

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

## Project overview

This project focuses on proactive threat hunting in the healthcare sector by identifying and analysing Advanced Persistent Threat (APT) organizations that attack the industry using the MITRE ATT&CK framework.

### Aim

- Determine which APTs are focused on healthcare.
- Examine their TTPs, or tactics, techniques, and procedures.
- Use MITRE Navigator to see the threat landscape.
- To identify common attack vectors, compare APTs.

### Objective

- Recognize the MITRE ATT&CK framework and how it applies to actual threat hunting.
- Use Hipaa journal to investigate APTs aimed at the healthcare industry.
- In MITRE ATT&CK Navigator, map discovered APTs to pertinent TTPs.
- Conduct a comparative study to identify assault patterns that overlap.

### Tools and resources used

- Hipaa Journal: To obtain APT threat intelligence relevant to the healthcare industry.
- MITRE ATT&CK Navigator: This tool maps APT to the appropriate TTPs.
- MITRE ATT&CK Framework: For the taxonomy of structured adversary conduct.
- OSINT Research: To verify TTP information from publicly available sources.

### Steps in the Project

- Comprehending the MITRE ATT&CK Framework
  - Researched the structure of the MITRE ATT&CK framework:
    - The reasons behind an attack are known as tactics (e.g., Initial Access, Persistence, Defense Evasion).
    - Techniques: How an attack is carried out, such as phishing or credential dumps.
    - Procedures: Practical applications of methods
  - Examine APTs Unique to the Industry identified APT groups aimed at healthcare using a study published in the Hipaa Journal. Discovered the following:

#### APT41:

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)
Drive-by Compromise	Command and Scripting Interpreter (4/13)	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)
Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (1/14)	Account Manipulation (1/7)	Build Image on Host	Credentials from Password Stores (1/6)
External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Autostart Execution (1/14)	Debugger Evasion	Exploitation for Credential Access
Hardware Additions	ESXi Administration Command	Cloud Application Integration	Boot or Logon Initialization	Deobfuscate/Decode Files or Information	Forced Authentication
Phishing (1/4)	Exploitation for Client Execution	Compromise Host Software Binary	Boot or Logon Initialization	Deploy Container	Forge Web Credentials (0/2)
Replication Through				Direct Volume Access	
				Domain or Tenant	

Researchers have identified APT41 as a threat group that is both financially driven and a Chinese state-sponsored espionage organization. APT41 has been active since at least 2012 and has been seen to target a variety of businesses in 14 countries, including but not limited to the healthcare, telecom, technology, banking, education, retail, and video gaming sectors. Using a variety of malware and tools to accomplish mission goals is one of the noteworthy habits. Public reporting on organizations like BARIUM and Winnti Group at least partially coincides with APT41.

#### APT10:

Access 11 techniques	Execution 17 techniques	Persistence 23 techniques	Escalation 14 techniques	Defense Evasion 47 techniques	Access 17 techniques	Discovery 34 techniques	Movement 9 techniques	Collection 17 techniques
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	Adversary-in-the-Middle (0/4)
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)
Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (0/14)	Account Manipulation (0/7)	BITS Jobs	Credentials from Password Stores (0/6)	Browser Information Discovery	Lateral Tool Transfer	Audio Capture
External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Autostart Execution (0/14)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection
Hardware Additions	ESXi Administration Command	Cloud Application Integration	Cloud Application Integration	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (2/8)	Browser Session Hijacking
Phishing (1/4)	Exploitation for Client Execution	Compromise Host Software Binary	Boot or Logon Initialization	Delay Execution	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data
Replication Through			Boot or Logon Initialization	Deobfuscate/Decode Files or Information		Cloud Storage Object Discovery		Data from
				Deploy Container		Container and		
				Direct Volume Access				

Known as menuPass, Threat group menuPass has been active since at least 2006. It is known that several members of menuPass worked for the Huaying Haitai Science & Technology Development Company and collaborated with the Tianjin State Security Bureau of the Chinese Ministry of State Security (MSS).

With a focus on Japanese companies, menuPass has targeted the worldwide healthcare, defense, aerospace, finance, maritime, biotechnology, energy, and government sectors. The organization reportedly targeted a university, manufacturing and mining firms, and managed IT service providers (MSPs) in 2016 and 2017.

#### APT22:

Techniques	23 techniques	14 techniques	47 techniques	17
tration nd	Account Manipulation (0/7)	Abuse Elevation Control Mechanism (0/6)	Abuse Elevation Control Mechanism (0/6)	Adve the-M (0/4)
nd and g ter	BITS Jobs (0/14)	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute (0/4)
er tration nd	Boot or Logon Initialization Scripts (0/5)	Account Manipulation (0/7)	BITS Jobs	Cred from Passw Store
er	Cloud Application Integration	Boot or Logon Autostart Execution (0/14)	Build Image on Host	Explo for C Acce
tration nd	Compromise Host Software Binary	Boot or Logon Initialization Scripts	Debugger Evasion	Force Auth
tion for on	Create		Delay Execution	Forge Cred (0/2)
			Deobfuscate/Decode Files or Information	Input
			Deploy Container	
			Direct Volume Access	
			Domain or Tenant Policy Modification	

Known as suckfly, Suckfly is a threat organization that has been active since at least 2014 and is based in China. seems to be concentrated on attacking political organizations and the healthcare industry, particularly pharmaceutical and biomedical companies. The organization is known to use sophisticated malware like PISCES, SOGU, FLATNOTE, ANGRYBELL, BASELESS, SEAWOLF, and LOGJAM to find unprotected public-facing web servers on victim networks and upload web shells.

