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:

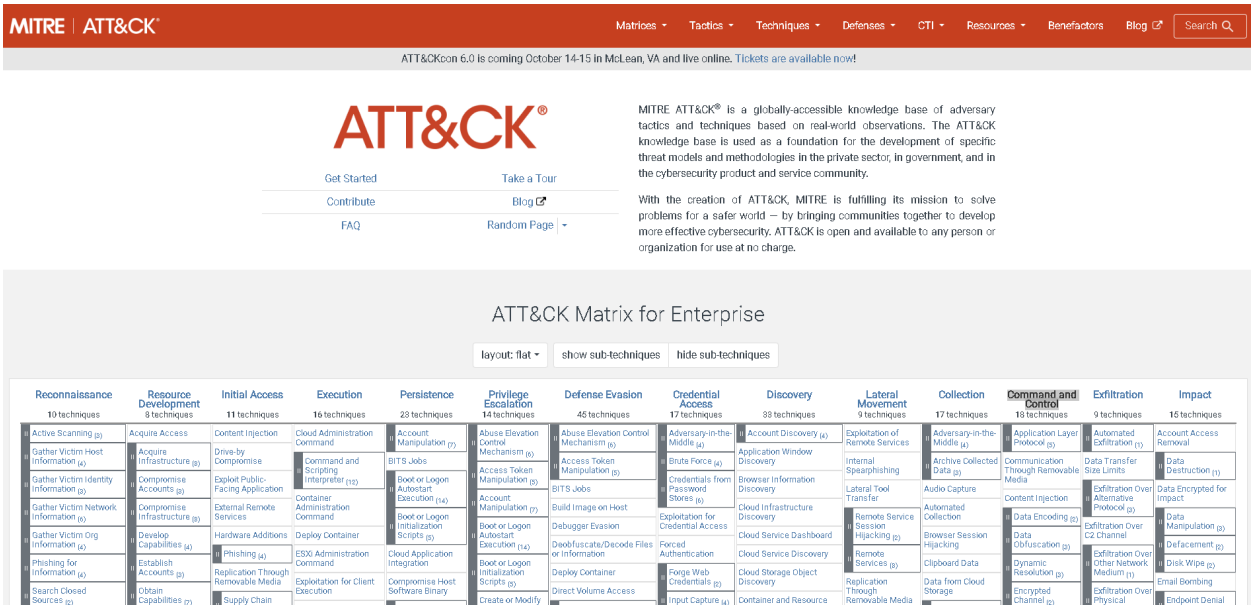
- Identify healthcare-targeted APTs.
- Analyze their **Tactics, Techniques, and Procedures (TTPs)**.
- Visualize the threat landscape using **MITRE Navigator**.
- Compare APTs to find common attack vectors.

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.
- I found the following:

> One of the most active threat groups is known as APT41 (also BARIUM, Winnti, LEAD, WICKED SPIDER, WICKED PANDA, Blackfly, Suckfly, Winnti Umbrella, and Double Dragon). The group has been active since at least 2007 and is known to target U.S. healthcare organizations, most commonly with the goal of obtaining intellectual property to pass to the Chinese government, which operationalizes the technology to bring it to market. The group also engages in espionage and digital extortion and is known to conduct financially motivated cyberattacks, although those operations may be for personal gain rather than at the request of the Chinese government. APT41 aggressively exploits known vulnerabilities, often within hours after public disclosure, as was the case with the ProxyLogon and Log4J vulnerabilities. Once initial access has been gained, the group moves laterally within networks and establishes persistent access, often remaining in networks undetected for long periods while data of interest is exfiltrated. The group has an extensive arsenal of malware and uses well-known security tools in its attacks, such as a customized version of Cobalt Strike, Acunetix, Nmap, JexBoss, and Sqlmap.
>
> APT10 (also known as Menupass Team, Stone Panda, Red Apollo, Cicada, CVNX, HOGFISH, and Cloud Hopper) engages in cyberespionage and cyberwarfare activities and has a focus on military and intelligence data. The group is known to leverage zero-day vulnerabilities to gain access to the networks of targets of interest and uses a variety of custom and public tools to achieve its aims. APT10

    - **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

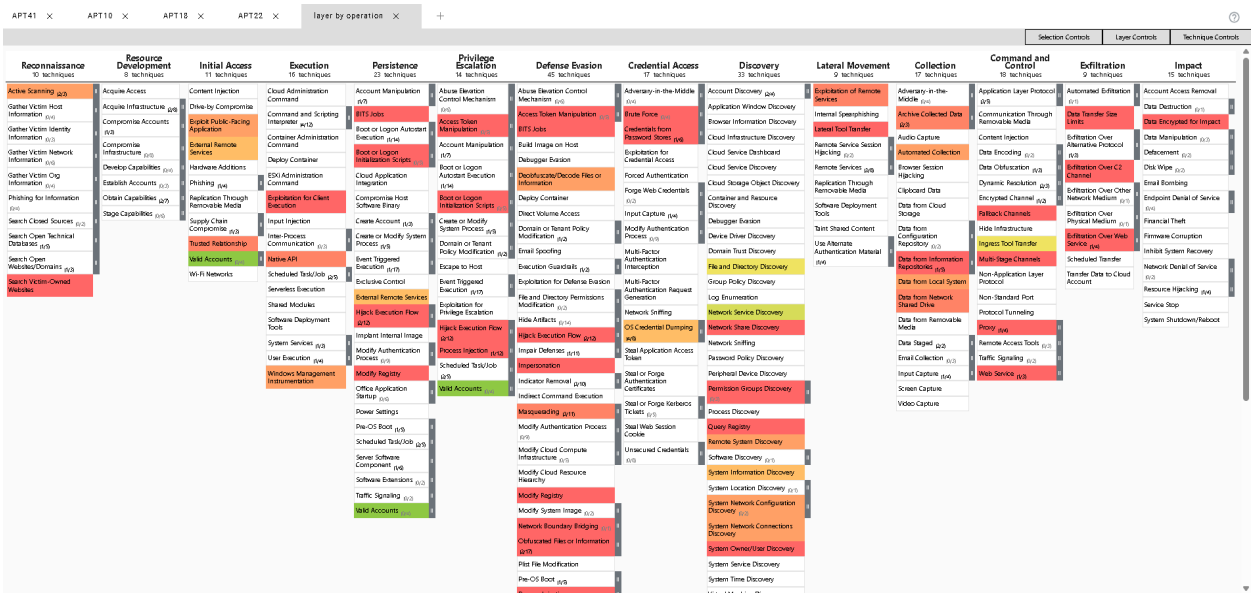
- For each APT, I identified their key TTPs from MITRE:
    - Example (APT41):
        - T1078 – Valid Accounts
        - T1059 – Command and Scripting Interpreter
        - T1027 – Obfuscated Files or Information

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.