

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

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., <a href="#">Drive-by Target</a> followed by <a href="#">Drive-by Compromise</a> ), 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., <a href="#">Ingress Tool Transfer</a> ) 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., <a href="#">Drive-by Target</a> ), 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 <a href="#">Windows Remote Management</a> and <a href="#">VNC</a> 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

TECHNIQUES

- Initial Access
  - Content Injection**
  - Drive-by Compromise
  - Exploit Public-Facing Application
  - External Remote Services
  - Hardware Additions
  - Phishing
  - Replication Through Removable Media
  - Supply Chain Compromise
  - Trusted Relationship
  - Valid Accounts
  - Wi-Fi Networks
- Execution

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.<sup>[1]</sup>

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) <sup>[2]</sup>
- From the side, where malicious content is injected and races to the client as a fake response to requests of a legitimate online server <sup>[3]</sup>

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."<sup>[3][1]</sup>

ID: T1659

Sub-techniques: No sub-techniques

① Tactics: [Initial Access](#), [Command and Control](#)

① Platforms: Linux, Windows, macOS

Version: 1.0

Created: 01 September 2023

Last Modified: 15 April 2025

[Version](#) [Permalink](#)

## Procedure Examples

ID	Name	Description
<a href="#">S1088</a>	<a href="#">Disco</a>	<a href="#">Disco</a> 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. <sup>[5]</sup>
<a href="#">G1019</a>	<a href="#">MoustachedBouncer</a>	<a href="#">MoustachedBouncer</a> has injected content into DNS, HTTP, and SMB replies to redirect specifically-targeted victims to a fake Windows Update page to download malware. <sup>[5]</sup>

## Mitigations

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

- Hardware Additions
- Phishing**
- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Spearphishing Voice
- Replication Through Removable Media
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts
- Wi-Fi Networks
- Execution

# 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](#)).<sup>[1][2]</sup> Another way to accomplish this is by [Email Spoofing](#)<sup>[3]</sup> the identity of the sender, which can be used to fool both the human recipient as well as automated security tools.<sup>[4]</sup> or by including the intended target as a party to an existing email thread that includes malicious files or links (i.e., "thread hijacking").<sup>[5]</sup>

ID: T1566

Sub-techniques: [T1566.001](#), [T1566.002](#), [T1566.003](#), [T1566.004](#)

① Tactic: [Initial Access](#)

① Platforms: Identity Provider, Linux, Office Suite, SaaS, Windows, macOS

Contributors: Liora Itkin; Liran Ravich, CardinalOps; Ohad Zaidenberg, @ohad\_mz; Philip Winther; Scott Cook, Capital One

Version: 2.7

Created: 02 March 2020

Last Modified: 24 October 2025

[Version](#) [Permalink](#)

## TECHNIQUES

- Hardware Additions
- Phishing**
  - Spearphishing Attachment
  - Spearphishing Link
  - Spearphishing via Service
  - Spearphishing Voice
- Replication Through Removable Media
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts
- Wi-Fi Networks
- Execution

## Procedure Examples

ID	Name	Description
G1049	AppleJeus	AppleJeus has used spearphishing emails to distribute malicious payloads.
G0001	Axiom	Axiom has used spear phishing to initially compromise victims. <sup>[10][11]</sup>
G0115	GOLD SOUTHFIELD	GOLD SOUTHFIELD has conducted malicious spam (malspam) campaigns to gain access to victim's machines. <sup>[12]</sup>
S0009	Hikit	Hikit has been spread through spear phishing. <sup>[11]</sup>
G1032	INC Ransom	INC Ransom has used phishing to gain initial access. <sup>[13][14]</sup>
S1139	INC Ransomware	INC Ransomware campaigns have used spearphishing emails for initial access. <sup>[14]</sup>
G0094	Kimsuky	Kimsuky has used spearphishing to gain initial access and intelligence. <sup>[15][16]</sup>
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. <sup>[17][18][19]</sup>
G1041	Sea Turtle	Sea Turtle used spear phishing to gain initial access to victims. <sup>[20]</sup>

## GROUPS

- Aoqin Dragon
- AppleJeus**
- APT-C-23
- APT-C-36
- APT1
- APT12
- APT16
- APT17
- APT18
- APT19
- APT28
- APT29
- APT3
- APT30
- APT32

## AppleJeus

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 TEMPhermit, 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.<sup>[2]</sup> 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.<sup>[3][4]</sup>

ID: G1049

① 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](#)

## Associated Group Descriptions

Name	Description
Gleaming Pisces	<sup>[5]</sup>
Citrine Sleet	<sup>[5]</sup>

- **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 ...

