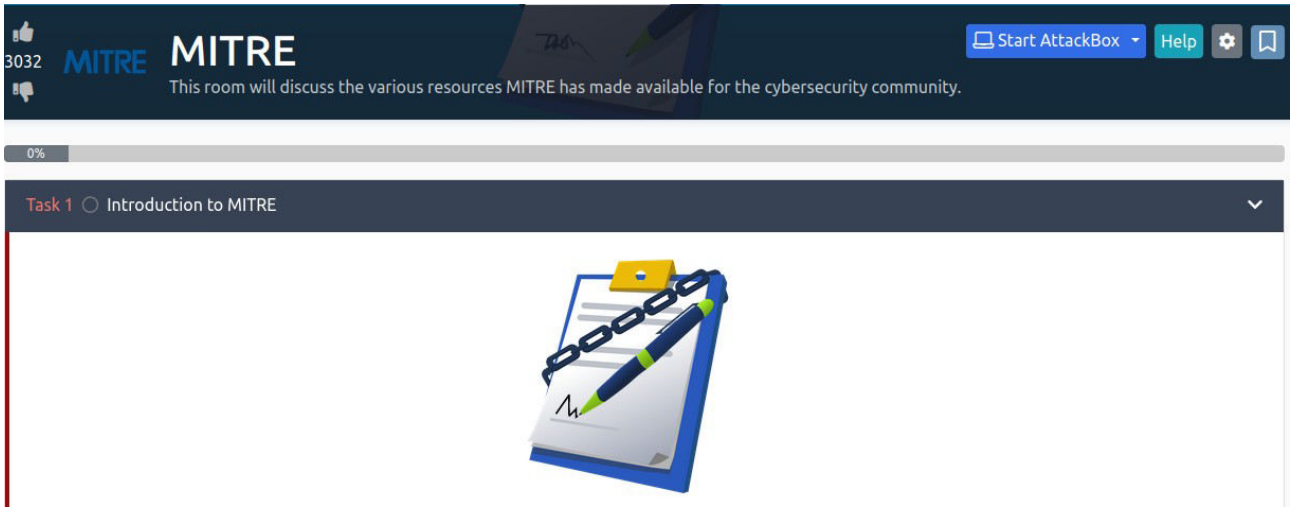
Eric Mwenda

MITRE

https://tryhackme.com/p/Ericm



Introduction to MITRE.

MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.
MITRE is usually associated with CVE (Common Vulnerabilities and Exposure). MITRE researches in many areas, outside of cybersecurity, for the 'safety, stability, and well-being of our nation.' These areas include artificial intelligence, health informatics, space security, to name a few.

Basic Terminology.

APTs
APT stands for Advanced Persistent Threat. This threats can be carried out by a team/group or even a country that engages in long-term attacks against Organizations and countries.
APT groups are quite common but can only be detected with the right implementations in place.

TTP
TTP stands for Tactic, Techniques and Procedures.
- Tactic is the adversary's goal and objective.
- Techniques is how the adversary achives the goal or objective.
- Procedures is how the technique is executed.

ATT&CK®
From this section I learnt that MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations..
I also got to learn that MITRE began to address the need to record and document common TTPs (Tactics, Techniques and Procedures) that APT (Advanced Persistent Threat) groups used against enterprise Windows networks in 2013. This started with an internal project known as FMX (Fort Meade Experiment). Within this project, selected security professionals were tasked to emulated adversarial TTPs against a network, and data was collected from the attacks on this network. The

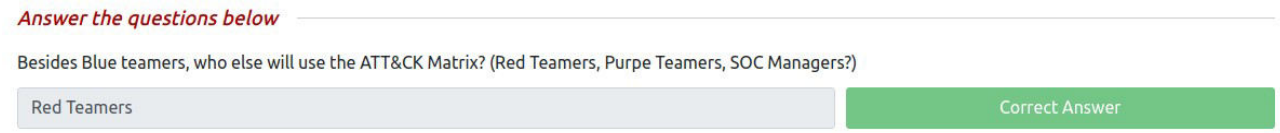
gathered data helped construct the beginning pieces of what we know today as the ATT&CK® framework.

Phishing – Phishing is a technique that frauds practice of sending emails or other messages targeting reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.
All forms of phishing are electronically delivered using social engineering.
Targeted phishing is know as spear phishing.

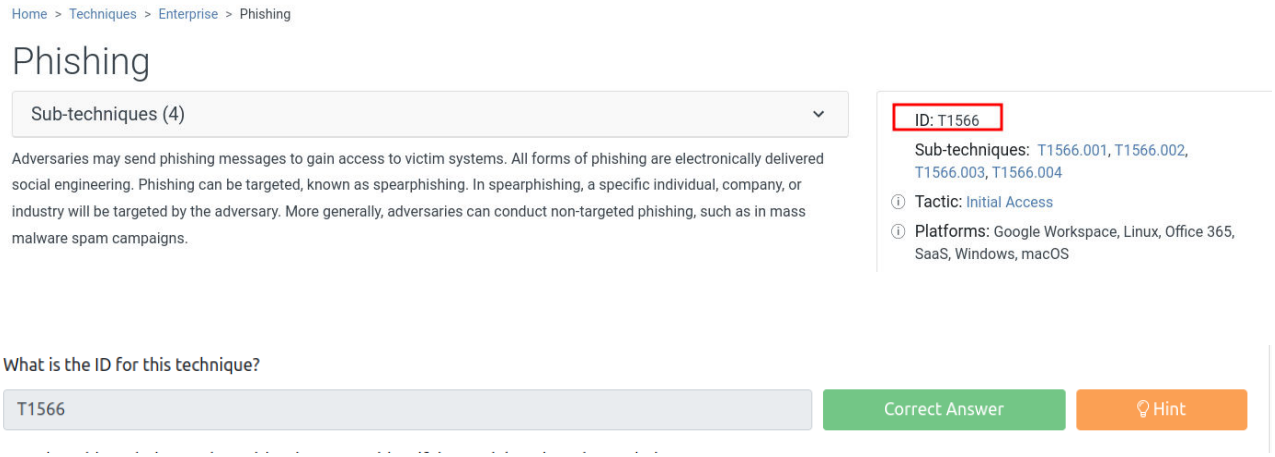
Questions.

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

ANS: <u>Red Teamers.</u> A red team is a group that pretends to be an enemy, attempts a physical or digital intrusion against an organization then reports back so that the organization can improve their defenses.

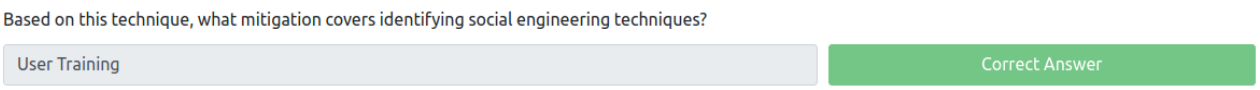


2. What is the ID for this technique? **ANS: <u>T1566.</u>**



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

ANS: <u>User Training.</u> Social engineering training gives people the tools they need to recognize threats, which grooms more discerning, responsible employees who are better equipped to protect both themselves and their organization.



4. What are the data sources for Detection? **(**format: source1,source2,source3 with no spaces after commas) **ANS: Application Log,File,Network Traffic**

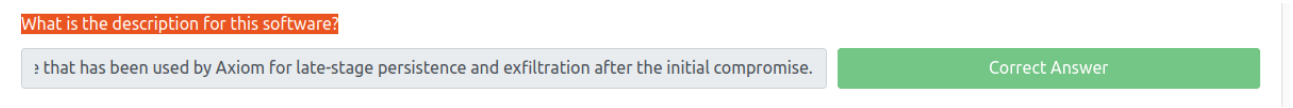
5. What groups have used spear-phishing in their campaigns? (**format: group1,group2**)
ANS: Axiom,GOLD SOUTHFIELD

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]

6. Based on the information for the first group, what are their associated groups?
ANS: Group 72

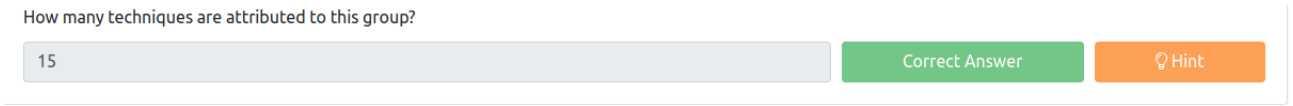
7. What software is associated with this group that lists phishing as a technique?
ANS: Hikit

8. What is the description for Hikit software?
ANS: Hikit is malware that has been used by Axiom for late-stage persistence and exfiltration after the initial compromise.



