Threat Hunting in the Healthcare Sector using MITRE ATT&CK

Prepared by: Temitope C Folowosele

Date: 11 November 2025

Prepared by: Temitope Folowosele

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

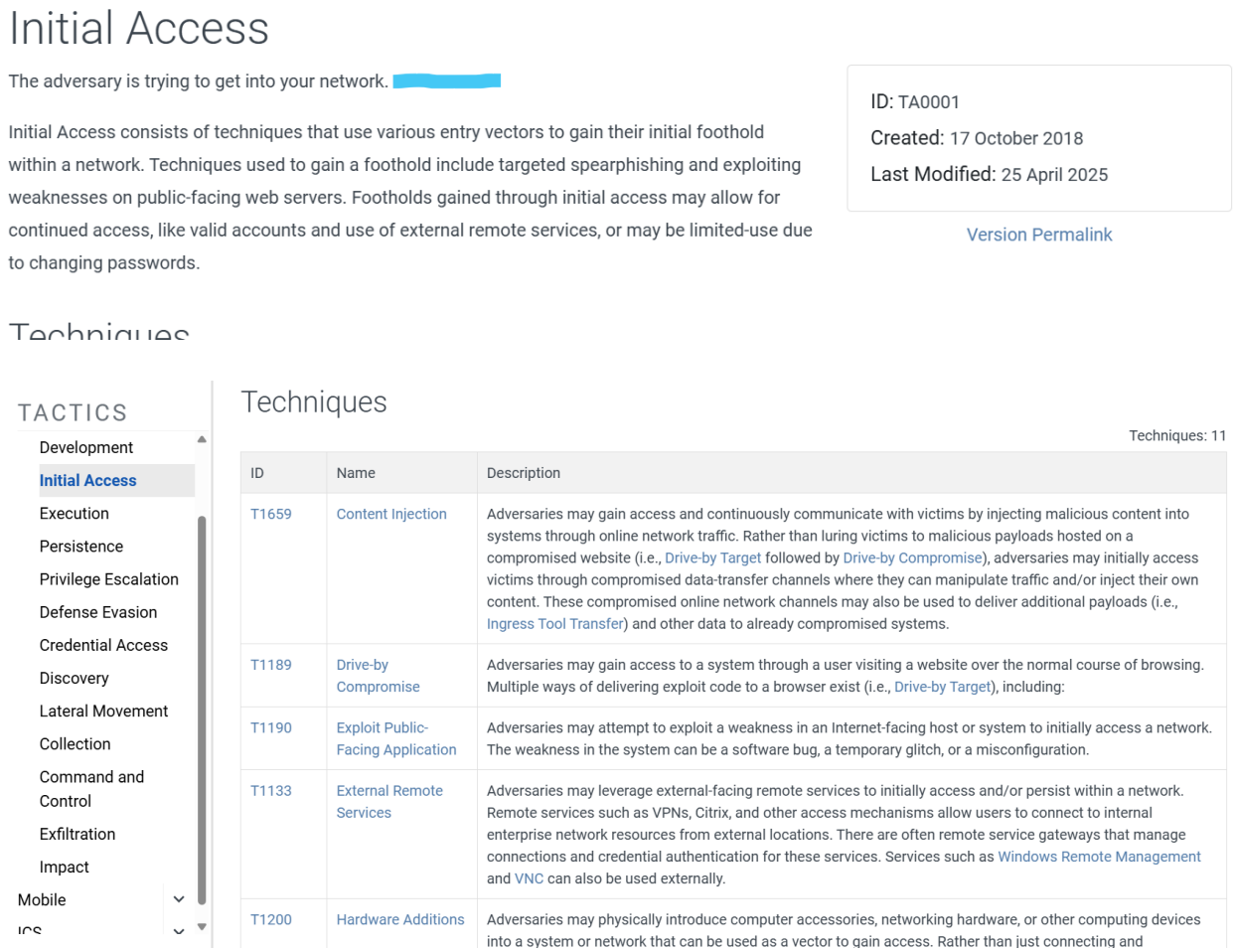
- **SOCRadar Labs** – For retrieving healthcare-specific APT threat intelligence.
- **MITRE ATT&CK Navigator** – For mapping APT TTPs.
- **MITRE ATT&CK Framework** – For structured adversary behavior taxonomy.
- **OSINT Research** – To cross-check TTP details from open sources.

Prepared by: Temitope Folowosele

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). Tactics for initial access screenshot is below
  - **Techniques** – The how of an attack (e.g., phishing, credential dumping).
  - **Procedures** – Real-world implementations of techniques.



Initial Access

The adversary is trying to get into your network.

Initial Access consists of techniques that use various entry vectors to gain their initial foothold within a network. Techniques used to gain a foothold include targeted spearphishing and exploiting weaknesses on public-facing web servers. Footholds gained through initial access may allow for continued access, like valid accounts and use of external remote services, or may be limited-use due to changing passwords.

ID: TA0001
Created: 17 October 2018
Last Modified: 25 April 2025

Version Permalink

Techniques

TACTICS

- Development
- Initial Access
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

