

MITRE

ASSIGNMENT REPORT

**Peter Kinyumu,
cs-sa07-24067,
May 15th, 2024.**

1. INTRODUCTION

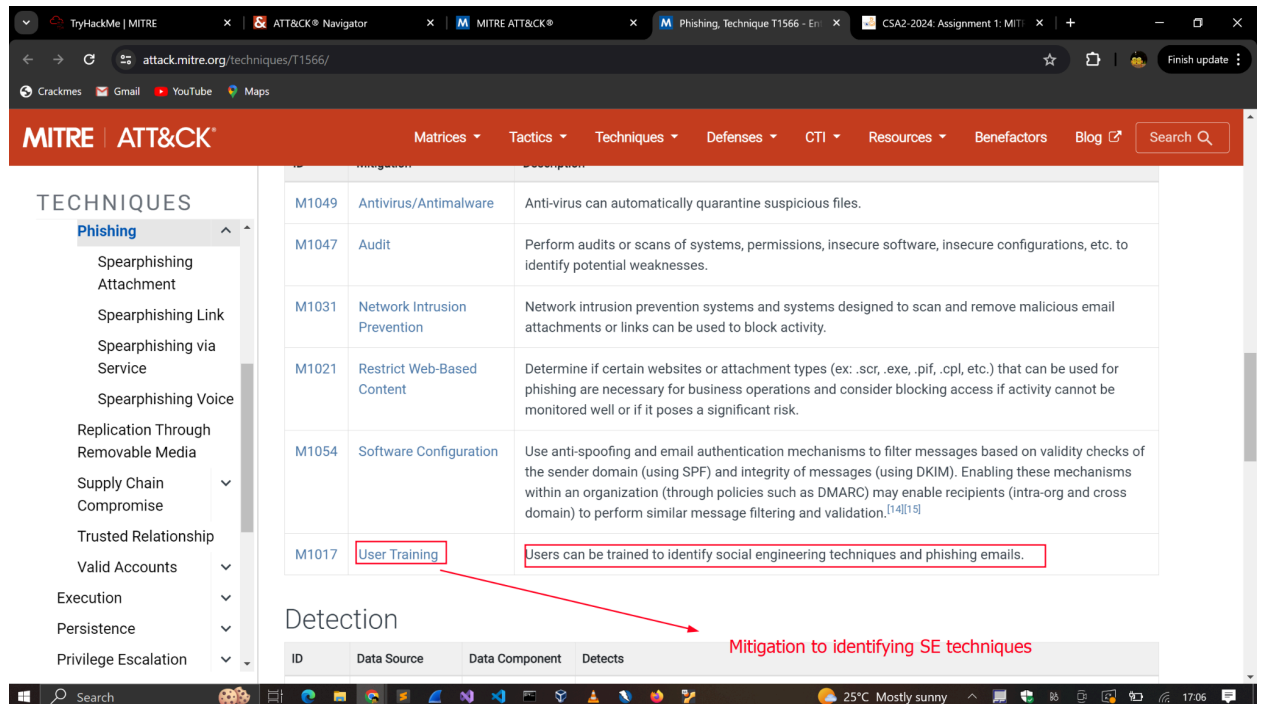
This assignment focused on the various projects Mitre Co-operation created for the cybersecurity community, such as the Mitre ATT&CK Framework, the Cyber Analytics Repository(CAR) knowledge base, the Mitre ENGAGE Framework, and Mitre DEFEND. It explored these resources and how to use them to understand attackers' modulus operandi(Tactics, Techniques and Procedures) and hence effectively detect and prevent them.

2. ANSWERS TO QUESTIONS

ATT&CK Framework

The questions below will help you become more familiar with the ATT&CK®. It is recommended to start answering the questions from the [Phishing page](#). Note, that this link is for version 8 of the ATT&CK Matrix.

- Besides Blue teamers, who else will use the ATT&CK Matrix? (Red Teamers, Purple Teamers, SOC Managers?)
Red Teamers
- What is the ID for this technique?
Phishing is a technique within the Initial access Tactic with an ID T1566
- Based on this technique, what mitigation covers identifying social engineering techniques?



The screenshot shows the MITRE ATT&CK framework website. The left sidebar lists various techniques, with 'Phishing' highlighted. The main content area displays a table of techniques, including 'User Training' (M1017). A red box highlights the 'User Training' technique, and a red arrow points from it to the text 'Mitigation to identifying SE techniques'.

ID	Technique	Description
M1049	Antivirus/Antimalware	Anti-virus can automatically quarantine suspicious files.
M1047	Audit	Perform audits or scans of systems, permissions, insecure software, insecure configurations, etc. to identify potential weaknesses.
M1031	Network Intrusion Prevention	Network intrusion prevention systems and systems designed to scan and remove malicious email attachments or links can be used to block activity.
M1021	Restrict Web-Based Content	Determine if certain websites or attachment types (ex: .scr, .exe, .pif, .cpl, etc.) that can be used for phishing are necessary for business operations and consider blocking access if activity cannot be monitored well or if it poses a significant risk.
M1054	Software Configuration	Use anti-spoofing and email authentication mechanisms to filter messages based on validity checks of the sender domain (using SPF) and integrity of messages (using DKIM). Enabling these mechanisms within an organization (through policies such as DMARC) may enable recipients (intra-org and cross domain) to perform similar message filtering and validation. ^{[14][15]}
M1017	User Training	Users can be trained to identify social engineering techniques and phishing emails.

Mitigation to identifying SE techniques

d. What are the data sources for Detection? (format: source1,source2,source3 with no spaces after commas)

The screenshot shows the MITRE ATT&CK website with the 'Detection' techniques page. The 'Data Source' column is highlighted with a red box, showing the following data:

ID	Data Source	Data Component	Detects
DS0015	Application Log	Application Log Content	Monitor for third-party application logging, messaging, and/or other artifacts that may send phishing messages to gain access to victim systems. Filtering based on DKIM+SPF or header analysis can help detect when the email sender is spoofed. ^{[14][15]} URL inspection within email (including expanding shortened links) can help detect links leading to known malicious sites. Detonation chambers can be used to detect these links and either automatically go to these sites to determine if they're potentially malicious, or wait and capture the content if a user visits the link.
DS0022	File	File Creation	Monitor call logs from corporate devices to identify patterns of potential voice phishing, such as calls to/from known malicious phone numbers. Correlate these records with system events.
DS0029	Network Traffic	Network Traffic Content	Monitor for newly constructed files from a phishing messages to gain access to victim systems.

e. What groups have used spear-phishing in their campaigns? (format: group1,group2)

The screenshot shows the MITRE ATT&CK website with the 'Procedure Examples' table. The 'Name' column is highlighted with a red box, showing the following data:

ID	Name	Description
G0001	Axiom	Axiom has used spear phishing to initially compromise victims. ^{[8][9]}
G0115	GOLD SOUTHFIELD	GOLD SOUTHFIELD has conducted malicious spam (malspam) campaigns to gain access to victim's machines. ^[10]
S0009	Hikit	Hikit has been spread through spear phishing. ^[9]
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. ^{[11][12][13]}

f. Based on the information for the first group, what are their associated groups?

