

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.

APT41 X menuPass APT10 X APT18 X Turla X evilnum X layer by operation X + ?										
Selection Controls Layer Controls Technique Controls										
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	La Mov	
11 techniques	8 techniques	11 techniques	17 techniques	23 techniques	14 techniques	47 techniques	17 techniques	34 techniques	9 tec	
Active Scanning (2/3)	Scanning IP Blocks Vulnerability Scanning Wordlist Scanning	Acquire Access Acquire Infrastructure (1/8)	Content Injection Drive-by Compromise	Cloud Administration Command Command and Scripting Interpreter (4/13)	Account Manipulation (1/7) BITS Jobs Boot or Logon Autostart Execution (1/14)	Abuse Elevation Control Mechanism (0/6) Access Token Manipulation (0/5) BITS Jobs Build Image on Host Debugger Evasion Delay Execution Deobfuscate/Decode Files or Information Deploy Container	Adversary-in-the-Middle (0/4) Brute Force (0/4) Credentials from Password Stores (1/6) Exploitation for Credential Access Forced Authentication	Account Discovery (2/4) Application Window Discovery Browser Information Discovery Cloud Infrastructure Discovery Cloud Service Dashboard Cloud Service Discovery Cloud Storage Object	Exploit Remote Service Internal Spear Lateral Transfer Remote Service Session Hijackii Remote Service Replica	
Gather Victim Host Information (0/4)	Client Configurations Firmware Hardware Software	Compromise Accounts (1/3) Compromise Infrastructure (0/8)	Exploit Public-Facing Application External Remote Services	Container Administration Command Deploy Container ESXi Administration Command	Account Manipulation (1/7) Boot or Logon Autostart Execution (1/14)					
Gather Victim Identity Information (0/3)		Develop Capabilities (0/4)	Hardware Additions							
Gather Victim Network Information (0/4)		Establish Accounts	Phishing							

APT10 threat Group Tactics and Techniques Mapping.

APT41 X menuPass APT10 X APT18 X Turla X evilnum X layer by operation X + ?										
Selection Controls Layer Controls Technique Controls										
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collecti
11 techniques	8 techniques	11 techniques	17 techniques	23 techniques	14 techniques	47 techniques	17 techniques	34 techniques	9 techniques	17 techni
Active Scanning (0/3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (0/7)	Abuse Elevation Control Mechanism (0/6)	Abuse Elevation Control Mechanism (0/6)	Adversary-in-the-Middle (0/4)	Account Discovery (1/4)	Exploitation of Remote Services (1/4)	Adversary-ir the-Middle (0/4)
Gather Victim Host Information (0/4)	Acquire Infrastructure (1/8)	Drive-by Compromise	Command and Scripting Interpreter (2/13)	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (1/3)
Gather Victim Identity Information (0/3)	Compromise Accounts (0/3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (0/14)	Access Token Manipulation (0/5)	BITS Jobs	Credentials from Password Stores (0/6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Account Manipulation (0/7)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection
Gather Victim Org Information (0/4)	Develop Capabilities (0/4)	Hardware Additions	ESXi Administration Command	Cloud Application Integration	Boot or Logon Autostart Execution (0/14)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (2/8)	Browser Session Hijacking
Phishing for Information (0/4)	Establish Accounts (0/2)	Phishing (1/4)	Compromise			Delay Execution Deobfuscate/Decode Files or Information Deploy Container	Forge Web	Cloud Service Discovery Cloud Storage Object	Replication Through	Clipboard Data

APT18 Threat Group Tactics and Techniques Mapping.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
11 techniques	8 techniques	11 techniques	17 techniques	23 techniques	14 techniques	47 techniques	17 techniques	34 techniques	9 techniques	17 techniques
Search Threat Vendor Data		Valid Accounts (0/4)	Native API	Event Triggered Execution (0/18)	Domain or Tenant Policy Modification (0/2)	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	File and Directory Discovery	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/6)
Search Victim-Owned Websites		Wi-Fi Networks	Poisoned Pipeline Execution	Exclusive Control	Escape to Host	File and Directory Permissions Modification (0/2)	Multi-Factor Authentication Request Generation	Group Policy Discovery		Data from Local System
			Scheduled Task/Job (1/5)	External Remote Services	Event Triggered Execution (0/18)	Hide Artifacts (0/14)	Network Sniffing	Local Storage Discovery		Data from Network Shared Drives
			Serverless Execution	Hijack Execution Flow (0/12)	Exploitation for Privilege Escalation	Hijack Execution Flow (0/12)	OS Credential Dumping (0/8)	Log Enumeration		Data from Removable Media
			Shared Modules	Implant Internal Image	Hijack Execution Flow (0/12)	Impair Defenses (0/12)	Steal Application Access Token	Network Service Discovery		Data Staged (0/2)
			Software Deployment Tools	Modify Authentication Process (0/9)	Process Injection (0/12)	Indicator Removal (1/10)	Steal or Forge Authentication Certificates	Network Share Discovery		Email Collection (0/3)
			System Services (0/3)	Modify Registry	Scheduled Task/Job (1/5)	Indirect Command Execution	Steal or Forge Kerberos Tickets (0/5)	Password Policy Discovery		Input Capture (0/4)
			User Execution (0/5)	Office Application Startup (0/6)	Valid Accounts	Masquerading (0/12)	Steal Web Session Cookie	Peripheral Device Discovery		Screen Capture
			Windows Management Instrumentation			Modify Authentication Process (0/9)		Permission Groups Discovery (0/3)		
						Modify Cloud Compute Infrastructure				

TURLA Threat Group Tactics and Techniques Mapping.

