Threat Hunting in the Healthcare Sector using MITRE ATT&CK

Project Overview

This project focuses on **proactive threat hunting** within the **healthcare industry**, leveraging the **MITRE ATT&CK framework** to identify and analyze Advanced Persistent Threat (APT) groups targeting the sector.

The objective was to:

- Identify healthcare-targeted APTs.
- Analyze their **Tactics, Techniques, and Procedures (TTPs)**.
- Visualize the threat landscape using **MITRE Navigator**.
- Compare APTs to find common attack vectors.

Objectives

1. Understand the MITRE ATT&CK framework and its application to real-world threat hunting.
2. Research APTs targeting the healthcare sector using SOCRadar Labs.
3. Map identified APTs to relevant TTPs in MITRE ATT&CK Navigator.
4. Perform a comparative analysis to highlight overlapping attack patterns.

Tools & Resources

- **SOCRadar Labs** – For retrieving healthcare-specific APT threat intelligence.
- **MITRE ATT&CK Navigator** – For mapping APT TTPs.
- **MITRE ATT&CK Framework** – For structured adversary behavior taxonomy.
- **OSINT Research** – To cross-check TTP details from open sources.

Project Steps

1. Understanding the MITRE ATT&CK Framework

- Studied the MITRE ATT&CK framework structure:
    - **Tactics** – The *why* of an attack (e.g., Initial Access, Persistence, Defense Evasion).
    - **Techniques** – The *how* of an attack (e.g., phishing, credential dumping).
    - **Procedures** – Real-world implementations of techniques.

2. Research APTs Peculiar to the Sector

- Used SOCRadar Labs to identify **APT groups** targeting healthcare.
- Found the following:
    - **APT41** – China-based cyber-espionage group.

- **APT10** – Menu Pass are known to have acted in association with the Chinese Ministry of State Security's (MSS) Tianjin State Security Bureau and worked for the Huaying Haitai Science and Technology Development Company.
- **APT18** – Suspected threat group that has operated since at least 2009 and has targeted a range of industries, including technology, manufacturing, human rights groups, government, and medical.
- **APT22** – Chinese cyber espionage group targeting multiple sectors including healthcare.

3. Highlight of the TTPs

- For each APT, identified their key TTPs from MITRE:
  - Example (APT41):
    - T1078 – Valid Accounts
    - T1059 – Command and Scripting Interpreter
    - T1027 – Obfuscated Files or Information

4. Map APTs to TTPs using MITRE Navigator

- Created **individual layers** in MITRE Navigator for each APT.
- Color-coded:
  - Red – Techniques confirmed in public reports.
  - Orange – Techniques suspected but unconfirmed.
  - Green – Techniques with existing detection measures.

5. Compare the APTs

- Imported all four APT layers into a **combined Navigator view**.
- Noted **common techniques** across multiple APTs, such as:
  - T1566 – Phishing
  - T1078 – Valid Accounts
  - T1059 – Command and Scripting Interpreter

Findings

- Many healthcare-targeted APTs rely on **phishing** and **valid accounts** for initial access.
- Credential dumping and obfuscation are common across groups.
- Persistent techniques like **scheduled tasks** and **remote services** are frequently used.