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

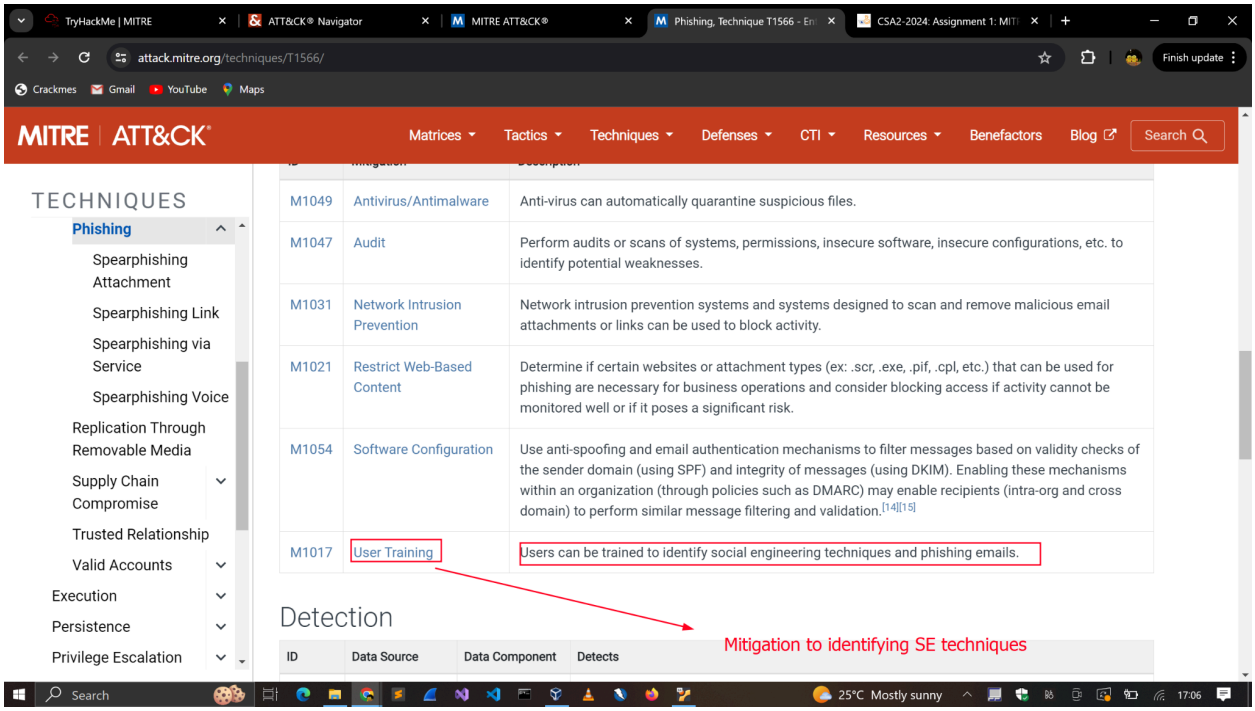
ATT&CK Framework

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.

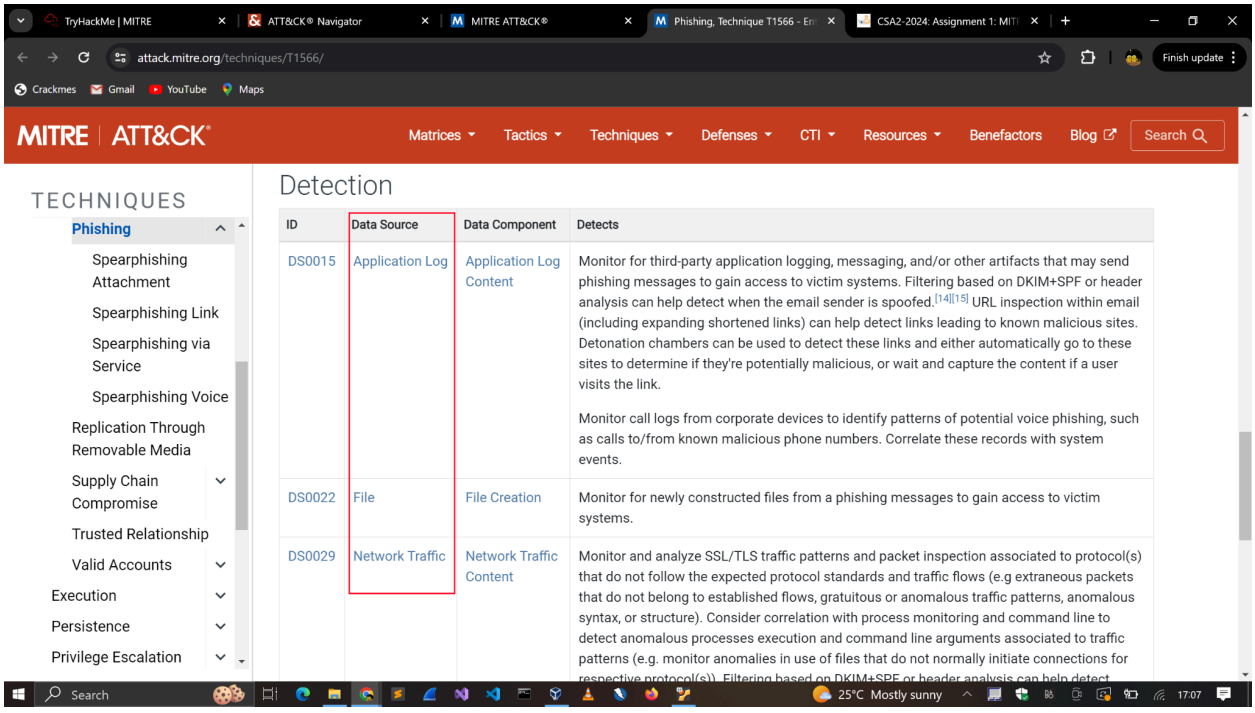
a. **Besides Blue teamers, who else will use the ATT&CK Matrix? (Red Teamers, Purpe Teamers, SOC Managers?)**
   Red Teamers

b. **What is the ID for this technique?**
   Phishing is a technique within the Initial access Tactic with an ID T1566

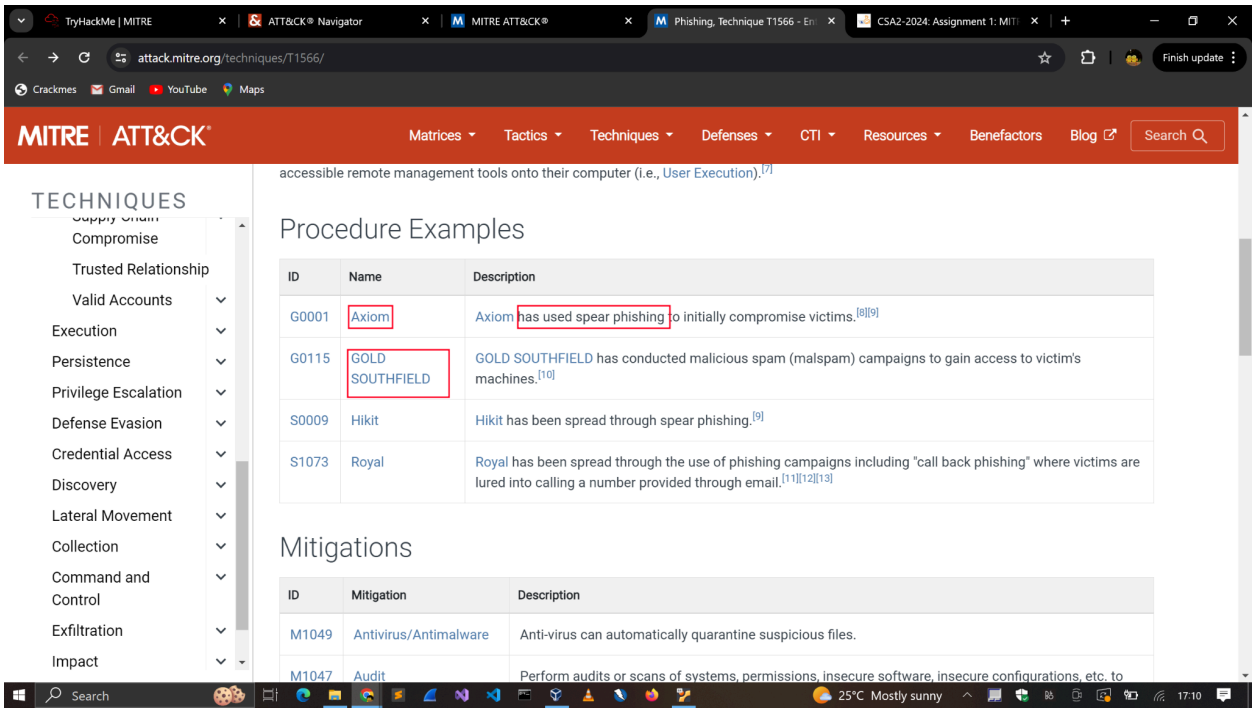
c. **Based on this technique, what mitigation covers identifying social engineering techniques?**