The screenshot shows the MITRE ATT&CK website. The sidebar on the left lists various groups, with 'Axiom' selected. The main content area displays the 'Axiom' group page. The 'Associated Group Descriptions' table shows 'Group 72' as an associated group. The 'Techniques Used' table lists 'Acquire Infrastructure: DNS' as a technique used by Axiom.

GROUPS

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

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: 20 March 2023

[Version Permalink](#)

Associated Group Descriptions

Name	Description
Group 72	[4]

Techniques Used

Domain	ID	Name	Use
Enterprise	T1583	Acquire Infrastructure: DNS	Axiom has acquired dynamic DNS services for use in the targeting of

g. What software is associated with this group that lists phishing as a technique?

The screenshot shows the MITRE ATT&CK website. The sidebar on the left lists various groups, with 'Axiom' selected. The main content area displays the 'Axiom' group page. The 'Software' table lists 'Hikit' as a software associated with Axiom. The 'Techniques' table lists 'Phishing' as a technique used by Axiom.

GROUPS

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

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: 20 March 2023

[Version Permalink](#)

Software

ID	Name	References	Techniques
S0021	Derusbi	[5][4]	Audio Capture, Command and Scripting Interpreter: Unix Shell, Encrypted Channel: Symmetric Cryptography, Fallback Channels, File and Directory Discovery, Indicator Removal: Timestamp, Indicator Removal: File Deletion, Input Capture: Keylogging, Non-Application Layer Protocol, Non-Standard Port, Process Discovery, Process Injection: Dynamic-link Library Injection, Query Registry, Screen Capture, System Binary Proxy Execution: Regsvr32, System Information Discovery, System Owner/User Discovery, Video Capture
S0032	gh0st RAT	[4][5]	Boot or Logon Autostart Execution: Registry Run Keys / Startup Folder, Command and Scripting Interpreter, Create or Modify System Process: Windows Service, Data Encoding: Standard Encoding, Deobfuscate/Decode Files or Information, Dynamic Resolution: Fast Flux DNS, Encrypted Channel: Symmetric Cryptography, Encrypted Channel, Hijack Execution Flow: DLL Side-Loading, Indicator Removal: Clear Windows Event Logs, Indicator Removal: File Deletion, Ingress Tool Transfer, Input Capture: Keylogging, Modify Registry, Native API, Non-Application Layer Protocol, Process Discovery, Process Injection, Query Registry, Screen Capture, Shared Modules, System Binary Proxy Execution: Rundll32, System Information Discovery, System Services: Service Execution
S0009	Hikit	[5][4]	Application Layer Protocol: Web Protocols, Command and Scripting Interpreter: Windows Command Shell, Data from Local System, Encrypted Channel: Symmetric Cryptography, Hijack Execution Flow: DLL Search Order Hijacking, Ingress Tool Transfer, Phishing, Proxy: Internal Proxy, Rootkit, Subvert Trust Controls: Code Signing Policy Modification, Subvert Trust Controls: Install Root Certificate

h. What is the description for this software?

After clicking the link to the software , the description read - “Hikit is malware that has been used by Axiom for late stage persistence and exfiltration after the initial compromise.”

i. This group overlaps (slightly) with which other group?

MITRE | ATT&CK®

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

ATT&CK v15.1 has been released! Check out the [blog post](#) or [release notes](#) for more information.

GROUPS

- Axiom
- BackdoorDiplomacy
- BITTER
- 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: 20 March 2023

[Version Permalink](#)

Associated Group Descriptions

Name	Description
Group 72	[4]

Techniques Used

ATT&CK® Navigator Layers ▾

j. How many techniques are attributed to this group?

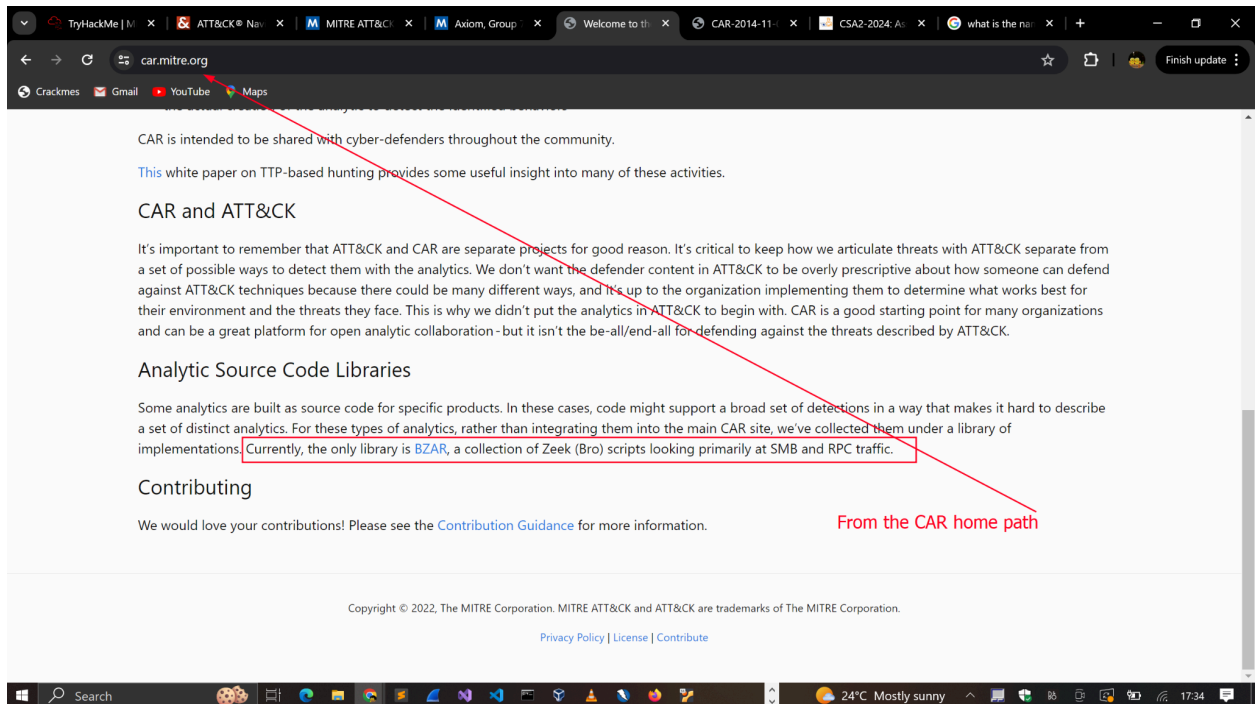
I recorded a count of 15.