Mobile

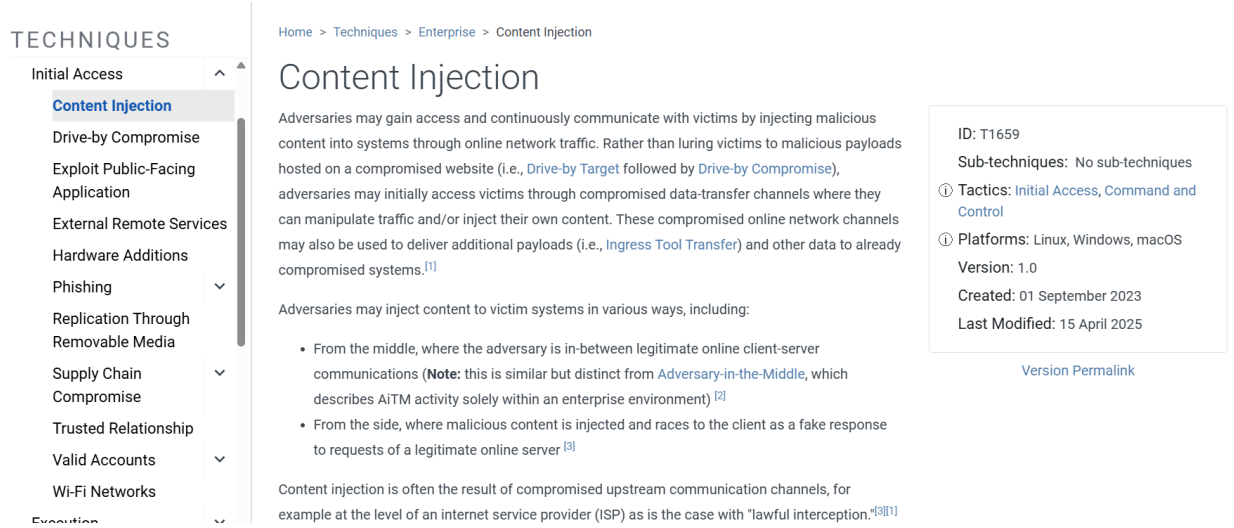
ICS

Techniques

Techniques: 11

ID	Name	Description
T1659	Content Injection	Adversaries may gain access and continuously communicate with victims by injecting malicious content into systems through online network traffic. Rather than luring victims to malicious payloads hosted on a compromised website (i.e., Drive-by Target followed by Drive-by Compromise), adversaries may initially access victims through compromised data-transfer channels where they can manipulate traffic and/or inject their own content. These compromised online network channels may also be used to deliver additional payloads (i.e., Ingress Tool Transfer) and other data to already compromised systems.
T1189	Drive-by Compromise	Adversaries may gain access to a system through a user visiting a website over the normal course of browsing. Multiple ways of delivering exploit code to a browser exist (i.e., Drive-by Target), including:
T1190	Exploit Public-Facing Application	Adversaries may attempt to exploit a weakness in an Internet-facing host or system to initially access a network. The weakness in the system can be a software bug, a temporary glitch, or a misconfiguration.
T1133	External Remote Services	Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as Windows Remote Management and VNC can also be used externally.
T1200	Hardware Additions	Adversaries may physically introduce computer accessories, networking hardware, or other computing devices into a system or network that can be used as a vector to gain access. Rather than just connecting and

Prepared by: Temitope Folowosele

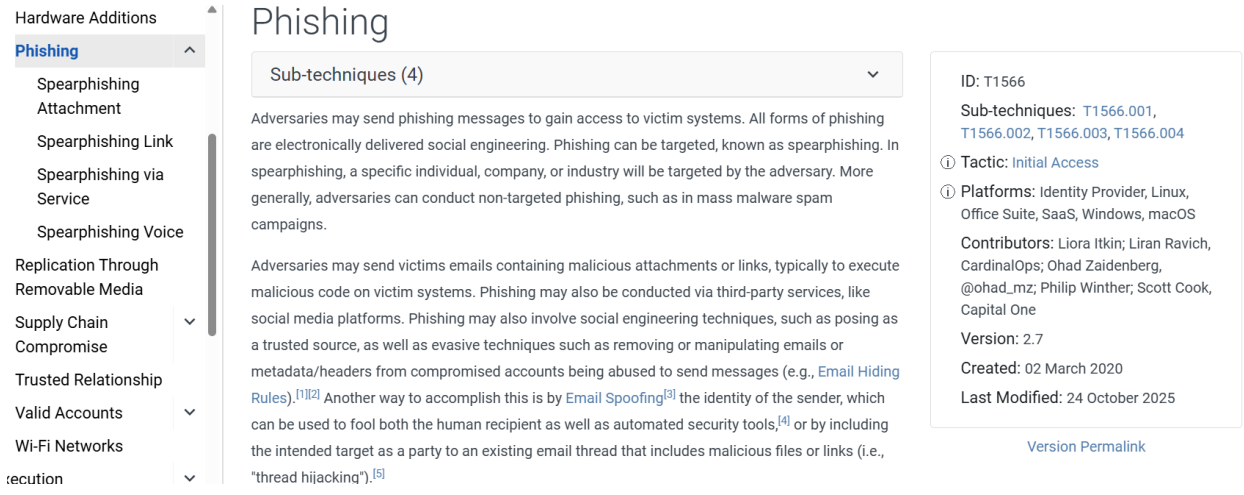


Procedure Examples

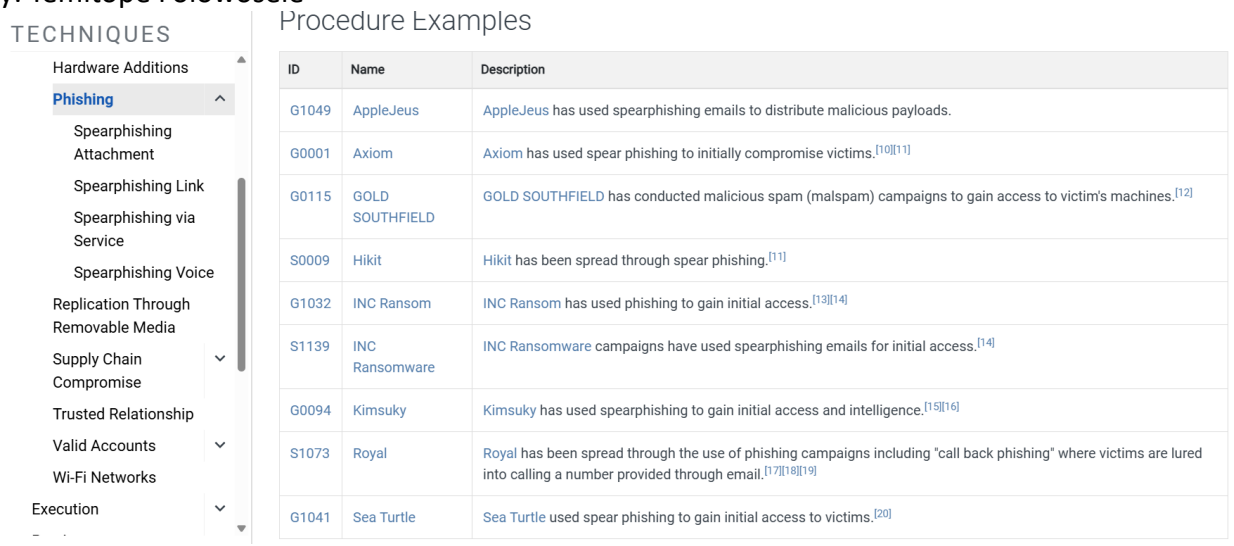
ID	Name	Description
S1088	Disco	Disco has achieved initial access and execution through content injection into DNS, HTTP, and SMB replies to targeted hosts that redirect them to download malicious files.[5]
G1019	MoustachedBouncer	MoustachedBouncer has injected content into DNS, HTTP, and SMB replies to redirect specifically-targeted victims to a fake Windows Update page to download malware.[5]