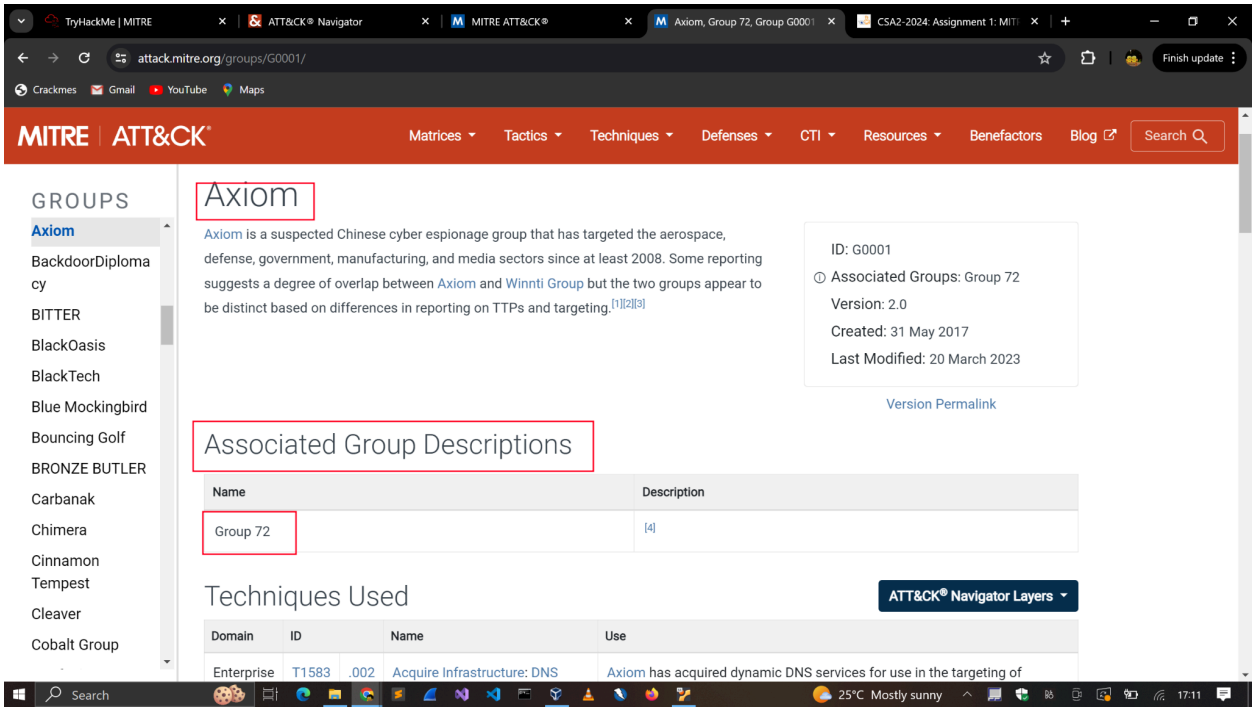
d. What are the data sources for Detection? (format: source1,source2,source3 with no spaces after commas)



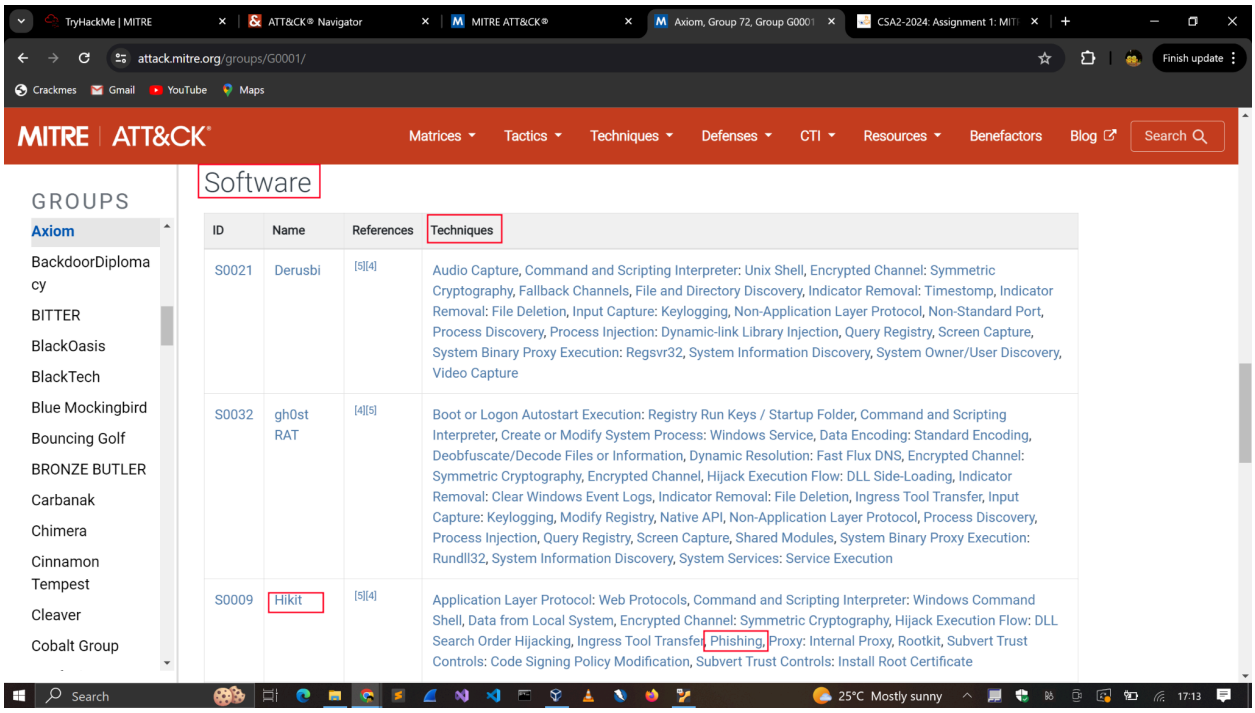
e. What groups have used spear-phishing in their campaigns? (format: group1,group2)



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



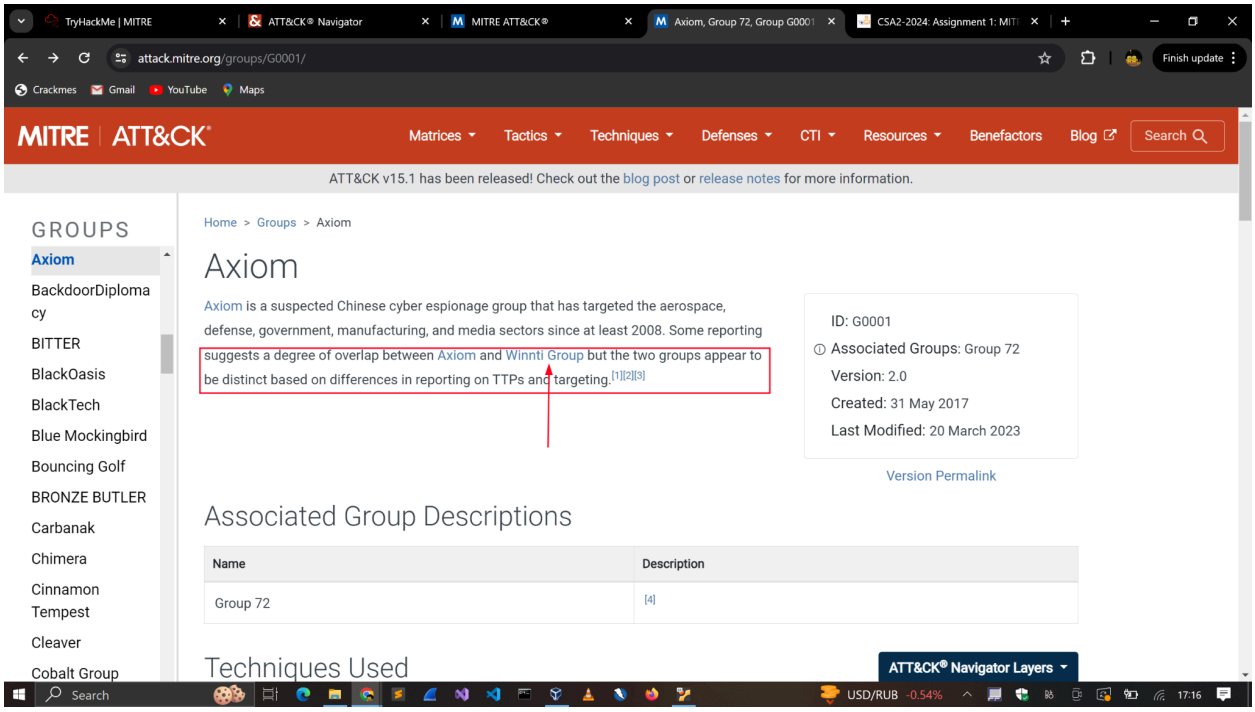
g. What software is associated with this group that lists phishing as a technique?



