

Prepared by: Temitope Folowosele

Threat Hunting in the Healthcare Sector using MITRE ATT&CK

Prepared by: Temitope C Folowosele

Date: 11 November 2025

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.

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

| Techniques | | |
|------------|-----------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| 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 |

[Home](#) > [Techniques](#) > [Enterprise](#) > [Content Injection](#)

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.^[1]

Adversaries may inject content to victim systems in various ways, including:

- From the middle, where the adversary is in-between legitimate online client-server communications (**Note:** this is similar but distinct from [Adversary-in-the-Middle](#), which describes AITM activity solely within an enterprise environment)^[2]
- From the side, where malicious content is injected and races to the client as a fake response to requests of a legitimate online server^[3]

Content injection is often the result of compromised upstream communication channels, for example at the level of an internet service provider (ISP) as is the case with "lawful interception."^{[3][1]}

ID: T1659
 Sub-techniques: No sub-techniques
 Tactic: [Initial Access](#), [Command and Control](#)
 Platform: Linux, Windows, macOS
 Version: 1.0
 Created: 01 September 2023
 Last Modified: 15 April 2025
[Version Permalink](#)

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. |

[Hardware Additions](#)

[Phishing](#)

Phishing

[Sub-techniques \(4\)](#)

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.

Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](#)).^{[1][2]} Another way to accomplish this is by [Email Spoofing](#)^[3] the identity of the sender, which can be used to fool both the human recipient as well as automated security tools,^[4] or by including the intended target as a party to an existing email thread that includes malicious files or links (i.e., "thread hijacking").^[5]

ID: T1566
 Sub-techniques: [T1566.001](#), [T1566.002](#), [T1566.003](#), [T1566.004](#)
 Tactic: [Initial Access](#)
 Platform: Identity Provider, Linux, Office Suite, SaaS, Windows, macOS
 Contributors: Liora Itkin; Liran Ravich, CardinalOps; Ohad Zaiderberg, @ohad_mz; Philip Winther; Scott Cook, Capital One
 Version: 2.7
 Created: 02 March 2020
 Last Modified: 24 October 2025
[Version Permalink](#)

| TECHNIQUES | | | Procedure Examples | | |
|-------------------------------------|--|--|--------------------|-----------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| | | | ID | Name | Description |
| Hardware Additions | | | G1049 | AppleJeus | AppleJeus has used spearphishing emails to distribute malicious payloads. |
| Phishing | | | G0001 | Axiom | Axiom has used spear phishing to initially compromise victims. ^{[10][11]} |
| Spearphishing Attachment | | | G0115 | GOLD SOUTHFIELD | GOLD SOUTHFIELD has conducted malicious spam (malspam) campaigns to gain access to victim's machines. ^[12] |
| Spearphishing Link | | | S0009 | Hikit | Hikit has been spread through spear phishing. ^[11] |
| Spearphishing via Service | | | G1032 | INC Ransom | INC Ransom has used phishing to gain initial access. ^{[13][14]} |
| Spearphishing Voice | | | S1139 | INC Ransomware | INC Ransomware campaigns have used spearphishing emails for initial access. ^[14] |
| Replication Through Removable Media | | | G0094 | Kimsuky | Kimsuky has used spearphishing to gain initial access and intelligence. ^{[15][16]} |
| Supply Chain Compromise | | | S1073 | Royal | Royal has been spread through the use of phishing campaigns including "call back phishing" where victims are lured into calling a number provided through email. ^{[17][18][19]} |
| Trusted Relationship | | | G1041 | Sea Turtle | Sea Turtle used spear phishing to gain initial access to victims. ^[20] |
| Valid Accounts | | | | | |
| Wi-Fi Networks | | | | | |
| Execution | | | | | |