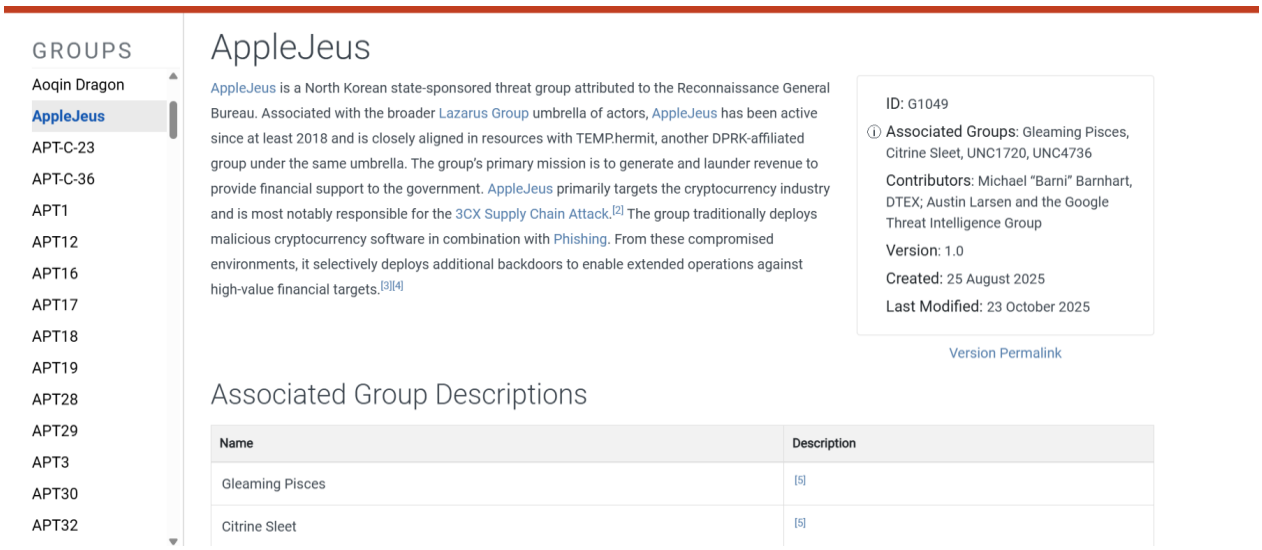
Mitigations

ID	Mitigation	Description
M1041	Encrypt Sensitive Information	Where possible, ensure that online traffic is appropriately encrypted through services such as trusted VPNs.
M1021	Restrict Web-Based Content	Consider blocking download/transfer and execution of potentially uncommon file types known to be used in adversary campaigns.