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?**

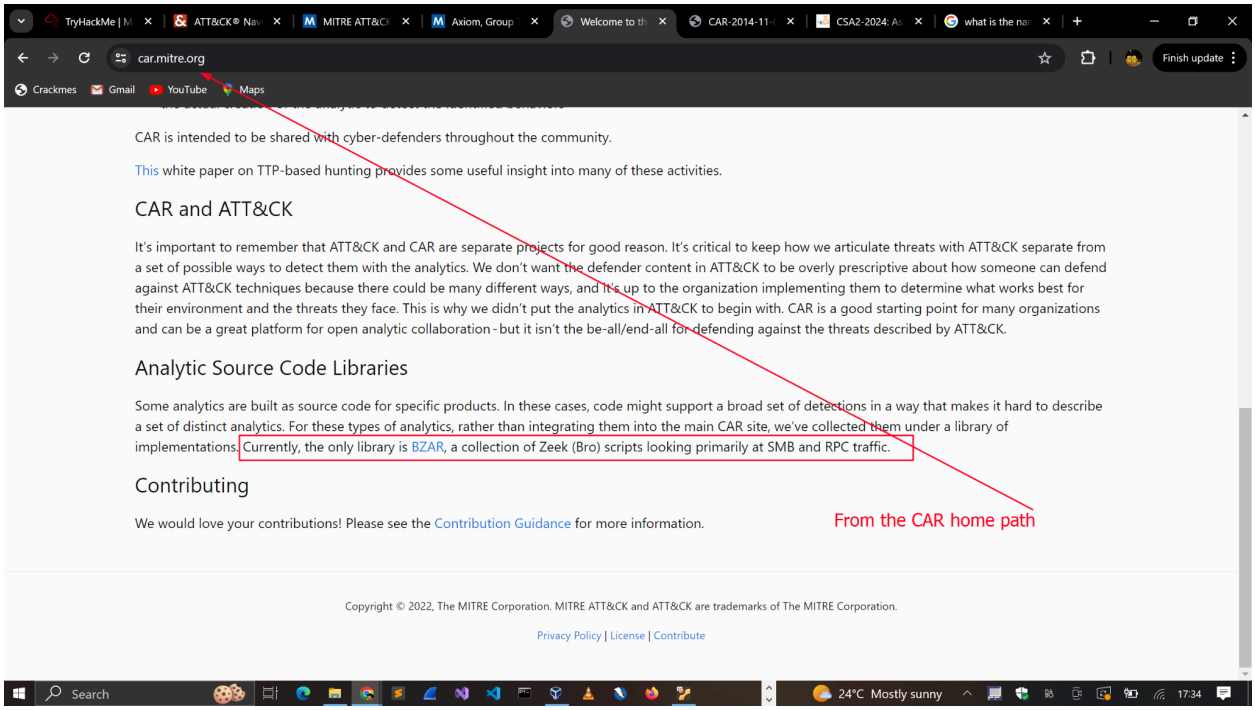


j. **How many techniques are attributed to this group?**
I recorded a count of 15.

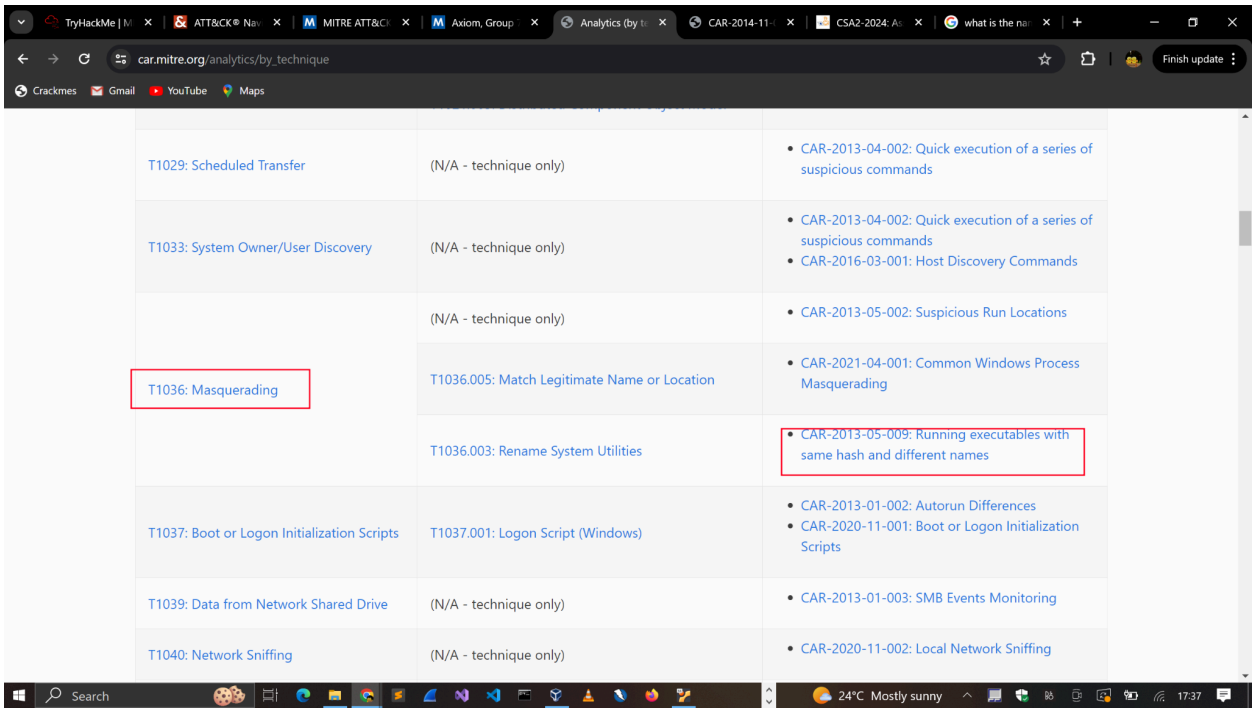
Cyber Analytics Repository

a. **What tactic has an ID of TA0003?**
Persistence

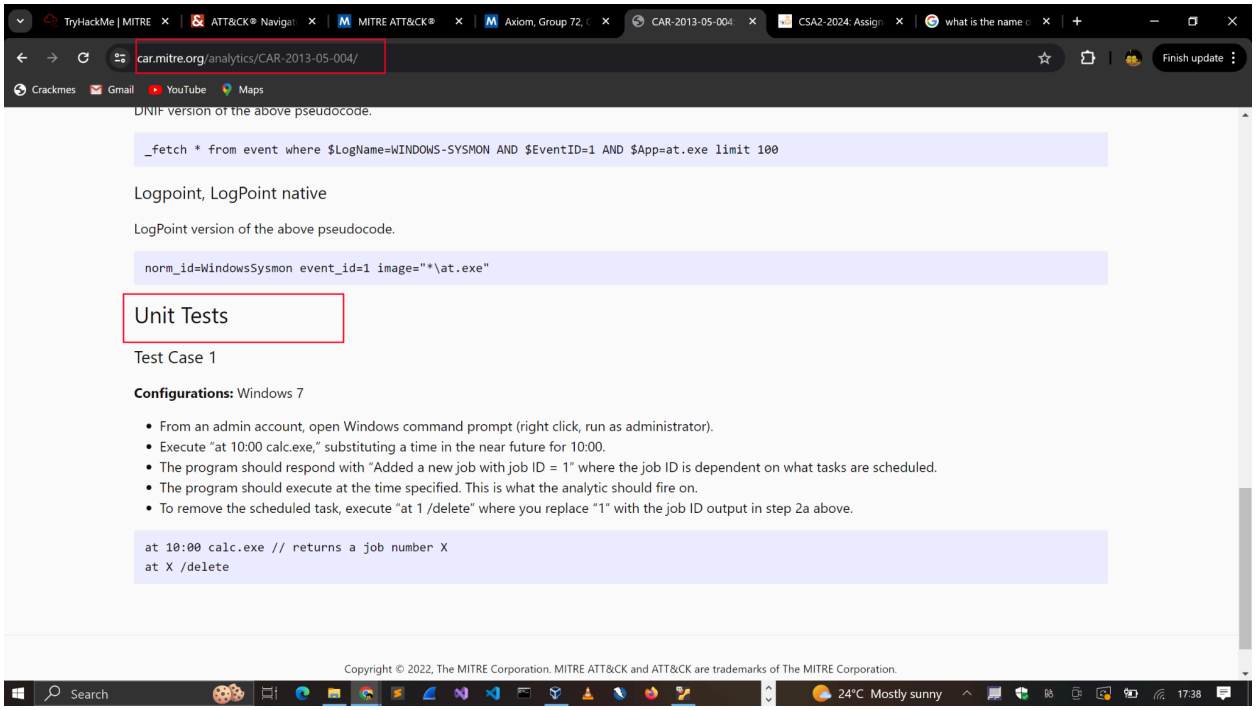
b. **What is the name of the library that is a collection of Zeek (BRO) scripts?**