Cyber Analytics Repository

a. What tactic has an ID of TA0003?

Persistence

b. What is the name of the library that is a collection of Zeek (BRO) scripts?



c. What is the name of the technique for running executables with the same hash and different names?

T1029: Scheduled Transfer	(N/A - technique only)	<ul style="list-style-type: none"> CAR-2013-04-002: Quick execution of a series of suspicious commands
T1033: System Owner/User Discovery	(N/A - technique only)	<ul style="list-style-type: none"> CAR-2013-04-002: Quick execution of a series of suspicious commands CAR-2016-03-001: Host Discovery Commands
	(N/A - technique only)	<ul style="list-style-type: none"> CAR-2013-05-002: Suspicious Run Locations
T1036: Masquerading	T1036.005: Match Legitimate Name or Location	<ul style="list-style-type: none"> CAR-2021-04-001: Common Windows Process Masquerading
	T1036.003: Rename System Utilities	<ul style="list-style-type: none"> CAR-2013-05-009: Running executables with same hash and different names
T1037: Boot or Logon Initialization Scripts	T1037.001: Logon Script (Windows)	<ul style="list-style-type: none"> CAR-2013-01-002: Autorun Differences CAR-2020-11-001: Boot or Logon Initialization Scripts
T1039: Data from Network Shared Drive	(N/A - technique only)	<ul style="list-style-type: none"> CAR-2013-01-003: SMB Events Monitoring
T1040: Network Sniffing	(N/A - technique only)	<ul style="list-style-type: none"> CAR-2020-11-002: Local Network Sniffing

d. Examine CAR-2013-05-004, besides Implementations, what additional information is provided to analysts to ensure coverage for this technique?

b. What is the name of the resource to aid you with the engagement activity from the previous question?

A quick search of “Persona” from the Engage search bar revealed the resource.

The screenshot shows the MITRE Engage website with a search bar in the top right corner containing the text "Persona". The search results on the left include a link to the "PERSONA PROFILE WORKSHEET", a brief description of the tool, and links to "MATRIX" and "PRIVACY POLICY". The "RECENT POSTS" section on the right lists several links: "Engage Brand Guide", "Starter Kit (Printable)", "Engage Glossary", "Operation Data Template", and "10-Step Process". The "RECENT COMMENTS" section shows "No comments to show."

c. Which engagement activity baits a specific response from the adversary?

The screenshot shows the MITRE Engage website with a search bar in the top right corner containing the text "LURES". The search results on the left include a link to the "LURES" activity, a brief description of the tool, and links to "MATRIX" and "PRIVACY POLICY". The "RECENT POSTS" section on the right lists several links: "Engage Brand Guide", "Starter Kit (Printable)", "Engage Glossary", "Operation Data Template", and "10-Step Process". The "RECENT COMMENTS" section shows "No comments to show."

d. What is the definition of Threat Model?

From Mitre Engage > Prepare tab > Threat model, a threat model is defined as a risk assessment that models organizational strengths and weaknesses.

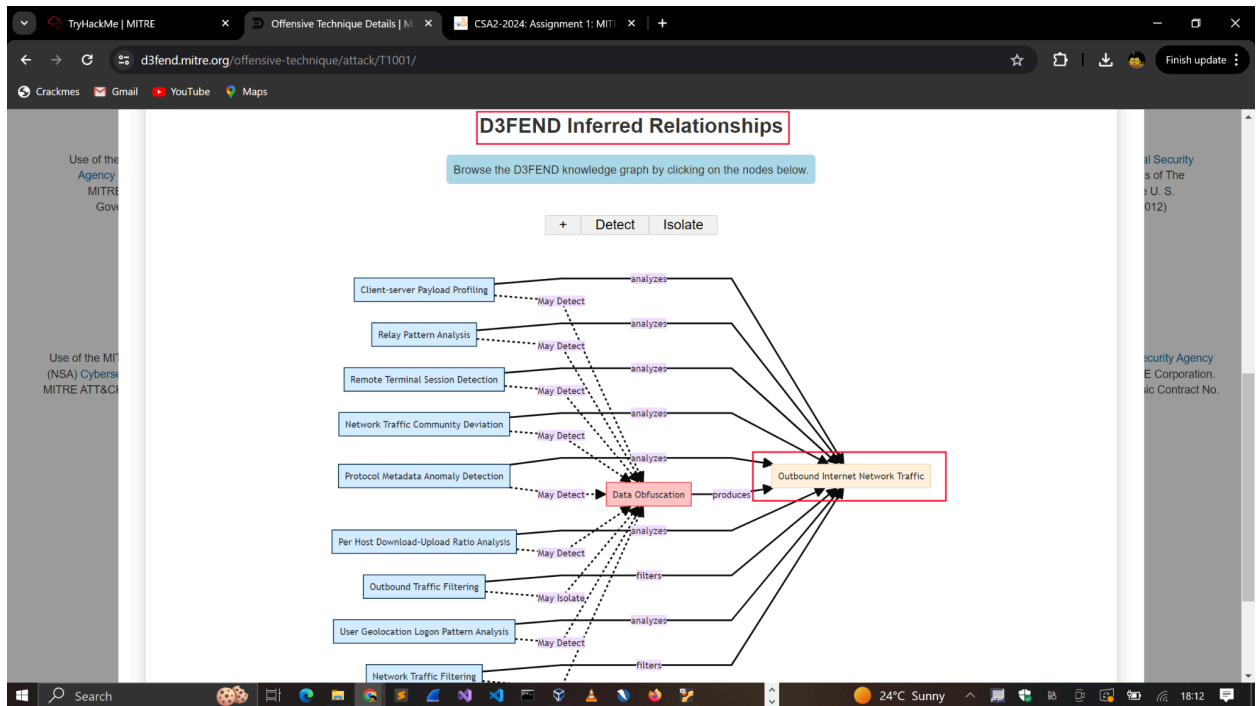
MITRE DEFEND

a. What is the first MITRE ATT&CK technique listed in the ATT&CK Lookup dropdown?

