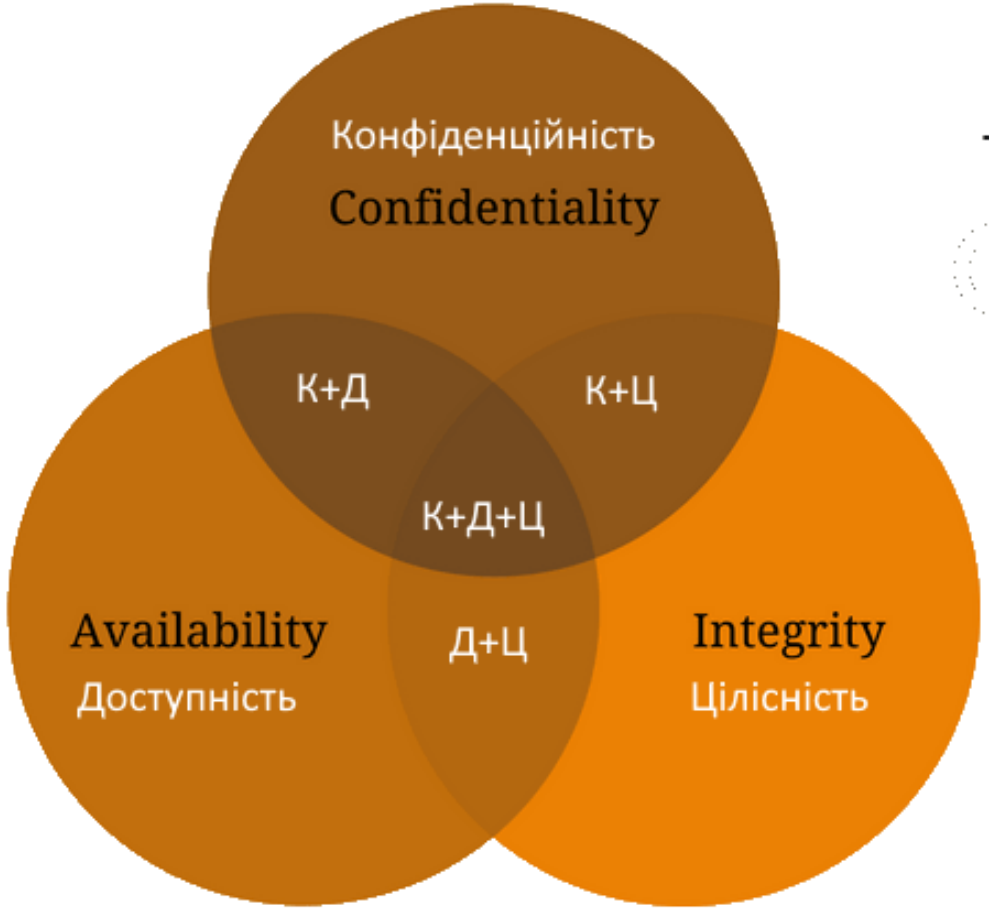
Безпека інформації в умовах повномасштабної війни

Інформаційна безпека спрямована на забезпечення конфіденційності, цілісності та доступності інформації.