9. This group overlaps (slightly) with which other group?
ANS: Winnti Group

10. How many techniques are attributed to this group?
ANS: 15

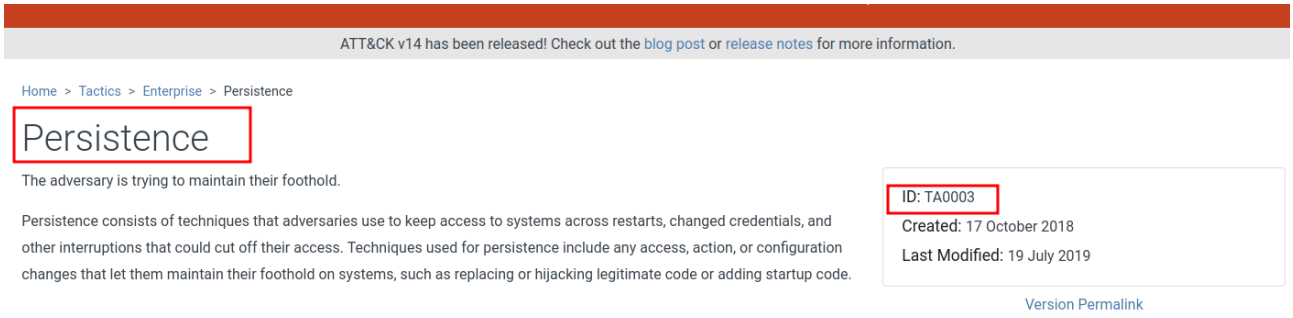


CAR Knowledge Base.

CAR – This represents Cyber Analytics Repository
CAR defines a data model that is leveraged in its pseudocode representations but also includes implementations directly targeted at specific tools (e.g., Splunk, EQL) in its analytics.

Questions

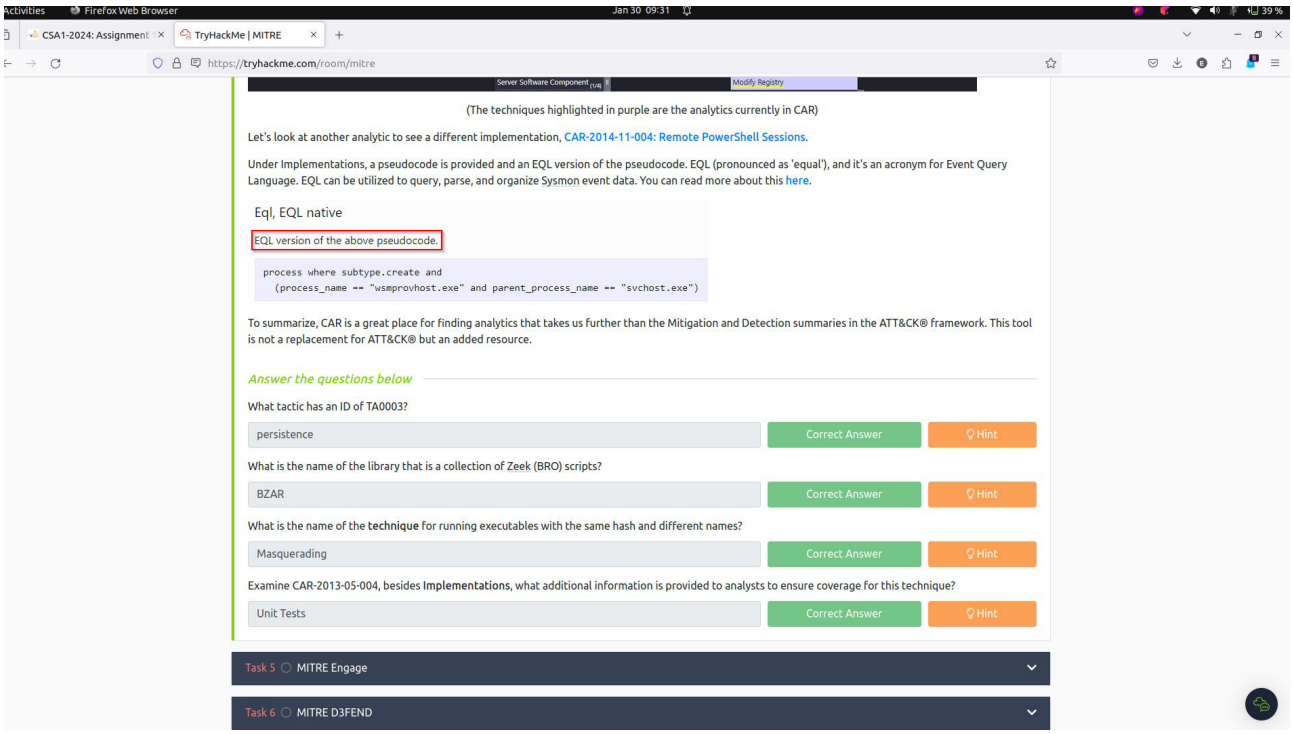
1. What tactic has an ID of TA0003? **ANS: persistence**



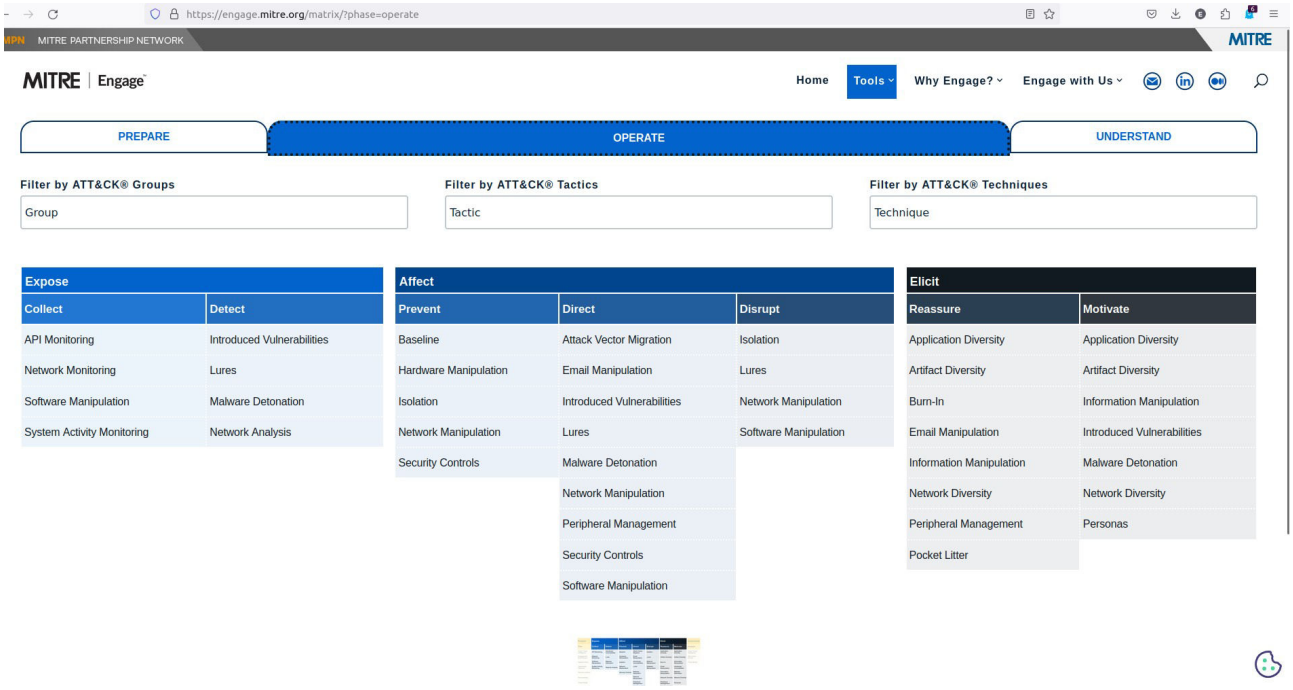
2. What is the name of the library that is a collection of Zeek (BRO) scripts? **ANS: <u>BZAR</u>**

3. What is the name of the technique for running executables with the same hash and different names? ANS: **<u>Masquerading</u>**

4. Examine CAR-2013-05-004, besides Implementations, what additional information is provided to analysts to ensure coverage for this technique? **ANS: <u>Unit Tests</u>**