| GROUPS | | AppleJeus | |
|--------------|--|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--|
| Aoqin Dragon | | AppleJeus is a North Korean state-sponsored threat group attributed to the Reconnaissance General Bureau. Associated with the broader Lazarus Group umbrella of actors, AppleJeus has been active since at least 2018 and is closely aligned in resources with TEMP:hermit, another DPRK-affiliated group under the same umbrella. The group's primary mission is to generate and launder revenue to provide financial support to the government. AppleJeus primarily targets the cryptocurrency industry and is most notably responsible for the 3CX Supply Chain Attack. ^[2] The group traditionally deploys malicious cryptocurrency software in combination with Phishing. From these compromised environments, it selectively deploys additional backdoors to enable extended operations against high-value financial targets. ^{[3][4]} | |
| AppleJeus | | | |
| APT-C-23 | | | |
| APT-C-36 | | | |
| APT1 | | | |
| APT12 | | | |
| APT16 | | | |
| APT17 | | | |
| APT18 | | | |
| APT19 | | | |
| APT28 | | | |
| APT29 | | | |
| APT3 | | | |
| APT30 | | | |
| APT32 | | | |

Associated Group Descriptions

| Name | Description |
|-----------------|-------------|
| Gleaming Pisces | [5] |
| Citrine Sleet | [5] |

ID: G1049
 ⓘ Associated Groups: Gleaming Pisces, Citrine Sleet, UNC1720, UNC4736
 Contributors: Michael "Barni" Barnhart, DTEX, Austin Larsen and the Google Threat Intelligence Group
 Version: 1.0
 Created: 25 August 2025
 Last Modified: 23 October 2025

[Version Permalink](#)

- **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.

85 apt groups found in HealthCare & Social Assistance

| Group Name | Aliases | Country |
|-------------------|--------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| APT Iran | Phosphorus , COBALT GYPSY , Ballistic Bobcat ITG13 ... |  Lebanon  Iran ... |
| Lazarus Group | Hidden Cobra , Storm-1789 , Guardians of Peace Appleworm ... |  Philippines  Chile ... |
| APT42 | APT 42 GreenBravo |  USA  Middle East ... |
| Gold Ionic | ionic Gold Ionic |  Germany  United Kingdom ... |
| NoName057 | NoName057 , NoName05716 , Nnm05716 05716nnm |  Lebanon  Russian Federation ... |
| APT37 | APT 37 , Opal Sleet , Hermit ITG10 ... |  USA  China ... |
| Energetic Bear | Dragonfly , Iron Liberty , Electrum Ghost Blizzard ... |  Tunisia  Cote d'Ivoire ... |
| Predatory Sparrow | Indra Gonjeshke Darande |  Lebanon  China ... |

+77 Threat Actors

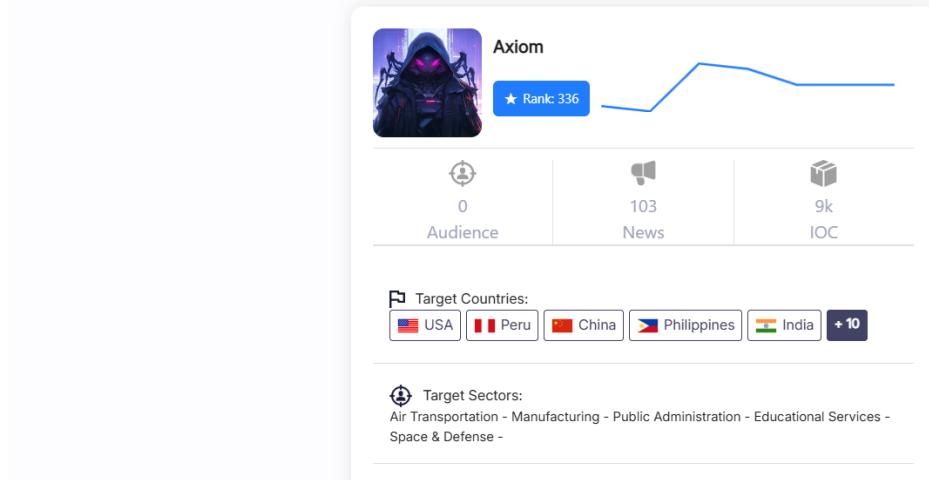
- Found the following:
 - **APT41** – China-based cyber-espionage group.