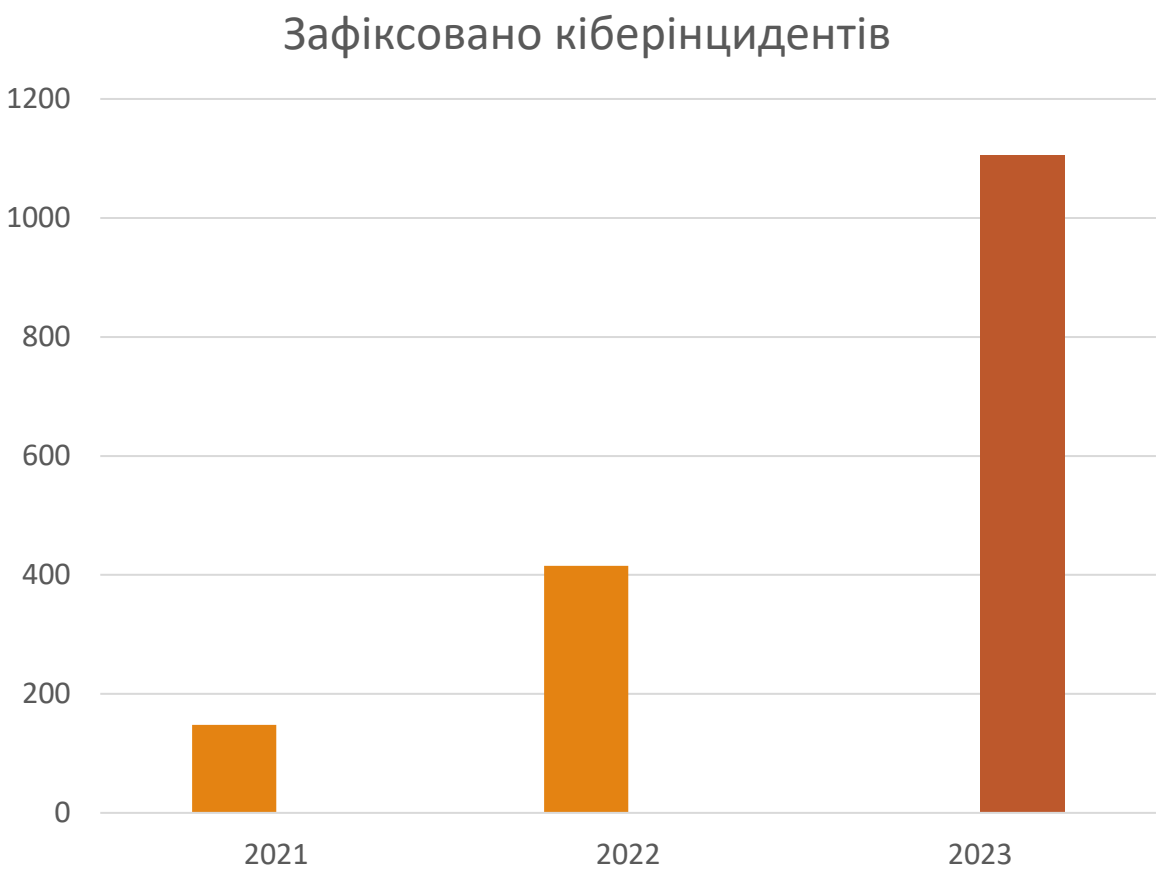
Основні цілі інформаційної безпеки включають:

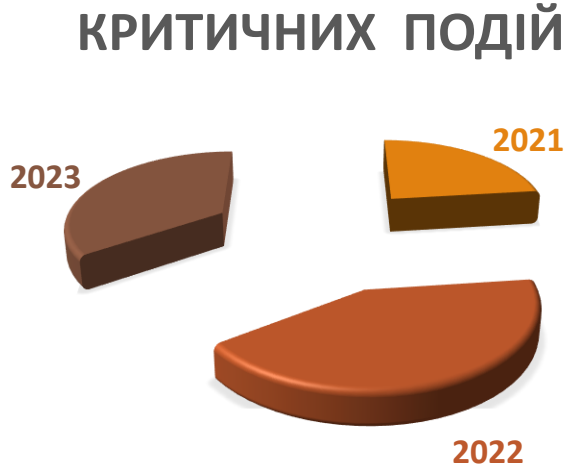
1. **Конфіденційність**
2. **Цілісність**
3. **Доступність**

eAdvise

CERT-UA
Computer Emergency Response Team of Ukraine

Звіт Держспецзв'язку та CERT-UA за 2023 рік





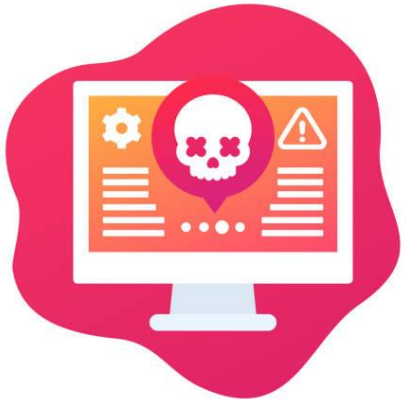
eAdvise

ЦІЛЬОВІ СЕКТОРИ

eAdvise

Загрози інформації безпеки

Шкідливе програмне забезпечення (віруси) - програмне забезпечення, яке перешкоджає роботі комп'ютера, збирає конфіденційну інформацію або отримує доступ до інформаційно-комунікаційних систем.