The screenshot shows the MITRE DEFEND website interface. The browser address bar displays 'd3fend.mitre.org'. The page header includes the MITRE logo and navigation links: matrix, artifacts, taxonomies, about, resources, contribute, faq, blog. The main heading is 'DEFEND™' with the subtitle 'A knowledge graph of cybersecurity countermeasures 0.15.0'. Below this, there is a search bar labeled 'Search D3FEND's 679 Artifacts' and a 'D3FEND Lookup' button. The 'ATT&CK Lookup' dropdown menu is open, showing a list of techniques. The first technique listed is 'T1001 - Data Obfuscation'. The background of the page features a grid of categories under the heading 'Detect', including File Analysis, Identifier Analysis, Message Analysis, Network Traffic Analysis, Platform Monitoring, Process Analysis, User Behavior Analysis, Execution Isolation, Network Isolation, and Decoy Environment.

Detect							Isolate		Decoy
File Analysis	Identifier Analysis	Message Analysis	Network Traffic Analysis	Platform Monitoring	Process Analysis	User Behavior Analysis	Execution Isolation	Network Isolation	Decoy Environment
Dynamic Analysis	Homograph Detection	Sender MTA Reputation Analysis	Administrative Network Activity Analysis	File Integrity Monitoring	Database Query String Analysis	Authentication Event Thresholding	Executable Allowlisting	Broadcast Domain Isolation	Connected Honeynet
Emulated File Analysis	Identifier Activity Analysis	Sender Reputation Analysis	Byte Sequence Emulation	Firmware Behavior Analysis	File Access Pattern Analysis	Authorization Event Thresholding	Executable Denylisting	DNS Allowlisting	Integrated Honeynet
File Content Analysis	Identifier Reputation Analysis		Certificate Analysis	Firmware Embedded Monitoring Code	Indirect Branch Call Analysis	Credential Compromise Scope Analysis	Hardware-based Process Isolation	DNS Denylisting	Standalone Honeynet
File Content Rules	Domain Name Reputation Analysis		Active Certificate Analysis	Firmware Verification	Process Code Segment Verification	Domain Account Monitoring	IO Port Restriction	Forward Resolution Domain Denylisting	
File Hashing	File Hash Reputation Analysis		Passive Certificate Analysis	Peripheral Firmware Verification	Process Self-	Job Function Access	Kernel-based Process Isolation	Hierarchical Domain Denylisting	

b. In D3FEND Inferred Relationships, what does the ATT&CK technique from the previous question produce?

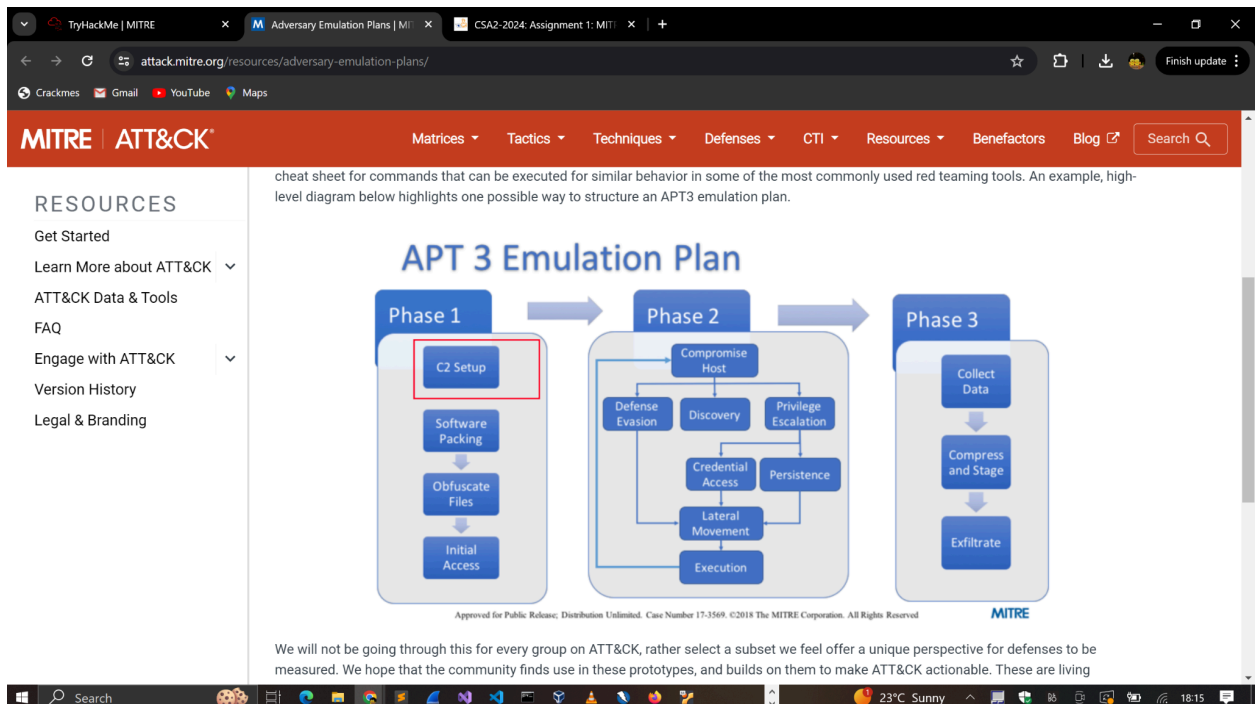


ATT&CK Emulation Plans

There are several ATT&CK® Emulation Plans currently available: APT3, APT29, and FIN6. Review the emulation plans to answer the questions below.

- a. In Phase 1 for the APT3 Emulation Plan, what is listed first?