Prepared by: Temitope Folowosele





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

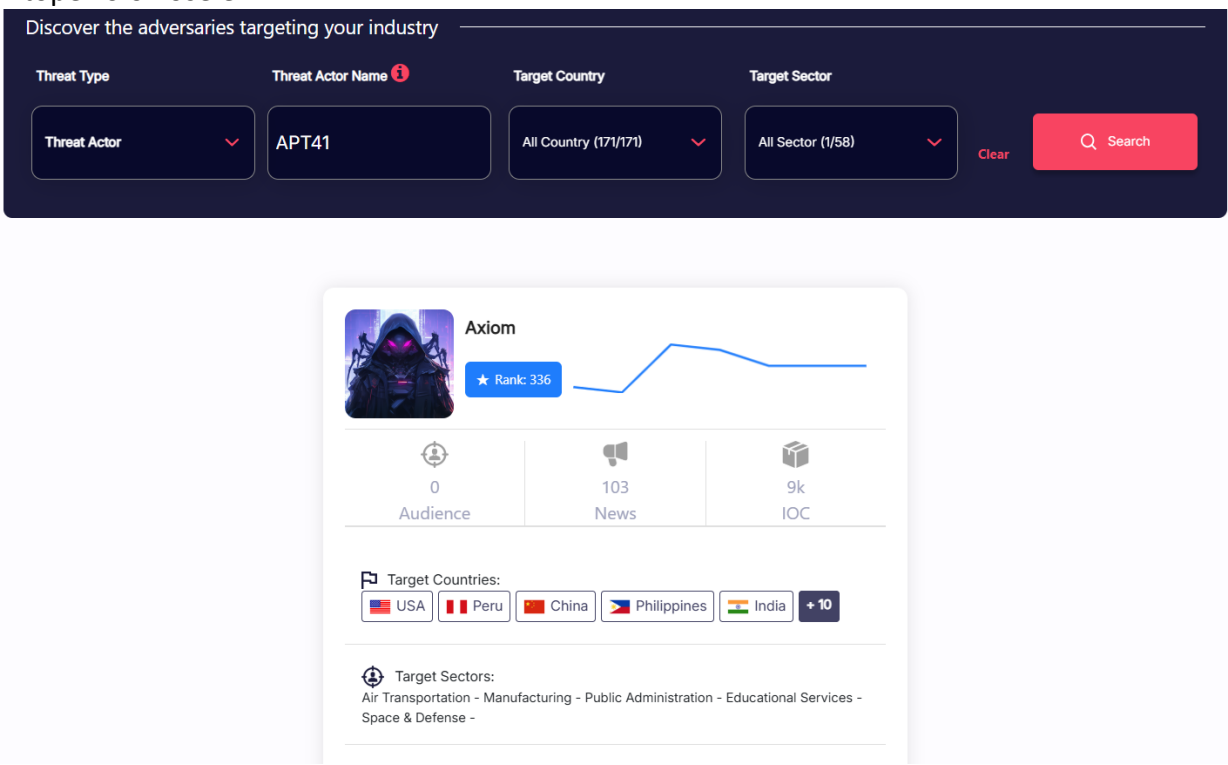
2. Research APTs Peculiar to the Sector

- Used SOCRadar Labs to identify **APT groups** targeting healthcare.

Prepared by: Temitope Folowosele

- Found the following:
  - **APT41** – China-based cyber-espionage group.

Prepared by: Temitope Folowosele



Prepared by: Temitope Folowosele

Axiom

★ Rank: 336

0	103	9k
Audience	News	IOC

Target Countries:

USA | Peru | China | Philippines | India | + 10

Target Sectors:

Air Transportation - Manufacturing - Public Administration - Educational Services - Space & Defense -

Associated Malware/Software:

Derusbi | elf.speculoos | gh0st RAT | osx.winnti | ZxShell | + 13

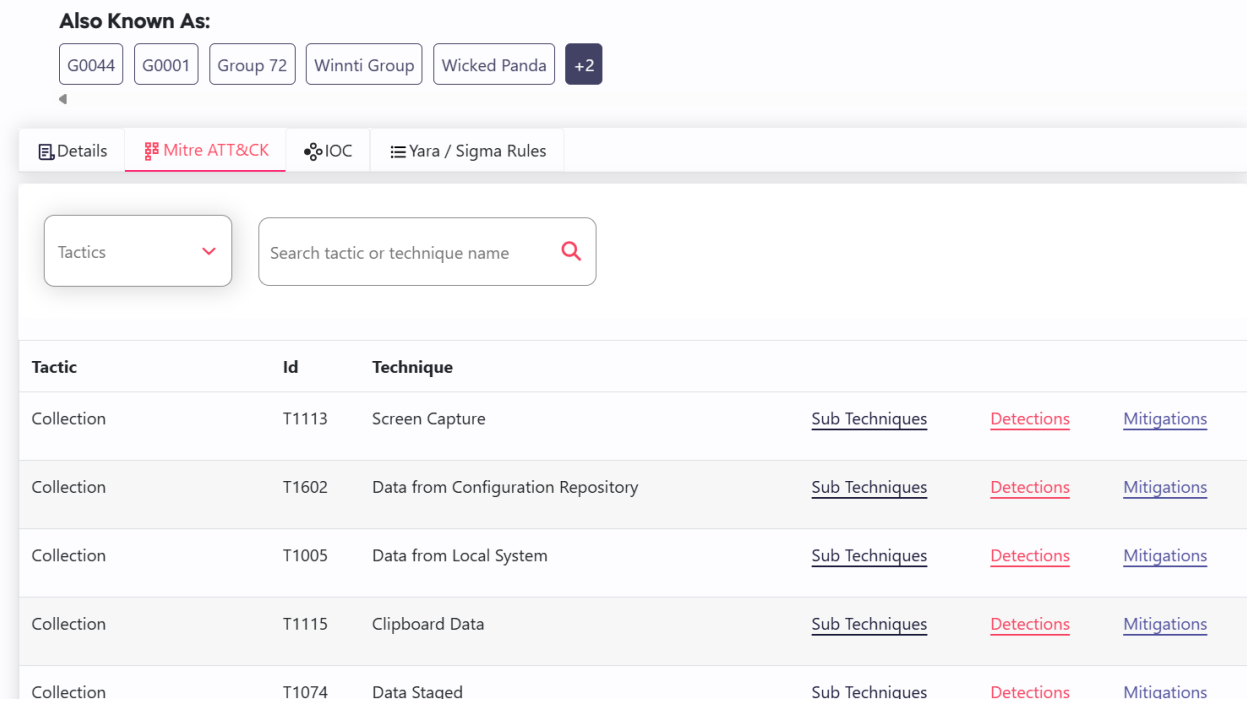
Related CVE's:

CVE-2025-4428 | CVE-2025-4427 | CVE-2025-31324 | CVE-2025-30406 | CVE-2025-29824 | + 196

ATT&CK IDs:

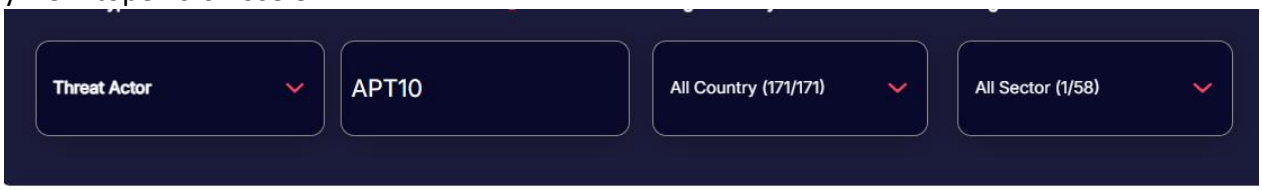
T1003.001 - LSASS Memory | T1573.002 - Asymmetric Cryptography