Класифікація шкідливого програмного забезпечення - мережеві хробаки, троянські програми, клавіатурні шпигуни, зомбі, та ін.

Загрози для мобільних пристроїв

Шкідливе програмне забезпечення які зловмисники використовують для мобільних пристроїв дозволяє:

- Перехоплювати всі здійснені дзвінки
- Показувати вміст СМС-листування
- Показувати данні про відвідані сайти
- Знімати камерою телефона оточення користувача
- Визначення його місце розташування
- Включати мікрофон і записувати всі розмови

eAdvise

КІЛЬКІСТЬ ІНЦИДЕНТІВ ПРОТИ ТИП ІНЦИДЕНТУ

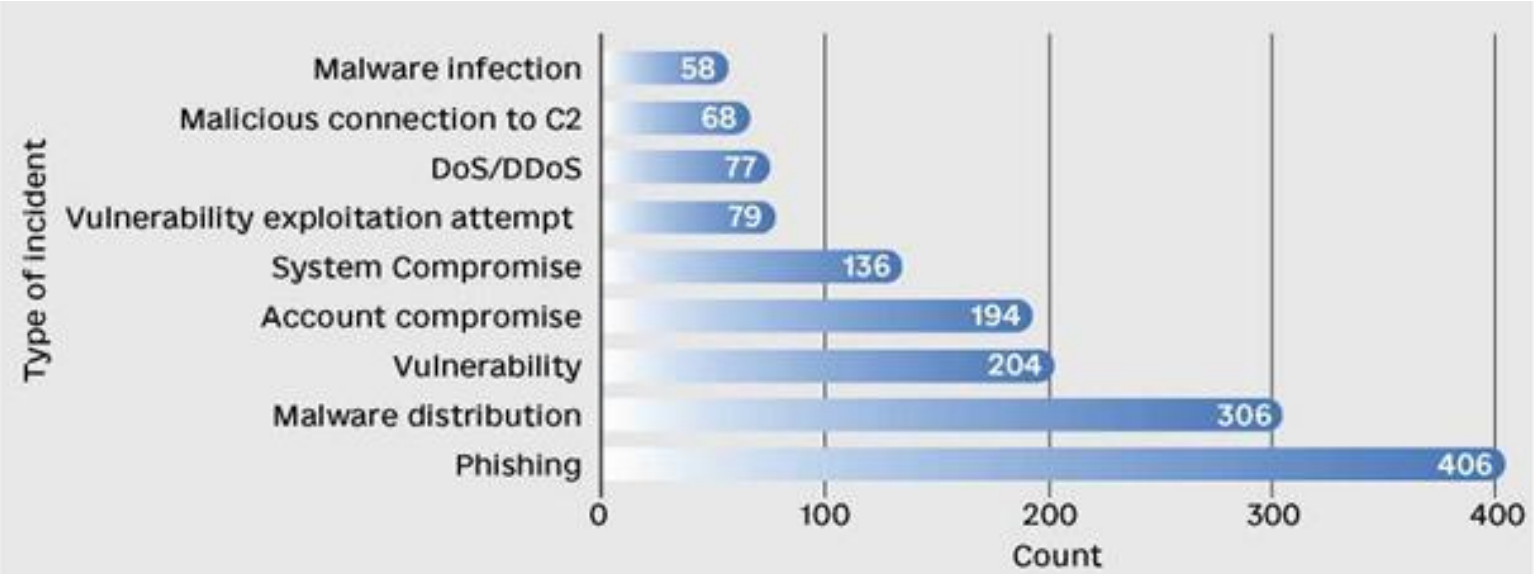


Figure 3. Distribution of incident types registered during H1'2023.

