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

Prepared by: Biliaminu B. Salawu
Cybersecurity Analyst
Date: 11/11/2025

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 **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 behaviour 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, Defence Evasion).
Techniques – The *how* of an attack (e.g., phishing, credential dumping).
Procedures – Real-world implementations of techniques.

I conducted and examined a threat group APT (Advanced Persistent Groups) common to a particular region and sector, the way they carry out their threats/attack etc
Following is a screenshot of their tactics and techniques.

2. Research APTs Peculiar to the Sector

I Used SOCRadar Labs to identify **APT groups** targeting healthcare.
Found the following:

APT41 – China-based cyber-espionage group and has been in existence since 2012 and their notable behaviours include using a wide range of malware and tools to complete mission objectives

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.

Turla – also known as Shell Crew is 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.

Evilnum also known as TA4563 OR G0120 Joint worm is a financially motivated threat group that has been active since at least 2018 and they are common ATP threat to Albania and Canada Health & Social Assistance.

3. Highlight of the TTPs

Identifying key TTPs from MITRE:

APT41:
T1078 – Valid Accounts
T1059 – Command and Scripting Interpreter
T1027 – Obfuscated Files or Information

APT10 menuPass:
1140: Phishing
T1078 – Valid Accounts

Evilrum
T1140 – Deobfuscate/decode file or password

Turla
T1566 – Phishing
T1078 – Valid Accounts
T1059 – Command and Scripting Interpreter
T1555 – Credential from stored password

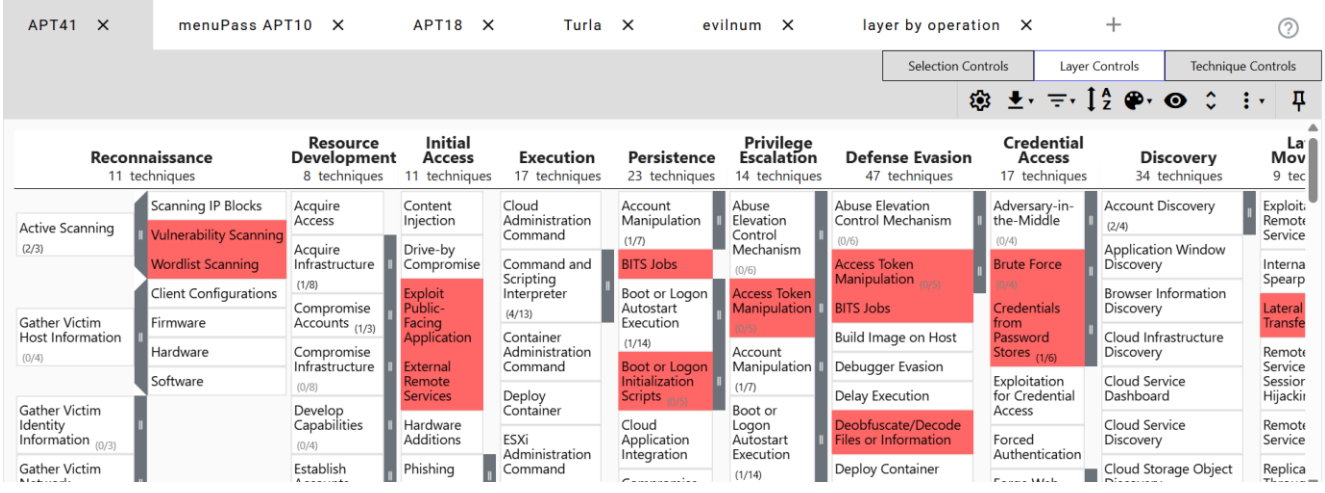
4. Map APTs to TTPs using MITRE Navigator

I Created **individual layers** in MITRE Navigator for each APT.
Color-coded:

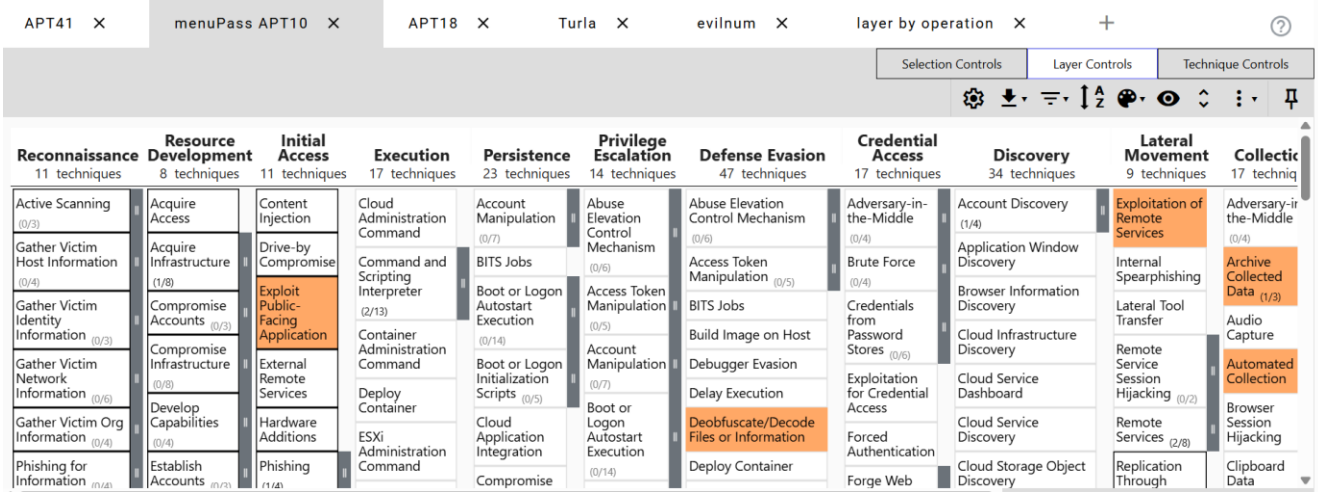
Red – Techniques confirmed in public reports.
Orange – Techniques suspected but unconfirmed.
Green – Techniques with existing detection measures.
Yellow –
LemonGreen – Technique confirmed for Turla threat group

I conducted and examined a threat group APT (Advanced Persistent Groups) common to a particular region and sector, the way they carry out their threats/attack etc
Following is a screenshot of their tactics and techniques.

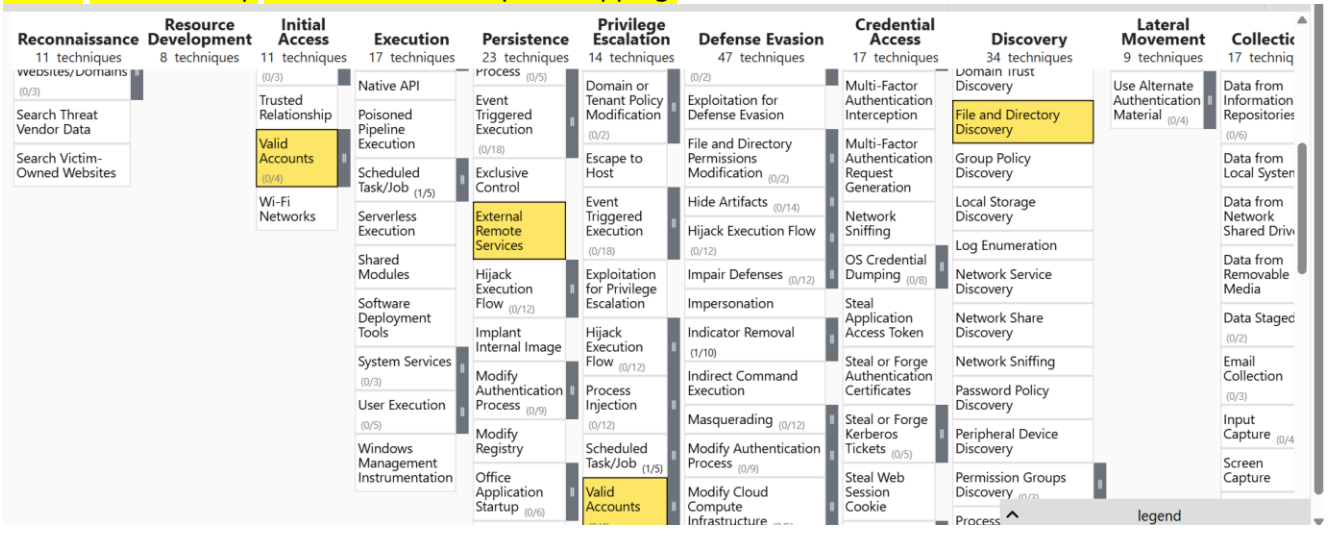
APT41 threat Group Tactics and Techniques Mapping.