MITRE Engage

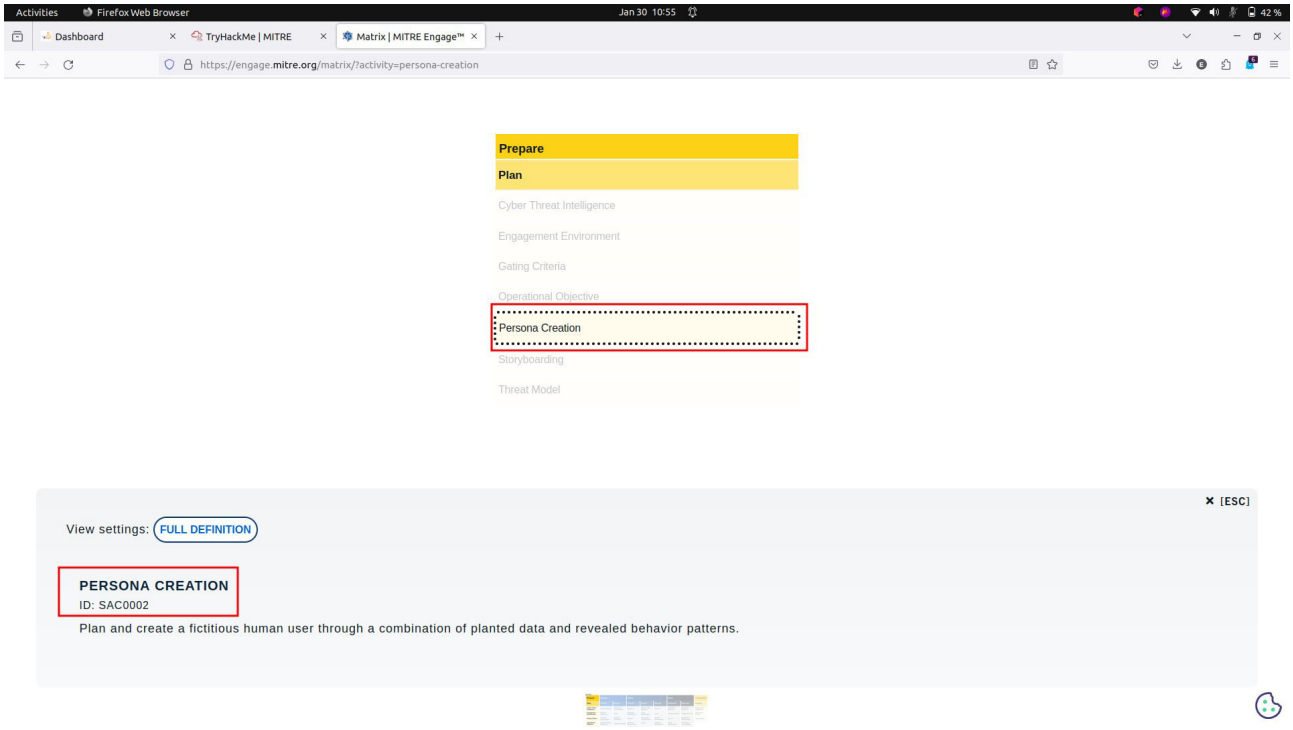


In this section I gained basic knowledge about the Engage Matrix website, which has different categories. This categories are explained as follows:-

1. Prepare – This focuses on a set of operational actions that will lead to your desired outcome (input)
2. Expose – This is when adversaries when they trigger your deployed deception activities
3. Affect – Here is where adversaries by performing malicious actions they impact negatively on operations
4. Elicit – This is gathering information by observing the adversary and learn more about their modus operandi (TTPs)
5. Understand – In this category we have the outcomes of the operational actions (output)

Question

1. Under Prepare, what is ID SAC0002? **ANS: Persona Creation**

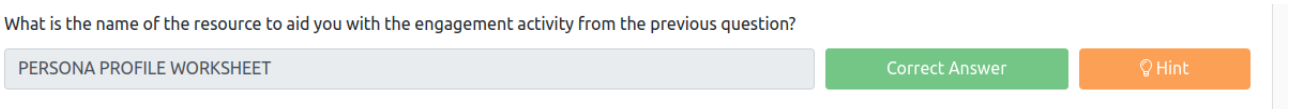


Answer the questions below

Under Prepare, what is ID SAC0002?

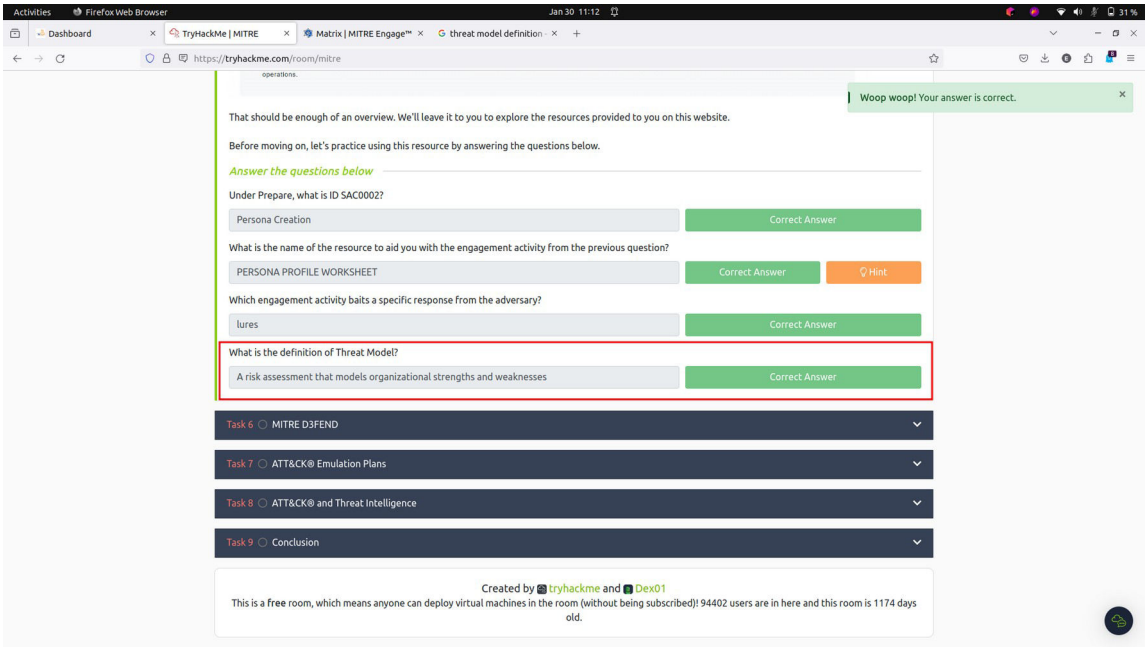
Persona Creation — Correct Answer

2. What is the name of the resource to aid you with the engagement activity from the previous question? **ANS: PERSONA PROFILE WORKSHEET**



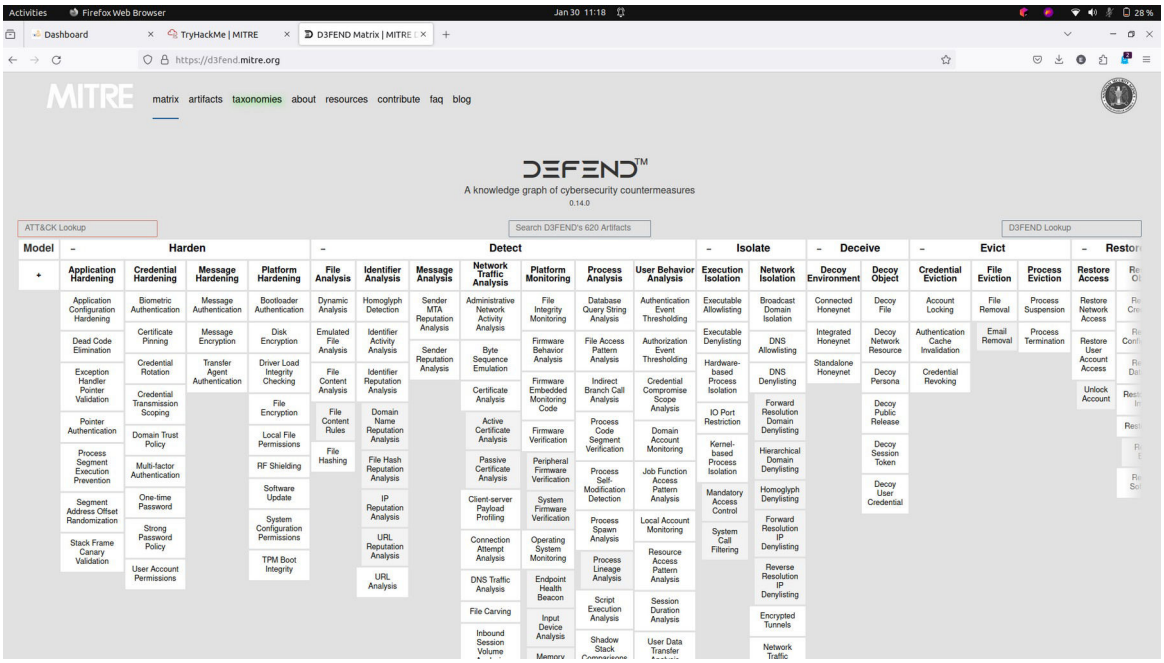
3. Which engagement activity baits a specific response from the adversary? **ANS: Lures**

4. What is the definition of Threat Model? **ANS: <u>A risk assessment that models organizational strengths and weaknesses</u>**