З рисунка 3 — поширеності методів, зафіксованих CERT-UA, стає очевидним, що **фішинг** був найбільш помітною тактикою, яку використовували зловмисники в першому півріччі 2023 року. Однак зараження шкідливим програмним забезпеченням, пов'язане з командно-адміністративними з'єднаннями (C2) і зламами через відомі вразливості, які можна використовувати, або компрометацію облікових записів, виділяється як улюблені та високоефективні стратегії в усіх напрямках.

eAdvise

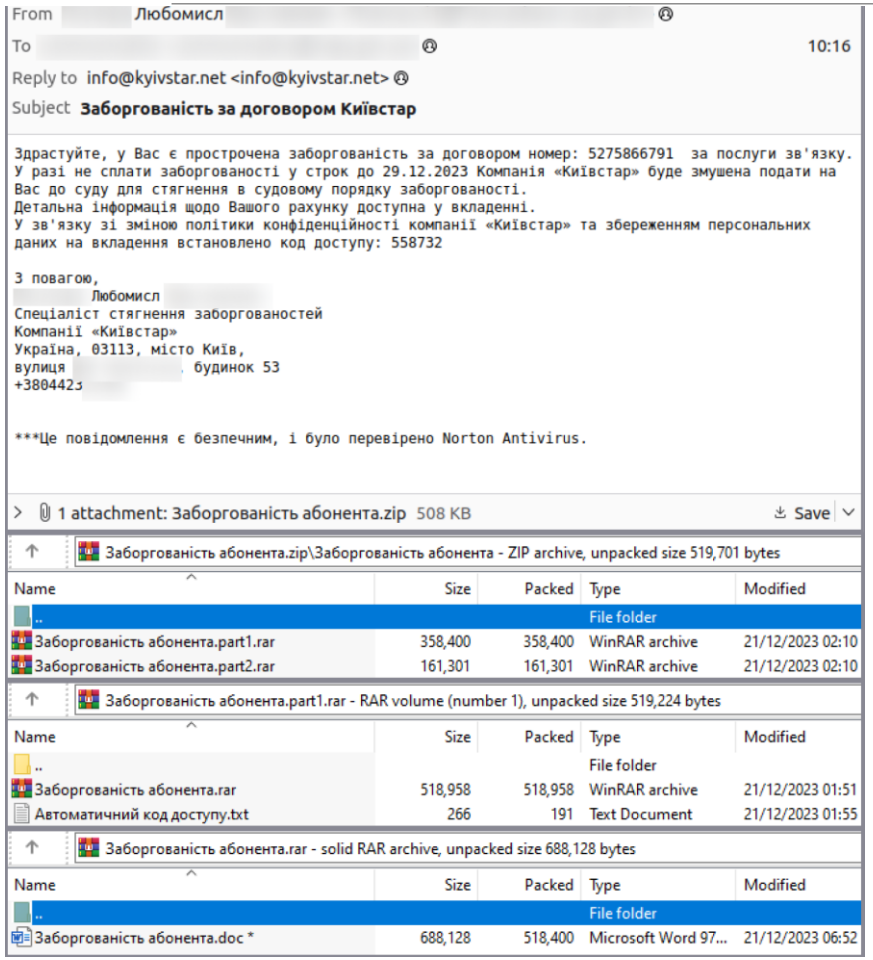
Фішинг - Соціальна інженерія - маніпуляція (шахрайство)

Фішинг — найпоширеніший метод виманювання конфіденційної інформації. В його основі лежить вплив на емоції користувачів Інтернету — примус або маніпуляція.

Соціальна інженерія стала невід'ємною частиною кібершахраїв. Це спеціальна методика маніпуляції, яка допомагає змусити людину віддати зловмисникам необхідні дані використовуючи людські слабкості – тобто емоції та природну поведінку жертви. Сьогодні існує чимало методів використання соціальної інженерії, в основі – маніпуляція людськими страхами, зацікавленістю або довірою.

eAdvise

Приклад інциденту з використанням фішенгу



21.12.2023 зафіксовано масове розповсюдження електронних листів з тематикою "Заборгованості за договором Київстар" та вкладенням у вигляді архіву "Заборгованість абонента.zip". Зазначений ZIP-архів містить розділений на 2 частини RAR-архів "Заборгованість абонента.rar", в якому знаходиться однойменний архів захищений паролем. У випадку відкриття такого архіву та запуску виконуваних файлів, відбувався запуск програми для віддаленого управління RemcosRAT.