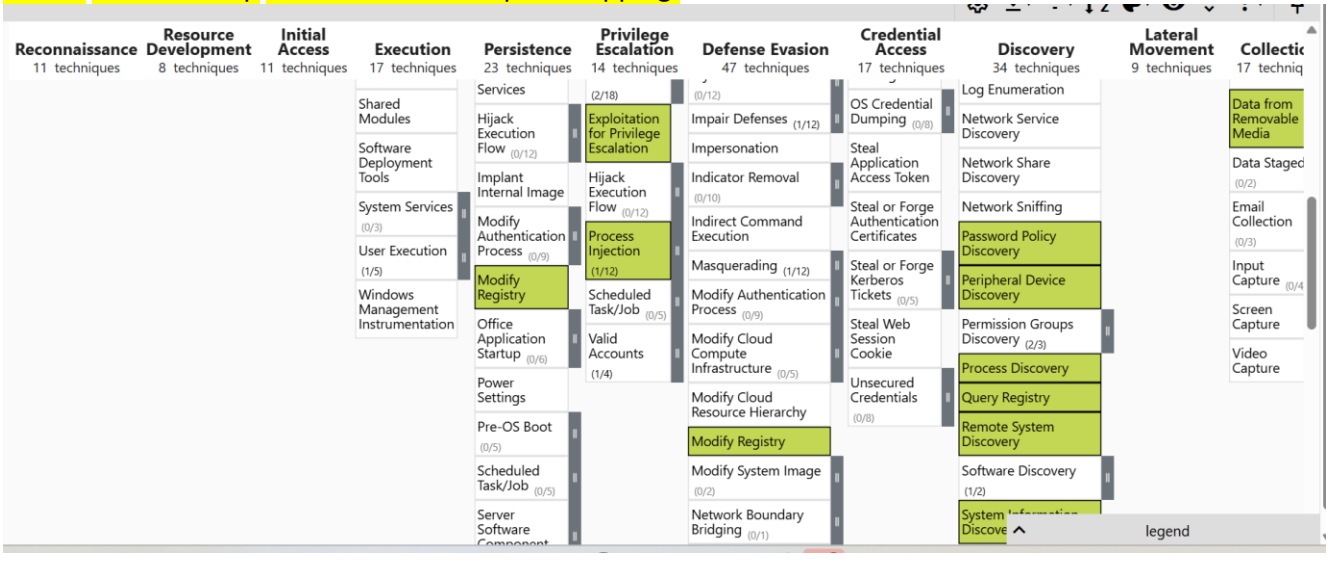
APT10 threat Group Tactics and Techniques Mapping.