<https://attack.mitre.org/resources/adversary-emulation-plans/>



b. Under Persistence, what binary was replaced with cmd.exe?

One of the resources listed under the Adversary emulation plans for APT3 was the APT# emulation plan manual below.

https://attack.mitre.org/docs/APT3_Adversary_Emulation_Plan.pdf

The screenshot displays a web browser window with the Adobe Acrobat PDF viewer open to the document 'APT3_Adversary_Emulation_Plan.pdf'. The document is titled 'Approved for Public Release: Distribution Unlimited. Case Number 17-3569. ©2018 The MITRE Corporation. All Rights Reserved'. The section '3.2.1.3 Persistence' is highlighted, featuring a diagram and descriptive text. The diagram, titled 'Figure 5 APT3 Persistence ATT&CK Techniques', shows a central box labeled 'Persistence' connected to five techniques: 'Accessibility Features ATTACK:T1015', 'Start Folder ATTACK:T1060', 'New Service ATTACK:T1050', 'Schtasks ATTACK:T1053', and 'Legitimate Credentials ATTACK:T1078'. The text to the right of the diagram explains that APT3 used multiple methods for persistence, including creating a service [23] (T1050 - New Service), creating a scheduled task [2] (T1053 - Scheduled Task), and placing scripts in the Startup Folder [7] (T1060 - Registry Run Keys/Start Folder). It specifically notes that APT3 replaced the Sticky Keys binary (C:\Windows\System32\sethc.exe) with cmd.exe [T1015 - Accessibility Features] and enabled Remote Desktop Protocol (RDP) if it is not already enabled [T1076 - Remote Desktop Protocol]. This technique allows an operator to open a command prompt when connected over RDP without providing valid credentials [23]. Additionally, it mentions that APT3 has been known to create or enable accounts, for example 'support_388945a0', and add them to the local admin group [23] [T1136 - Create Account]. Presumably this is done for easier future access. A recommendation is provided: 'Recommendation: On new hosts, establish persistence by creating a service or schtasks. On systems where RDP capabilities are desired, it might also be useful to enable sticky keys and RDP.' The section '3.2.1.4 Credential Access' is partially visible at the bottom.

Approved for Public Release:
Distribution Unlimited. Case Number 17-3569. ©2018 The MITRE Corporation. All Rights Reserved

3.2.1.3 Persistence

Figure 5 APT3 Persistence ATT&CK Techniques

APT3 has used multiple methods for persistence: creating a service [23] (T1050 - New Service), creating a scheduled task [2] (T1053 - Scheduled Task), and also by placing scripts in the Startup Folder [7] (T1060 - Registry Run Keys/Start Folder).

APT3 has replaced the Sticky Keys binary (C:\Windows\System32\sethc.exe) with cmd.exe [T1015 - Accessibility Features] and enabled Remote Desktop Protocol (RDP) if it is not already enabled [T1076 - Remote Desktop Protocol]. This specific Persistence technique has an added benefit of allowing an operator to open a command prompt when connected over RDP without having to provide valid credentials [23].

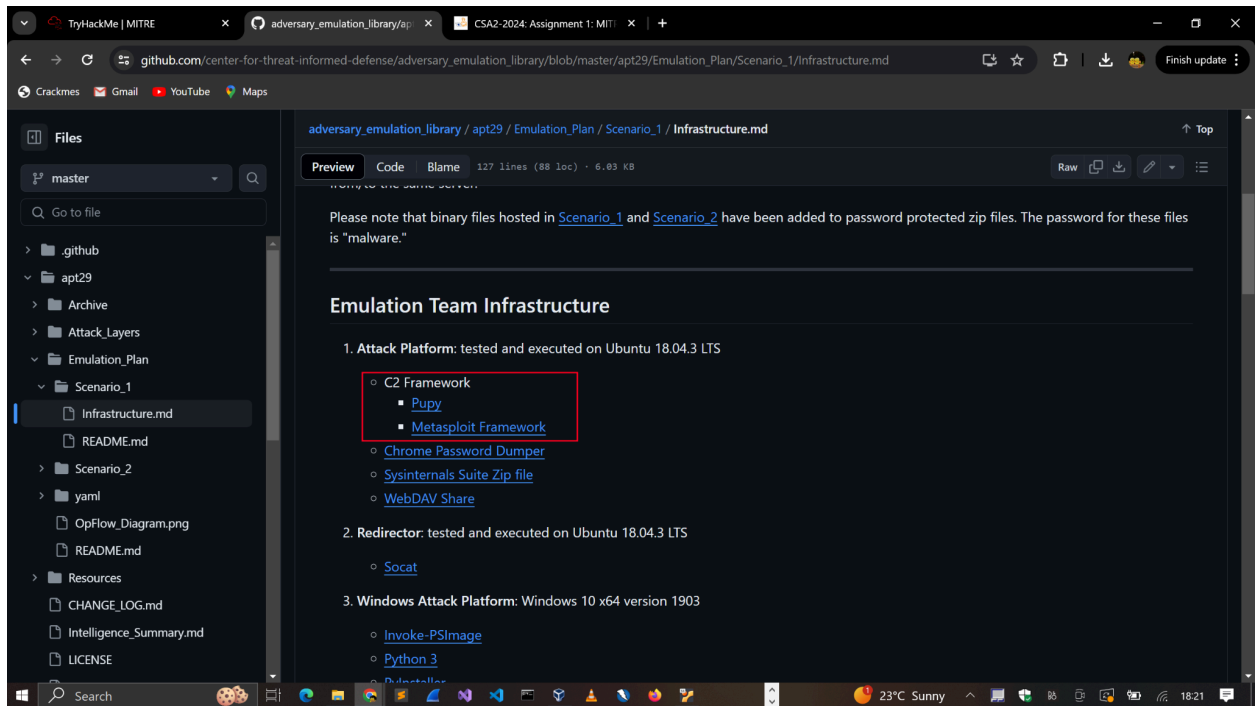
APT3 has been known to create or enable accounts, for example "support_388945a0", and add them to the local admin group [23] [T1136 - Create Account]. Presumably this is done for easier future access.

Recommendation: On new hosts, establish persistence by creating a service or schtasks. On systems where RDP capabilities are desired, it might also be useful to enable sticky keys and RDP.