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

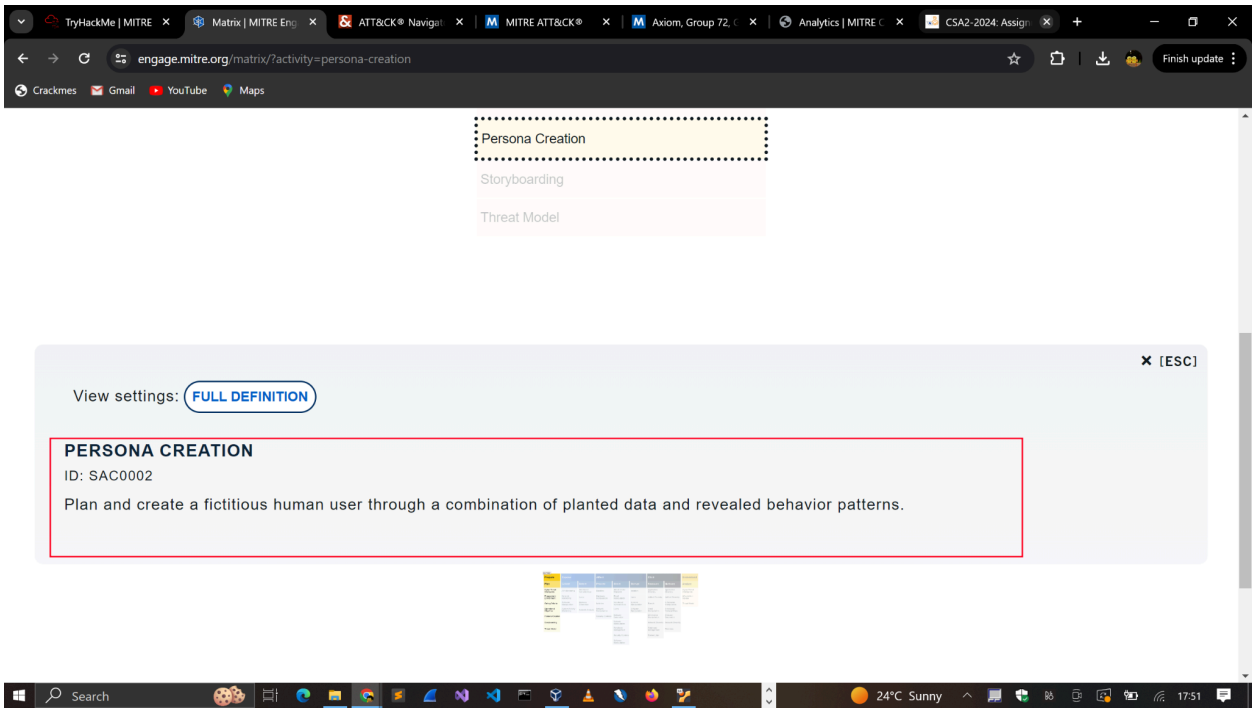


d. Examine CAR-2013-05-004, besides Implementations, what additional information is provided to analysts to ensure coverage for this technique?



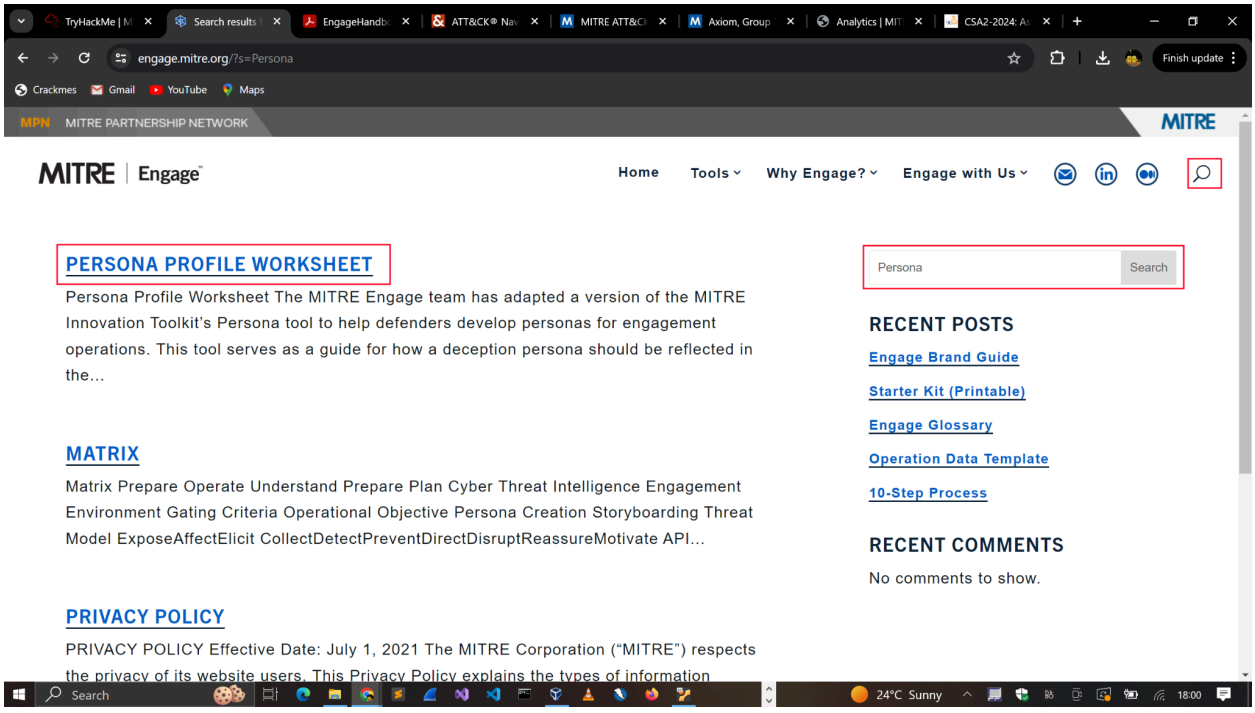
MITRE ENGAGE

a. Under Prepare, what is ID SAC0002?

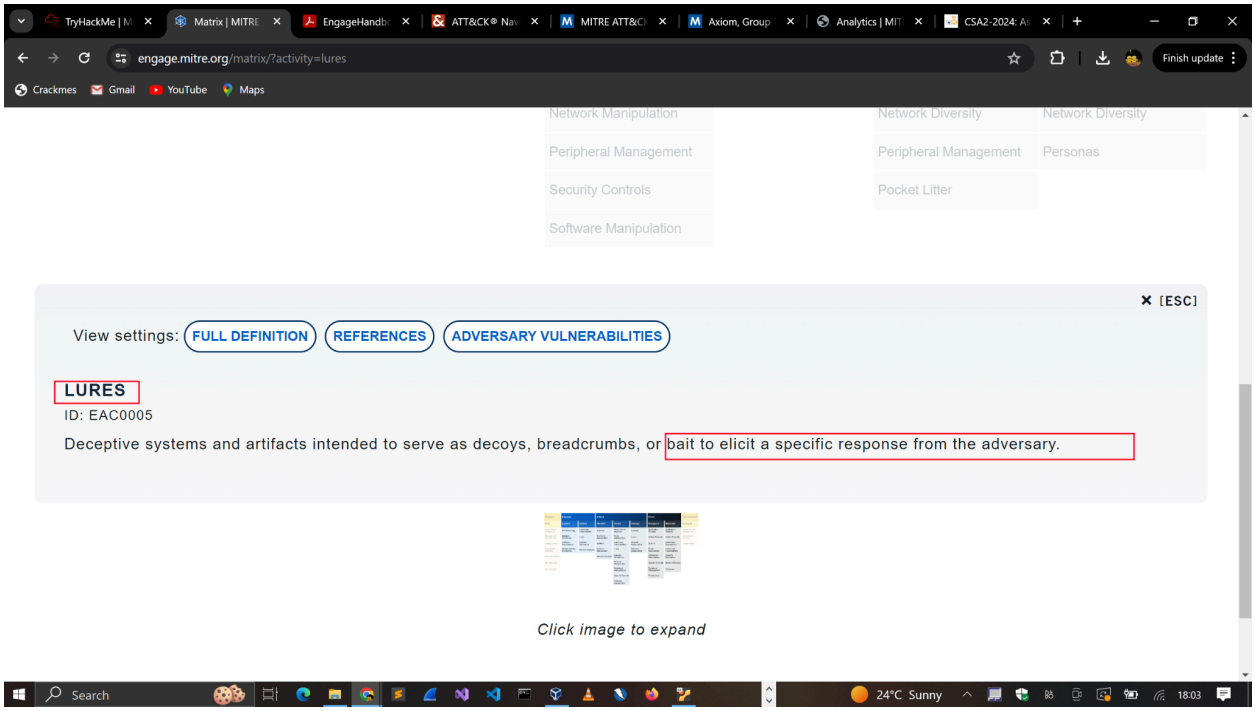


b. What is the name of the resource to aid you with the engagement activity from the previous question?