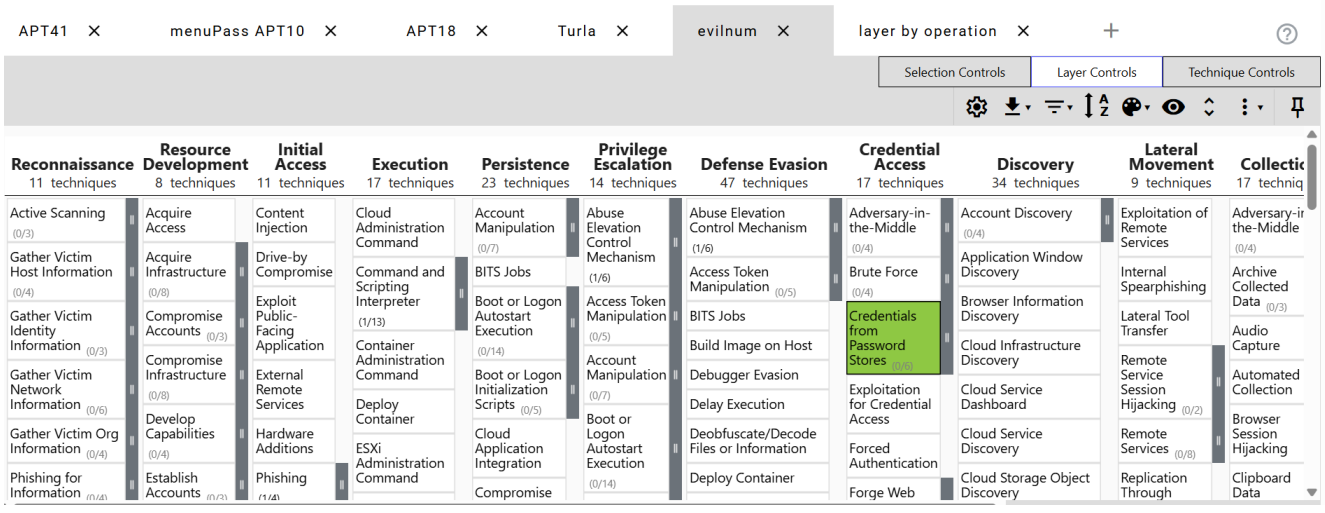
APT18 Threat Group Tactics and Techniques Mapping.



TURLA Threat Group Tactics and Techniques Mapping.