3.2.1.4 Credential Access

c. Examining APT29, what C2 frameworks are listed in Scenario 1 Infrastructure? (format: tool1,tool2)

https://github.com/center-for-threat-informed-defense/adversary_emulation_library/tree/master/apt29



- d. What C2 framework is listed in Scenario 2 Infrastructure?
PoshC2
- e. Examine the emulation plan for Sandworm. What webshell is used for Scenario 1?
Check MITRE ATT&CK for the Software ID for the webshell. What is the id?
(format: webshell,id)

TryHackMe | MITRE | adversary_emulation_library/sandworm

github.com/center-for-threat-informed-defense/adversary_emulation_library/tree/master/sandworm

Crackmes | Gmail | YouTube | Maps

Files

master

Go to file

menu_pass

micro_emulation_plans

ocean_lotus

oilrig

resources

sandworm

Emulation_Plan

Hashes

Intelligence_Summary

Operations_Flow

Resources

yara-rules

.gitignore

LICENSE

NOTICE.txt

README.md

adversary_emulation_library / sandworm /

YARA Rules

YARA rules are provided to assist the community in researching, preventing, and detecting malware specimens used in this emulation plan.

Emulation Key Software

- P.A.S. webshell
- Exaramel
- NotPetya
- OraDump/LaZagne Variant
- Win64/Spy.KeyLogger.G

Scenario Walkthrough

- Detection Scenario - Step by Step walkthrough of Scenario's procedures (9 steps).
- Protection Scenario - Step by Step walkthrough of Scenario's procedures (3 tests)

For Analysts

- Operation Flow - High-level summary of the scenario & infrastructure with diagrams.
- Intelligence Summary - General overview of the Adversary with links to reporting used throughout the scenario.

TryHackMe | MITRE | adversary_emulation_library/sandworm | CSA2-2024: Assignment 1: MITRE | Sandworm Team, ELECTRUM, T...

attack.mitre.org/groups/G0034/

Crackmes | Gmail | YouTube | Maps

MITRE | ATT&CK

Matrices | Tactics | Techniques | Defenses | CTI | Resources | Benefactors | Blog | Search

GROUPS

Sandworm Team

Scarlet Mimic

Scattered Spider

SideCopy

Sidewinder

Silence

Silent Librarian

SilverTerrier

Sowbug

Stealth Falcon

Strider

Suckfly

TA2541

TA459

TA505

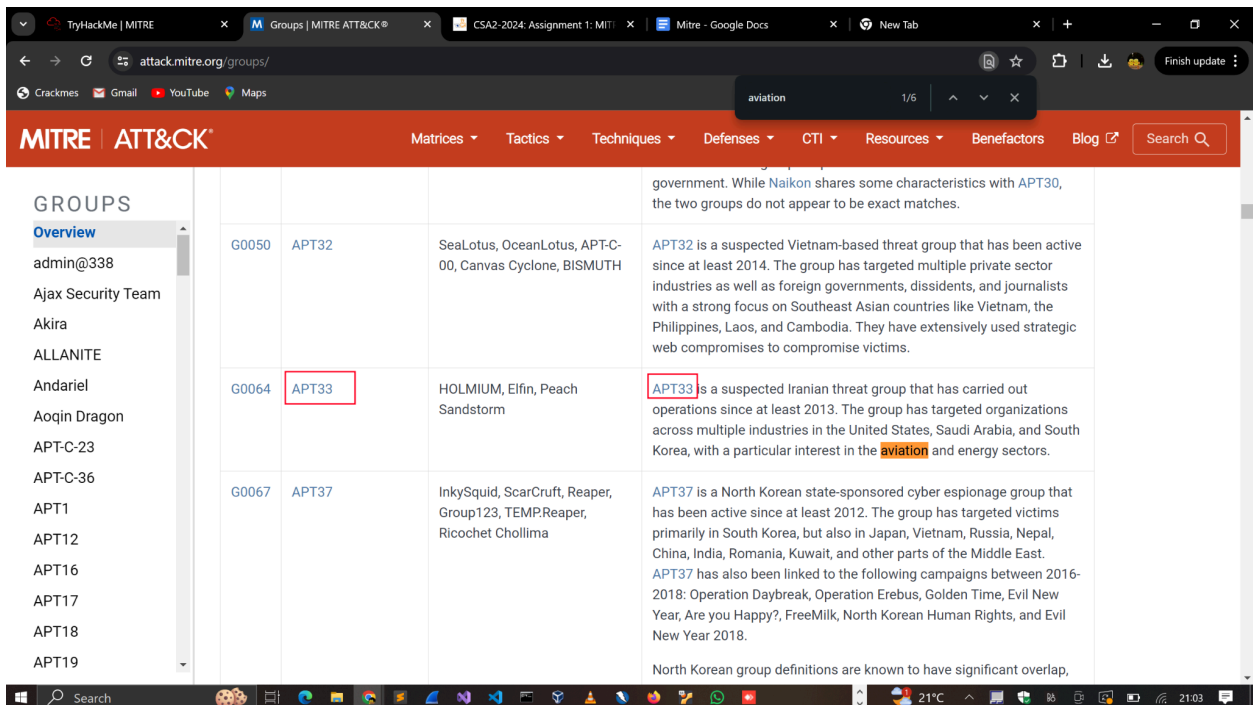
	Destroyer		Indicator Removal: Clear Windows Event Logs, Inhibit System Recovery, Lateral Tool Transfer, Network Share Discovery, OS Credential Dumping: LSASS Memory, Remote Services: SMB/Windows Admin Shares, Remote System Discovery, Service Stop, System Network Configuration Discovery, System Services: Service Execution, System Shutdown/Reboot, Windows Management Instrumentation
S0598	P.A.S. Webshell	[33]	Account Discovery: Local Account, Application Layer Protocol: Web Protocols, Brute Force: Password Guessing, Command and Scripting Interpreter: Data from Information Repositories, Data from Local System, Deobfuscate/Decode Files or Information, File and Directory Discovery, File and Directory Permissions Modification: Linux and Mac File and Directory Permissions Modification, Indicator Removal: File Deletion, Ingress Tool Transfer, Network Service Discovery, Obfuscated Files or Information, Server Software Component: Web Shell, Software Discovery
S1058	Prestige	[11]	Command and Scripting Interpreter: PowerShell, Data Encrypted for Impact, Domain or Tenant Policy Modification: Group Policy Modification, File and Directory Discovery, Inhibit System Recovery, Modify Registry, Native API, Scheduled Task/Job: Scheduled Task, Service Stop
S0029	PsExec	[17]	Create Account: Domain Account, Create or Modify System Process: Windows Service, Lateral Tool Transfer, Remote Services: SMB/Windows Admin Shares, System Services: Service Execution

References

ATT&CK and Threat Intelligence

Scenario: You are a security analyst who works in the aviation sector. Your organization is moving their infrastructure to the cloud. Your goal is to use the ATT&CK® Matrix to gather threat intelligence on APT groups who might target this particular sector and use techniques targeting your areas of concern. You are checking to see if there are any gaps in coverage. After selecting a group, look over the selected group's information and their tactics, techniques, etc.