477 Threat Actors

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

Discover the adversaries targeting your industry

Threat Type

Threat Actor Name ⓘ

Target Country

Target Sector

Threat Actor


APT41

All Country (171/171)

All Sector (1/58)


Clear


Search





Axiom

★ Rank: 336





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 -



Axiom

★ Rank: 336



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 -



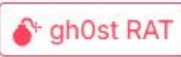
Associated Malware/Software:



Derusbi



elf.speculoos



gh0st RAT



osx.winnti



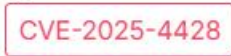
ZxShell



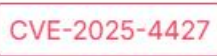
+13



Related CVE's:



CVE-2025-4428



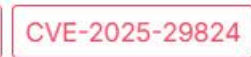
CVE-2025-4427



CVE-2025-31324



CVE-2025-30406



CVE-2025-29824



+196



ATT&CK IDs:



T1003.001 - LSASS Memory



T1573.002 - Asymmetric Cryptography



Prepared by: Temitope Folowosele

**Also Known As:**

G0044 G0001 Group 72 Winnti Group Wicked Panda +2

◀

Details **Mitre ATT&CK** IOC Yara / Sigma Rules

Tactics ▼ Search tactic or technique name 🔍

Tactic	Id	Technique			
Collection	T1113	Screen Capture	<a href="#">Sub Techniques</a>	<a href="#">Detections</a>	<a href="#">Mitigations</a>
Collection	T1602	Data from Configuration Repository	<a href="#">Sub Techniques</a>	<a href="#">Detections</a>	<a href="#">Mitigations</a>
Collection	T1005	Data from Local System	<a href="#">Sub Techniques</a>	<a href="#">Detections</a>	<a href="#">Mitigations</a>
Collection	T1115	Clipboard Data	<a href="#">Sub Techniques</a>	<a href="#">Detections</a>	<a href="#">Mitigations</a>
Collection	T1074	Data Staged	<a href="#">Sub Techniques</a>	<a href="#">Detections</a>	<a href="#">Mitigations</a>


- **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			
Collection	T1119	Automated Collection	<a href="#">Sub Techniques</a>	<a href="#">Detections</a>	<a href="#">Mitigations</a>
Collection	T1074	Data Staged	<a href="#">Sub Techniques</a>	<a href="#">Detections</a>	<a href="#">Mitigations</a>
Collection	T1005	Data from Local System	<a href="#">Sub Techniques</a>	<a href="#">Detections</a>	<a href="#">Mitigations</a>
Collection	T1560	Archive Collected Data	<a href="#">Sub Techniques</a>	<a href="#">Detections</a>	<a href="#">Mitigations</a>
Collection	T1213	Data from Information Repositories	<a href="#">Sub Techniques</a>	<a href="#">Detections</a>	<a href="#">Mitigations</a>

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:

SodiumAPT 4ScandiumTG-0416Samurai Panda+13

Details

Mitre ATT&CK

IOC

Yara / Sigma Rules

Tactics

Search tactic or technique name

Tactic	Id	Technique			
Collection	T1114	Email Collection	<a href="#">Sub Techniques</a>	<a href="#">Detections</a>	<a href="#">Mitigations</a>
Collection	T1560	Archive Collected Data	<a href="#">Sub Techniques</a>	<a href="#">Detections</a>	<a href="#">Mitigations</a>
Collection	T1005	Data from Local System	<a href="#">Sub Techniques</a>	<a href="#">Detections</a>	<a href="#">Mitigations</a>
Collection	T1213	Data from Information Repositories	<a href="#">Sub Techniques</a>	<a href="#">Detections</a>	<a href="#">Mitigations</a>
Collection	T1530	Data from Cloud Storage	<a href="#">Sub Techniques</a>	<a href="#">Detections</a>	<a href="#">Mitigations</a>

MITRE | ATT&CK

MatricesTacticsTechniquesDefensesCTIResourcesBenefactorsBlogSearch

Axiom

X

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...

