Threat Intelligence & Hunting in the Healthcare Sector using MITRE ATT&CK

Prepared by: Dada A. Ojuko

Role: Cybersecurity Analyst

Date: November, 2025

Project Overview

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

The objective was to:

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

Objectives

a) Understand the MITRE ATT&CK framework and its application to real-world threat hunting.

b) Research APTs targeting the healthcare sector using SOCRadar Labs.

c) Map identified APTs to relevant TTPs in MITRE ATT&CK Navigator.

d) Perform a comparative analysis to highlight overlapping attack patterns.

Tools & Resources

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

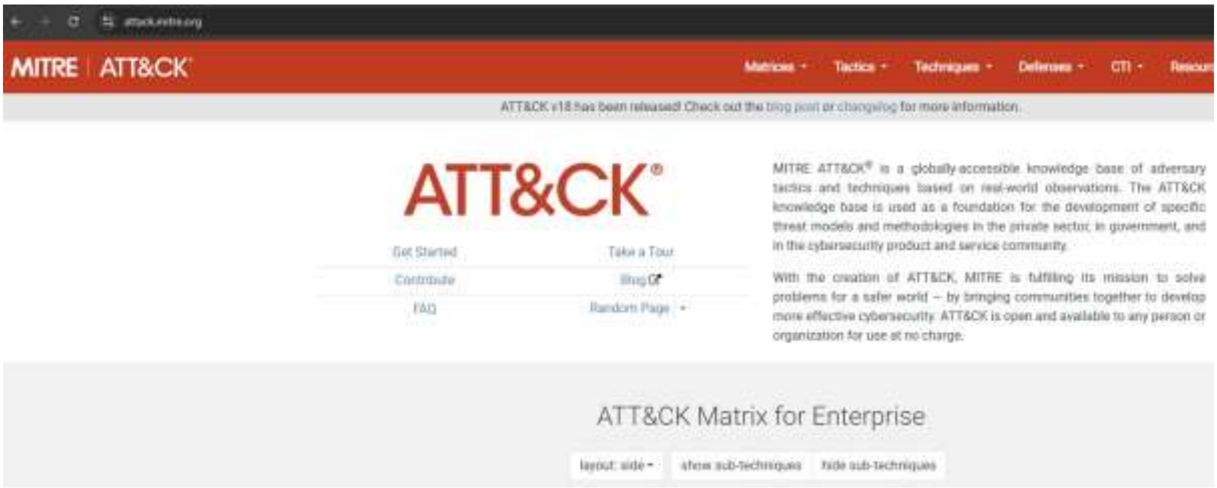
Project Procedures

1. The MITRE ATT&CK framework

The **MITRE ATT&CK Framework** is a globally recognized, knowledge-based matrix that categorizes and documents the behaviors adversaries use during cyberattacks. It provides a structured way to understand how attackers operate across the full lifecycle of an intrusion, helping security teams better detect, analyze, and respond to threats.

At the core of MITRE ATT&CK are **TTPs — Tactics, Techniques, and Procedures**:

- **Tactics** represent the **attacker's goals or objectives**, such as gaining initial access, executing malicious code, or moving laterally within a network.
- **Techniques** describe **how adversaries achieve those goals**, such as phishing, credential scraping, or remote execution.
- **Procedures** are the **specific implementation details** of a technique, including the exact tools, commands, or malware used by a threat group.



ATT&CK v18 has been released! Check out the blog post or changelog for more information.

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations. The ATT&CK knowledge base is used as a foundation for the development of specific threat models and methodologies in the private sector, in government, and in the cybersecurity product and service community.

With the creation of ATT&CK, MITRE is fulfilling its mission to solve problems for a safer world — by bringing communities together to develop more effective cybersecurity. ATT&CK is open and available to any person or organization for use at no charge.

ATT&CK Matrix for Enterprise

By leveraging TTPs within the MITRE ATT&CK framework, organizations move beyond signature-based detection and focus on **behavior-based analysis**, making their defences more resilient against evolving adversaries.

2. Researched APTs peculiar to Healthcare Sector

To identify the various APT groups targeting the Healthcare sector, I used SOCRadar Labs to find the following:

- **APT10** – menuPass 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.
- **APT41** – China-based cyber-espionage group, has been in existence since 2012. Their notable behavior include using a wide range of malware tools to complete mission objectives.
- **Evilnum** – They are a financially motivated threat group that has been active since at least 2018.
- **Turla** – They are a cyber-espionage threat group that has been attributed to Russia's Federal Security Service (FSB). They have compromised victims in over 50 countries since at least 2004, spanning a range of industries including government, embassies, military, education, research and pharmaceutical companies.

