**Аналіз Кібератак**

**Аналіз атаки “Salt Typhoon Espionage Campaign”, APT-групою Salt Typhoon(Ghost Emperor). 2024-2025 рік на телекомунікаційні компанії США.**

*Опис кібер групи:*

Група керується Міністерством державної безпеки, зовнішньою розвідкою та таємною поліцією Китаю. Акцент групи робиться на цілях контр розвідки та на крадіжці даних ключової корпоративної інтелектуальної власності.

Результати вивчення діяльності групи говорять про те, що група є організованою з чітким розподілом праці, саме тому атаки, спрямовані на різні регіони та галузі, запускаються різними суб’єктами, що свідчить про те, що група складається з різних команд. Початок атак на установи фіксується з 2023 року.

**Опис атаки:**

Здійснена масштабна шпигунська кампанія проти телекомунікаційних компаній, університетів та урядових структур США. Зловмисники експлуатували вразливості в мережевих пристроях Cisco\* (CVE-2023-20198\*, CVE-2023-20273\*), створювали GRE\* - тунелі для прихованого зв’язку та впроваджували шкідливе ПЗ для перехоплення метаданих, записів дзвінків і доступу до «систем lawful intercept»\*.

**Аналіз тріади CIA:**

*Confidentiality*:

Зловмисники отримали доступ до конфіденційних телекомунікаційних даних, записів розмов, метаданих, внутрішніх систем.

*Integrity:*

Немає підтверджень про зміну або пошкодження даних

*\*можливо атаку зробили прихованою, тому що на меті було довготривале шпигунство.*

*Availability*:

Якщо взяти до уваги, що сервіси залишались доступними, то можна зробити висновок, що мета саме цієї атаки - шпигунство.

**Заходи безпеки:**

Використання багатофакторної автентифікації(MFA)

* C - запобігання несанкціонованому доступу

Оновлення патчей та прошивок:

* C - Для унеможливлення використання CVE

Сегментація мережи використання “Zero Trust”

* CI - обмеження «горизонтального руху» по інфраструктурі

Моніторинг логів та мережевих пристроїв

* CIA - Виявлення «тунелів» та аномальної активності

**Висновки**:

Ми бачимо, що навіть без порушення доступності чи цілісності, *шпигунство через мережеві пристрої* може мати критичні наслідки.

Що важливо пам’ятати та тримати в полі зору:

* регулярно оновлювати прошивки
* впроваджувати «Zero Trust»
* моніторити мережу на рівні пристроїв
* моніторити мережу на рівні серверів
* міжнародна координація реагування на кібер загрози

На прикладі цієї атаки, можна побачити, що *ML та агентні системи* можуть бути використані для автоматичного виявлення прихованих загроз у телекомунікаційній інфраструктурі.

**Аналіз атаки “Snowflake Data Breach” групою “Scattered Spider” протягом квітня - травня 2024 року.**

*Опис кібер групи:*

Група Scattered Spider, відома як UNC3944, відома завдяки причетності до атак на Caesar Entertainment, та MGM Resort International, також атакувала Visa та Marks & Spenser та інші. Використовували CVE-2015-2291 пов’язану з анти DoS програмному забезпеченні у Windows. Використовує легально розроблені інструменти, вважається що має глибоке розуміння AWS, AZUR.

**Опис атаки:**

У квітні-травні 2024 року зазначена вище APT-група здійснила атаку на хмарну платформу Snowflake, з викраденням даних у користувачів цієї платформи. Данні були екс-фільтровані\* виставлені на продаж з подальшим шантажем компаній та вимогами що до викупу отриманої інформації.

Данні отримані через “infostealer malware”\*, використовувались для отримання AT&T, Ticketmaster, Santander

**Аналіз тріади CIA:**

*Confidentiality*:

Зловмисники отримали доступ до конфіденційної інформації клієнтів Snowflake, фінансові записи, персональні дані, службові документи. Частина даних була викладена на хакерських форумах.

*Integrity:*

Немає підтверджень, що дані були змінені або пошкоджені, атака була спрямована на викрадення.

*Availability*:

Сервіси Snowflake залишались доступними, атака мала на меті проникнення та викрадення без мети порушення роботи платформи.

