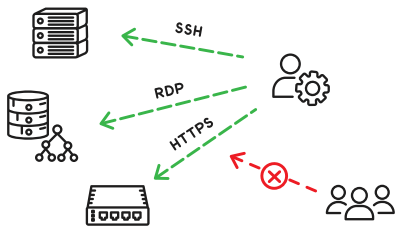


СЕГМЕНТАЦІЯ МЕРЕЖІ

Інформаційні системи, які передбачають доступ з мережі Інтернет та розгорнуті в межах периметру ІКС організації (WEB, MAIL, etc), повинні знаходитись у відокремленій демілітаризованій зоні (DMZ). При цьому умовна компрометація будь-якого з сегментів такої мережі не повинна створити передумов для розвитку атаки вглиб локальної мережі і/або стосовно інших активів.



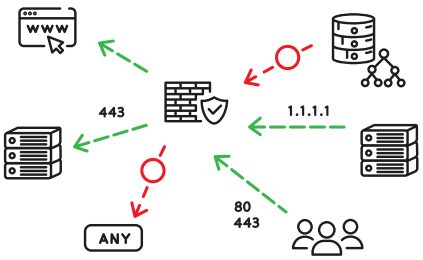
ОБМЕЖЕННЯ АДМІНІСТРАТИВНИХ АКАУНТІВ



Віддалений доступ (наприклад, RDP), і особливо доступ до інтерфейсів адміністрування серверного та мережевого обладнання, має бути дозволений для конкретних користувачів з визначених робочих місць (IP-адреса).

Фільтрація інформаційних потоків здійснюється засобами штатних (хостових) і окремих міжмережевих екранів, а також інших механізмів (наприклад, TCP Wrappers).

ФІЛЬТРАЦІЯ ВИХІДНИХ («EGRESS») ІНФОРМАЦІЙНИХ ПОТОКІВ



Доступ користувачів до ресурсів мережі Інтернет має бути реалізовано через міжмережевий екран (проксі-сервер) з підтримкою автентифікації та з обмеженням за типовими портами. Можливість встановлення вихідних мережевих з'єднань із серверного обладнання (в т.ч. DMZ) має бути відсутня або обмежена за принципом «заборонено все, що явно не дозволено» з урахуванням мінімальної необхідності.

ФУНКЦІОНУЮЧІ ПРОГРАМНІ ЗАСОБИ ЗАХИСТУ: НА ПК ТА СЕРВЕРАХ

Чи знаєте ви, що означають події з ідентифікаторами 1116, 1117 в журналі Windows Defender? Чи налаштовано антивіруси на серверах? Чи маєте змогу централізованого моніторингу та керування засобами захисту?

КОНТРОЛЬ ПРОГРАМ, У Т.Ч. ЛЕГІТИМНИХ УТИЛІТ

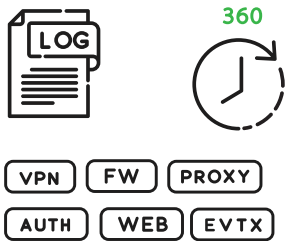
Для здійснення кібератак дедалі частіше використовуються штатні компоненти операційної системи. Можливість запуску звичайними користувачами таких утиліт повинна бути обмежена: wscript.exe, cscript.exe, mshta.exe, powershell.exe. Кращою практикою є використання AppLocker на основі білого списку.

НЕВЖЕ РОЗМІР ЖУРНАЛІВ НА ВАШИХ WINDOWS-СЕРВЕРАХ СКЛАДАЄ 21МБ?

За замовчуванням розмір основних журналів Windows (Security, System, Application) обмежено 21МБ, чого вистачає для реєстрації подій протягом декількох останніх годин. Типовий розмір журналів рекомендовано підвищити до 2ГБ. Крім того, використання інструменту Sysmon надасть значних переваг.

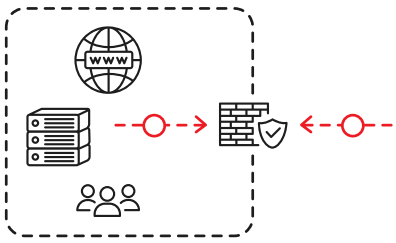
УЯВНА КІБЕРАТАКА: ЧИ Є «ЛОГИ» ДЛЯ ДОСЛІДЖЕННЯ?

Одна з проблем під час реагування - відсутність і/або недостатня повнота і часова ємність журнальних файлів. Рекомендовано зберігати журнали подій протягом 180 - 360 діб, для чого доцільно розгорнути окремий syslog-сервер; налаштувати формат часу згідно RFC3339. Звертаємо увагу, що на pfSense/Mikrotik за замовчуванням розмір логів значно обмежено.



БУДЬТЕ ГОТОВІ ДО «ІЗОЛЯЦІЇ»

Якщо завтра ви отримаєте нотифікацію щодо присутності зловмисників у мережі — чи готові ви до заборони вхідних та вихідних інформаційних потоків за умови забезпечення контрольованого функціонування критичних підсистем? Чи передбачена, при цьому, можливість виконання технічних робіт, у т.ч. в режимі віддаленого доступу?



МАЄТЕ МОЖЛИВІСТЬ ОПЕРАТИВНОГО ОБМІНУ ІНФОРМАЦІЄЮ ІЗ CERT-UA?

Під час реагування на інцидент значна кількість часу витрачається на пошук контактів та організацію взаємодії. Зв'яжіться із CERT-UA заздалегідь, організуйте канали зв'язку, надайте ідентифікатори вашої ІКС та активів для додаткового моніторингу та своєчасного інформування.

Повідомити про інцидент: incidents@cert.gov.ua
+38 (044) 281-88-25, +38 (044) 281-88-05
+38 (044) 281-88-01 (цілодобово)

Щодо інцидентів у відповідних секторах також можуть допомогти:

ЗСУ:
csoc@post.mil.gov.ua

СБУ:
support@dis.gov.ua

НБУ:
csirt-nbu@nbu.gov.ua

Російські кібероперації аналітика за II півріччя 2023 року

Державна служба
спеціального зв'язку
та захисту інформації
України