Winnti 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 Winnti Group.[4] ID: G0044 ⓘ Associated Groups: Blackfly Contributors: Edward Millington Version: 1.2 Created: 31 May 2017 Last Modified: 16 Apr...

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 Versi...

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 encrvoted data prior to exfiltration.[7] S0093 Backdoor.Oldrea Backdoor.Oldrea writes collected data to a tempoorary file in an encrvoted

**MITRE | ATT&CK®** Matrices ▾ Tactics ▾ Techniques ▾ Defenses ▾ CTI ▾ Resources ▾ Benefactors Blog ↗

ATT&CK v18 has been released! Check out the [blog post](#) or [changelog](#) for more information.

**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.<sup>[1][2][3]</sup>

ID: G0001  
 ① 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. <sup>[5]</sup>
		.003 Acquire Infrastructure: Virtual Private Server	Axiom has used VPS hosting providers in targeting of intended victims. <sup>[5]</sup>
Enterprise	T1560	Archive Collected Data	Axiom has compressed and encrypted data prior to exfiltration. <sup>[5]</sup>
Enterprise	T1584	.005 Compromise Infrastructure: Botnet	Axiom has used large groups of compromised machines for use as proxy nodes. <sup>[5]</sup>
Enterprise	T1005	Data from Local System	Axiom has collected data from a compromised network. <sup>[5]</sup>
Enterprise	T1001	.002 Data Obfuscation: Steganography	Axiom has used steganography to hide its C2 communications. <sup>[5]</sup>

## 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**.

Prepared by: Temitope Folowosele

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

The screenshot displays the MITRE ATT&CK Navigator v5.2.0 interface. It features a grid of attack techniques organized into columns representing MITRE categories: Resource Development (8 techniques), Initial Access (11 techniques), Execution (17 techniques), Persistence (23 techniques), Privilege Escalation (14 techniques), Defense Evasion (47 techniques), Credential Access (17 techniques), Discovery (34 techniques), Lateral Movement (9 techniques), Collection (17 techniques), Command and Control (18 techniques), Exfiltration (9 techniques), and Impact (15 techniques). The 'Initial Access' column is highlighted, showing techniques like 'Drive-by Compromise', 'Exploit Public-Facing Application', 'External Remote Services', 'Hardware Additions', 'Phishing', 'Replication Through Removable Media', and 'Supply Chain Compromise'. The 'Persistence' column shows techniques like 'Account Manipulation', 'BITS Jobs', 'Boot or Logon Autostart Execution', 'Container Administration Command', 'Deploy Container', 'ESXi Administration Command', 'Input Injection', 'Exploitation for Client Execution', and 'Inter-Process Communication'. The 'Privilege Escalation' column shows techniques like 'Abuse Elevation Control Mechanism', 'Access Token Manipulation', 'BITS Jobs', 'Build Image on Host', 'Debugger Evasion', 'Delay Execution', 'Decobfuscate/Decode Files or Information', 'Deploy Container', 'Direct Volume Access', 'Domain or Tenant Policy Modification', 'Email Spoofing', 'Execution Guardrails', and 'Domain or Local System Administrator'. The 'Defense Evasion' column shows techniques like 'Abuse Elevation Control Mechanism', 'Access Token Manipulation', 'BITS Jobs', 'Build Image on Host', 'Debugger Evasion', 'Delay Execution', 'Decobfuscate/Decode Files or Information', 'Deploy Container', 'Direct Volume Access', 'Domain or Tenant Policy Modification', 'Email Spoofing', 'Execution Guardrails', and 'Domain or Local System Administrator'. The 'Credential Access' column shows techniques like 'Adversary-in-the-Middle', 'Brute Force', 'Credentials from Password Stores', 'Exploitation for Credential Access', 'Forced Authentication', 'Forge Web Credentials', 'Input Capture', 'Modify Authentication Process', and 'Multi-Factor Authentication'. The 'Discovery' column shows techniques like 'Account Discovery', 'Application Window Discovery', 'Browser Information Discovery', 'Cloud Infrastructure Discovery', 'Cloud Service Dashboard', 'Cloud Service Discovery', 'Cloud Storage Object Discovery', 'Container and Resource Discovery', 'Debugger Evasion', 'Device Driver Discovery', and 'Domain Trust Discovery'. The 'Lateral Movement' column shows techniques like 'Exploitation of Remote Services', 'Internal Spearphishing', 'Lateral Tool Transfer', 'Remote Service Session Hijacking', 'Remote Services', 'Replication Through Removable Media', 'Software Deployment Tools', 'Taint Shared Content', and 'Use Alternate Authentication Mechanism'. The 'Collection' column shows techniques like 'Adversary-in-the-Middle', 'Archive Collected Data', 'Audio Capture', 'Automated Collection', 'Browser Session Hijacking', 'Clipboard Data', 'Data from Cloud Storage', 'Data from Configuration Repository', 'Data from File Shares', and 'Data from Network Shares'. The 'Command and Control' column shows techniques like 'Application Layer Protocol', 'Communication Through Removable Media', 'Content Injection', 'Data Encoding', 'Data Obfuscation', 'Dynamic Resolution', 'Encrypted Channel', 'Fallback Channels', and 'Hide Infrastructure'. The 'Exfiltration' column shows techniques like 'Automated Exfiltration', 'Data Transfer Size Limits', 'Exfiltration Over Alternative Protocol', 'Exfiltration Over C2 Channel', 'Exfiltration Over Other Network Medium', and 'Exfiltration Over Physical Medium'. The 'Impact' column shows techniques like 'Account Access Removal', 'Data Destruction', 'Data Encrypted for Impact', 'Data Manipulation', 'Defacement', 'Disk Wipe', 'Email Bombing', 'Endpoint Denial of Service', 'Financial Theft', 'Firmware Corruption', 'Inhibit System Recovery', and 'Network Denial of Service'.