- a. What is a group that targets your sector who has been in operation since at least 2013?



The screenshot shows the MITRE ATT&CK Groups page. The left sidebar lists various groups, with APT33 highlighted. The main table displays details for APT33, including its ID (G0064), name (APT33), and description. The description states that APT33 is a suspected Iranian threat group that has carried out operations since at least 2013, targeting organizations across multiple industries in the United States, Saudi Arabia, and South Korea, with a particular interest in the aviation and energy sectors.

GROUPS	Overview	admin@338	Ajax Security Team	Akira	ALLANITE	Andariel	Aoqin Dragon	APT-C-23	APT-C-36	APT1	APT12	APT16	APT17	APT18	APT19
G0050	APT32	SeaLotus, OceanLotus, APT-C-00, Canvas Cyclone, BISMUTH		APT32 is a suspected Vietnam-based threat group that has been active since at least 2014. The group has targeted multiple private sector industries as well as foreign governments, dissidents, and journalists with a strong focus on Southeast Asian countries like Vietnam, the Philippines, Laos, and Cambodia. They have extensively used strategic web compromises to compromise victims.											
G0064	APT33	HOLMIUM, Elfir, Peach Sandstorm		APT33 is a suspected Iranian threat group that has carried out operations since at least 2013. The group has targeted organizations across multiple industries in the United States, Saudi Arabia, and South Korea, with a particular interest in the aviation and energy sectors.											
G0067	APT37	InkySquid, ScarCruft, Reaper, Group123, TEMPReaper, Ricochet Chollima		APT37 is a North Korean state-sponsored cyber espionage group that has been active since at least 2012. The group has targeted victims primarily in South Korea, but also in Japan, Vietnam, Russia, Nepal, China, India, Romania, Kuwait, and other parts of the Middle East. APT37 has also been linked to the following campaigns between 2016-2018: Operation Daybreak, Operation Erebus, Golden Time, Evil New Year, Are you Happy?, FreeMilk, North Korean Human Rights, and Evil New Year 2018.											

- b. As your organization is migrating to the cloud, is there anything attributed to this APT group that you should focus on? If so, what is it?
- c. What tool is associated with the technique from the previous question?

The screenshot shows the MITRE ATT&CK Groups page for APT33. The left sidebar lists various groups, with APT33 selected. The main table displays techniques associated with APT33. The 'Cloud Accounts' technique is highlighted in the table.

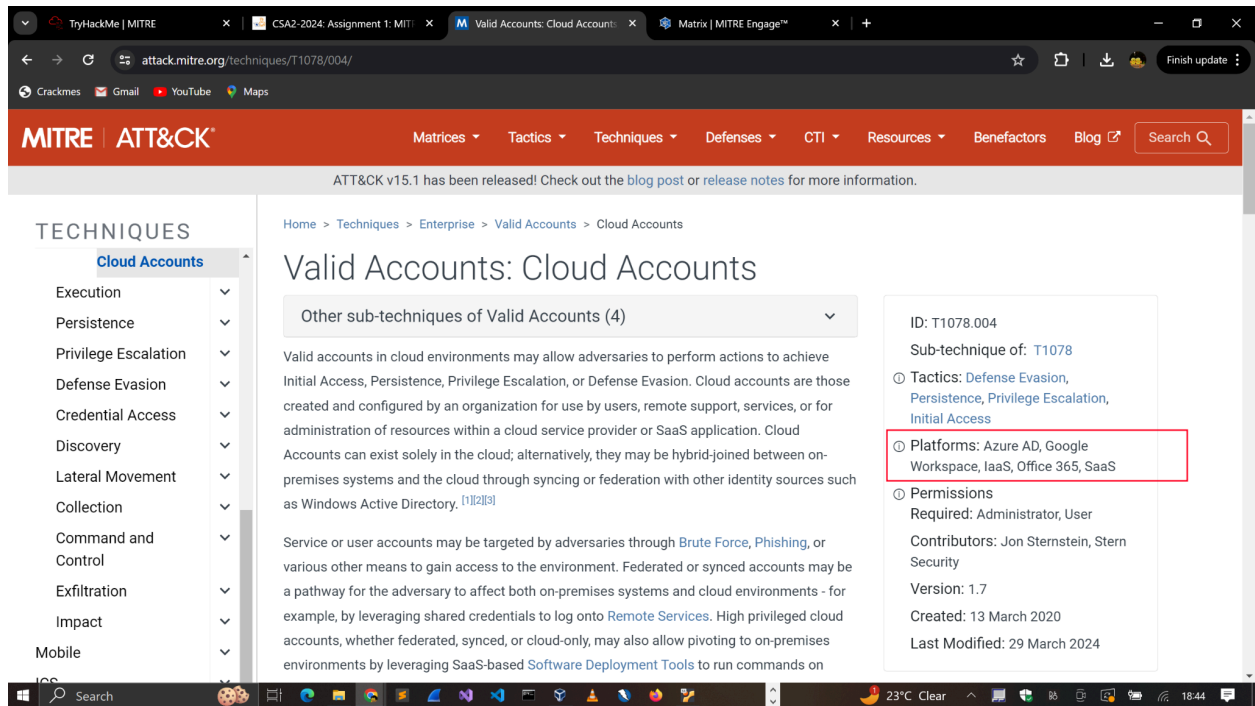
Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	APT33 has created a scheduled task to execute a .vbe file multiple times a day. ^[4]
Enterprise	T1552	.001	Unsecured Credentials: Credentials In Files	APT33 has used a variety of publicly available tools like LaZagne to gather credentials. ^{[4][6]}
		.006	Unsecured Credentials: Group Policy Preferences	APT33 has used a variety of publicly available tools like Gpppassword to gather credentials. ^{[4][6]}
Enterprise	T1204	.001	User Execution: Malicious Link	APT33 has lured users to click links to malicious HTML applications delivered via spearphishing emails. ^{[1][4]}
		.002	User Execution: Malicious File	APT33 has used malicious e-mail attachments to lure victims into executing malware. ^[3]
Enterprise	T1078		Valid Accounts	APT33 has used valid accounts for initial access and privilege escalation. ^{[2][6]}
		.004	Cloud Accounts	APT33 has used compromised Office 365 accounts in tandem with Ruler in an attempt to gain control of endpoints. ^[3]
ICS	T0852		Screen Capture	APT33 utilize backdoors capable of capturing screenshots once installed on a system. ^{[7][8]}
ICS	T0853		Scripting	APT33 utilized PowerShell scripts to establish command and control and install files for execution. ^{[9][10]}