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
11 techniques	8 techniques	11 techniques	17 techniques	23 techniques	14 techniques	47 techniques	17 techniques	34 techniques	9 techniques	17 techniques
			Shared Modules	Services (2/18)	Exploitation for Privilege Escalation	Impair Defenses (1/12)	OS Credential Dumping (0/8)	Log Enumeration		Data from Removable Media (0/2)
			Software Deployment Tools	Hijack Execution Flow (0/12)	Hijack Execution Flow (0/12)	Impersonation	Steal Application Access Token	Network Service Discovery		Data Staged (0/2)
			System Services (0/3)	Implant Internal Image	Process Injection (1/12)	Indicator Removal (0/10)	Steal or Forge Authentication Certificates	Network Sniffing		Email Collection (0/3)
			User Execution (1/5)	Modify Authentication Process (0/9)	Scheduled Task/Job (0/5)	Indirect Command Execution	Steal or Forge Kerberos Tickets (0/5)	Password Policy Discovery		Input Capture (0/4)
			Windows Management Instrumentation	Modify Registry	Valid Accounts (1/4)	Masquerading (1/12)	Steal Web Session Cookie	Peripheral Device Discovery		Screen Capture
				Office Application Startup (0/6)		Modify Authentication Process (0/9)	Unsecured Credentials (0/8)	Permission Groups Discovery (2/3)		Video Capture
				Power Settings		Modify Cloud Compute Infrastructure (0/5)		Process Discovery		
				Pre-OS Boot (0/5)		Modify Cloud Resource Hierarchy		Query Registry		
				Scheduled Task/Job (0/5)		Modify Registry		Remote System Discovery		
				Server Software Component		Modify System Image (0/2)		Software Discovery (1/2)		
						Network Boundary Bridging (0/1)		System Information Discovery		

Evilrum Threat Group Tactics and Techniques Mapping.

APT41 X

menuPass APT10 X

APT18 X

Turla X

evilnum X

layer by operation X

+

?

Selection Controls

Layer Controls

Technique Controls

⚙️

📄

🔍

📏

🔍

🔍

🔍

🔍

🔍

🔍

🔍

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
11 techniques	8 techniques	11 techniques	17 techniques	23 techniques	14 techniques	47 techniques	17 techniques	34 techniques	9 techniques	17 techniques
Active Scanning (0/3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (0/7)	Abuse Elevation Control Mechanism (1/6)	Abuse Elevation Control Mechanism (1/6)	Adversary-in-the-Middle (0/4)	Account Discovery (0/4)	Exploitation of Remote Services (0/4)	Adversary-in-the-Middle (0/4)
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Drive-by Compromise	Command and Scripting Interpreter (1/13)	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)
Gather Victim Identity Information (0/3)	Compromise Accounts (0/3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (0/14)	Access Token Manipulation (0/5)	BITS Jobs	Credentials from Password Stores (2/6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture
Gather Victim Network Information (0/6)	Compromise Infrastructure (0/8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Account Manipulation (0/7)	Debugger Evasion	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection
Gather Victim Org Information (0/4)	Develop Capabilities (1/4)	Hardware Additions	ESXi Administration Command	Cloud Application Integration	Boot or Logon Autostart Execution (0/14)	Delay Execution	Forced Authentication	Cloud Service Dashboard	Remote Services (0/8)	Browser Session Hijacking
Phishing for Information (0/14)	Establish Accounts (0/2)	Phishing (1/4)		Compromise		Deobfuscate/Decode Files or Information	Forge Web	Cloud Service Discovery	Replication Through	Clipboard Data
						Deploy Container		Cloud Storage Object Discovery		

5. Compare the APTs

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

ATT&CK v18 has been released! Check out the [blog post](#) or [changelog](#) for more information.