Окрім того, зафіксовано розповсюдженя листів з темою "Запит СБУ" та вкладенням у вигляді архіву "Документи.zip", що містить захищений паролем та розділений на 3 частини RAR-архів "Запит.rar". В останньому знаходиться виконуваний файл "Запит.exe". У випадку відкриття такого архівуархіву та запуску виконуваних файлів, відбувався запуск програми для віддаленого управління RemcosRAT.

CERT-UA опублікував звіт про кібератаку: https://cert.gov.ua/article/6276824

eAdvise

Приклад інциденту орієнтований на медіа-агентство

УКРІНФОРМ

17 січня 2023 року в телеграм-каналі CyberArmyofRussia_Reborn оприлюднила дані, щодо порушення штатного режиму функціонування Українського національного інформаційного агентства "Укрінформ".

«Хактивісти» стверджували, що «спалили» жертву, «всю мережеву інфраструктуру» організації, щоб запобігти заповненню веб-сайту новинами.

Пізніше CERT-UA опублікував звіт про кібератаку з тією ж метою та часом, але дійшов висновку, що зловмисниками здійснено невдалу спробу порушення штатного режиму роботи комп'ютерів користувачів. Дослідили, що цю кібератаку здійснила група «UAC-0082 (Sandworm, пов’язана з Головним центром спеціальних технологій ГРУ).

Основна мета: скомпрометувати державне інформаційне агентство України та створити ґрунт для підвищення ефективності пропаганди.
https://cert.gov.ua/article/4818341

eAdvise

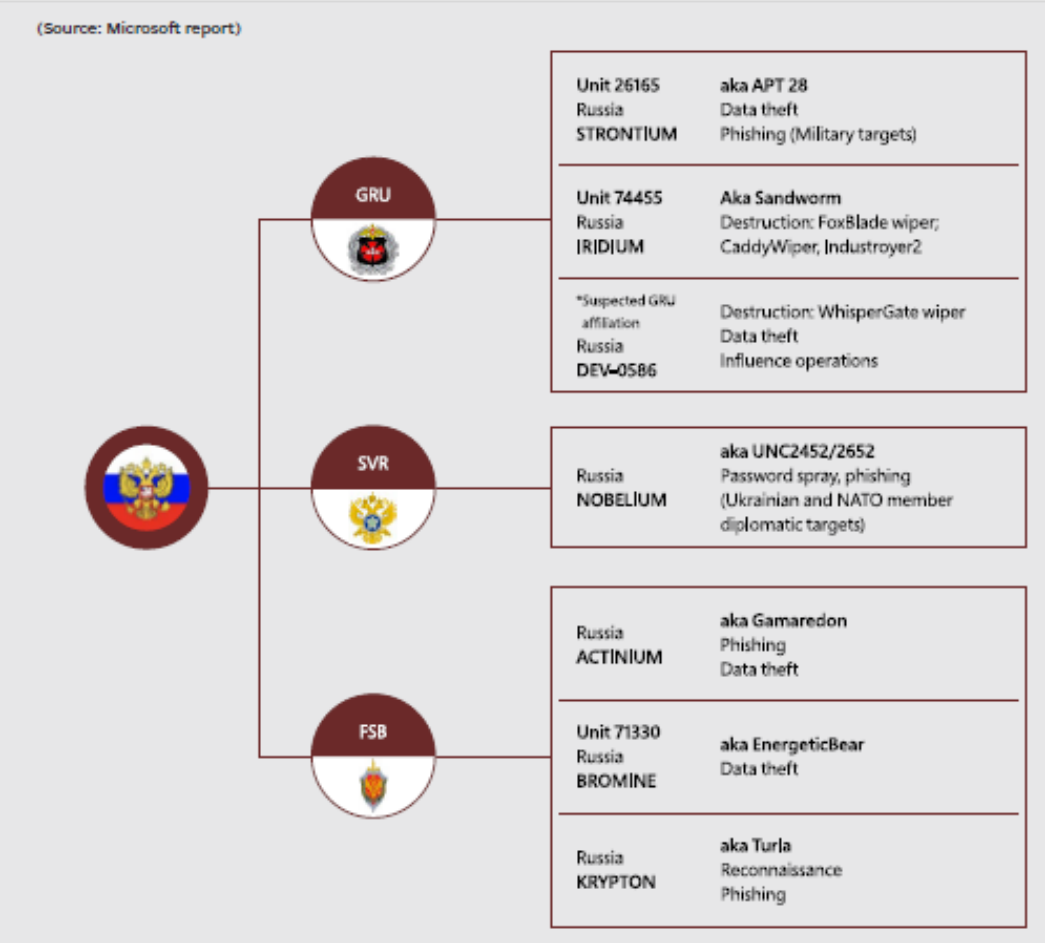
Приклад інциденту орієнтований у відношенні українських провайдерів