The screenshot displays the MITRE ATT&CK Navigator v5.2.0 interface with the 'Create New Layer' dialog box open. The dialog box has a dark theme and contains the following sections:

- Create New Layer**: A section with two options: 'Create a new empty layer' and 'Load a layer from your computer or a URL'.
- Create Layer from Other Layers**: A section with a dropdown menu labeled 'domain\*' and a text input field for 'score expression'. Below these is a dropdown menu labeled 'gradient'.
- Instructions**: A section with text explaining how to use constants (numbers) and layer variables (yellow, above) to write an expression for the initial value of scores in the new layer. It also provides a link to a full list of supported operations and a list of available layer variables: 'a' (Axiom), 'b' (Stone Panda), and 'c' (Wekby).
- Footer**: A section with the text 'MITRE ATT&CK® Navigator v5.2.0'.

# Prepared by: Temitope Folowosele

Axiom X Stone Panda X Wekby X layer by operation X +											
Selection Controls Layer Controls Technique Controls											
Q X 🔒 ⋮											
Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control
11 techniques	8 techniques	11 techniques	17 techniques	23 techniques	14 techniques	47 techniques	17 techniques	34 techniques	9 techniques	17 techniques	18 techniques
Active Scanning (0/3)	Acquire Access (0/3)	Content Injection (0/3)	Cloud Administration Command (0/7)	Account Manipulation (0/7)	Abuse Elevation Control Mechanism (0/5)	Abuse Elevation Control Mechanism (0/5)	Adversary-in-the-Middle (0/4)	Account Discovery (0/4)	Exploitation of Remote Services (0/4)	Adversary-in-the-Middle (0/4)	Application Layer Protocol (0/3)
Gather Victim Host Information (0/4)	Acquire Infrastructure (0/8)	Drive-by Compromise (0/3)	Command and Scripting Interpreter (1/13)	BITS Jobs (0/3)	Access Token Manipulation (0/3)	Access Token Manipulation (0/3)	Brute Force (0/4)	Application Window Discovery (0/4)	Internal Spearphishing (0/4)	Archived Collected Data (0/3)	Communication Through Removable Media (0/3)
Gather Victim Identity Information (0/3)	Compromise Accounts (0/2)	Exploit Public-Facing Application (0/3)	Container Administration Command (1/14)	Boot or Logon Autostart Execution (0/13)	Access Token Manipulation (0/3)	Access Token Manipulation (0/3)	Credentials from Password Stores (0/4)	Browser Information Discovery (0/4)	Lateral Tool Transfer (0/4)	Audio Capture (0/3)	Data Transfer Size Limits (0/3)
Gather Victim Network Information (0/6)	Compromise Infrastructure (1/8)	External Remote Services (0/3)	Deploy Container (0/3)	Boot or Logon Initialization Scripts (0/5)	Account Manipulation (0/7)	Build Image on Host (0/4)	Exploitation for Credential Access (0/2)	Cloud Infrastructure Discovery (0/4)	Remote Service Session Hijacking (1/2)	Automated Collection (0/2)	Exfiltration Over Alternative Protocol (0/3)
Gather Victim Org Information (0/6)	Develop Capabilities (0/6)	Hardware Additions (0/3)	ESXi Administration Command (0/3)	Cloud Application Integration (0/3)	Boot or Logon Autostart Execution (1/14)	Deobfuscate/Decode Files or Information (0/2)	Forced Authentication (0/2)	Cloud Service Dashboard (0/2)	Remote Services (1/8)	Data Encoding (0/3)	Exfiltration Over C2 Channel (0/3)
Phishing for Information (0/4)	Establish Accounts (0/2)	Phishing (0/3)	Exploitation for Client Execution (0/3)	Compromise Host Software Binary (0/3)	Boot or Logon Initialization Scripts (0/3)	Deploy Container (0/2)	Forge Web Credentials (0/4)	Cloud Storage Object Discovery (0/2)	Replication Through Removable Media (0/2)	Clipboard Data (0/2)	Exfiltration Over Other Network Medium (0/3)
Search Closed Sources (0/2)	Obtain Capabilities (0/2)	Replication Through Removable Media (0/2)	Input Injection (0/3)	Create Account (0/3)	Direct Volume Access (0/2)	Domain or Tenant Policy Modification (0/2)	Input Capture (0/2)	Container and Resource Discovery (0/2)	Software Deployment Tools (0/2)	Data from Cloud Storage (0/2)	Encrypted Channel (0/3)
Search Open Technical Databases (0/2)	Stage Capabilities (0/3)	Supply Chain Compromise (0/3)	Inter-Process Communication (0/3)	Create or Modify System Process (0/3)	Email Spoofing (0/2)	Execution Guardrails (0/2)	Modify Authentication Process (0/6)	Debugger Evasion (0/2)	Taint Shared Content (0/2)	Data from Configuration Repository (0/2)	Fallback Channels (0/3)
Search Open Websites/Domains (0/3)			Native API (0/3)	Domain or Tenant Policy Modification (0/3)	Domain or Tenant Policy Modification (0/3)		Multi-Factor Authentication (0/2)	Domain Trust Discovery (0/2)	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/4)	Ingress Tool Transfer (0/3)