**Заходи безпеки:**

Використання багатофакторної автентифікації(MFA)

* C - Впровадження MFA (більшість аккаунтів не мало цього захисту)

Моніторинг поведінки та облікових записів(UEBA,SIEM)\*

* CI - Виявлення IP, контроль часу доступу та обсягу запитів

Перевірка облікових даних

* C - Зменшення ризику довготривалого використання викрадених паролів

Захист від infostealer malware

* С - sandbox, антивірус, контроль доступу до даних браузера

Шифрування даних при збереженні та у процесі передачі

* С - Запобігає розшифровці викрадених даних

**Висновки**:

Маємо зазначити такі пункти обов’язкові для виконання:

* MFA - на даному етапі розвитку технологій є обов’язковим для виконання
* Захист даних на платформах є спільною відповідальністю як користувача , так і компанії яка надає дані послуги.
* Info stealers - є одним з векторів атак які треба враховувати

Інформація яка була знайдена стосовно атаки на Snowflake показує що захист облікових даних є важливою частиною безпеки.

*Словник пояснення термінів:*

APT - група:

Advanced - використовують складні техніки (бекдори, zero-day),

Persistent - намагаються довгостроково закріплюватись у системі,

Thread - їх основна мета шпигунство та саботаж, що є реальною прихованою загрозою.

CISCO - компанія яка виробляє мережеве обладнання, маршрутизатори, комутатори, VPN, firewall.

CVE-2023-20198 - Уразливість в операційній системі Cisco IOS XE, яка дозволяє створити обліковий запис адміністратора без автентифікації (зміна налаштування, перехоплення трафіку).

CVE-2023-20273 - Уразливість, яка дозволяє виконувати довільний код на пристрої Cisco після отримання доступу (встановлення ПЗ, бекдор і тд).

CVE-2015-2291 - Intel Ethernet Diagnostics Driver for Windows. Дозволяє локально викликати DoS через IOCTL - запити. Можна загрузити драйвер для ескалації привілеїв.

GRE - тунелі (Generic Routing Encapsulation) - Мережевий протокол, який дозволяє створити «тунель» між двома пристроями - як приватний канал поверх Інтернету (прихована передача даних).

Система «lawful intercept» - Законні системи для прослуховування дзвінків і трафіку, використовуються спецслужбами, поліцією, операторами зв’язку.

Впровадження “Zero Trust” - Модель безпеки, де ***нікому не довіряють за замовчуванням***, кожен доступ перевіряється, навіть всередині мережі(обмеження руху зловмисника, автентифікація на кожному рівні, обмежує ризик виникнення внутрішньої загрози)

Snowflake - одна з хмарних платформ

Infostealer - тип ПЗ направлений на викрадення логінів, паролів, cookies та іншу інформацію, з можливою передачею даних на сервер до зловмисника. Може поширюватись через фішинг, заражені сайти, ПЗ. Приклади: Meta Stealer(MacOS), Raccoon Stealer(Maar), Vidar(HTTP, FTP), LummarC2(може обходити антивіруси) та подібні

IOCTL-запити - Input/Output Control - команди для пристроїв для керування їхньою поведінкою.

UEBA - User and Entity Behavior Analytics - технологія для аналізу поведінки користувачів і пристроїв у мережі для виявлення аномалій.

SIEM - Security Information and Event Management - Платформа яка збирає аналізує та корелює лог-файли з таких систем як сервери, мережі, додатки. Важливий для SOC спеціалістів.

***Можливі*** *інструменти використані зловмисниками, та у випадку моделювання атаки для тренування (ІМХО)*:

**Salt Typhoon Espionage Campaign**

ОС: Kali-Linux, Parrot, Arch Linux, Ubuntu(модифікована та налаштована)

Інструменти: nmap, nikto, zenmap, Metasploit, Wireshark, BurpSuite, JohnTheRipper(Hashcat + - ), Cisco Torch, CGE(Cisco Global Explorer)

\* можливо написані самостійно скрипти

**Snowflake Data Breach**

ОС: Kali-Linux, Parrot, Arch Linux, Ubuntu(модифікована та налаштована)

Інструменти: Metasploit, PyExfil, SG1, PacketWhisper, OpenBullet, SentryMBA, SNIPR, STORMб Maltego, Spiderfoot, theHarvester, GoogleDorks, cURL, WinSCP, Win-RAR/7-zip, PyLock, LockBit, BloodHound/SharpHound, Mimikatz, APT29, PowerView та подібні