

# 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.

MITRE | ATT&CK

Matrices • Tactics • Techniques • Defenses • CTI • Resources • Benefactors • Blog [🔗](#)

Search Q

ATT&CKcon 6.0 is coming October 14-15 in McLean, VA and live online. Tickets are available now!

ATT&CK®

Get Started

Take a Tour

Contribute

Blog [🔗](#)

FAQ

Random Page | -

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

layout: flat • show sub-techniques hide sub-techniques

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
10 techniques	8 techniques	11 techniques	16 techniques	23 techniques	14 techniques	45 techniques	17 techniques	39 techniques	9 techniques	17 techniques	19 techniques	9 techniques	16 techniques
Active Scanning (3)	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation (7)	Abuse Elevation Control Mechanism (6)	Abuse Elevation Control Mechanism (6)	Adversary-in-the-Middle (4)	Account Discovery (4)	Exploitation of Remote Services	Adversary-in-the-Middle (4)	Application Layer Protocol (3)	Automated Exfiltration (7)	Account Access Removal
Gather Victim Host Information (4)	Acquire Infrastructure (3)	Drive-by Compromise	Command and Scripting Interpreter (12)	BITS Jobs	Access Token Manipulation (5)	Access Token Manipulation (5)	Brute Force (4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction (1)
Gather Victim Identity Information (3)	Compromise Accounts (3)	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (3)	Account Manipulation (3)	Credentials from Password Stores (3)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol (3)	Data Encrypted for Impact
Gather Victim Network Information (4)	Compromise Infrastructure (3)	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (3)	Account Manipulation (7)	Build Image on Host	Debugger Evasion	Cloud Infrastructure Discovery	Remote Service Session Hijacking (3)	Automated Collection	Data Encoding (3)	Exfiltration Over C2 Channel	Data Manipulation (3)
Gather Victim Org Information (4)	Develop Capabilities (4)	Hardware Additions	ESXi Administration Command	Boot or Logon Autostart Execution (14)	Account Manipulation (7)	Debugger Evasion	Exploitation for Credential Access	Cloud Service Dashboard	Remote Session Hijacking (3)	Browser Session Hijacking	Data Obfuscation (3)	Exfiltration Over Other Network Medium (1)	Data Removal (3)
Phishing for Information (4)	Establish Accounts (3)	Phishing (4)	ESXi Administration Command	Cloud Application Integration	Boot or Logon Initialization Scripts (3)	Debugger Evasion	Exploitation for Credential Access	Cloud Service Discovery	Remote Services (3)	Clipboard Data	Dynamic Resolution (3)	Exfiltration Over Physical	Device Wipe (3)
Search Closed Sources (3)	Obtain Capabilities (7)	Replication Through Removable Media	Exploitation for Client Execution	Compromise Host Software Binary	Boot or Logon Initialization Scripts (3)	Deploy Container	Forge Web Credentials (3)	Cloud Storage Object Discovery	Replication Through Removable Media	Data from Cloud Storage	Encrypted Channel (3)	Exfiltration Over Physical	Email Bombing
		Supply Chain		Create or Modify	Create or Modify	Direct Volume Access	Input Capture (4)	Container and Resource					Endpoint Denial

# 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

APT41 ×

APT10 ×

APT18 ×

APT22 ×

Layer by operation ×

+

Section Controls

Layer Controls

Technique Controls

Reconnaissance		Resource Development		Initial Access		Execution		Persistence		Privilege Escalation		Defense Evasion		Credentialess Access		Discovery		Lateral Movement		Collection		Command and Control		Exfiltration		Impact	
10 techniques		6 techniques		11 techniques		11 techniques		12 techniques		14 techniques		40 techniques		17 techniques		27 techniques		17 techniques		17 techniques		10 techniques		9 techniques		15 techniques	
Active Scanning <span>g23</span>		Acquire Assets		Content Injection		Cloud Administration		Account Manipulation		Abuse Escalation		Abuse Escalation		Adversary in the Middle		Account Discovery		Exploitation of Remote Services		Adversary in the Middle		Application Layer Protocol		Automated Exfiltration		Account Access Removal	
Gather Victim Host Information <span>g15</span>		Acquire Infrastructure <span>g23</span>		Divide by Zero Exploit <span>g23</span>		Command and Scripting Interpreter <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Gather Victim Identity Information <span>g15</span>		Compromise Credentials <span>g15</span>		Exploit Public-Facing Application <span>g15</span>		Command and Scripting Interpreter <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Gather Victim Network Information <span>g15</span>		Compromise Credentials <span>g15</span>		Exploit Public-Facing Application <span>g15</span>		Command and Scripting Interpreter <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Gather Victim Open Information <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account Access Removal <span>g15</span>	
Search for Open Technical Details <span>g15</span>		Establish Accounts <span>g15</span>		Hardware Additions <span>g15</span>		EDP Administration <span>g15</span>		Account Manipulation <span>g15</span>		Abuse Escalation <span>g15</span>		Abuse Escalation <span>g15</span>		Adversary in the Middle <span>g15</span>		Account Discovery <span>g15</span>		Exploitation of Remote Services <span>g15</span>		Adversary in the Middle <span>g15</span>		Application Layer Protocol <span>g15</span>		Automated Exfiltration <span>g15</span>		Account	

## 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.