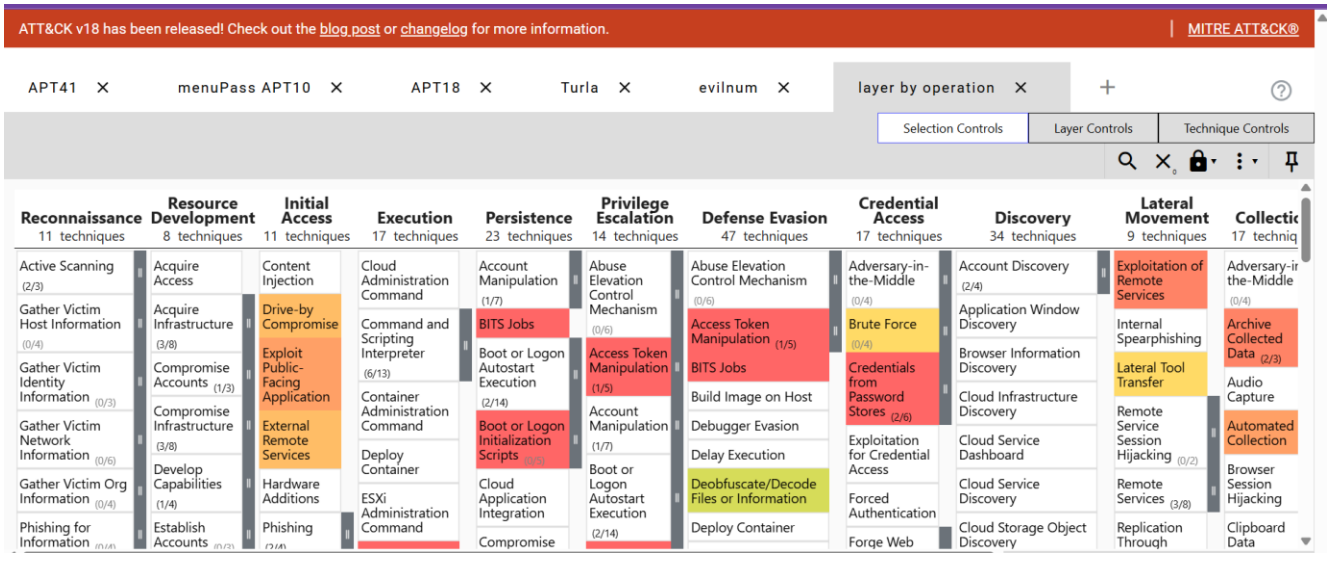


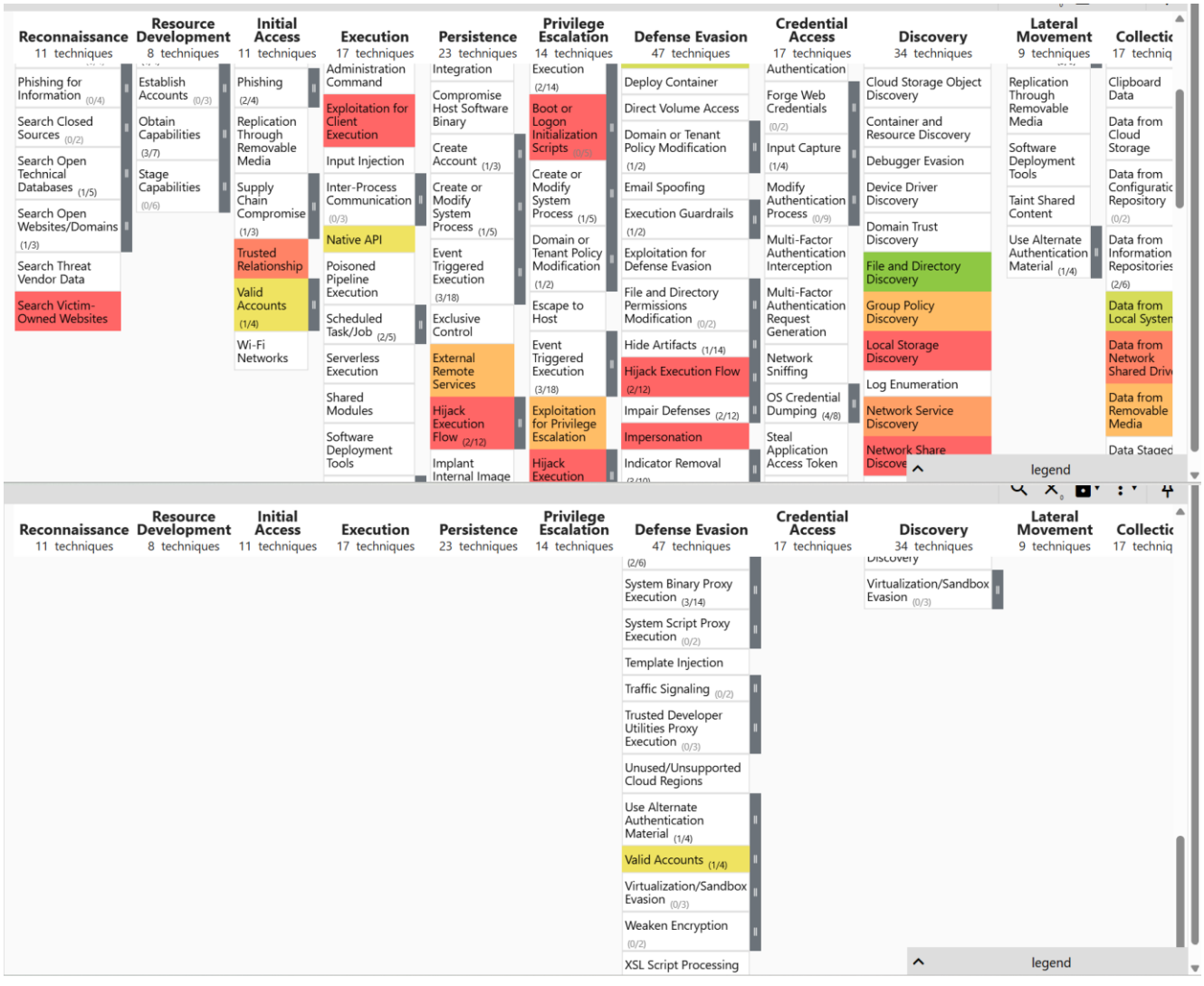
Evilrum Threat Group Tactics and Techniques Mapping.