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control
11 techniques	8 techniques	11 techniques	17 techniques	23 techniques	14 techniques	47 techniques	17 techniques	34 techniques	9 techniques	17 techniques	18 techniques
Search Open Websites/Domains (0/3)	Acquire Access (0/3)	Content Injection (0/3)	Cloud Administration Command (0/7)	Account Manipulation (0/7)	Abuse Elevation Control Mechanism (0/5)	Abuse Elevation Control Mechanism (0/5)	Adversary-in-the-Middle (0/4)	Account Discovery (0/4)	Exploitation of Remote Services (0/4)	Adversary-in-the-Middle (0/4)	Application Layer Protocol (0/3)
Search Threat Vendor Data (0/3)	Acquire Infrastructure (0/8)	Drive-by Compromise (0/3)	Command and Scripting Interpreter (1/13)	BITS Jobs (0/3)	Access Token Manipulation (0/3)	Access Token Manipulation (0/3)	Brute Force (0/4)	Application Window Discovery (0/4)	Internal Spearphishing (0/4)	Archived Collected Data (0/3)	Communication Through Removable Media (0/3)
Search Victim-Owned Websites (0/3)	Compromise Accounts (0/2)	Exploit Public-Facing Application (0/3)	Container Administration Command (1/14)	Boot or Logon Autostart Execution (0/13)	Access Token Manipulation (0/3)	Access Token Manipulation (0/3)	Credentials from Password Stores (0/4)	Browser Information Discovery (0/4)	Lateral Tool Transfer (0/4)	Audio Capture (0/3)	Data Transfer Size Limits (0/3)
	Compromise Infrastructure (1/8)	External Remote Services (0/3)	Deploy Container (0/3)	Boot or Logon Initialization Scripts (0/5)	Account Manipulation (0/7)	Build Image on Host (0/4)	Exploitation for Credential Access (0/2)	Cloud Infrastructure Discovery (0/4)	Remote Service Session Hijacking (1/2)	Automated Collection (0/2)	Exfiltration Over Alternative Protocol (0/3)
	Develop Capabilities (0/6)	Hardware Additions (0/3)	ESXi Administration Command (0/3)	Cloud Application Integration (0/3)	Boot or Logon Autostart Execution (1/14)	Deobfuscate/Decode Files or Information (0/2)	Forced Authentication (0/2)	Cloud Service Dashboard (0/2)	Remote Services (1/8)	Data Encoding (0/3)	Exfiltration Over C2 Channel (0/3)
	Establish Accounts (0/2)	Phishing (0/3)	Exploitation for Client Execution (0/3)	Compromise Host Software Binary (0/3)	Boot or Logon Initialization Scripts (0/3)	Deploy Container (0/2)	Forge Web Credentials (0/4)	Cloud Storage Object Discovery (0/2)	Replication Through Removable Media (0/2)	Clipboard Data (0/2)	Exfiltration Over Other Network Medium (0/3)
	Obtain Capabilities (0/2)	Replication Through Removable Media (0/2)	Input Injection (0/3)	Create Account (0/3)	Direct Volume Access (0/2)	Domain or Tenant Policy Modification (0/2)	Input Capture (0/2)	Container and Resource Discovery (0/2)	Software Deployment Tools (0/2)	Data from Cloud Storage (0/2)	Encrypted Channel (0/3)
	Stage Capabilities (0/3)	Supply Chain Compromise (0/3)	Inter-Process Communication (0/3)	Create or Modify System Process (0/3)	Email Spoofing (0/2)	Execution Guardrails (0/2)	Modify Authentication Process (0/6)	Debugger Evasion (0/2)	Taint Shared Content (0/2)	Data from Configuration Repository (0/2)	Fallback Channels (0/3)
			Native API (0/3)	Domain or Tenant Policy Modification (0/3)	Domain or Tenant Policy Modification (0/3)		Multi-Factor Authentication (0/2)	Domain Trust Discovery (0/2)	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/4)	Ingress Tool Transfer (0/3)