Prepared by: Temitope Folowosele

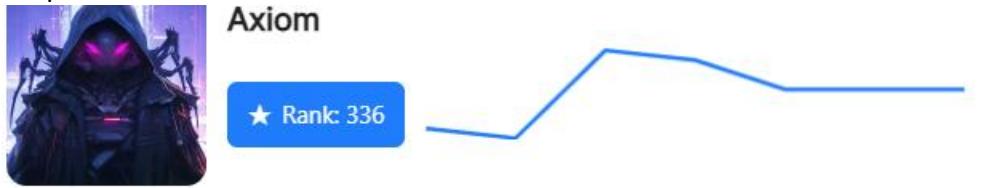
Discover the adversaries targeting your industry

| Threat Type | Threat Actor Name <small>i</small> | Target Country | Target Sector |
|--------------|------------------------------------|-----------------------|-------------------|
| Threat Actor | APT41 | All Country (171/171) | All Sector (1/58) |

Clear Search



Prepared by: Temitope Folowosele



0

Audience



103

News



9k

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

Also Known As:

G0044 G0001 Group 72 Winnti Group Wicked Panda +2

◀

The screenshot shows a web-based interface for threat intelligence analysis. At the top, there are tabs for 'Details', 'Mitre ATT&CK' (which is highlighted in red), 'IOC', and 'Yara / Sigma Rules'. Below the tabs, there are two search/filter boxes: one for 'Tactics' with a dropdown arrow and another for 'Search tactic or technique name' with a magnifying glass icon. The main content area is a table with the following columns: Tactic, Id, Technique, Sub Techniques, Detections, and Mitigations. The table lists five tactics under the 'Collection' category:

| Tactic | Id | Technique | Sub Techniques | Detections | Mitigations |
|------------|-------|------------------------------------|--------------------------------|----------------------------|-----------------------------|
| Collection | T1113 | Screen Capture | Sub Techniques | Detections | Mitigations |
| Collection | T1602 | Data from Configuration Repository | Sub Techniques | Detections | Mitigations |
| Collection | T1005 | Data from Local System | Sub Techniques | Detections | Mitigations |
| Collection | T1115 | Clipboard Data | Sub Techniques | Detections | Mitigations |
| Collection | T1074 | Data Staged | Sub Techniques | Detections | Mitigations |

- **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.

Threat Actor: APT10

All Country (171/171)

All Sector (1/58)



Stone Panda

★ Rank: 203

| | | |
|-------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|
|  0 Audience |  49 News |  6k IOC |
|-------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------|

 Target Countries:

 Philippines
 Singapore
 Norway
 Vietnam

 China
+ 24

 Target Sectors:

Public Administration - Space & Defense - Energy & Utilities -
Chemical&Pharmaceutical Manufacturing - National Security&International Affairs -

 Associated Malware/Software:

Also Known As:

menuPass Team
Stone Panda
Cicada
Red Apollo
ITG01
+16

◀

Details
Mitre ATT&CK
IOC
Yara / Sigma Rules
References

Tactics
▼
Search tactic or technique name
🔍

| Tactic | ID | Technique | Sub Techniques | Detections | Mitigations |
|------------|-------|------------------------------------|--------------------------------|----------------------------|-----------------------------|
| Collection | T1119 | Automated Collection | Sub Techniques | Detections | Mitigations |
| Collection | T1074 | Data Staged | Sub Techniques | Detections | Mitigations |
| Collection | T1005 | Data from Local System | Sub Techniques | Detections | Mitigations |
| Collection | T1560 | Archive Collected Data | Sub Techniques | Detections | Mitigations |
| Collection | T1213 | Data from Information Repositories | Sub Techniques | Detections | Mitigations |

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.