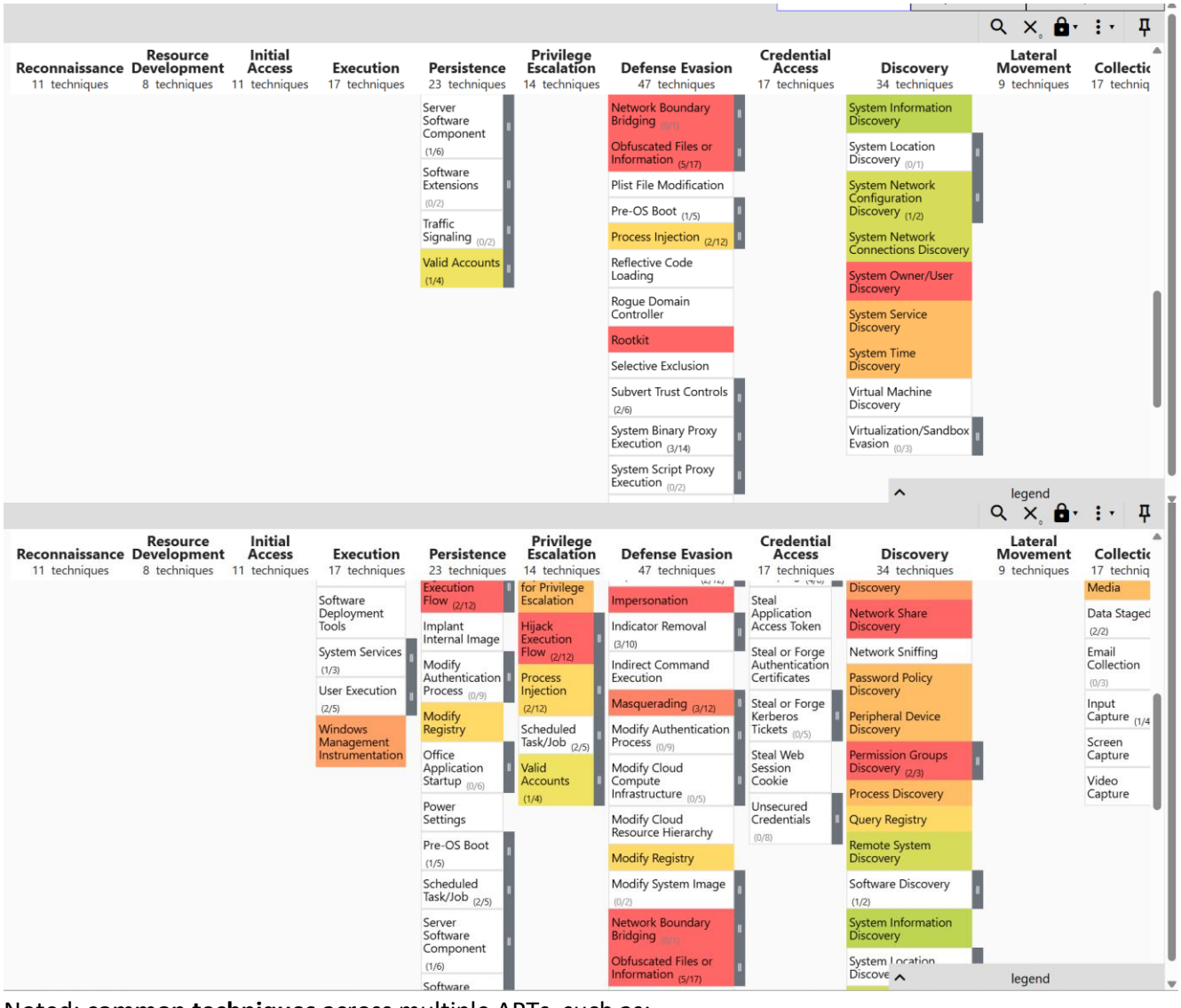


5. Compare the APTs

All five APT layers are imported into a **combined Navigator view**.