MITRE ATT&CK®

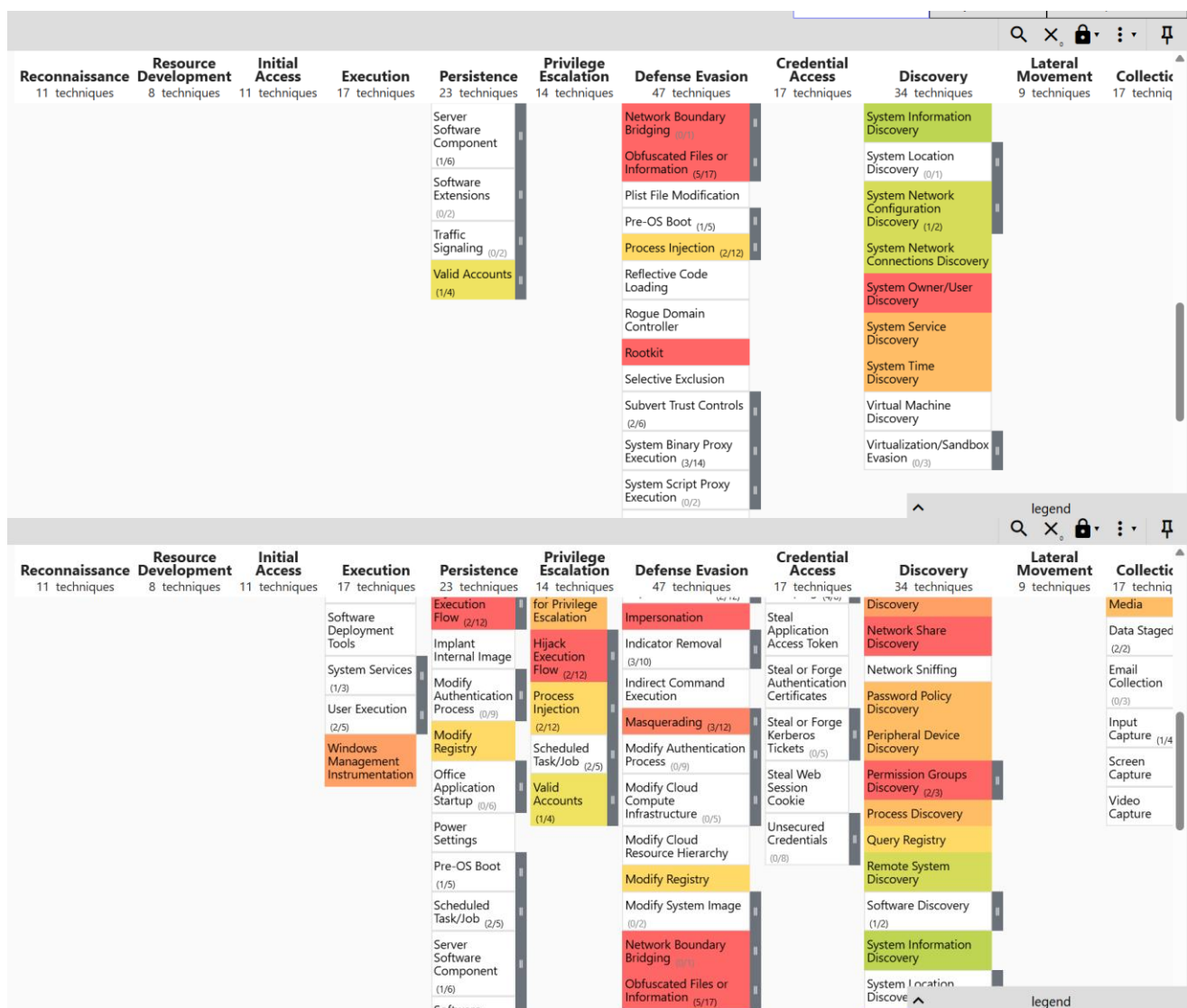
APT41 XmenuPass APT10 XAPT18 XTurla Xevilnum Xlayer by operation X+?

Selection ControlsLayer ControlsTechnique Controls

QX🔒⋮📌

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection
11 techniques	8 techniques	11 techniques	17 techniques	23 techniques	14 techniques	47 techniques	17 techniques	34 techniques	9 techniques	17 techniques
Active Scanning (2/3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (1/7)	Abuse Elevation Control Mechanism (0/6)	Abuse Elevation Control Mechanism (0/6)	Adversary-in-the-Middle (0/4)	Account Discovery (2/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/4)
Gather Victim Host Information (0/4)	Acquire Infrastructure (3/8)	Drive-by Compromise	Command and Scripting Interpreter (6/13)	BITS Jobs	Access Token Manipulation (1/5)	Access Token Manipulation (1/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (2/3)
Gather Victim Identity Information (0/3)	Compromise Accounts (1/3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (2/14)	Access Token Manipulation (1/5)	BITS Jobs	Credentials from Password Stores (2/6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture
Gather Victim Network Information (0/6)	Compromise Infrastructure (3/8)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (2/5)	Account Manipulation (1/7)	Debugger Evasion	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection
Gather Victim Org Information (0/4)	Develop Capabilities (1/4)	Hardware Additions	ESXi Administration Command	Cloud Application Integration	Boot or Logon Autostart Execution (2/14)	Delay Execution	Deobfuscate/Decode Files or Information	Cloud Service Dashboard	Remote Services (3/8)	Browser Session Hijacking
Phishing for Information (0/14)	Establish Accounts (0/2)	Phishing (1/4)		Compromise		Deploy Container	Forced Authentication	Cloud Service Discovery	Replication Through	Clipboard Data
							Forge Web	Cloud Storage Object Discovery		

[illegible]



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