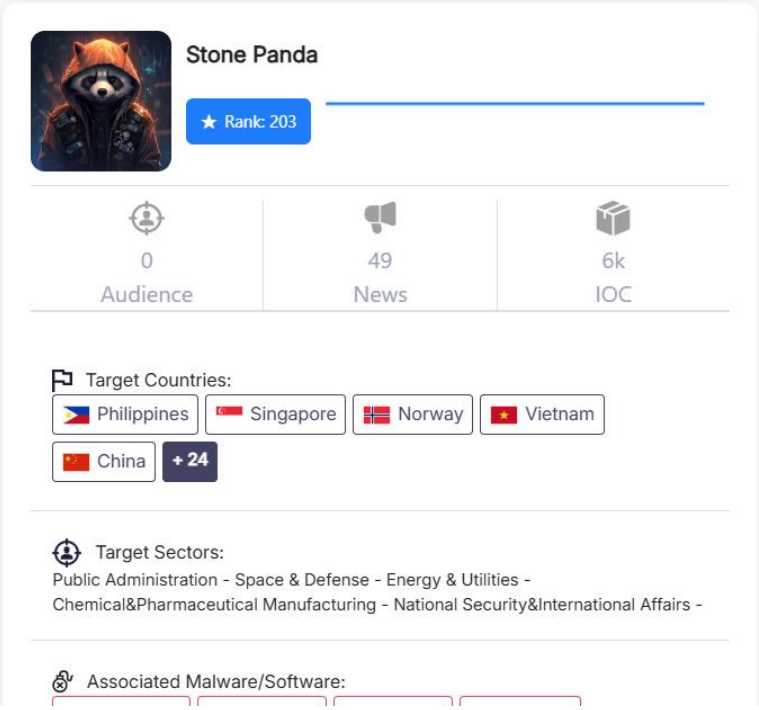
Prepared by: Temitope Folowosele

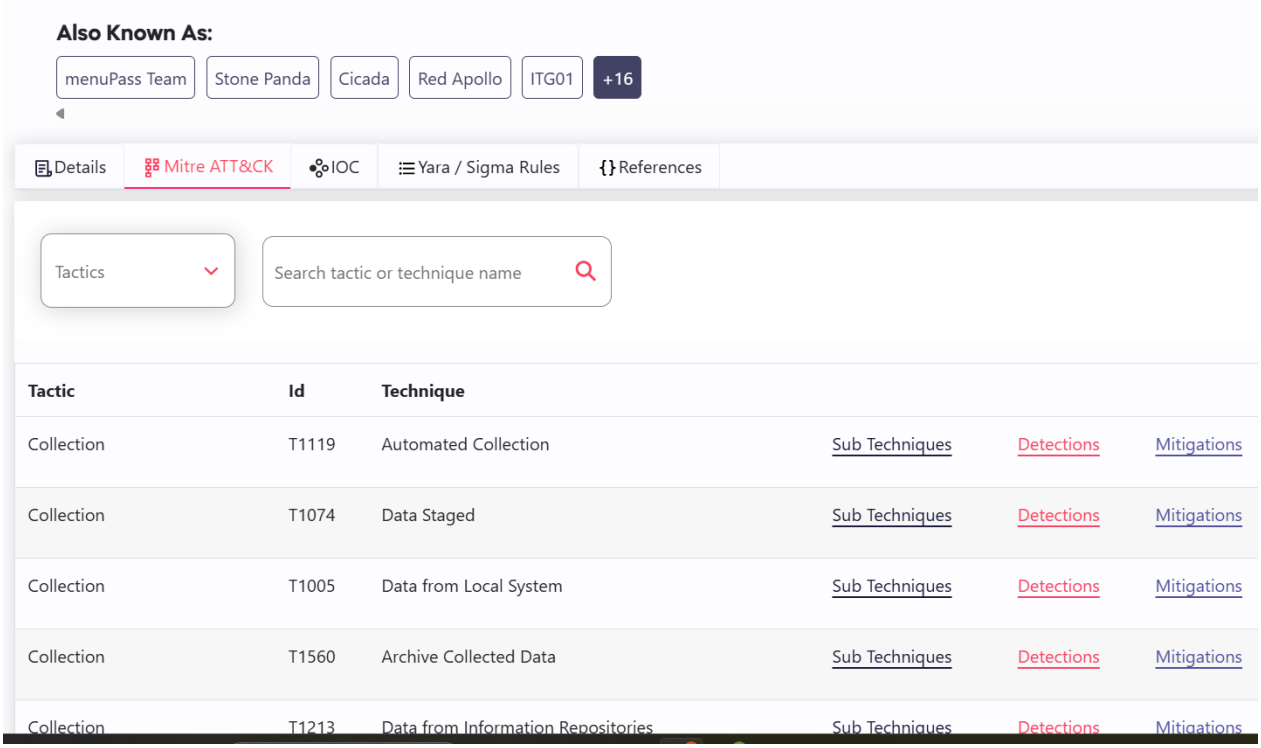


- **APT10** – Menu Pass are known to have acted in association with the Chinese Ministry of State Security's (MSS) Tianjin State Security Bureau and worked for the Huaying Haitai Science and Technology Development Company.