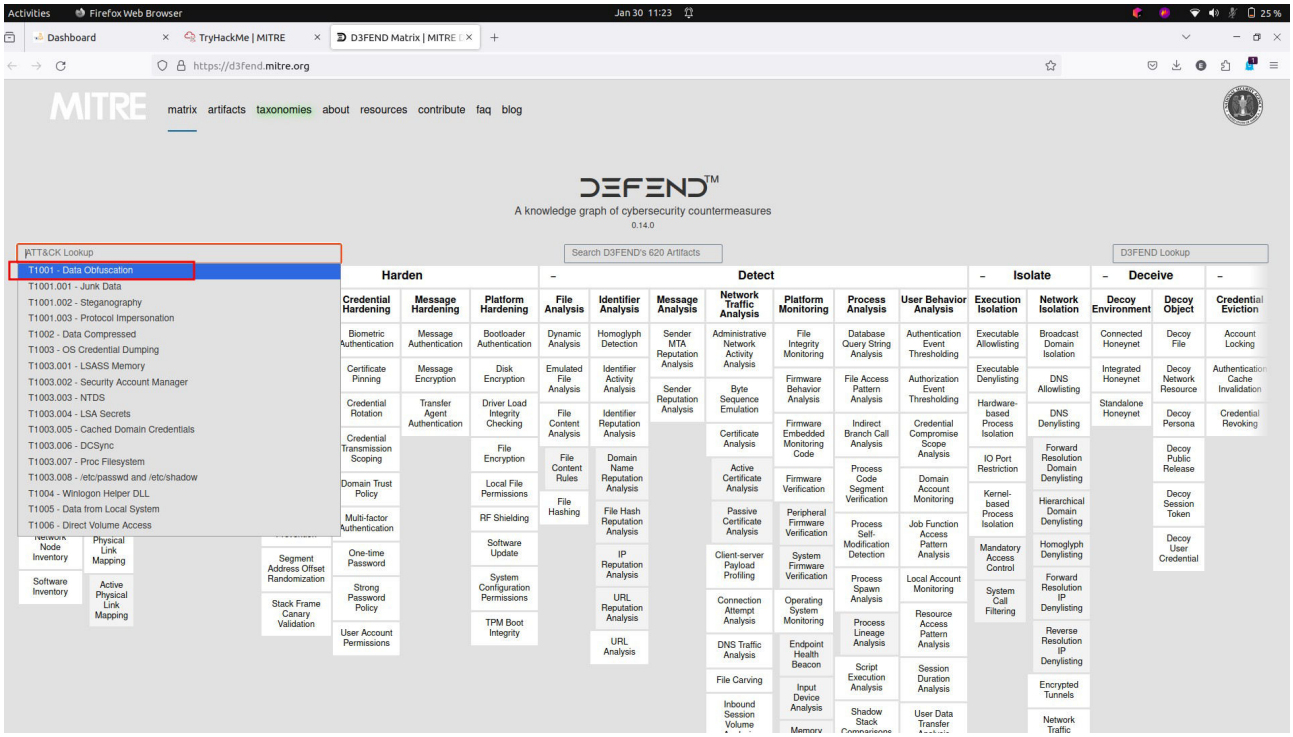
<u>MITRE D3FEND</u>

<u>D3FEND</u> stands for Detection, Denial, and Disruption Framework Empowering Network Defense.

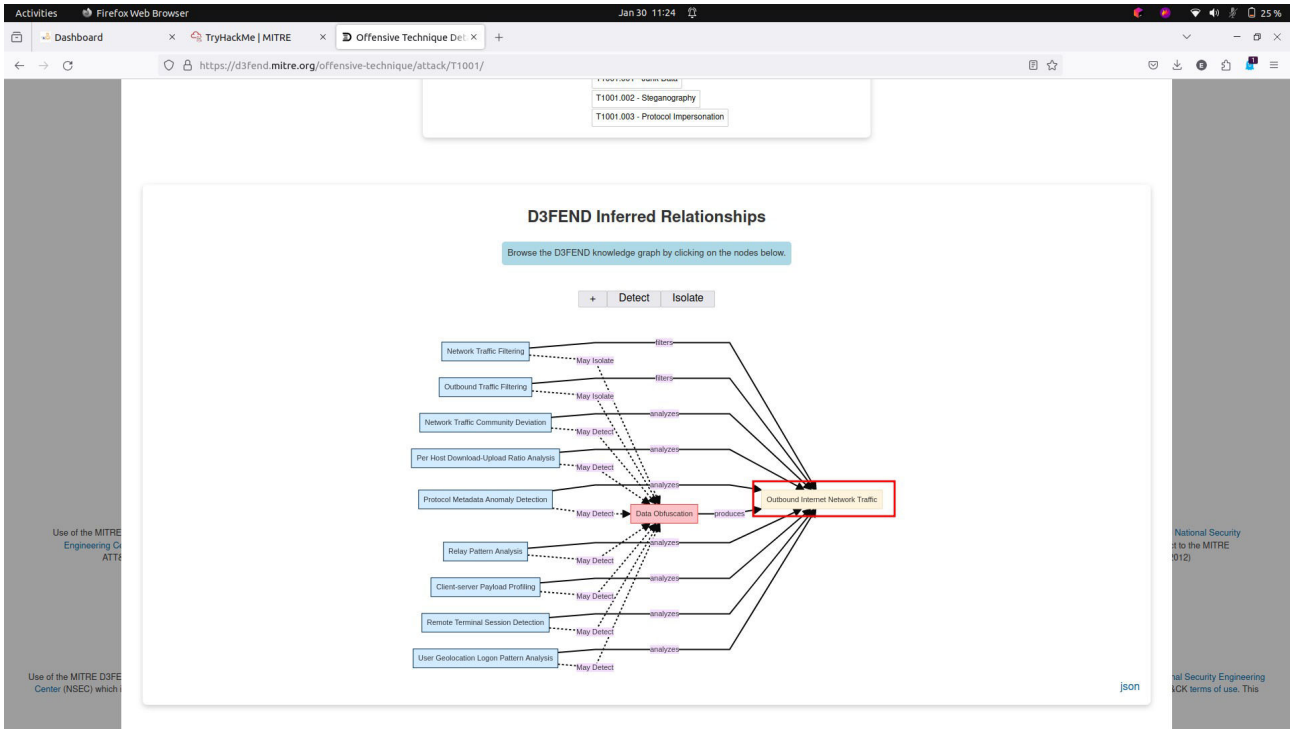


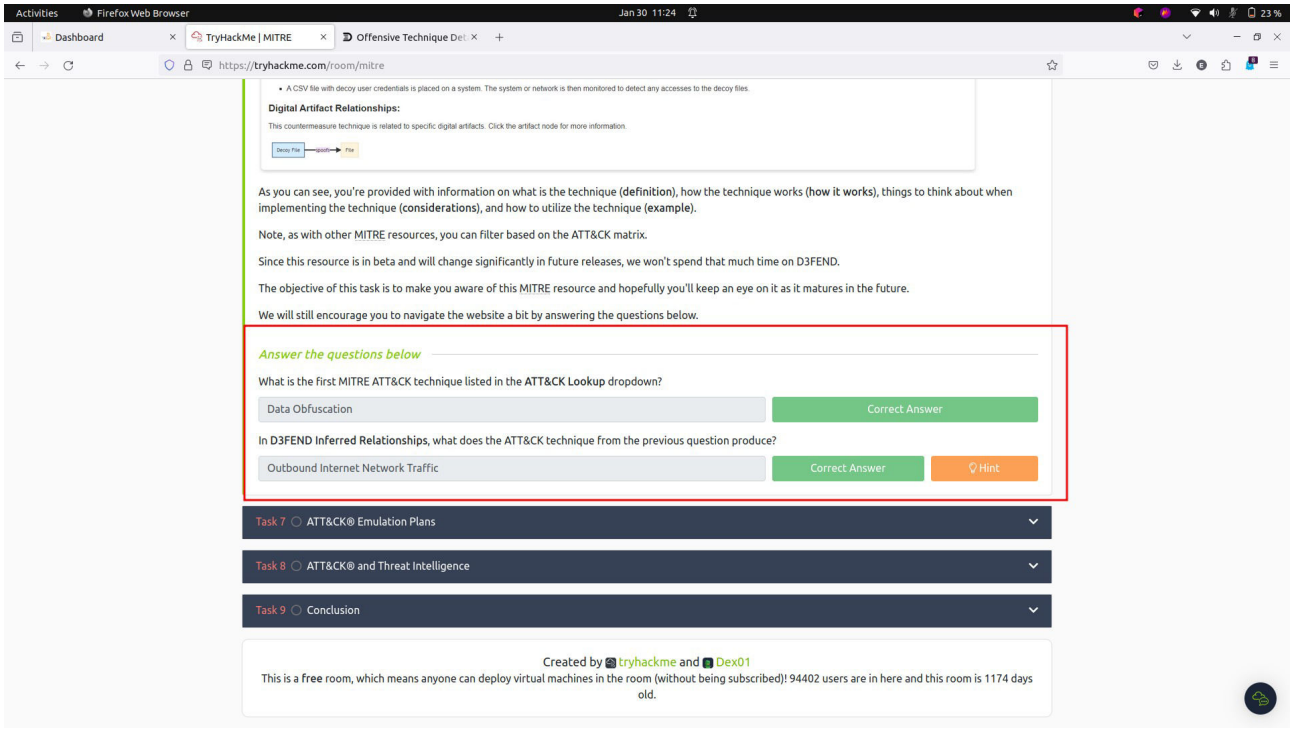
Questions.