3. Highlights of TTPs used by different APT groups

For each APT, I identified their key TTPs from MITRE

- Evilnum
    - T1219 – Remote Access Tools: Remote Desktop Software.
    - T1497 – Virtualization/Sandbox Evasion: System Checks.
- Turla
    - T1566 – Phishing: Spearphishing Link.
    - T1201 – Password Policy Discovery.
    - T1555 – Credentials from Password Stores: Windows Credential Manager.
- APT10 menuPass
    - T1078 – Valid Accounts.
    - T1566 – Phishing: Spearphishing Attachment.
- APT18

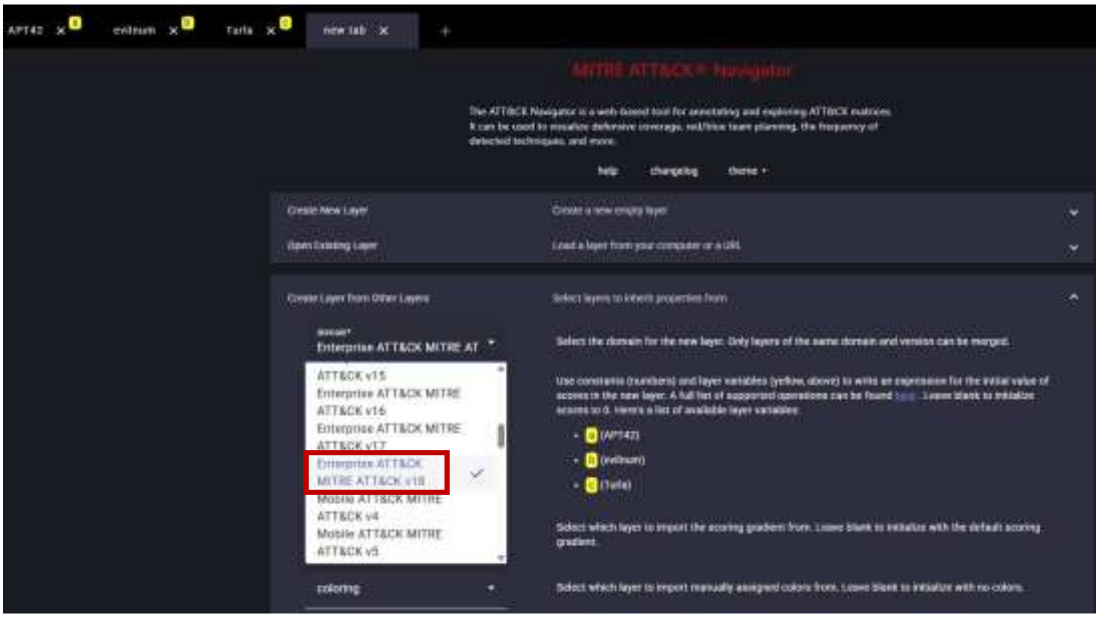
- T1083 – File and Directory Discovery.
- T1078 – Valid Accounts.
- T1133 – External Remote Services.

4. Using MITRE NAVIGATOR to Map APTs to TTPs

I created an individual layer for each APT groups in MITRE Navigator.

Colour Code:

- Red – Techniques confirmed in Public reports.
- Green – Techniques with existing detection measures.
- Orange – Techniques suspected but unconfirmed.



The ATT&CK Navigator is a web-based tool for annotating and exploring ATT&CK matrices. It can be used to visualize defensive coverage, red/blue team planning, the frequency of detected techniques, and more.

Create New Layer — Create a new empty layer

Open Existing Layer — Load a layer from your computer or a URL

Create Layer from Other Layers — Select layers to inherit properties from

domain*: Enterprise ATT&CK MITRE AT

ATT&CK v15
Enterprise ATT&CK MITRE ATT&CK v16
Enterprise ATT&CK MITRE ATT&CK v17
Enterprise ATT&CK MITRE ATT&CK v18 ✓
Mobile ATT&CK MITRE ATT&CK v4
Mobile ATT&CK MITRE ATT&CK v5

Select the domain for the new layer. Only layers of the same domain and version can be merged.