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



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

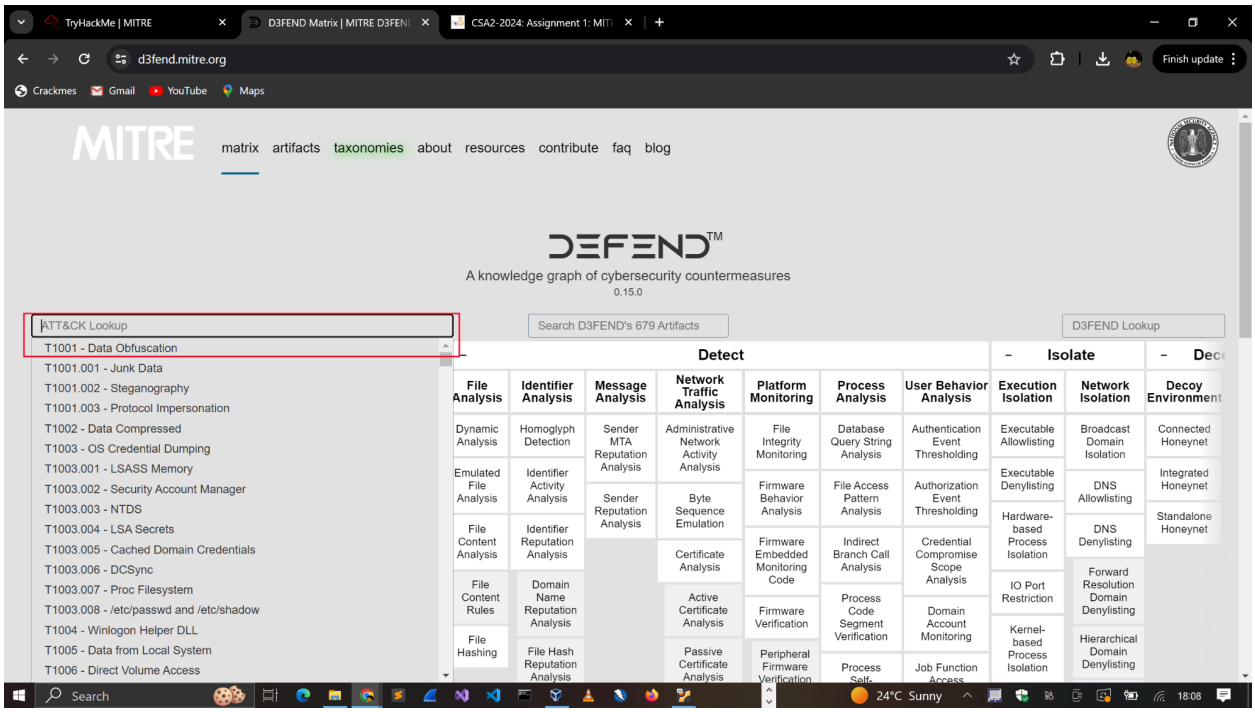


d. What is the definition of Threat Model?

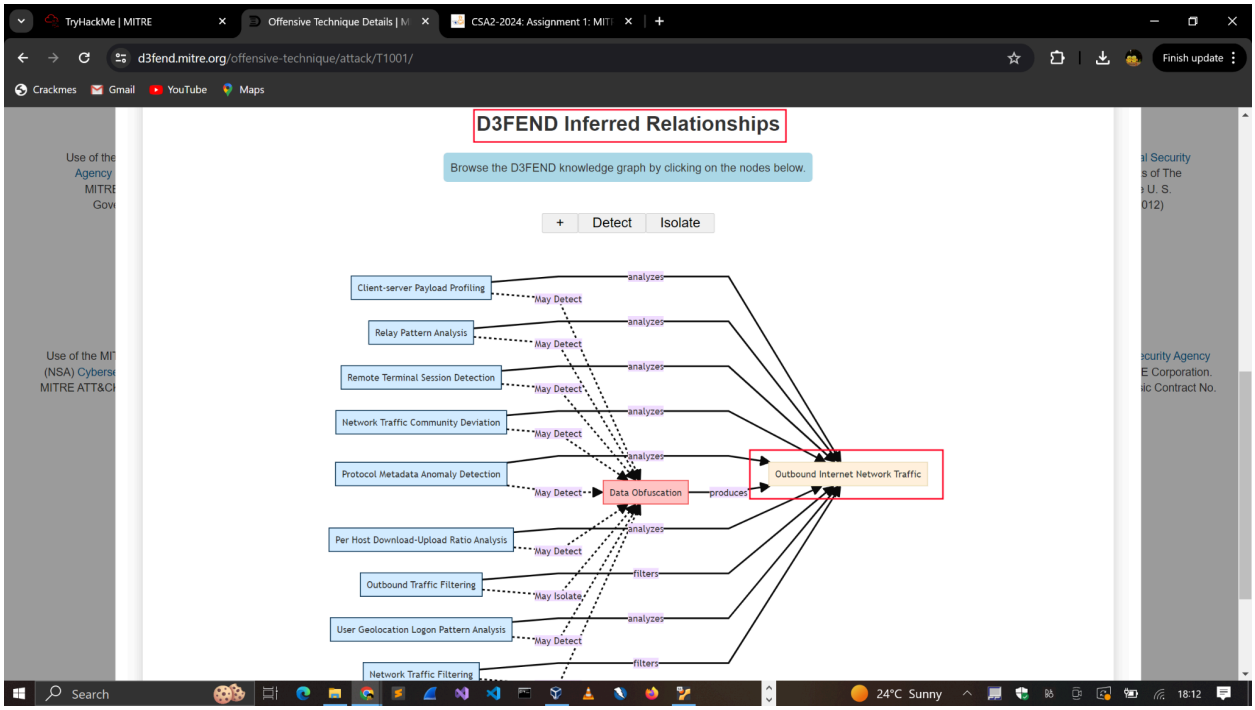
From Mitre Engage > Prepare tab > Threat model, a threat model is defined as a risk assessment that models organizational strengths and weaknesses.