1. What is the first MITRE ATT&CK technique listed in the ATT&CK Lookup dropdown? **ANS: Data Obfuscation**



2. In D3FEND Inferred Relationships, what does the ATT&CK technique from the previous question produces? **ANS: Outbound Internet Network Traffic**

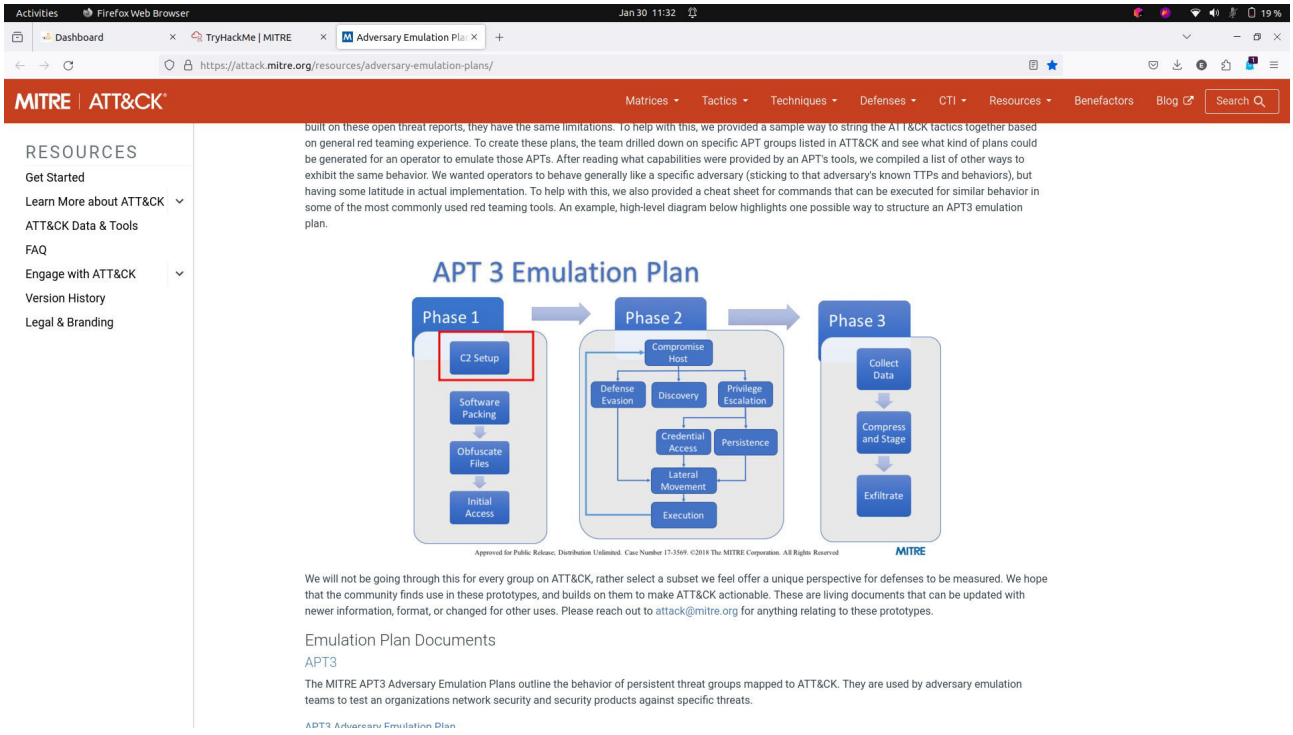




ATT&CK Emulation Plans

In this section another tool is introduced called: **CTID**
CTID – Stands for Center of Threat-Informed defense.

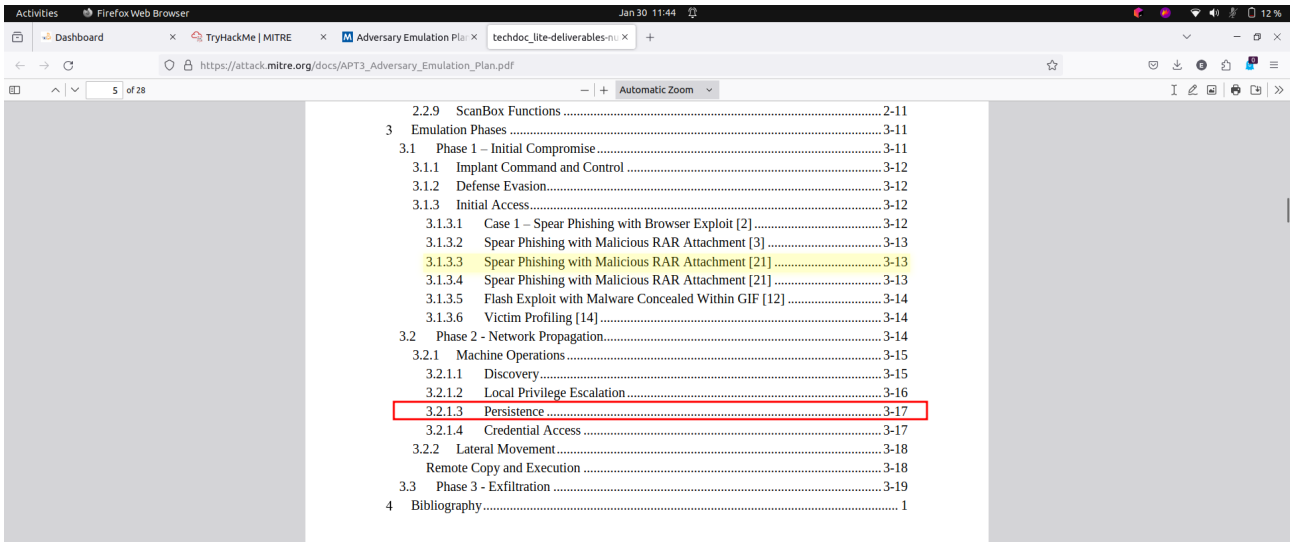
1. In Phase 1 for the APT3 Emulation Plan, what is listed first? **ANS: C2 Setup**