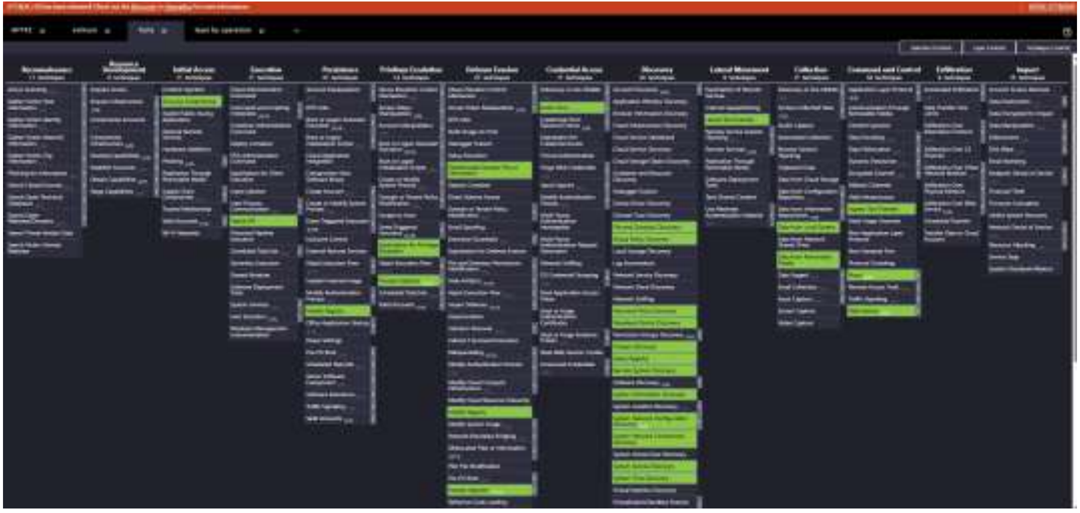
Use constants (numbers) and layer variables (yellow, above) to write an expression for the initial value of scores in the new layer. A full list of supported operations can be found here. Leave blank to initialize scores to 0. Here's a list of available layer variables:

- a (APT42)
- b (evilnum)
- c (Turla)

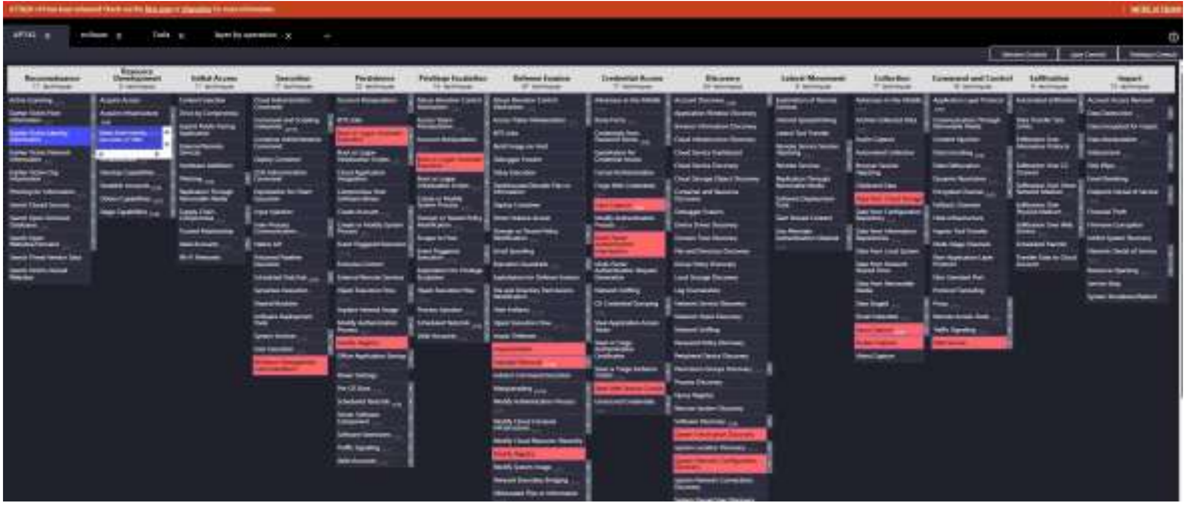
Select which layer to import the scoring gradient from. Leave blank to initialize with the default scoring gradient.

coloring — Select which layer to import manually assigned colors from. Leave blank to initialize with no colors.

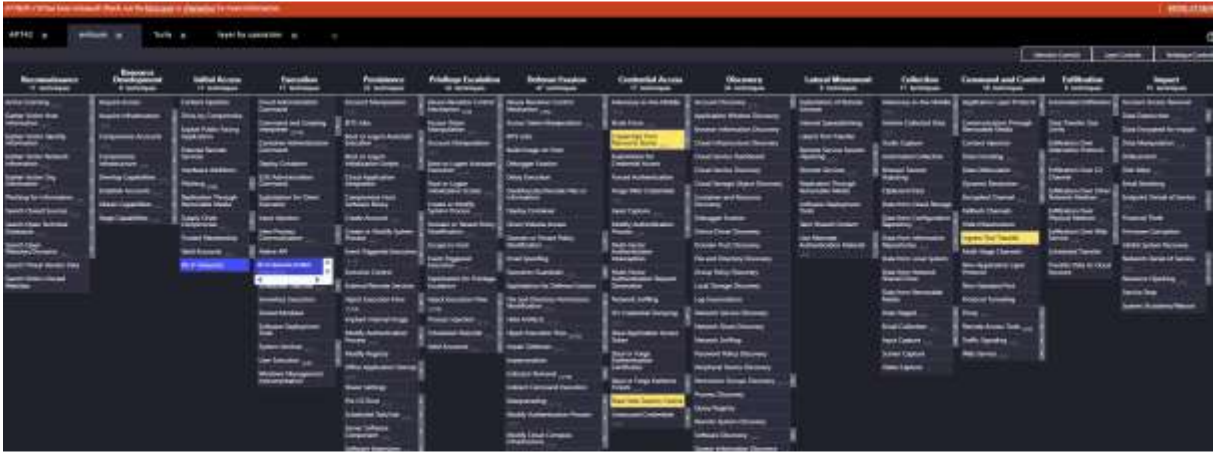
Turla threat Group Tactics and Techniques Mapping.