Wekby

★ Rank: 264

| | | |
|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|
|  0 Audience |  49 News |  2k IOC |
|----------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------|

 **Target Countries:**

 USA  UK  South Korea  Hong Kong  Japan

 **Target Sectors:**
Air Transportation - Construction - Public Administration - Educational Services -
Space & Defense -

 **Associated Malware/Software:**

 gh0st RAT  Pisloader  win.roseam  cmd
 win.httpbrowser **+ 2**

 **Related CVE's:**

 CVE-2023-38831  CVE-2023-36884  CVE-2022-47966
 CVE-2022-42475  CVE-2021-33764 **+ 7**

Prepared by: Temitope Folowosele

Also Known As:

Sodium | APT 4 | Scandium | TG-0416 | Samurai Panda | +13

Details

Mitre ATT&CK

IOC

Yara / Sigma Rules

Tactics

Search tactic or technique name



| Tactic | Id | Technique | Sub Techniques | Detections | Mitigations |
|------------|-------|------------------------------------|--------------------------------|----------------------------|-----------------------------|
| Collection | T1114 | Email Collection | Sub Techniques | Detections | Mitigations |
| Collection | T1560 | Archive Collected Data | Sub Techniques | Detections | Mitigations |
| Collection | T1005 | Data from Local System | Sub Techniques | Detections | Mitigations |
| Collection | T1213 | Data from Information Repositories | Sub Techniques | Detections | Mitigations |
| Collection | T1530 | Data from Cloud Storage | Sub Techniques | Detections | Mitigations |

MITRE | ATT&CK®

Matrices ▾ Tactics ▾ Techniques ▾ Defenses ▾ CTI ▾ Resources ▾ Benefactors Blog 🔍 Search ⚙

Axiom



Axiom, Group 72, Group G0001

Axiom Axiom is a suspected Chinese cyber espionage group that has targeted the aerospace, defense, government, manufacturing, and media sectors since at least 2008. Some reporting suggests a degr...

Winni Group, Blackfly, Group G0044

... east 2010. The group has heavily targeted the gaming industry, but it has also expanded the scope of its targeting.[1][2][3] Some reporting suggests a number of other groups, including **Axiom**, APT17, and Ke3chang, are closely linked to Winni Group.[4] ID: G0044 ⓘ Associated Groups: Blackfly Contributors: Edward Millington Version: 1.2 Created: 31 May 2017 Last Modified: 16 April...

Hikit, Software S0009

Hikit Hikit is malware that has been used by **Axiom** for late-stage persistence and exfiltration after the initial compromise.[1][2] ID: S0009 ⓘ Type: MALWARE ⓘ Platforms: Windows Contributors: Christopher Glycer, Mandiant, @cglycer Version: 1....

Zox, Software S0672

Zox Zox is a remote access tool that has been used by **Axiom** since at least 2008.[1] ID: S0672 ⓘ Associated Software: Gresim, ZoxRPC, ZoxPNG ⓘ Type: MALWARE ⓘ Platforms: Windows Version: 1.1 Created: 09 January 2022 Last Modified: 10 April 2024 Vers...

Archive Collected Data, Technique T1560 - Enterprise

... 2 APT32's backdoor has used LZMA compression and RC4 encryption before exfiltration.[5] S0456 Aria-body Aria-body has used ZIP to compress data gathered on a compromised host.[6] G0001 **Axiom Axiom** has compressed and encrypted data prior to exfiltration.[7] S0093 Backdoor.Oldrea Backdoor.Oldrea writes collected data to a temporary file in an encrypted

GROUPS

Aquatic Panda
Axiom
 BackdoorDiplomacy
 BITTER
 BlackByte
 BlackOasis
 BlackTech
 Blue Mockingbird
 Bouncing Golf
 BRONZE BUTLER
 Carbanak
 Chimera
 Cinnamon Tempest
 Cleaver
 Cobalt Group

Home > Groups > Axiom

Axiom

Axiom is a suspected Chinese cyber espionage group that has targeted the aerospace, defense, government, manufacturing, and media sectors since at least 2008. Some reporting suggests a degree of overlap between Axiom and Winnti Group but the two groups appear to be distinct based on differences in reporting on TTPs and targeting.^{[1][2][3]}

ID: G0001
 ⓘ Associated Groups: Group 72
 Version: 2.0
 Created: 31 May 2017
 Last Modified: 16 April 2025

[Version Permalink](#)