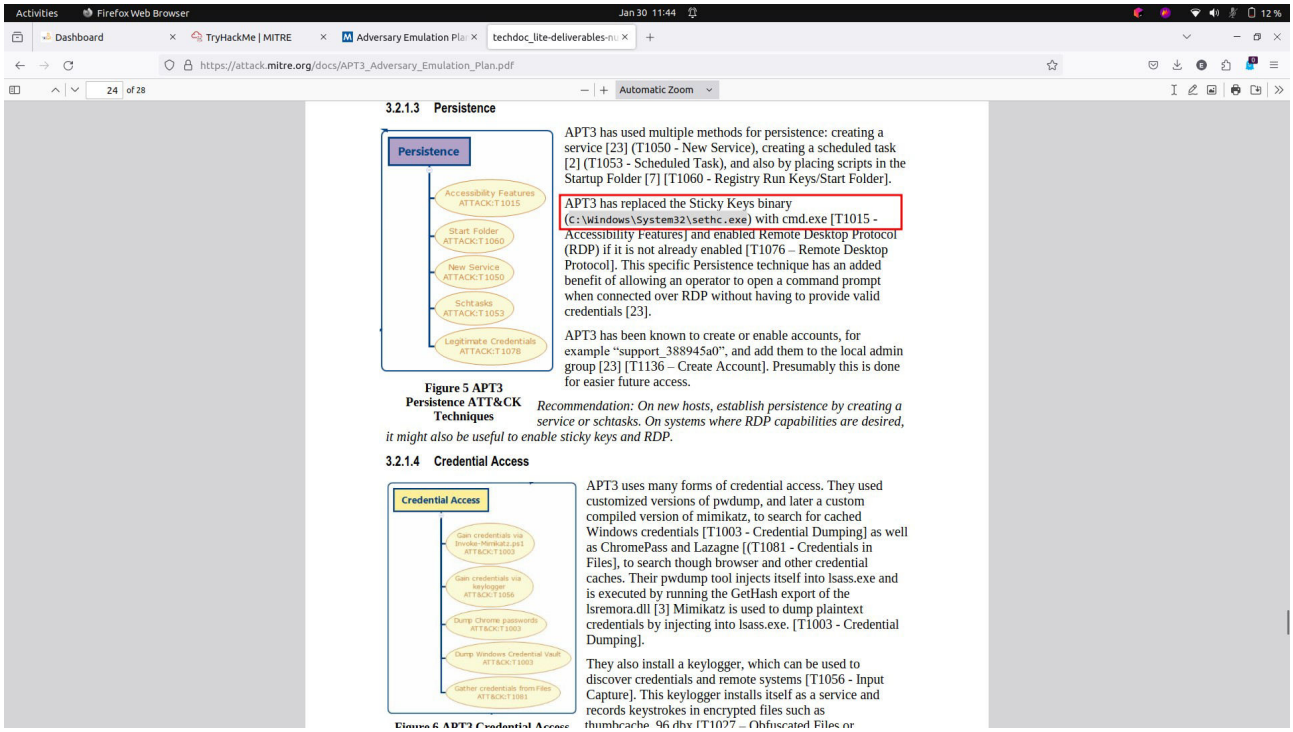


2. Under Persistence, what binary was replaced with cmd.exe? ANS: **sethc.exe**

APT3 Adversary Emulation Plan

By clicking on APT3 Adversary Emulation Plan link, a pdf file opens in a new tab which I then navigated under persistence where this statement catches my eye:- “APT3 has replaced the Sticky Keys binary
(C:\Windows\System32\sethc.exe) with cmd.exe”





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.

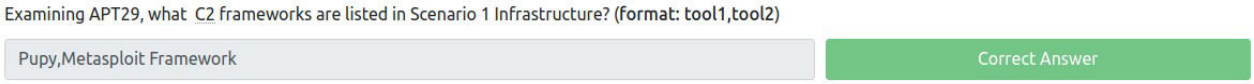
3.2.1.4 Credential Access

APT3 uses many forms of credential access. They used customized versions of pwdump, and later a custom compiled version of mimikatz, to search for cached Windows credentials [T1003 - Credential Dumping] as well as ChromePass and Lazagne [(T1081 - Credentials in Files], to search though browser and other credential caches. Their pwdump tool injects itself into lsass.exe and is executed by running the GetHash export of the lsremora.dll [3] Mimikatz is used to dump plaintext credentials by injecting into lsass.exe. [T1003 - Credential Dumping].

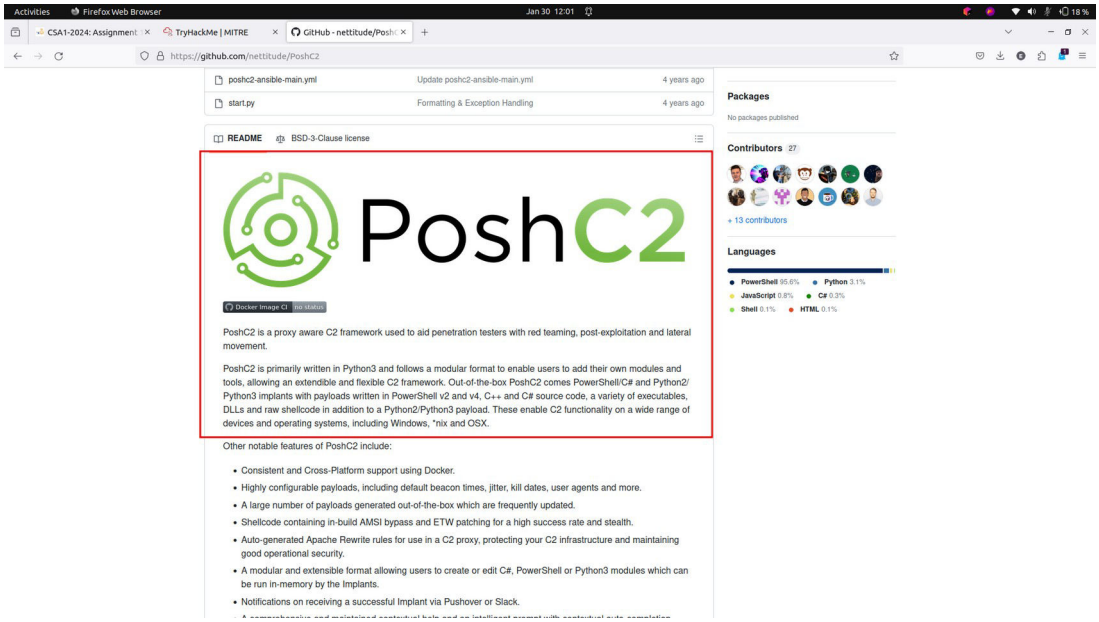
They also install a keylogger, which can be used to discover credentials and remote systems [T1056 - Input Capture]. This keylogger installs itself as a service and records keystrokes in encrypted files such as thumbcache_96.dbx [T1027 – Obfuscated Files or

Figure 6 APT3 Credential Access

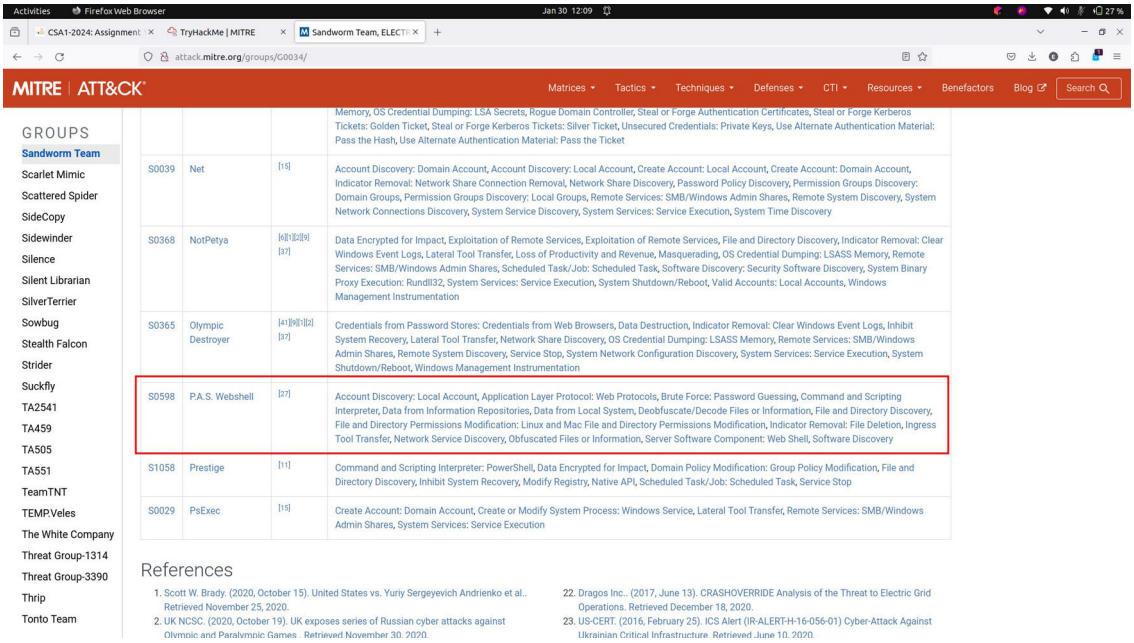
3. Examining APT29, what C2 frameworks are listed in Scenario 1 Infrastructure? (format: tool1,tool2) **ANS: Pupy,Metasploit Framework**