d. Referring to the technique from question 2, what mitigation method suggests using SMS messages as an alternative for its implementation?

The screenshot shows the MITRE ATT&CK Techniques page for Cloud Accounts. The left sidebar lists various techniques, with Cloud Accounts selected. The main table displays mitigation methods for Cloud Accounts. The 'Multi-factor Authentication' technique is highlighted in the table.

M1036	Account Use Policies	Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges. ^[16]
M1015	Active Directory Configuration	Disable legacy authentication, which does not support MFA, and require the use of modern authentication protocols instead.
M1032	Multi-factor Authentication	Use multi-factor authentication for cloud accounts, especially privileged accounts. This can be implemented in a variety of forms [e.g. hardware, virtual, SMS] and can also be audited using administrative reporting features. ^[17]
M1027	Password Policies	Ensure that cloud accounts, particularly privileged accounts, have complex, unique passwords across all systems on the network. Passwords and access keys should be rotated regularly. This limits the amount of time credentials can be used to access resources if a credential is compromised without your knowledge. Cloud service providers may track access key age to help audit and identify keys that may need to be rotated. ^[17]
M1026	Privileged Account Management	Review privileged cloud account permission levels routinely to look for those that could allow an adversary to gain wide access, such as Global Administrator and Privileged Role Administrator in Azure AD. ^{[18][19][20]} These reviews should also check if new privileged cloud accounts have been created that were not authorized. For example, in Azure AD environments configure alerts to notify when accounts have gone many days without using privileged roles, as these roles may be able to be removed. ^[21] Consider using temporary, just-in-time (JIT) privileged access to Azure AD resources rather than permanently assigning privileged roles. ^[20]
M1018	User Account Management	Periodically review user accounts and remove those that are inactive or unnecessary. Limit the ability for user accounts to create additional accounts.

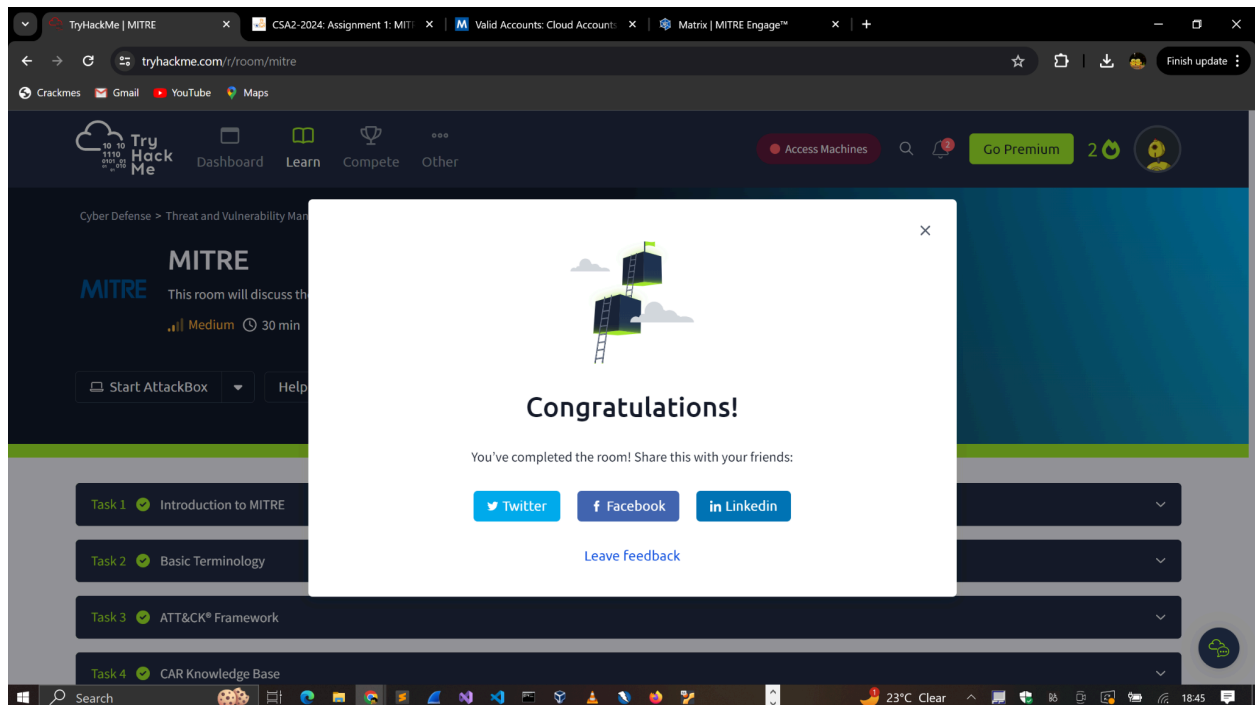
e. What platforms does the technique from question #2 affect?



3. MODULE COMPLETION

Profile link

<https://tryhackme.com/p/c1ph3rbnuk>



4. CONCLUSION

The assignment has been very comprehensive in helping me understand the different MITRE frameworks. I have learned how to use the ATT&CK Framework to understand different adversaries' behaviours, the CAR knowledge base to identify the data necessary to detect the adversary's behaviour, how to engage proactively with attackers using cyber deception and denial, and the defensive techniques listed in D3FEND to mitigate the tactics in ATT&CK.

Additionally, I have learnt how to gather threat intelligence information on APT groups that might be a threat to my sector to identify any gaps in our defensive strategies. This has been very insightful and great experience. I'm keen to exploring more and learning more in the upcoming chapters.