Associated Group Descriptions

| Name | Description |
|----------|-------------|
| Group 72 | [4] |

Techniques Used

ATT&CK® Navigator Layers ▾

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.
 - Orange – Techniques suspected but unconfirmed.
 - Green – Techniques with existing detection measures.
- 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

The screenshot shows the main interface of the MITRE ATT&CK Navigator. At the top, there are tabs for 'Axiom' (selected), 'Stone Panda', 'Wekby', and 'new tab'. Below the tabs are three rows of controls: 'Selection Controls', 'Layer Controls', and 'Technique Controls'. The main area is a grid of colored cards representing various attack techniques. The columns represent phases: Resource Development, Initial Access, Execution, Persistence, Privilege Escalation, Defense Evasion, Credential Access, Discovery, Lateral Movement, Collection, Command and Control, Exfiltration, and Impact. The rows represent specific techniques, each with a count of occurrences in parentheses. Some cards are highlighted in red, indicating they are part of the focus for this presentation.

| Resource Development | Initial Access | Execution | Persistence | Privilege Escalation | Defense Evasion | Credential Access | Discovery | Lateral Movement | Collection | Command and Control | Exfiltration | Impact |
|---------------------------------|-------------------------------------|-----------------------------------|--------------------------------------|-----------------------------------|-----------------------------------------|---------------------------------|----------------------------------|--------------------------------|--------------------------------|---------------------------------------|----------------------------------|------------------------|
| 8 techniques | 11 techniques | 17 techniques | 23 techniques | 14 techniques | 47 techniques | 17 techniques | 34 techniques | 9 techniques | 17 techniques | 18 techniques | 9 techniques | 15 techniques |
| Acquire Access | Content Injection | Cloud Administration Command | Account Manipulation | Abuse Elevation Control Mechanism | Adversary-in-the-Middle | Exploitation of Remote Services | Adversary-in-the-Middle | Application Discovery | Adversary-in-the-Middle | Application Layer Protocol | Automated Exfiltration | Account Access Removal |
| Acquire Infrastructure (2/8) | Drive-by Compromise | Command and Scripting Interpreter | BITS Jobs | Access Token Manipulation | Brute Force | Internal Spearphishing | Archive Collected Data | Application Window Discovery | Brute Force | Communication Through Removable Media | Data Destruction | |
| Compromise Accounts (0/3) | Exploit Public-Facing Application | Container Administration Command | Boot or Logon Autostart Execution | BITS Jobs | Credentials from Password Stores | Cloud Infrastructure Discovery | Cloud Service Dashboard | Browser Information Discovery | Cloud Infrastructure Discovery | Content Injection | Data Encrypted for Impact | |
| Compromise Infrastructure (1/8) | External Remote Services | Deploy Container | Boot or Logon Initialization Scripts | Account Manipulation | Debugger Evasion | Cloud Service Discovery | Cloud Storage Object Discovery | Cloud Service Discovery | Cloud Storage Object Discovery | Data Encoding | Data Manipulation (0/3) | |
| Develop Capabilities (0/4) | Hardware Additions | ESXi Administration Command | Cloud Application Integration | Delay Execution | Deobfuscate/Decode Files or Information | Cloud Storage Object Discovery | Container and Resource Discovery | Cloud Storage Object Discovery | Cloud Storage Object Discovery | Data Encoding | Defacement (0/2) | |
| Establish Accounts (0/2) | Phishing | Exploitation for Client Execution | Compromise Host Software Binary | Deploy Container | Direct Volume Access | Cloud Storage Object Discovery | Container and Resource Discovery | Cloud Storage Object Discovery | Cloud Storage Object Discovery | Data Encoding | Disk Wipe (0/2) | |
| Obtain Capabilities (0/7) | Replication Through Removable Media | Input Injection | Create Account | Domain or | Domain or Tenant Policy Modification | Cloud Storage Object Discovery | Debugger Evasion | Cloud Storage Object Discovery | Cloud Storage Object Discovery | Dynamic Resolution (0/3) | Email Bombing | |
| Stage Capabilities (0/5) | Supply Chain Compromise | Inter-Process Communication | Create or Modify System Process | Domain or | Email Spooling | Cloud Storage Object Discovery | Device Driver Discovery | Cloud Storage Object Discovery | Cloud Storage Object Discovery | Encrypted Channel (0/2) | Endpoint Denial of Service (0/4) | |
| | | Native API | Native API | Domain or | Execution Guardrails | Cloud Storage Object Discovery | Taint Shared Content | Domain Trust Discovery | Cloud Storage Object Discovery | Fallback Channels | Financial Theft | |
| | | | | Domain or | Multi-Factor | Cloud Storage Object Discovery | Use Alternate | Domain Trust Discovery | Domain Trust Discovery | Hide Infrastructure | Firmware Corruption | |
| | | | | | | Cloud Storage Object Discovery | | | | | Inhibit System Recovery | |
| | | | | | | | | | | | Network Denial of Service | |