#### APT18:

Source Component Techniques	Initial Access 11 techniques	Execution 17 techniques	Persistence 23 techniques	Privilege Escalation 14 techniques	Defense Evasion 47 techniques	Cred Ac 17 techniques
	Content Injection	Cloud Administration Command	Account Manipulation (0/7)	Abuse Elevation Control Mechanism (0/6)	Abuse Elevation Control Mechanism (0/6)	Adversary the-Mid (0/4)
	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)
	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution (1/14)	Account Manipulation (0/7)	BITS Jobs	Credentials from Password Stores
	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Autostart Execution (1/14)	Debugger Evasion	Exploitation for Credential Access
	Hardware Additions	ESXi Administration Command	Cloud Application Integration	Boot or Logon Initialization Scripts	Deobfuscate/Decode Files or Information	Forced Authentication
	Phishing (0/4)	Exploitation for Client Execution	Compromise Host Software Binary	Boot or Logon Initialization Scripts	Deploy Container	Forge Valid Credentials (0/2)
	Replication Through Removable		Create		Direct Volume Access	Input C
					Domain or Tenant Policy Modification	

This is a threat group that has been active since at least 2009 and has targeted a variety of industries, including industry, technology, government, human rights organizations, and the medical field. Also APT18 behind a 2014 attack on a healthcare provider that resulted in the theft of 4.5 million patient records. It is believed that the organization gained access to the network via taking advantage of the OpenSSL Heartbleed vulnerability.

### Highlight of the TTP

Determined the primary TTPs for each APT using MITRE:

#### ❖ APT41

- (T1078) Valid Accounts
- (T1027) Obfuscated Files or Information
- T1059: Command and Scripting Interpreter

#### ❖ APT10

- **(1074):** has prepped data before exfiltration on distant MSP systems or other victim networks
- **(1087):** has exported Active Directory data using the Microsoft administration tool csvde.exe.
- **(1140):** has decoded base64-encoded text from a dropper document sent to an email using certutil in a macro. Additionally, the gang decoded files on the victim's computer by using certutil -decode.

#### ❖ APT22

- **(1059):** Suckfly has employed a number of command-line-driven tools. With command and script interpreter
- **(1046):** Network service discovery
- **(1078):** Valid accounts

#### ❖ APT18

**(1071):** Application layer protocol

**(1547):** Booting or logo auto start execution

**(1070):** indicator removal

## Mapping APTs to TTPs using MITRE Navigator

The screenshot below illustrates the process I followed while mapping all four APTs together, along with the resulting outcomes.

Red: Methods verified by public reporting.

Orange: Unconfirmed but suspected techniques.

Green: Methods utilizing current detection techniques

Chain Compromise (1/3)	Communication (0/3)	Modify System Process (1/5)	System Process (1/5)	Execution Guardrails (1/2)	Authentication Process (0/9)	Discovery	Taint Share Content
Trusted Relationship	Native API	Event Triggered Execution (1/18)	Domain or Tenant Policy Modification (1/2)	Exploitation for Defense Evasion	Multi-Factor Authentication Interception	Domain Trust Discovery	Use Alternative Authentication Material
Valid Accounts (0/4)	Poisoned Pipeline Execution	Exclusive Control	Escape to Host	File and Directory Permissions Modification (0/2)	Multi-Factor Authentication Request Generation	File and Directory Discovery	
Wi-Fi Networks	Scheduled Task/Job (2/5)	External Remote Services	Event Triggered Execution (1/18)	Hide Artifacts (0/14)	Network Sniffing	Group Policy Discovery	
	Serverless Execution	Hijack Execution Flow (2/12)	Exploitation for Privilege Escalation	Hijack Execution Flow (2/12)	OS Credential Dumping (4/8)	Local Storage Discovery	
	Shared Modules	Implant Internal Image	Hijack Execution Flow (2/12)	Impersonation	Steal Application Access Token	Log Enumeration	
	Software Deployment Tools	Modify Authentication Process (0/9)	Process Injection (1/12)	Indicator Removal (3/10)	Steal or Forge Authentication Certificates	Network Service Discovery	
	System Services (1/3)	Modify Registry	Scheduled Task/Job (2/5)	Indirect Command Execution	Steal or Forge Kerberos Tickets (0/5)	Network Share Discovery	
	User Execution (1/5)	Office Application Startup	Valid Accounts	Masquerading (3/12)	Steal Web Session Cookie	Network Sniffing	
	Windows Management Instrumentation			Modify Authentication Process (0/9)		Password Policy Discovery	
				Modify Cloud Compute		Peripheral Device Discovery	
						Permission Groups Discovery	

Legend: Red (verified), Orange (suspected), Green (current detection techniques)

## Observation on the APTs

Examine the APTs.

- All four APT layers were imported into a single Navigator view.

From my research I Identified common strategies used by several APTs, including: Phishing (T1566) and valid accounts (T1078) Command and Scripting Interpreter (T1059)

## **Conclusion**

Phishing is frequently used by adversaries that target the healthcare industry to gain initial access, verify compromised accounts, and carry out credential dumps. They then use remote-access software and scheduled processes to stay persistent and steal papers that are subject to HIPAA regulations.