Reconnaissance 11 techniques
Phishing for Information (0/4)
Search Closed Sources (0/2)
Search Open Technical Databases (1/5)
Search Open Websites/Domains (1/3)
Search Threat Vendor Data
Search Victim-Owned Websites
Resource Development 8 techniques
Establish Accounts (0/3)
Obtain Capabilities (3/7)
Stage Capabilities (0/6)
Initial Access 11 techniques
Phishing (2/4)
Replication Through Removable Media
Supply Chain Compromise (1/3)
Trusted Relationship
Valid Accounts (1/4)
Wi-Fi Networks
Execution 17 techniques
Administration Command
Exploitation for Client Execution
Input Injection
Inter-Process Communication (0/3)
Native API
Poisoned Pipeline Execution
Scheduled Task/Job (2/5)
Serverless Execution
Shared Modules
Software Deployment Tools
Persistence 23 techniques
Integration
Compromise Host Software Binary
Create Account (1/3)
Create or Modify System Process (1/5)
Event Triggered Execution (3/18)
Exclusive Control
External Remote Services
Hijack Execution Flow (2/12)
Implant Internal Image
Privilege Escalation 14 techniques
Execution (2/14)
Boot or Logon Initialization Scripts (0/5)
Create or Modify System Process (1/5)
Domain or Tenant Policy Modification (1/2)
Escape to Host
Event Triggered Execution (3/18)
Exploitation for Privilege Escalation
Hijack Execution
Defense Evasion 47 techniques
Deploy Container
Direct Volume Access
Domain or Tenant Policy Modification (1/2)
Email Spoofing
Execution Guardrails (1/2)
Exploitation for Defense Evasion
File and Directory Permissions Modification (0/2)
Hide Artifacts (1/14)
Hijack Execution Flow (2/12)
Impair Defenses (2/12)
Impersonation
Indicator Removal
Credential Access 17 techniques
Authentication
Forge Web Credentials (0/2)
Input Capture (1/4)
Modify Authentication Process (0/9)
Multi-Factor Authentication Interception
Multi-Factor Authentication Request Generation
Network Sniffing
OS Credential Dumping (4/8)
Steal Application Access Token
Discovery 34 techniques
Cloud Storage Object Discovery
Container and Resource Discovery
Debugger Evasion
Device Driver Discovery
Domain Trust Discovery
File and Directory Discovery
Group Policy Discovery
Local Storage Discovery
Log Enumeration
Network Service Discovery
Network Share Discove
Lateral Movement 9 techniques
Replication Through Removable Media
Software Deployment Tools
Taint Shared Content
Use Alternate Authentication Material (1/4)
Collectic 17 techniq
Clipboard Data
Data from Cloud Storage
Data from Configuratic Repository (0/2)
Data from Information Repositories (2/6)
Data from Local Syster
Data from Network Shared Driv
Data from Removable Media
Data Staged
legend
Reconnaissance 11 techniques
Resource Development 8 techniques
Initial Access 11 techniques
Execution 17 techniques
Persistence 23 techniques
Privilege Escalation 14 techniques
Defense Evasion 47 techniques
(2/6)
System Binary Proxy Execution (3/14)
System Script Proxy Execution (0/2)
Template Injection
Traffic Signaling (0/2)
Trusted Developer Utilities Proxy Execution (0/3)
Unused/Unsupported Cloud Regions
Use Alternate Authentication Material (1/4)
Valid Accounts (1/4)
Virtualization/Sandbox Evasion (0/3)
Weaken Encryption (0/2)
XSL Script Processing
Credential Access 17 techniques
Discovery 34 techniques
Virtualization/Sandbox Evasion (0/3)
Lateral Movement 9 techniques
Collectic 17 techniq
legend



Noted: **common techniques** across multiple APTs, such as:

T1566 – Phishing

T1078 – Valid Accounts

T1059 – Command and Scripting Interpreter

T1555 – Credential from stored password

T1140 – Deobfuscate/decode file or password.

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