За період з 11.05.2023 по 27.09.2023 організованою групою зловмисників, що відстежується за ідентифікатором UAC-0165 (Sandworm, пов’язана з Головним центром спеціальних технологій ГРУ), здійснено втручання в інформаційно-комунікаційні системи (ІКС) не менше ніж 11 провайдерів телекомунікацій України, що, серед іншого, призвело до перебоїв в наданні послуг споживачам.

Найбільш пов'язана історія — https://cert.gov.ua/article/6123309 З моменту повномасштабного вторгнення в більшості інцидентів з UAC-0165 є здійснення руйнівних кібератак, які включають стирання серверів, збій систем віртуалізації, відключення активного мережевого обладнання, стирання систем зберігання даних і шифрування кінцевих точок. Протягом останніх 6 місяців вони розробляли нові варіанти шкідливого програмного забезпечення (їх більше 10 нових зразків) з використанням легальних утиліт (наприклад, SDelete, WinRaR) або вбудованих функцій систем (наприклад, сховищ NAS).

eAdvise

ХТО



Кібервійна стрімко розвивалася з 2022 року. Російські зловмисники знаходять нові та ефективні способи підтримки військових операцій Росії як на полі бою, так і проти цивільного населення.

На малюку зображені російськи групи Advanced Persistent Threat (APT) та їхні хакерські команди, які беруть участь у кампаніях атак на Україну.

Зафіксовано заявлені атаки щонайменше 23 очолюваних Росією кібертерористичних хакерських груп. Вони підпорядковані ФСБ, ГРУ та СЗР що служать наступальній військовій меті і атакують державний і приватний сектори незалежної держави.

Більш детально можна ознайомитись в звіті: «Російська кібертактика: уроки, вивчені у 2022 році».

eAdvise

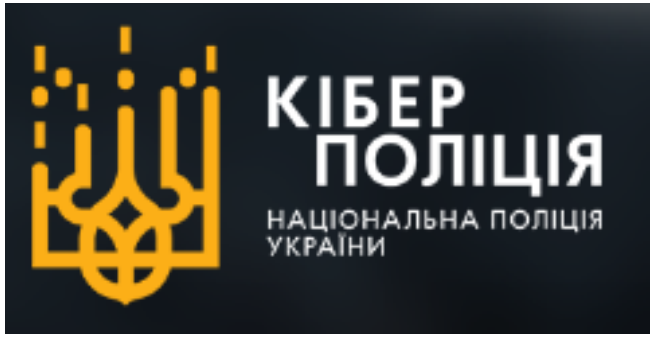
Обізнаність та навчання

- Слідкуйте за сучасними загрозами та новинами в галузі кібербезпеки.
- Беріть участь в тренінгах та курсах з кібербезпеки.

eAdvise

Своєчасне виявлення та реагування на інциденти

- Звертайте увагу незвичним або підозрілим активностям.
- Повідомляйте про будь-які підозрілі інциденти.



eAdvise

Для комунікації

НАШ ВЕБ-САЙТ

НАШ LINKEDIN

@EADVISE_HUB

eAdvise