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control
11 techniques	8 techniques	11 techniques	17 techniques	23 techniques	14 techniques	47 techniques	17 techniques	34 techniques	9 techniques	17 techniques	18 techniques
Search Open Websites/Domains (0/3)	Acquire Access (0/3)	Content Injection (0/3)	Cloud Administration Command (0/7)	Account Manipulation (0/7)	Abuse Elevation Control Mechanism (0/5)	Abuse Elevation Control Mechanism (0/5)	Adversary-in-the-Middle (0/4)	Account Discovery (0/4)	Exploitation of Remote Services (0/4)	Adversary-in-the-Middle (0/4)	Application Layer Protocol (0/3)
Search Threat Vendor Data (0/3)	Acquire Infrastructure (0/8)	Drive-by Compromise (0/3)	Command and Scripting Interpreter (1/13)	BITS Jobs (0/3)	Access Token Manipulation (0/3)	Access Token Manipulation (0/3)	Brute Force (0/4)	Application Window Discovery (0/4)	Internal Spearphishing (0/4)	Archived Collected Data (0/3)	Communication Through Removable Media (0/3)
Search Victim-Owned Websites (0/3)	Compromise Accounts (0/2)	Exploit Public-Facing Application (0/3)	Container Administration Command (1/14)	Boot or Logon Autostart Execution (0/13)	Access Token Manipulation (0/3)	Access Token Manipulation (0/3)	Credentials from Password Stores (0/4)	Browser Information Discovery (0/4)	Lateral Tool Transfer (0/4)	Audio Capture (0/3)	Data Transfer Size Limits (0/3)
	Compromise Infrastructure (1/8)	External Remote Services (0/3)	Deploy Container (0/3)	Boot or Logon Initialization Scripts (0/5)	Account Manipulation (0/7)	Build Image on Host (0/4)	Exploitation for Credential Access (0/2)	Cloud Infrastructure Discovery (0/4)	Remote Service Session Hijacking (1/2)	Automated Collection (0/2)	Exfiltration Over Alternative Protocol (0/3)
	Develop Capabilities (0/6)	Hardware Additions (0/3)	ESXi Administration Command (0/3)	Cloud Application Integration (0/3)	Boot or Logon Autostart Execution (1/14)	Deobfuscate/Decode Files or Information (0/2)	Forced Authentication (0/2)	Cloud Service Dashboard (0/2)	Remote Services (1/8)	Data Encoding (0/3)	Exfiltration Over C2 Channel (0/3)
	Establish Accounts (0/2)	Phishing (0/3)	Exploitation for Client Execution (0/3)	Compromise Host Software Binary (0/3)	Boot or Logon Initialization Scripts (0/3)	Deploy Container (0/2)	Forge Web Credentials (0/4)	Cloud Storage Object Discovery (0/2)	Replication Through Removable Media (0/2)	Clipboard Data (0/2)	Exfiltration Over Other Network Medium (0/3)
	Obtain Capabilities (0/2)	Replication Through Removable Media (0/2)	Input Injection (0/3)	Create Account (0/3)	Direct Volume Access (0/2)	Domain or Tenant Policy Modification (0/2)	Input Capture (0/2)	Container and Resource Discovery (0/2)	Software Deployment Tools (0/2)	Data from Cloud Storage (0/2)	Encrypted Channel (0/3)
	Stage Capabilities (0/3)	Supply Chain Compromise (0/3)	Inter-Process Communication (0/3)	Create or Modify System Process (0/3)	Email Spoofing (0/2)	Execution Guardrails (0/2)	Modify Authentication Process (0/6)	Debugger Evasion (0/2)	Taint Shared Content (0/2)	Data from Configuration Repository (0/2)	Fallback Channels (0/3)
			Native API (0/3)	Domain or Tenant Policy Modification (0/3)	Domain or Tenant Policy Modification (0/3)		Multi-Factor Authentication (0/2)	Domain Trust Discovery (0/2)	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/4)	Ingress Tool Transfer (0/3)