The screenshot shows the 'Create New Layer' section of the MITRE ATT&CK Navigator. It includes tabs for 'Axiom' (selected), 'Stone Panda', 'Wekby', and 'new tab'. Below the tabs are three rows of controls: 'help', 'changelog', and 'theme'. The main area has sections for 'Create New Layer', 'Create Existing Layer', 'Create Layer from Other Layers', and 'Import Scoring Gradient'.

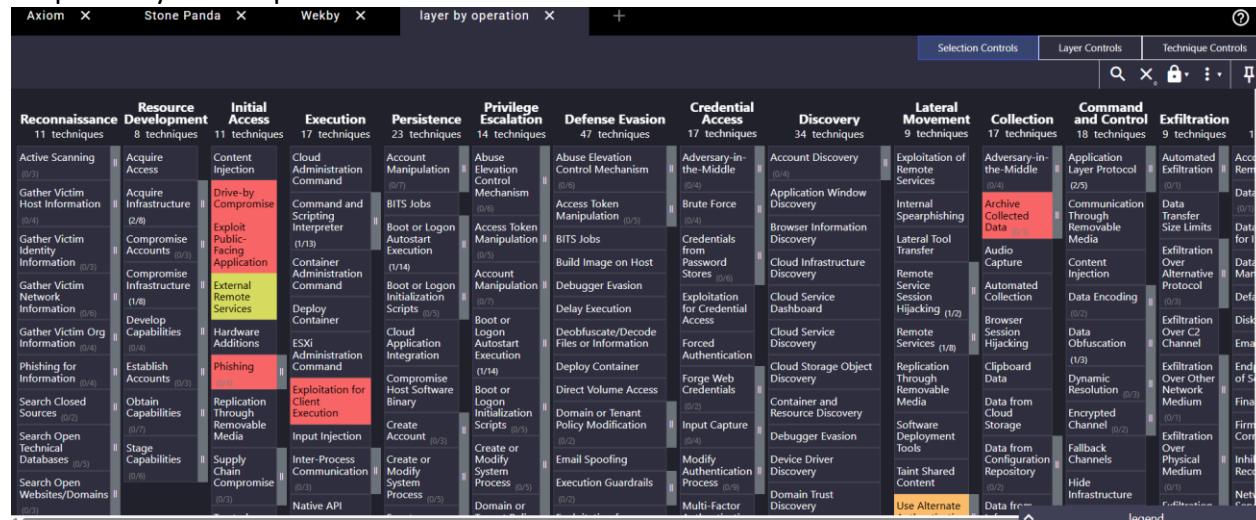
Create New Layer: Create a new empty layer.

Create Existing Layer: Load a layer from your computer or a URL.

Create Layer from Other Layers: Select layers to inherit properties from. A dropdown menu shows 'domain*' selected. A note says: 'Select the domain for the new layer. Only layers of the same domain and version can be merged.' Below this is a note about constants and layer variables, and a list of available domains: a (Axiom), b (Stone Panda), and c (Wekby).

Import Scoring Gradient: Select which layer to import the scoring gradient from. Leave blank to initialize with the default scoring gradient.

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.