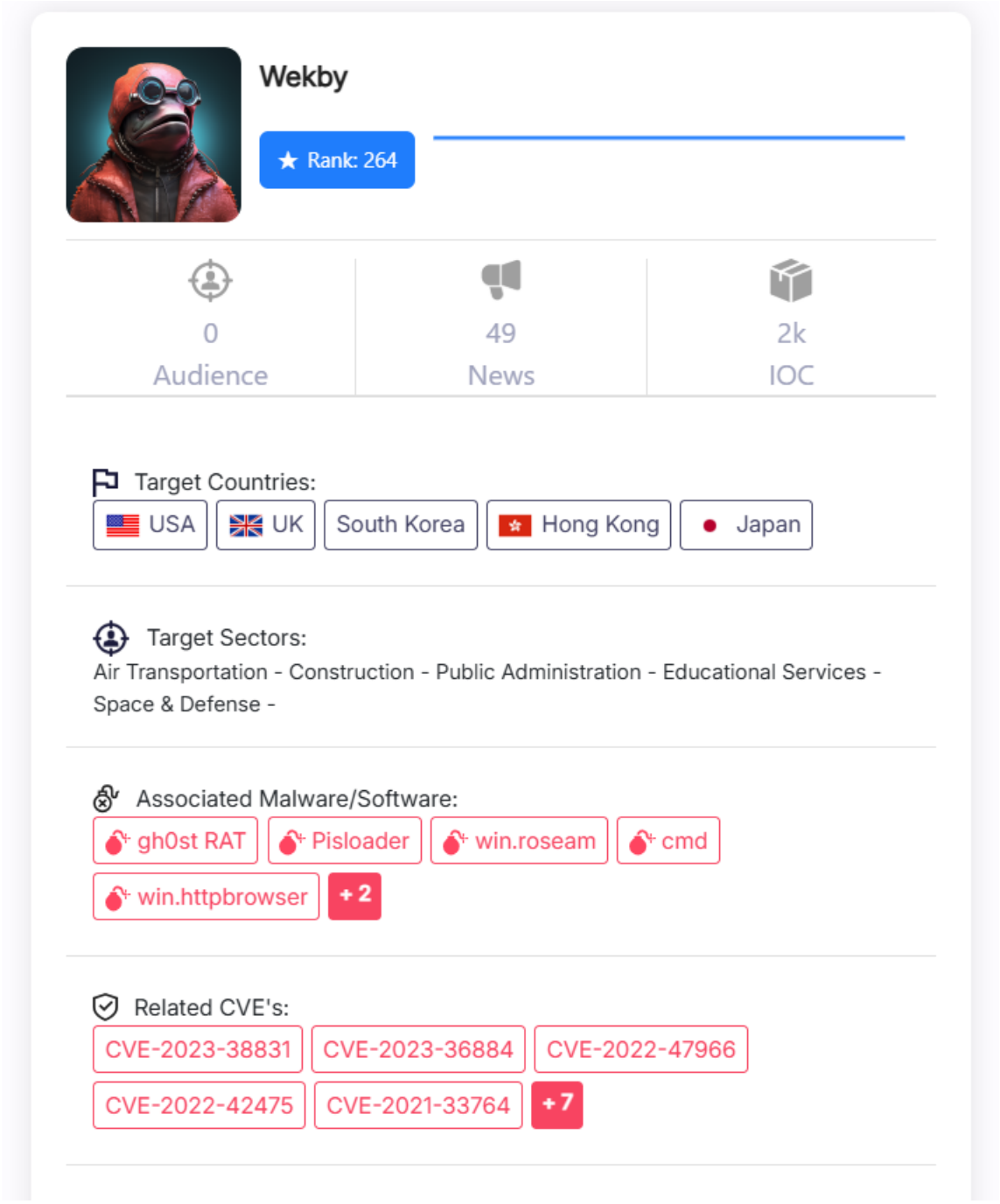
Prepared by: Temitope Folowosele



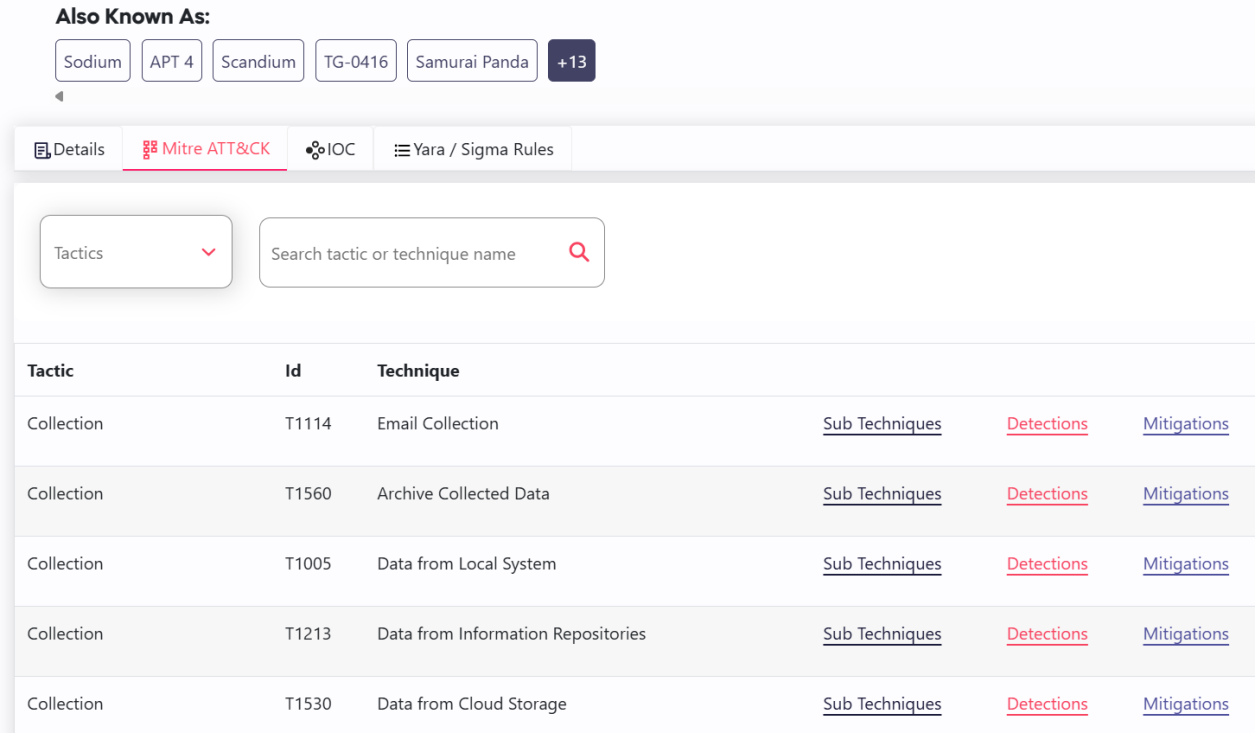


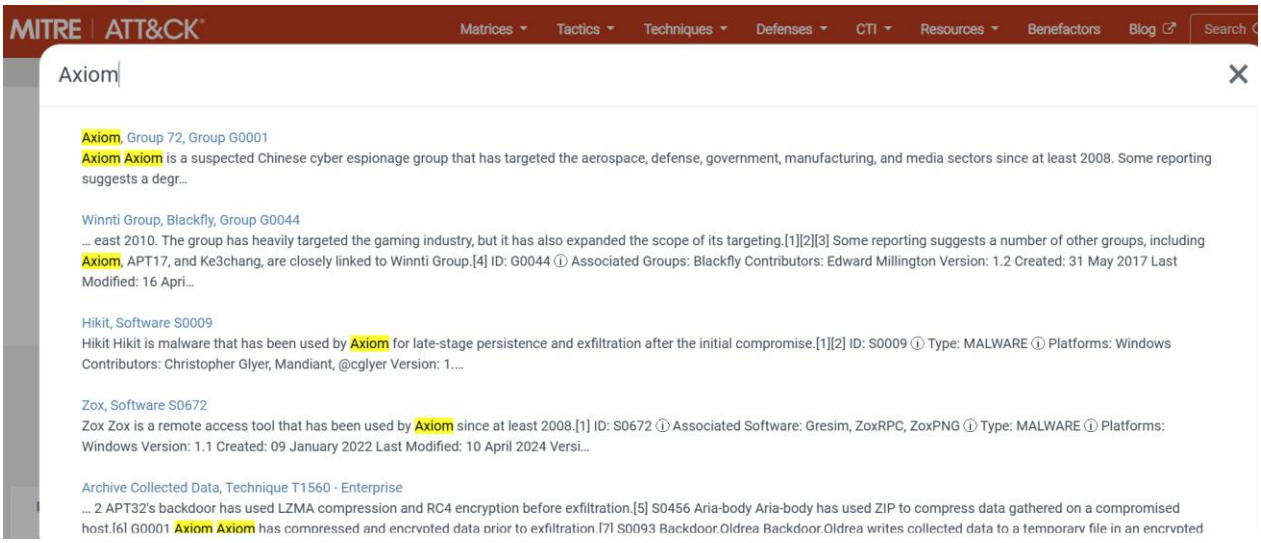


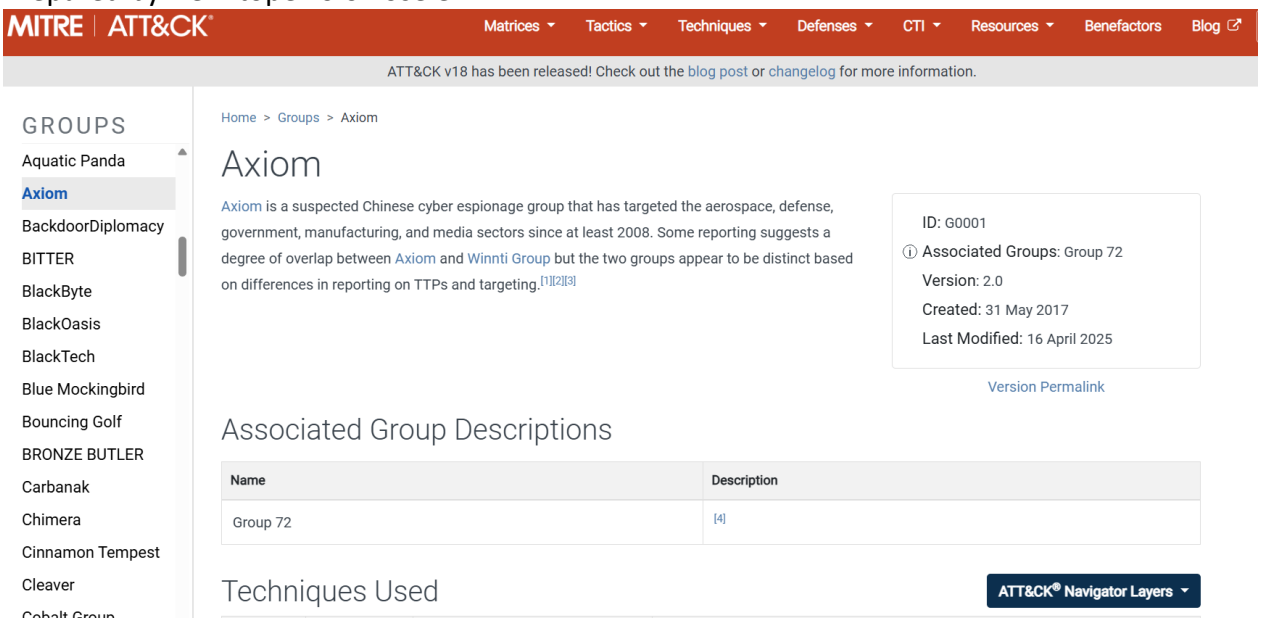
- **APT18** – Suspected threat group that has operated since at least 2009 and has targeted a range of industries, including technology, manufacturing, human rights groups, government, and medical.