APT42 threat Group Tactics and Techniques Mapping.



Evilnum threat Group Tactics and Techniques Mapping.

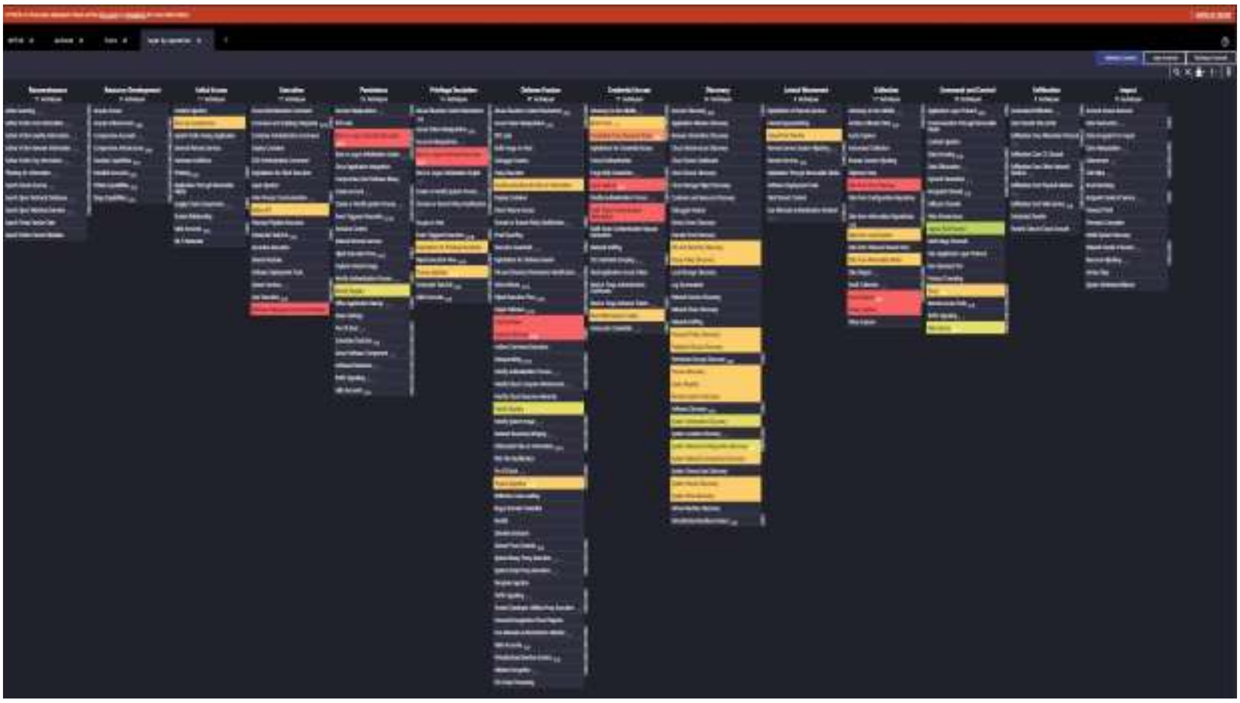


5. Comparing all APT Groups.

All APT Groups were imported in a combined layer of the Navigator view.

Common techniques across few APTs were noted:

- T1566 – Phishing
- T1078 – Valid Accounts
- T1555 – Credential from stored password



Conclusion

In conclusion, the threat landscape facing the healthcare sector continues to evolve as Advanced Persistent Threat (APT) groups increasingly target this industry with sophisticated, multi-stage attacks. Many healthcare-focused APTs consistently rely on **phishing campaigns and the abuse of valid user accounts** to gain their initial foothold, exploiting the human element and weak authentication practices. Once inside, attackers commonly employ **credential dumping and obfuscation techniques** to escalate privileges, evade detection, and maintain operational stealth within compromised environments. Their persistence is further strengthened through the use of **scheduled tasks, remote services, and other long-term access mechanisms** that allow them to operate quietly over extended periods.

These trends highlight the pressing need for healthcare organizations to strengthen security controls, enhance user awareness, and adopt robust monitoring and incident response strategies. Only through a layered defences approach can the sector effectively counter these persistent and highly adaptive adversaries.