MITRE DEFEND

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



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

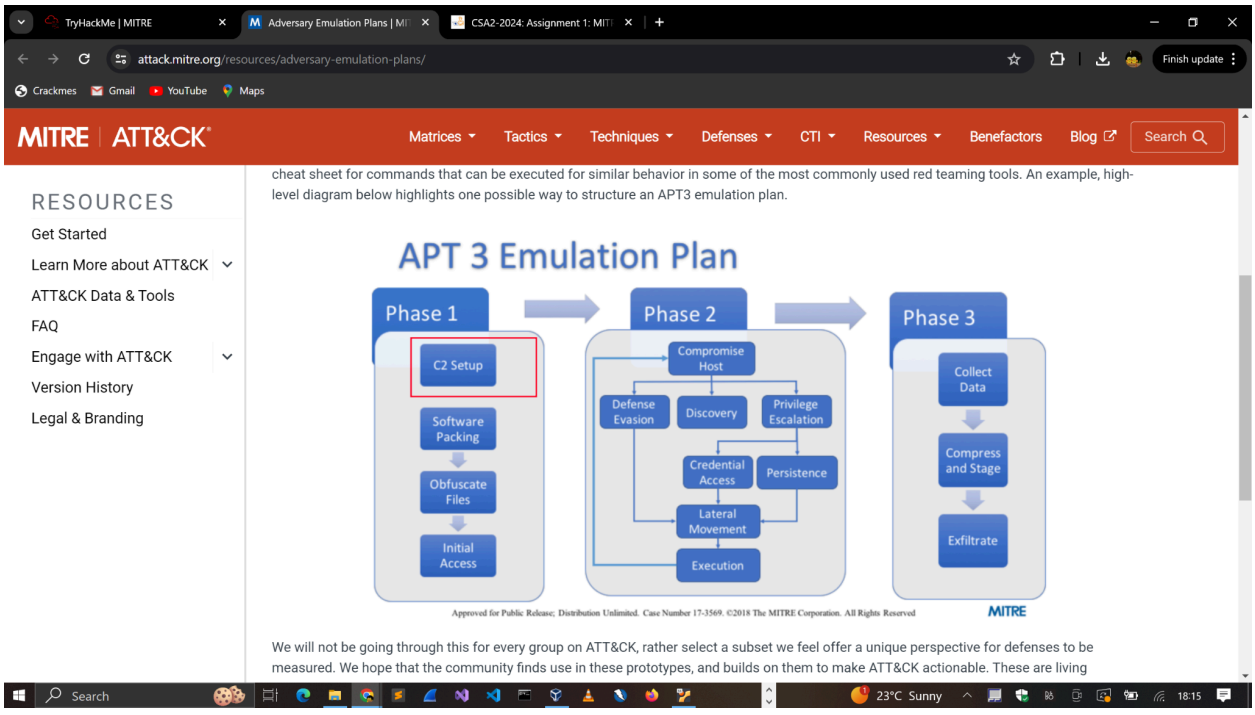


ATT&CK Emulation Plans

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

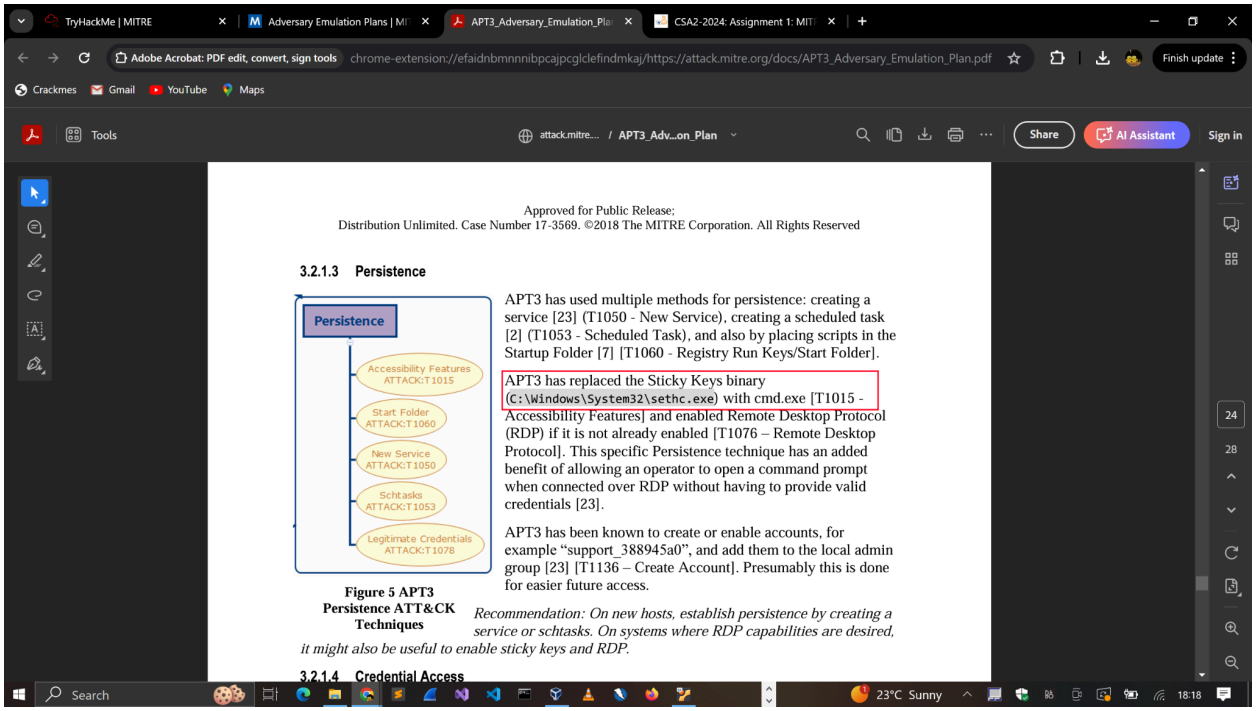
a. **In Phase 1 for the APT3 Emulation Plan, what is listed first?**

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



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].

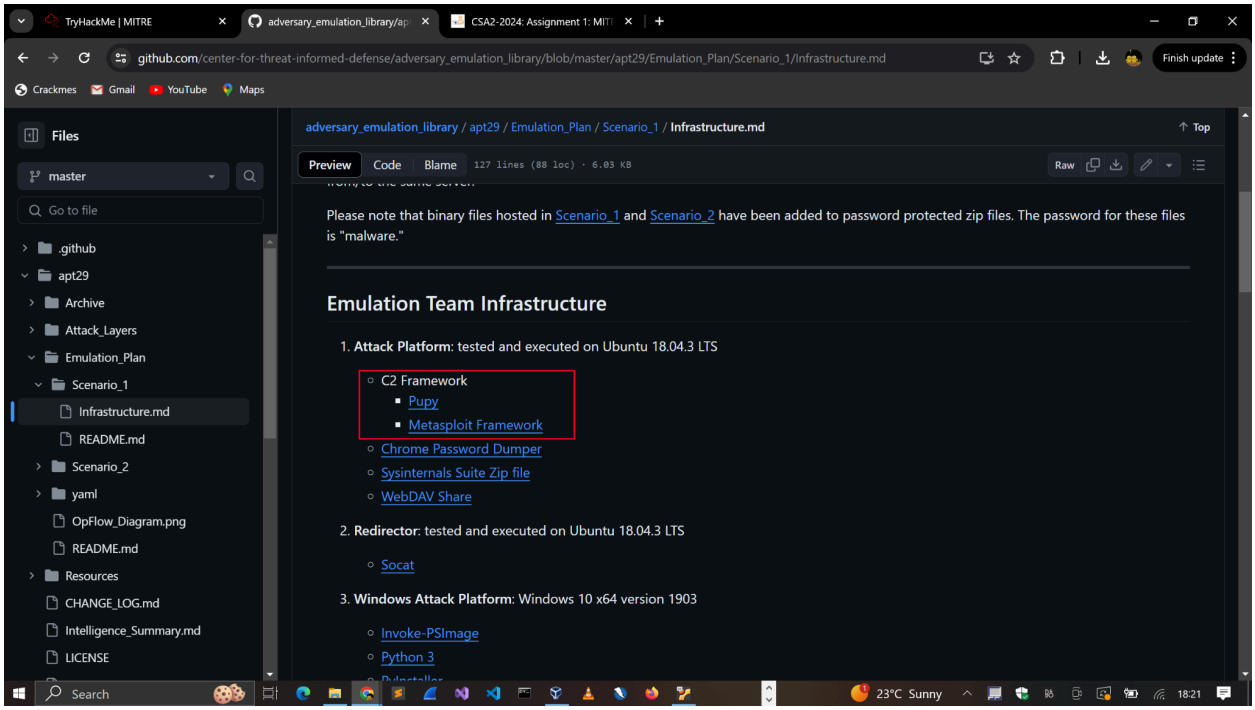
APT3 has been known to create or enable accounts, for example "support_388945a0", and add them to the local admin group [23] [T1136 – Create Account]. Presumably this is done for easier future access.

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)

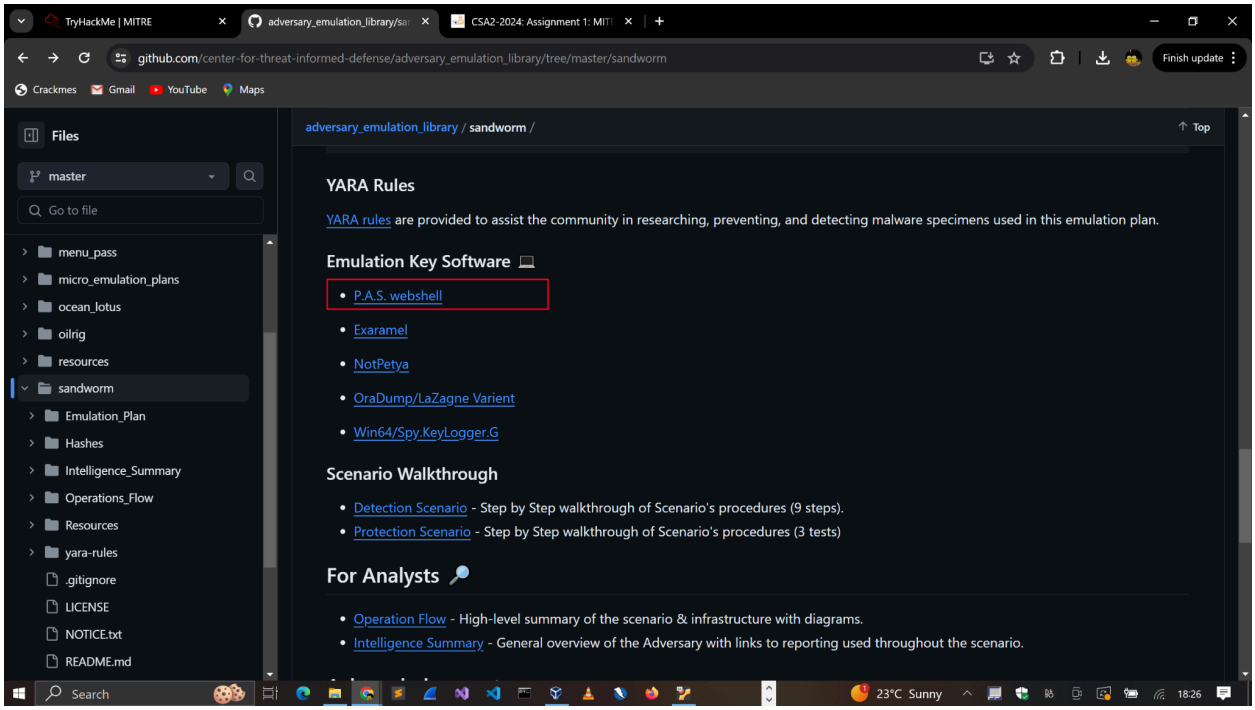
https://github.com/center-for-threat-informed-defense/adversary_emulation_library/tree/master/apt29