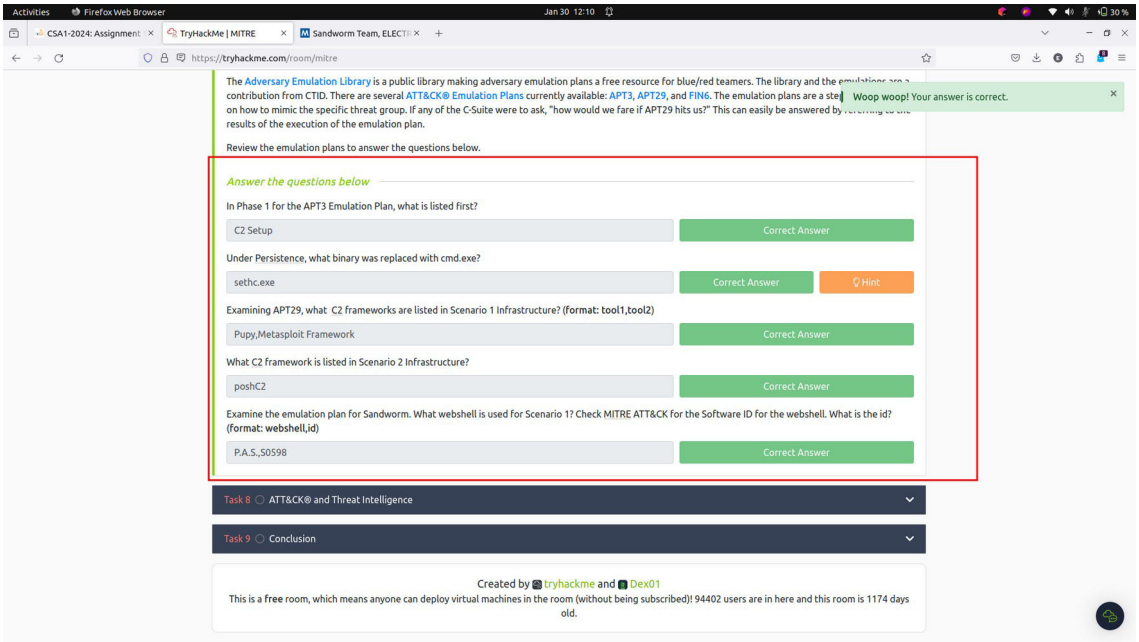


4. What C2 framework is listed in Scenario 2 Infrastructure? ANS: **PoshC2**



5. 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) **ANS: P.A.S.,S0598**





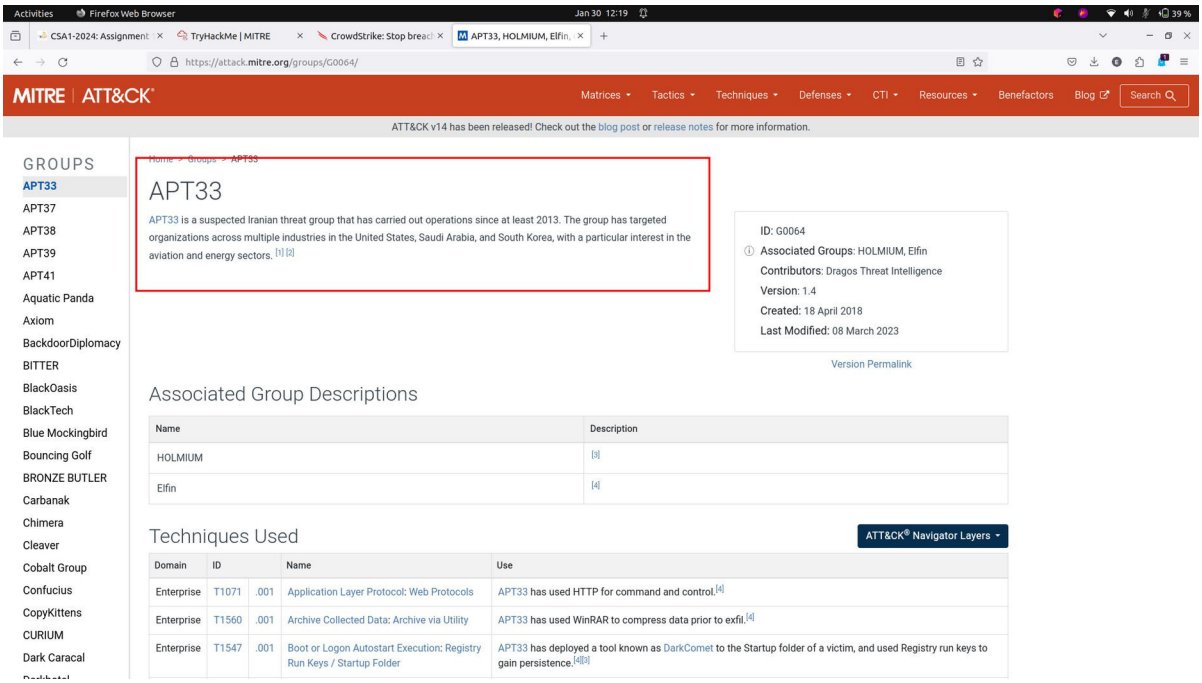
ATT&CK and Threat Intelligence

In this section I learnt about Threat Intelligence (TI) or Cyber Threat Intelligence (CTI) which is explained as the information, or TTPs (Tactics, Techniques and Procedures), attributed to the adversary.

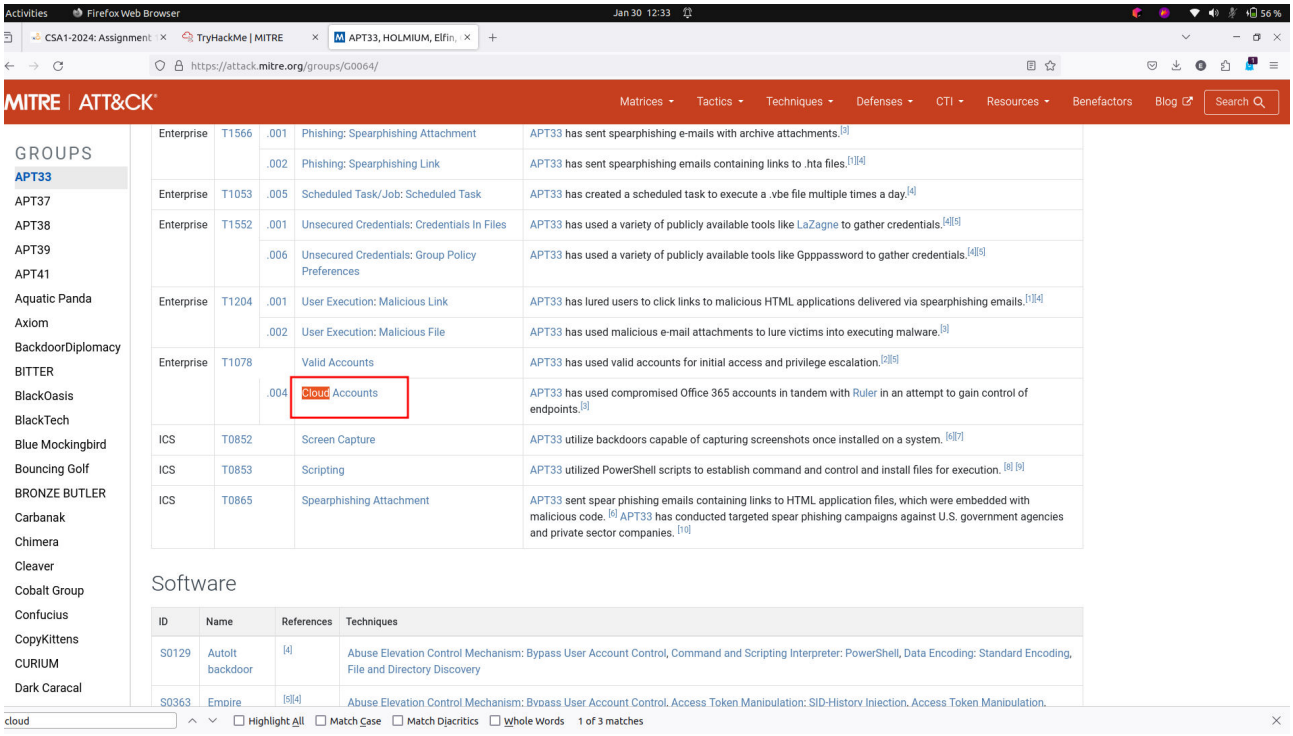
I have understood that it is important for a large organisation to have a separate teams that gathers threat intelligence for other teams within the organization, in order for the organisation to have a large amount of TI Information.

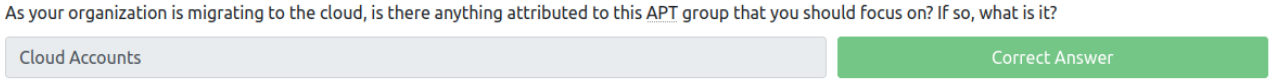
Questions

1. What is a group that targets your sector who has been in operation since at least 2013? **ANS: APT33**

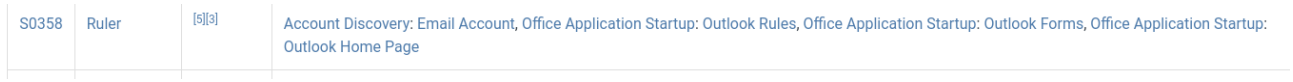


2. As your organization is migrating to the cloud, is there anything attributed to this APT group that you should focus on? If so, what is it? **ANS: <u>Cloud Accounts</u>**



