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

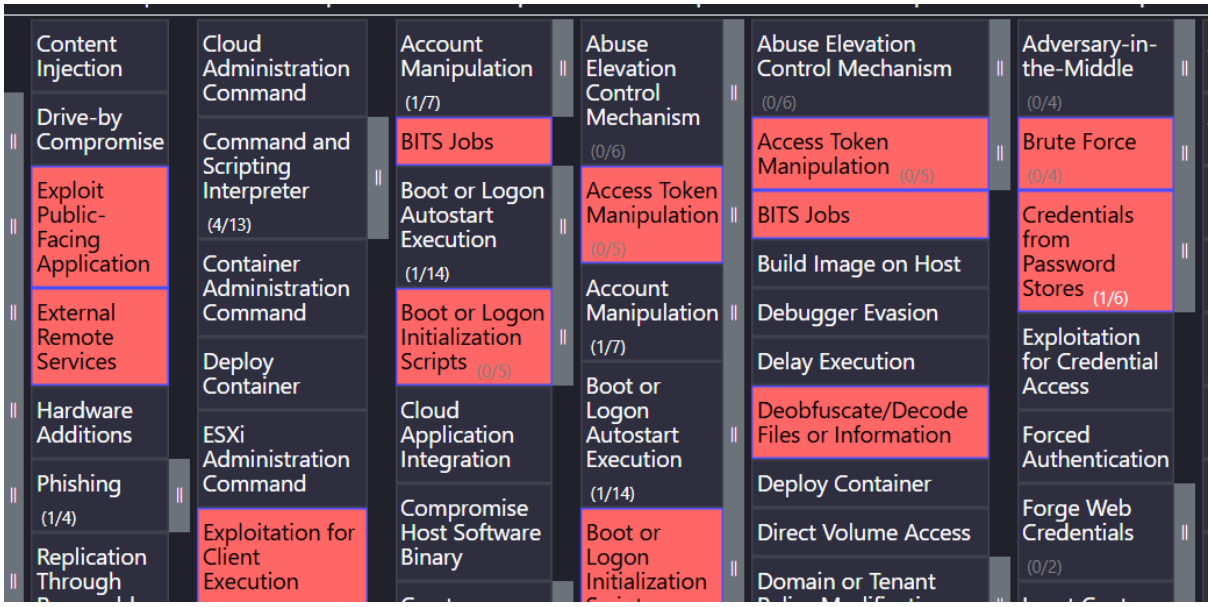
- Hipaa Journal: To obtain APT threat intelligence relevant to the healthcare industry.
- MITRE ATT&CK Navigator: This tool maps APT to the appropriate TTPs.
- MITRE ATT&CK Framework: For the taxonomy of structured adversary conduct.
- OSINT Research: To verify TTP information from publicly available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

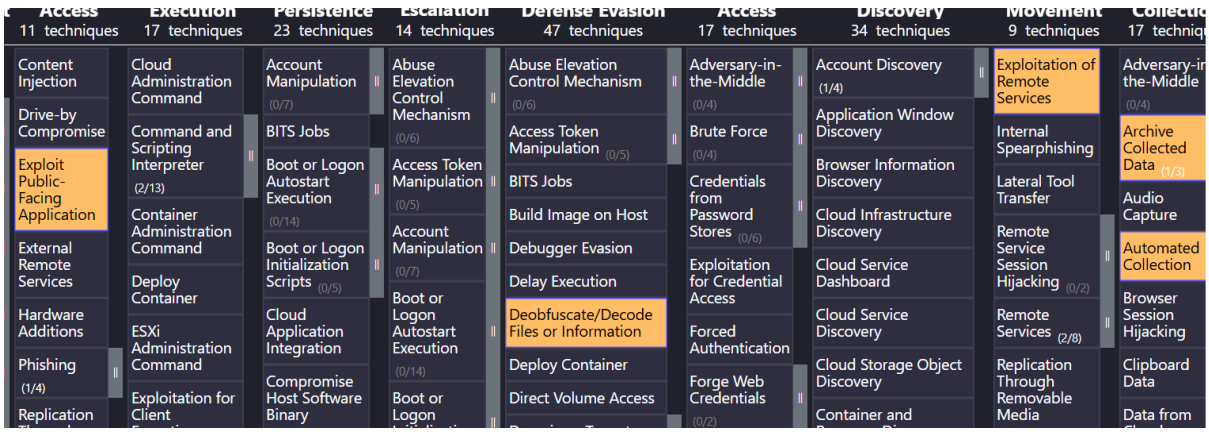
- Examine APTs Unique to the Industry identified APT groups aimed at healthcare using a study published in the Hipaa Journal. Discovered the following:

APT41:



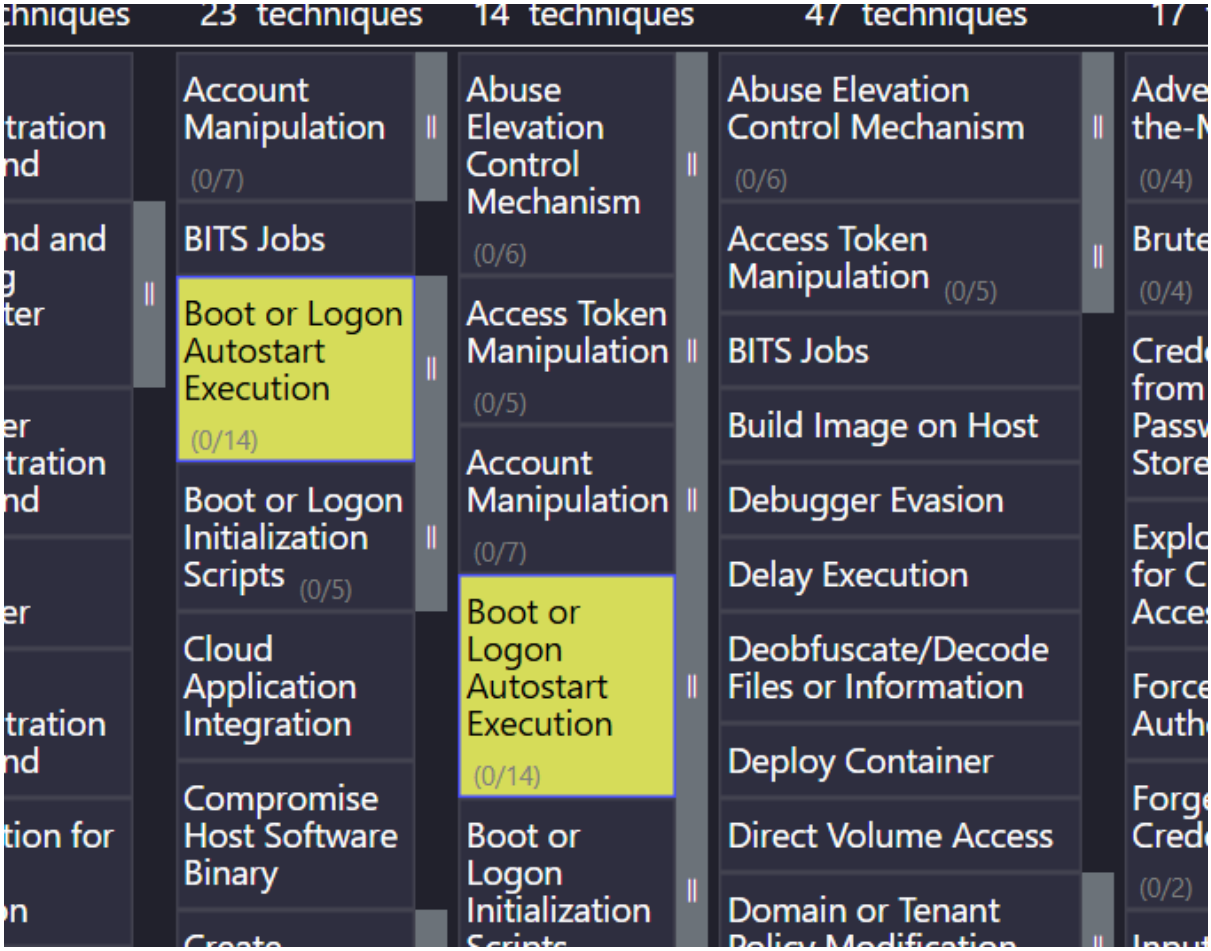
Researchers have identified APT41 as a threat group that is both financially driven and a Chinese state-sponsored espionage organization. APT41 has been active since at least 2012 and has been seen to target a variety of businesses in 14 countries, including but not limited to the healthcare, telecom, 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:



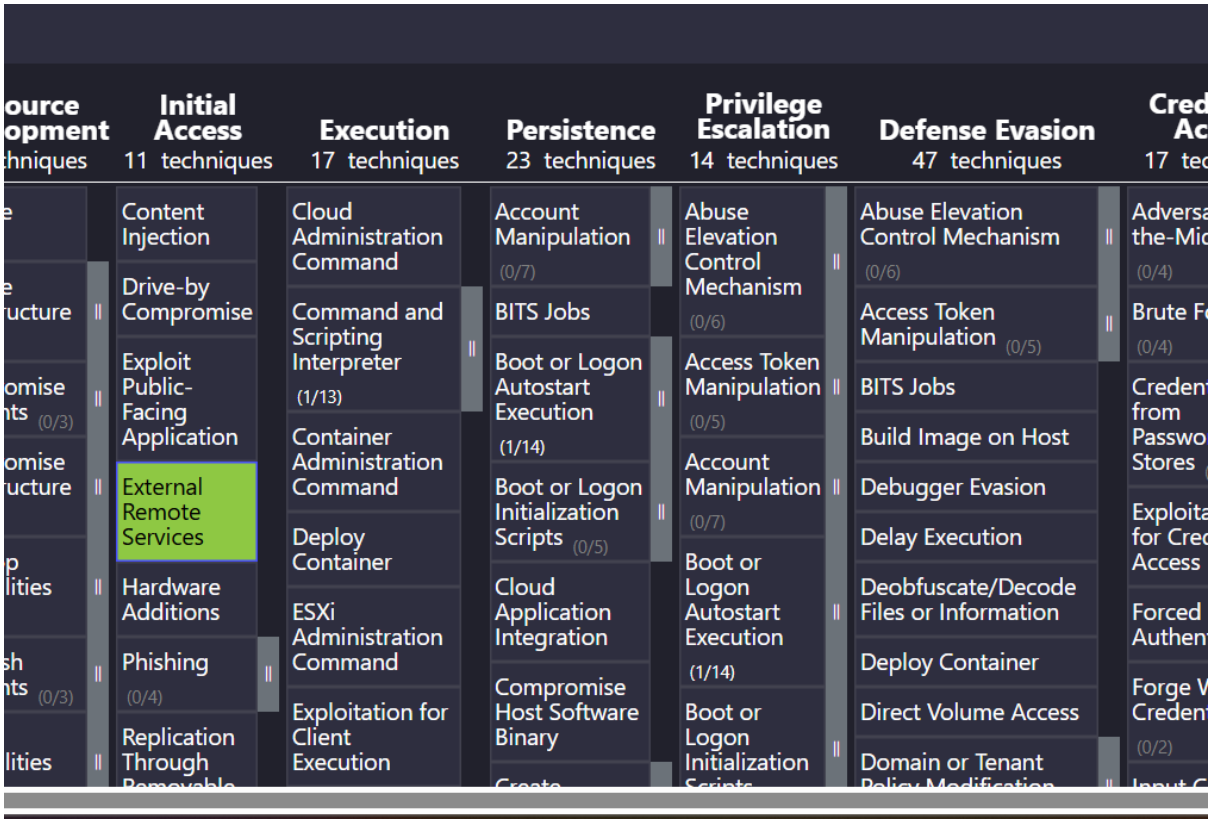
Known as menuPass, Threat group menuPass has been active since at least 2006. It is known that several members of menuPass worked for the Huaying Haitai Science & Technology Development Company and collaborated with the Tianjin State Security Bureau of the Chinese Ministry of State Security (MSS).
With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



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:



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.

Hightlight 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**

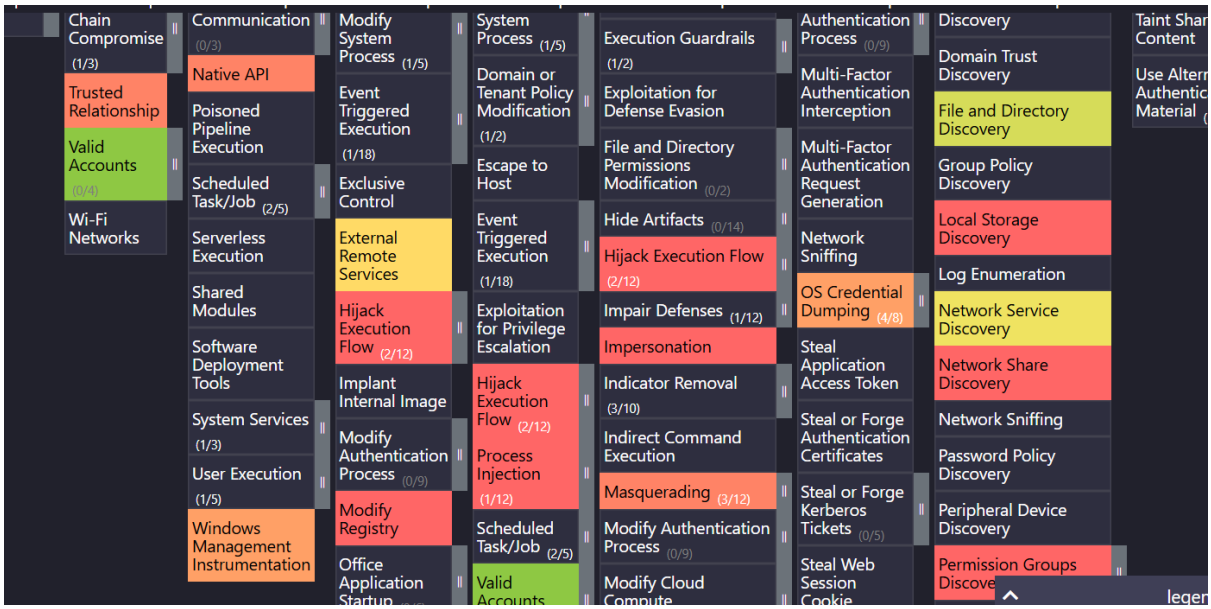
- **(1059):** Suckfly has employed a number of command-line-driven tools. With command and script interpreter
- **(1046):** Network service discovery
- **(1078):** Valid accounts

❖ **APT18**
(1071): Application layer protocol
(1547): Booting or logo auto start execution
(1070): indictor 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



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.