### 3. Highlight of the TTPs

Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command and Control	Exfiltration	Impact
Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation	Abuse Elevation Control Mechanism	Abuse Elevation Control Mechanism	Adversary-in-the-Middle	Account Discovery	Exploitation of Remote Services	Adversary-in-the-Middle	Application Layer Protocol	Automated Exfiltration	Account Access Removal
Acquire Infrastructure	Drive-by Compromise	Command and Scripting Interpreter	BITS Jobs	Access Token Manipulation	Access Token Manipulation	Brute Force	Application Window Discovery	Internal Spearphishing	Archive Collected Data	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Compromise Accounts	Exploit Public-Facing Application	Container Administration Command	Boot or Logon Autostart Execution	Account Manipulation	BITS Jobs	Credentials from Password Stores	Browser Information Discovery	Lateral Tool Transfer	Audio Capture	Content Injection	Exfiltration Over Alternative Protocol	Data Encrypted for Impact
Compromise Infrastructure	External Remote Services	Deploy Container	Boot or Logon Initialization Scripts	Account Manipulation	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking	Automated Collection	Data Encoding	Defacement	Data Manipulation
Develop Capabilities	Hardware Additions	ESXi Administration Command	Cloud Application Integration	Boot or Logon Autostart Execution	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services	Browser Session Hijacking	Data Obfuscation	Email Bombing	Disk Wipe
Establish Accounts	Phishing	Input Injection	Compromise Host Software Binary	Boot or Logon Initialization Scripts	Delay Execution	Forge Web Credentials	Cloud Storage Object Discovery	Replication Through Removable Media	Clipboard Data	Dynamic Resolution	Exfiltration Over Other Network Medium	Endpoint Denial of Service
Obtain Capabilities	Replication Through Removable Media	Exploitation for Client Execution	Create Account	Boot or Logon Initialization Scripts	Decfuscate/Decode Files or Information	Input Capture	Container and Resource Discovery	Software Deployment Tools	Data from Cloud Storage	Encrypted Channel	Financial Theft	Firmware Corruption
Stage Capabilities	Supply Chain Compromise	Inter-Process Communication	Create or Modify System Process	Create or Modify System Process	Domain or Tenant Policy Modification	Modify Authentication Process	Debugger Evasion	Taint Shared Content	Data from Configuration Repository	Fallback Channels	Inhibit System Recovery	Network Denial of Service

### 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.