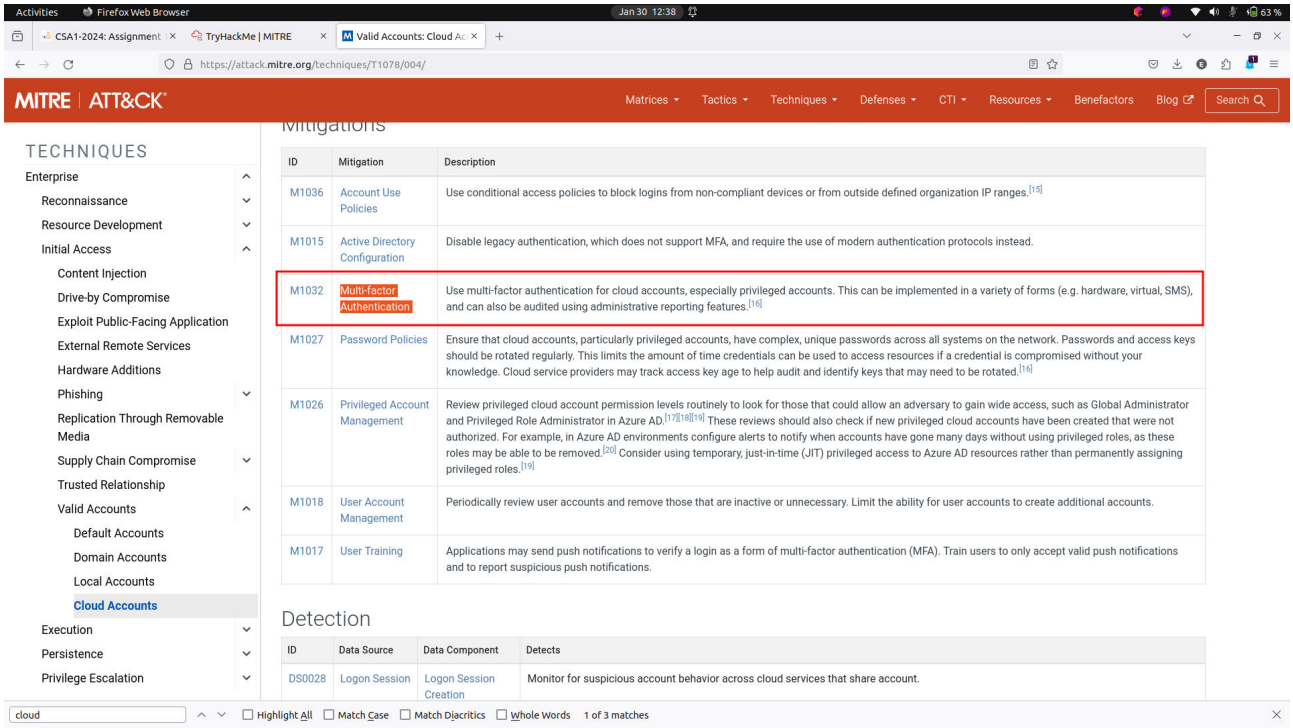


3. What tool is associated with the technique from the previous question? **ANS: <u>Ruler</u>**

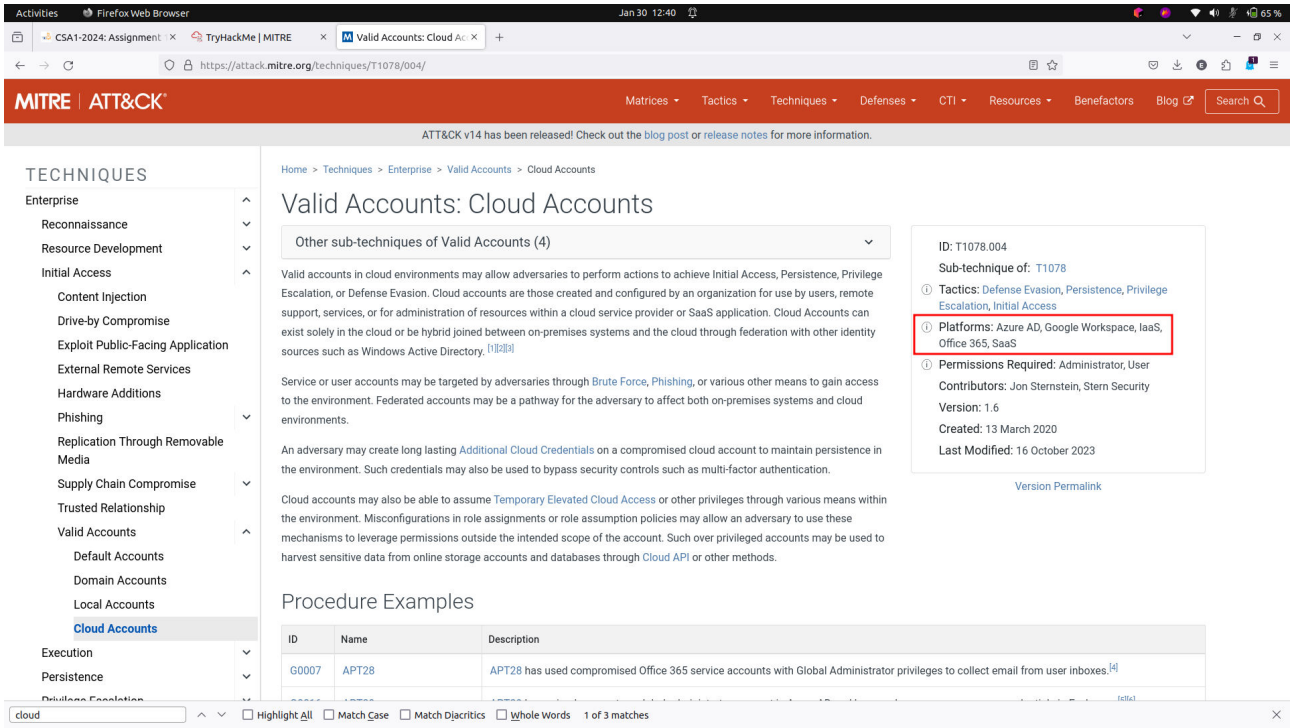


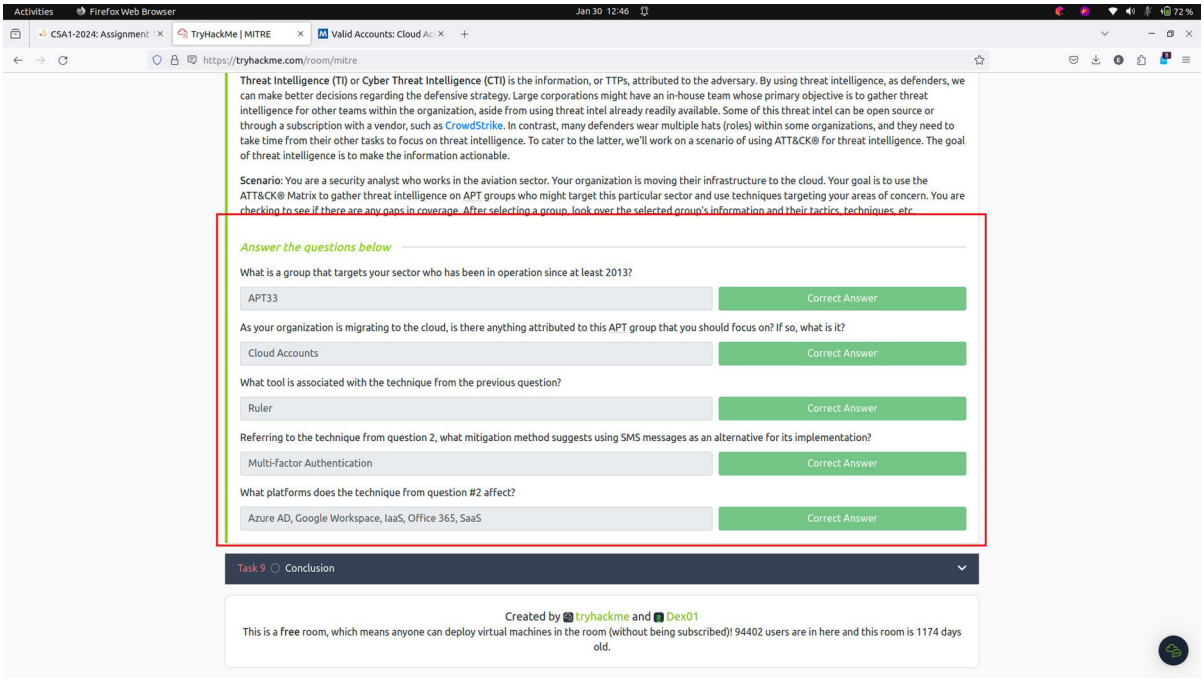
4. Referring to the technique from question 2, what mitigation method suggests using SMS messages as an alternative for its implementation? **ANS: <u>Multi-factor Authentication</u>**

On clicking the link cloud accounts, it gives more information about the topic too, this is where I find the mitigation method that suggests using SMS messages as an alternative for its implementation



5. What platforms does the technique from question #2 affect? ANS: **Azure AD, Google Workspace, IaaS, Office 365, SaaS**





Conclusion.

From this lab I have learnt on different how to extract intelligence from MITRE websites.
I now have a better understanding on MITRE ATT&CK knowledge base which describes the actions, tactics, and techniques commonly employed by cyber adversaries.
This room has provided me with practical knowledge and important skills in cybersecurity.

Thank you.