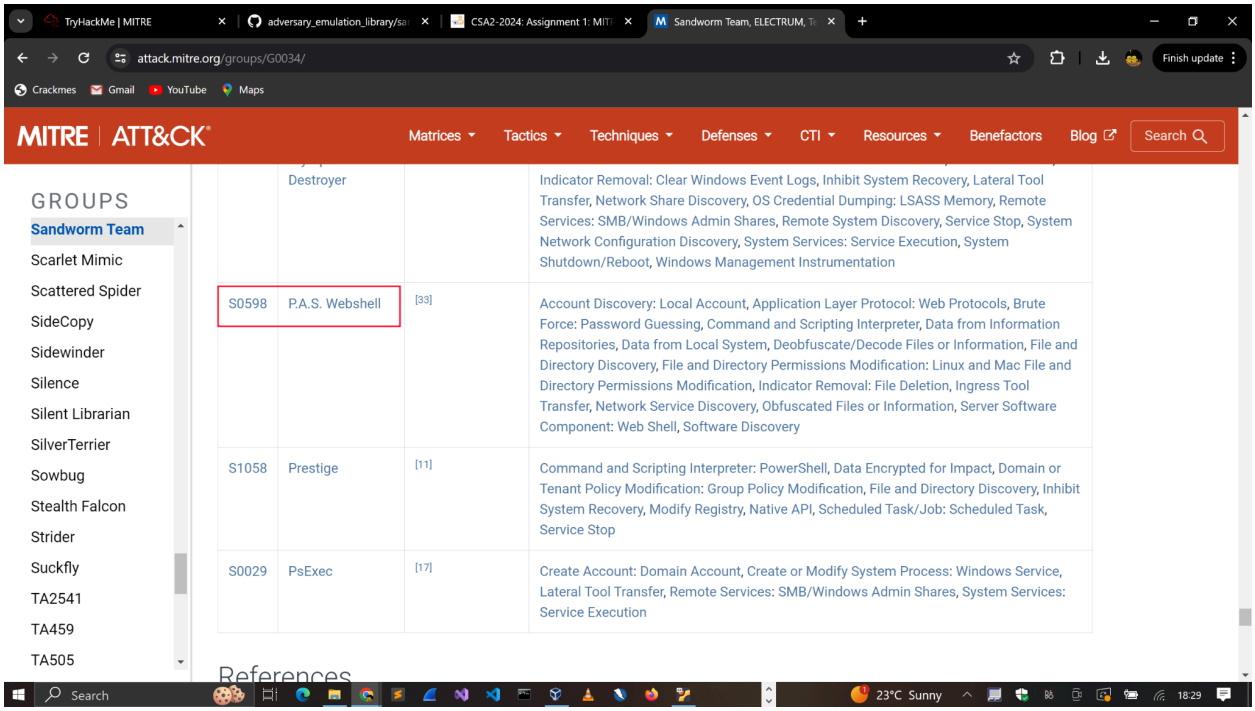


d. What C2 framework is listed in Scenario 2 Infrastructure?

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)

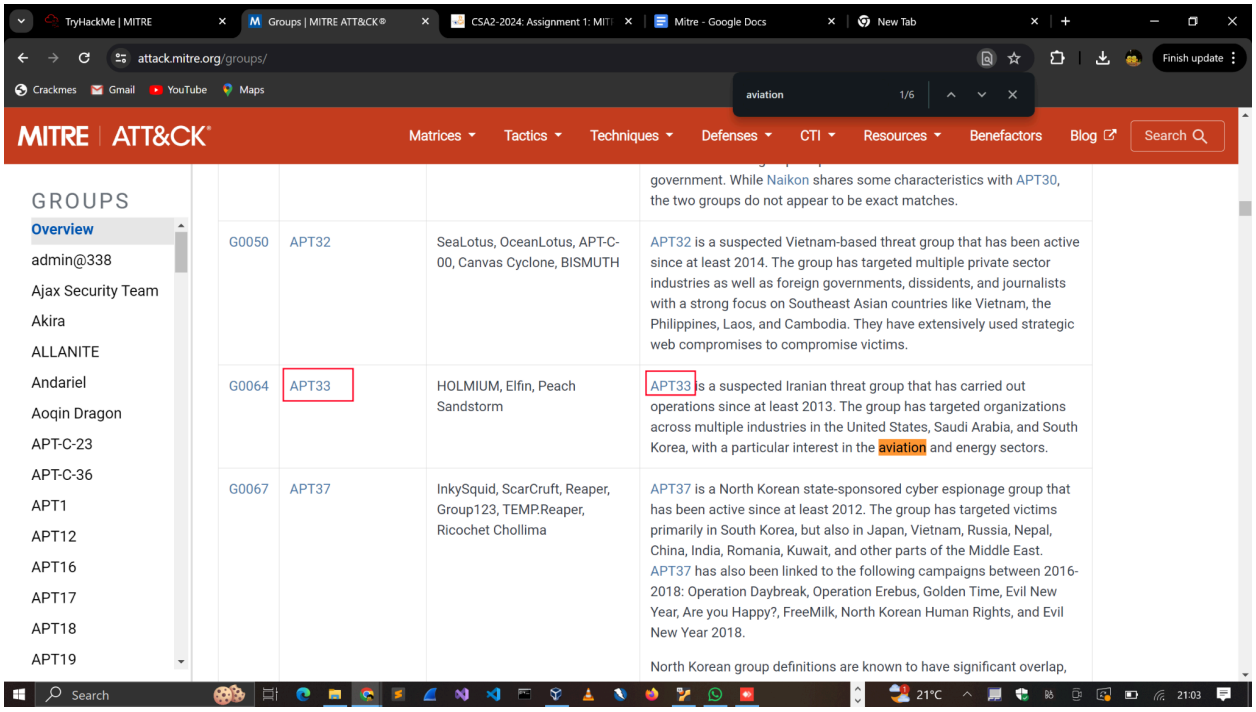

TryHackMe | MITRE
adversary_emulation_library/sa
CSA2-2024: Assignment 1: MIT
github.com/center-for-threat-informed-defense/adversary_emulation_library/tree/master/sandworm
Finish update
Crackmes
Gmail
YouTube
Maps
Files
master
Go to file
menu_pass
micro_emulation_plans
ocean_lotus
oilrig
resources
sandworm
Emulation_Plan
Hashes
Intelligence_Summary
Operations_Flow
Resources
yara-rules
.gitignore
LICENSE
NOTICE.txt
README.md
adversary_emulation_library / sandworm /
Top
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 Varient
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.
Search
23°C Sunny
18:26


TryHackMe | MITRE
adversary_emulation_library/sa
CSA2-2024: Assignment 1: MIT
Sandworm Team, ELECTRUM, T
attack.mitre.org/groups/G0034/
Finish update
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
Search
23°C Sunny
18:29

ATT&CK and Threat Intelligence

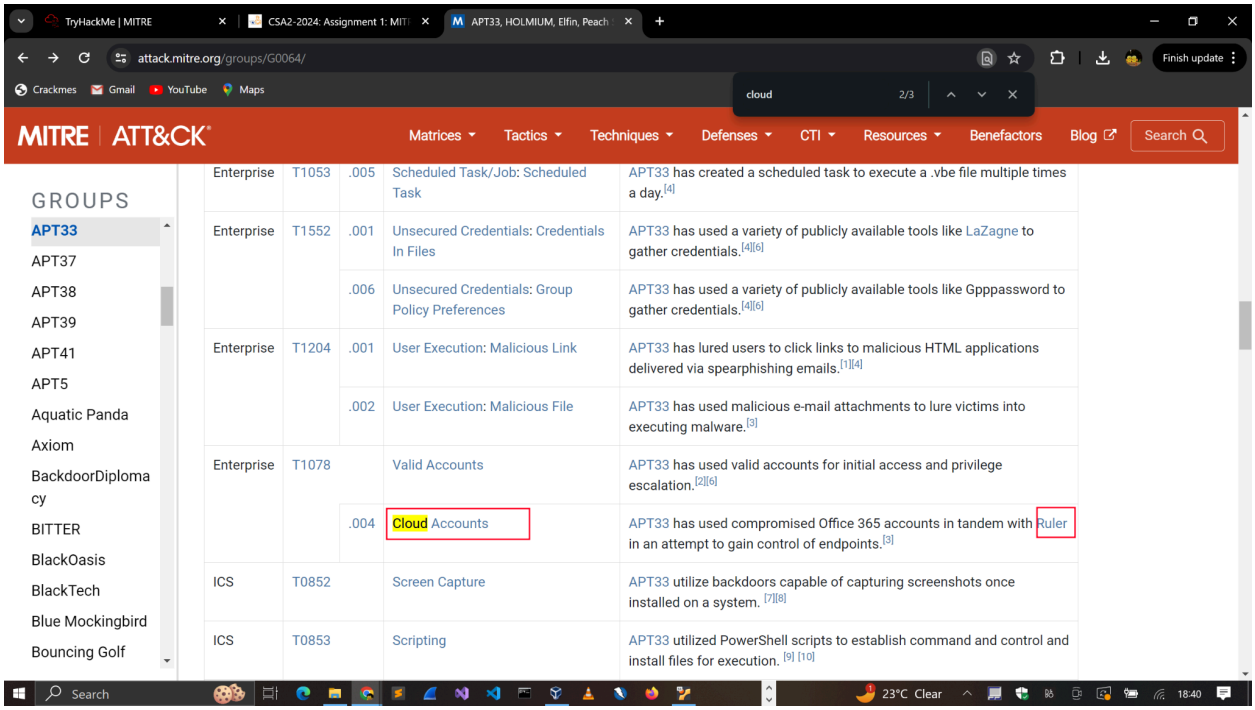
Scenario: You are a security analyst who works in the aviation sector. Your organization is moving their infrastructure to the cloud. Your goal is to use the ATT&CK® Matrix to gather threat intelligence on APT groups who might target this particular sector and use techniques targeting your areas of concern. 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?**