Prepared by: Temitope Folowosele







Techniques Used

ATT&CK® Navigator Layers

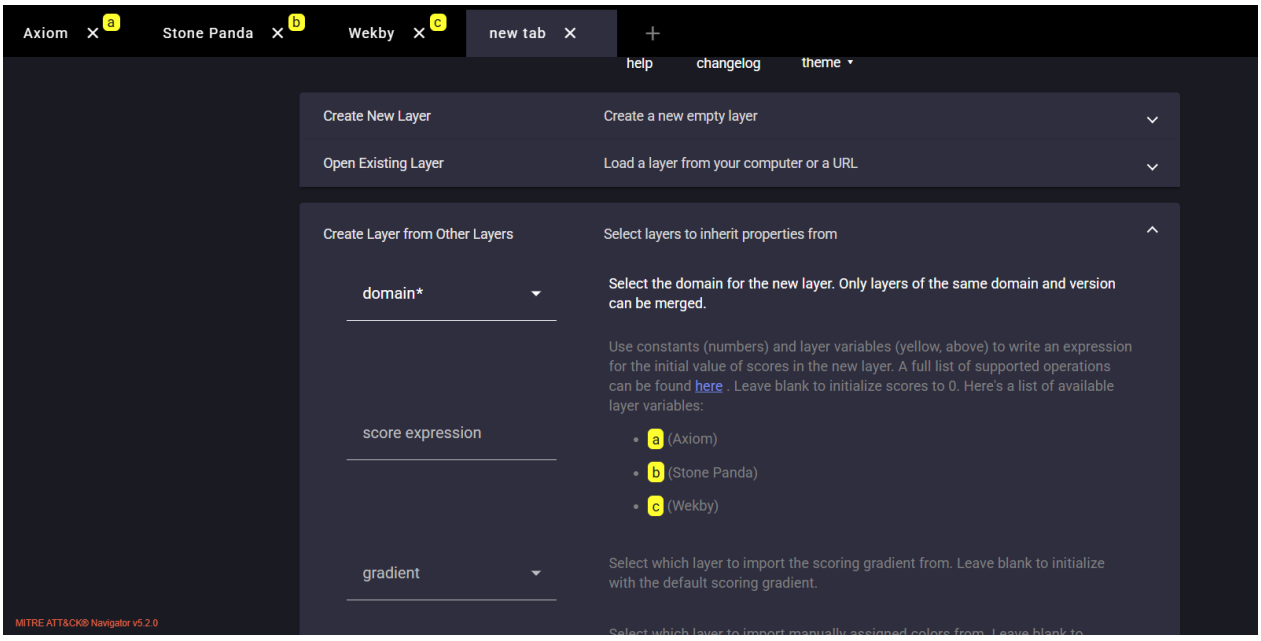
Domain	ID		Name	Use
Enterprise	T1583	.002	Acquire Infrastructure: DNS Server	Axiom has acquired dynamic DNS services for use in the targeting of intended victims.[5]
		.003	Acquire Infrastructure: Virtual Private Server	Axiom has used VPS hosting providers in targeting of intended victims.[5]
Enterprise	T1560		Archive Collected Data	Axiom has compressed and encrypted data prior to exfiltration.[5]
Enterprise	T1584	.005	Compromise Infrastructure: Botnet	Axiom has used large groups of compromised machines for use as proxy nodes.[5]
Enterprise	T1005		Data from Local System	Axiom has collected data from a compromised network.[5]
Enterprise	T1001	.002	Data Obfuscation: Steganography	Axiom has used steganography to hide its C2 communications.[5]

4. Map APTs to TTPs using MITRE Navigator

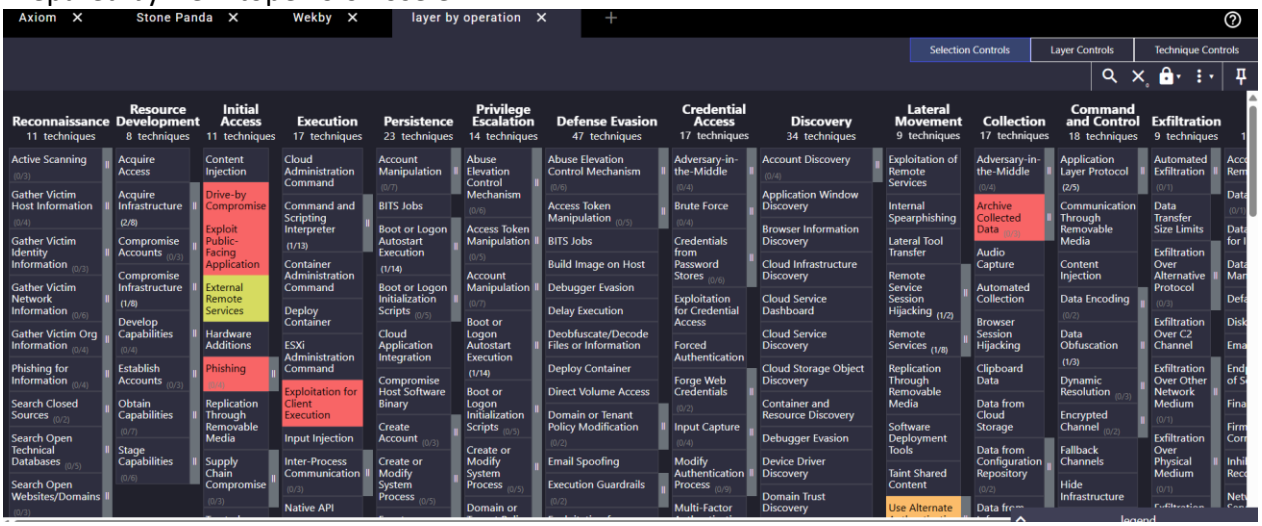
- Created **individual layers** in MITRE Navigator for each APT.
- Color-coded:
  - Red – Techniques confirmed in public reports. o Orange – Techniques suspected but unconfirmed. o Green – Techniques with existing detection measures. **5. Compare the APTs**
- Imported all four APT layers into a **combined Navigator view**.

Prepared by: Temitope Folowosele

- Noted **common techniques** across multiple APTs, such as:
  - T1566 – Phishing o T1078 – Valid Accounts
  - T1059 – Command and Scripting Interpreter



Prepared by: Temitope Folowosele



Prepared by: Temitope Folowosele

3. Highlight of the TTPs

-

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.