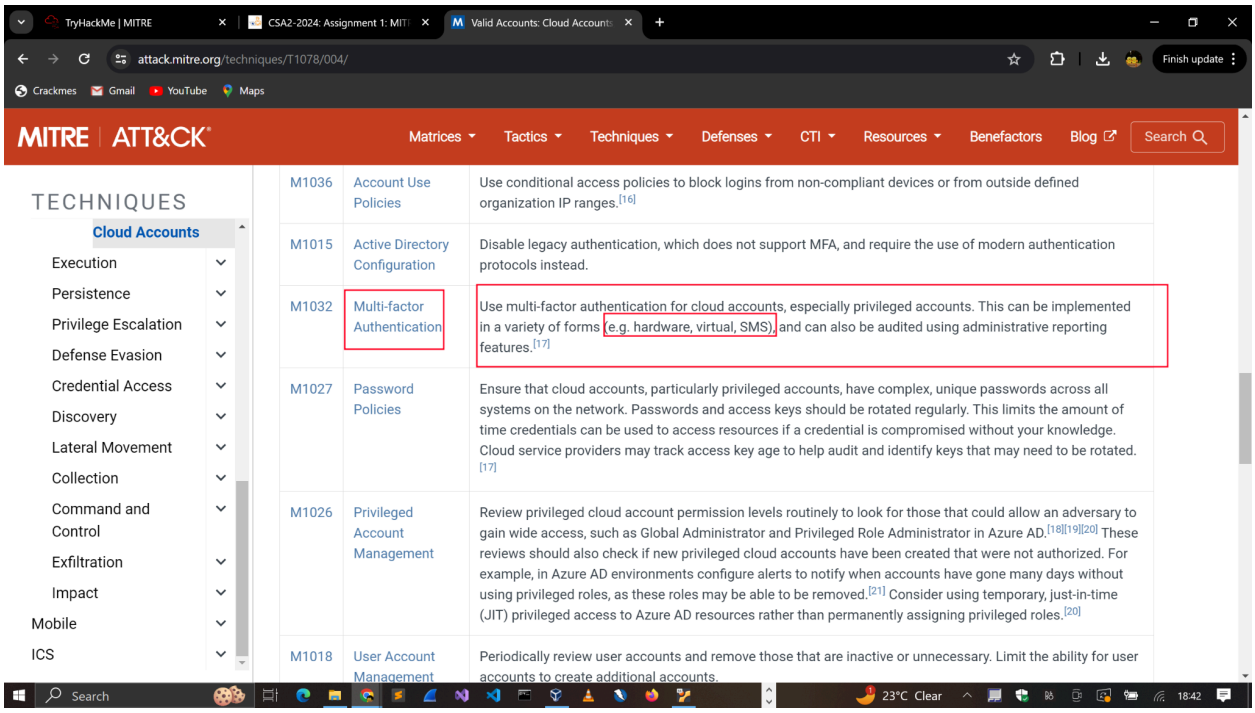


b. **As your organization is migrating to the cloud, is there anything attributed to this APT group that you should focus on? If so, what is it?**

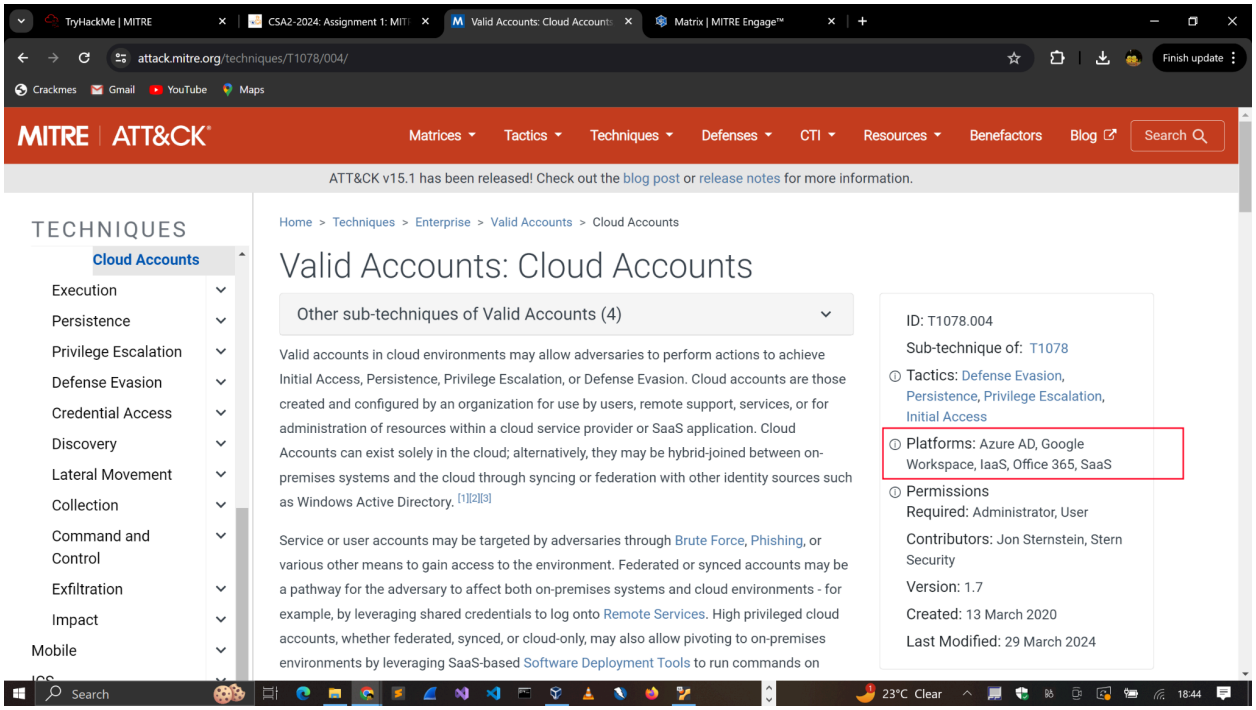
c. **What tool is associated with the technique from the previous question?**



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

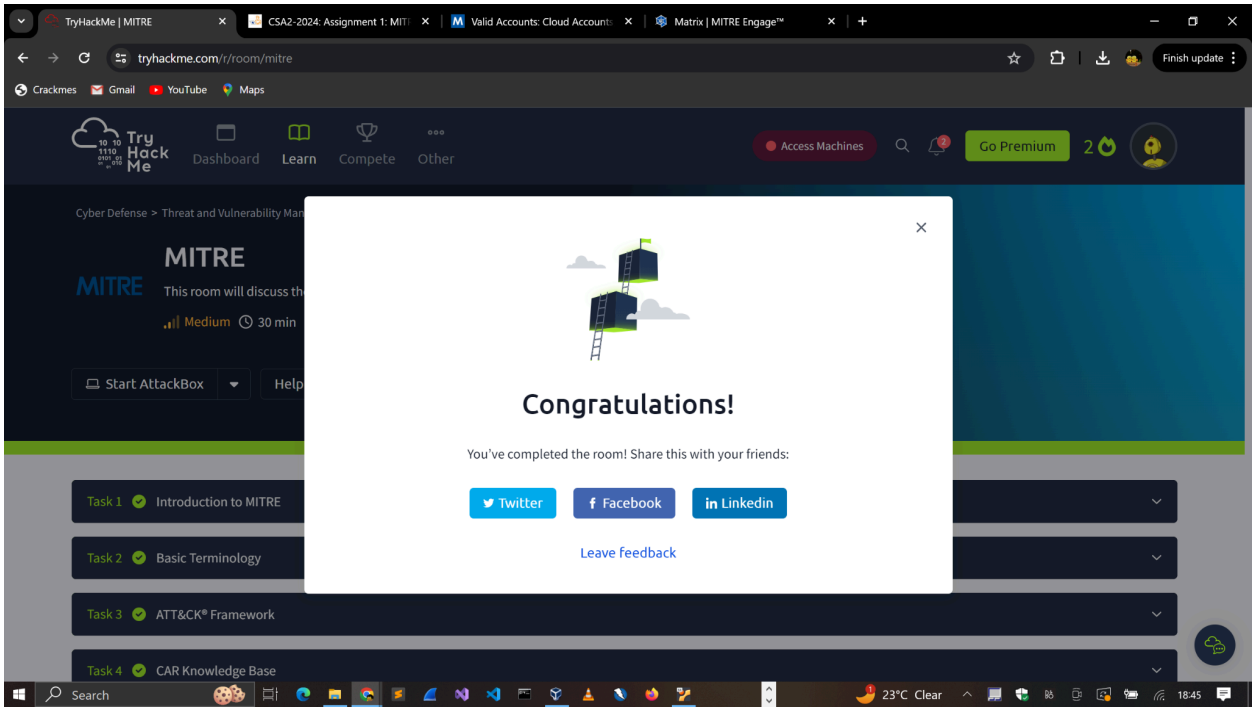


e. What platforms does the technique from question #2 affect?



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.