

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, Purple 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?

The screenshot shows a web browser with multiple tabs open. The active tab is 'attack.mitre.org/techniques/T1566/'. The page title is 'MITRE | ATT&CK®'. The left sidebar lists various attack techniques under the 'Phishing' category, including Spearphishing Attachment, Spearphishing Link, Spearphishing via Service, Spearphishing Voice, Replication Through Removable Media, Supply Chain Compromise, Trusted Relationship, Valid Accounts, Execution, Persistence, and Privilege Escalation. The main content area displays a table for the 'Phishing' technique. The table has columns for 'ID', 'Name', and 'Description'. The rows show:

ID	Name	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.

A red arrow points from the 'User Training' row to the 'Mitigation to identifying SE techniques' section at the bottom of the table.

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

TECHNIQUES

Phishing

- Spearphishing Attachment
- Spearphishing Link
- Spearphishing via Service
- Spearphishing Voice
- Replication Through Removable Media
- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts
- Execution
- Persistence
- Privilege Escalation

Detection

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 and analyze SSL/TLS traffic patterns and packet inspection associated to protocol(s) that do not follow the expected protocol standards and traffic flows (e.g. extraneous packets that do not belong to established flows, gratuitous or anomalous traffic patterns, anomalous syntax, or structure). Consider correlation with process monitoring and command line to detect anomalous processes execution and command line arguments associated to traffic patterns (e.g. monitor anomalies in use of files that do not normally initiate connections for respective protocol(s)). Filtering based on DKIM+SPF or header analysis can help detect.

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

TECHNIQUES

- Supply Chain Compromise
- Trusted Relationship
- Valid Accounts
- Execution
- Persistence
- Privilege Escalation
- Defense Evasion
- Credential Access
- Discovery
- Lateral Movement
- Collection
- Command and Control
- Exfiltration
- Impact

Procedure Examples

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]}

Mitigations

ID	Mitigation	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

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

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

Associated Group Descriptions

Name	Description
Group 72	[4]

Techniques Used

Domain	ID	Name	Use
Enterprise	T1583	.002	Acquire Infrastructure: DNS

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

Software

ID	Name	References	Techniques
S0021	Derusbi	[8][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?

The screenshot shows a web browser with multiple tabs open. The active tab is 'attack.mitre.org/groups/G0001/'. The page title is 'Axiom'. The left sidebar lists various groups, with 'Axiom' selected. The main content area contains a brief description of Axiom as a suspected Chinese cyber espionage group targeting aerospace, defense, government, manufacturing, and media sectors since at least 2008. It notes a degree of overlap with Winnti Group. To the right, a box displays group details: ID: G0001, Associated Groups: Group 72, Version: 2.0, Created: 31 May 2017, Last Modified: 20 March 2023. Below this are sections for 'Associated Group Descriptions' (listing Group 72) and 'Techniques Used'. The bottom of the screen shows a taskbar with various icons.

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?

CAR is intended to be shared with cyber-defenders throughout the community.

This white paper on TTP-based hunting provides some useful insight into many of these activities.

CAR and ATT&CK

It's important to remember that ATT&CK and CAR are separate projects for good reason. It's critical to keep how we articulate threats with ATT&CK separate from a set of possible ways to detect them with the analytics. We don't want the defender content in ATT&CK to be overly prescriptive about how someone can defend against ATT&CK techniques because there could be many different ways, and it's up to the organization implementing them to determine what works best for their environment and the threats they face. This is why we didn't put the analytics in ATT&CK to begin with. CAR is a good starting point for many organizations and can be a great platform for open analytic collaboration - but it isn't the be-all/end-all for defending against the threats described by ATT&CK.

Analytic Source Code Libraries

Some analytics are built as source code for specific products. In these cases, code might support a broad set of detections in a way that makes it hard to describe a set of distinct analytics. For these types of analytics, rather than integrating them into the main CAR site, we've collected them under a library of implementations. Currently, the only library is [BZAR](#), a collection of Zeek (Bro) scripts looking primarily at SMB and RPC traffic.

Contributing

We would love your contributions! Please see the [Contribution Guidance](#) for more information.

From the CAR home path

Copyright © 2022, The MITRE Corporation. MITRE ATT&CK and ATT&CK are trademarks of The MITRE Corporation.
[Privacy Policy](#) | [License](#) | [Contribute](#)

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

Technique ID	Description	Artifacts
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 commandsCAR-2016-03-001: Host Discovery Commands
T1036: Masquerading	(N/A - technique only)	<ul style="list-style-type: none">CAR-2013-05-002: Suspicious Run Locations
	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 DifferencesCAR-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?

car.mitre.org/analytics/CAR-2013-05-004/

```
_fetch * from event where $LogName=WINDOWS-SYSMON AND $EventID=1 AND $App=at.exe limit 100
```

Logpoint, LogPoint native

LogPoint version of the above pseudocode.

```
norm_id=WindowsSysmon event_id=1 image="*\at.exe"
```

Unit Tests

Test Case 1

Configurations: Windows 7

- From an admin account, open Windows command prompt (right click, run as administrator).
- Execute "at 10:00 calc.exe," substituting a time in the near future for 10:00.
- The program should respond with "Added a new job with job ID = 1" where the job ID is dependent on what tasks are scheduled.
- The program should execute at the time specified. This is what the analytic should fire on.
- To remove the scheduled task, execute "at 1 /delete" where you replace "1" with the job ID output in step 2a above.

```
at 10:00 calc.exe // returns a job number X
at X /delete
```

Copyright © 2022, The MITRE Corporation. MITRE ATT&CK and ATT&CK are trademarks of The MITRE Corporation.

MITRE ENGAGE

a. Under Prepare, what is ID SAC0002?

engage.mitre.org/matrix/?activity=persona-creation

Persona Creation

Storyboarding

Threat Model

View settings: [FULL DEFINITION](#)

PERSONA CREATION

ID: SAC0002

Plan and create a fictitious human user through a combination of planted data and revealed behavior patterns.

24°C Sunny 17:51

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 homepage with a search bar at the top containing "Persona". A red box highlights the search term. Below the search bar, there's a navigation menu with links to Home, Tools, Why Engage?, Engage with Us, and social media icons. To the right of the menu is a search bar with the word "Persona" and a "Search" button. On the left, there's a section titled "PERSONA PROFILE WORKSHEET" with a brief description of its purpose. On the right, there's a sidebar titled "RECENT POSTS" listing various Engage resources like "Engage Brand Guide" and "Starter Kit (Printable)". Below that is a "RECENT COMMENTS" section with a note that says "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 at the top containing "activity=lures". A red box highlights the search term. Below the search bar, there's a navigation menu with links to Network Manipulation, Peripheral Management, Security Controls, and Software Manipulation. To the right, there's a sidebar with Network Diversity and Personas. In the center, there's a detailed definition of "LURES" with ID EAC0005. A red box highlights the text "Deceptive systems and artifacts intended to serve as decoys, breadcrumbs, or bait to elicit a specific response from the adversary." Below the definition is a small image of a network diagram with a red box around it, and a link "Click image to expand".



d. What is the definition of Threat Model?

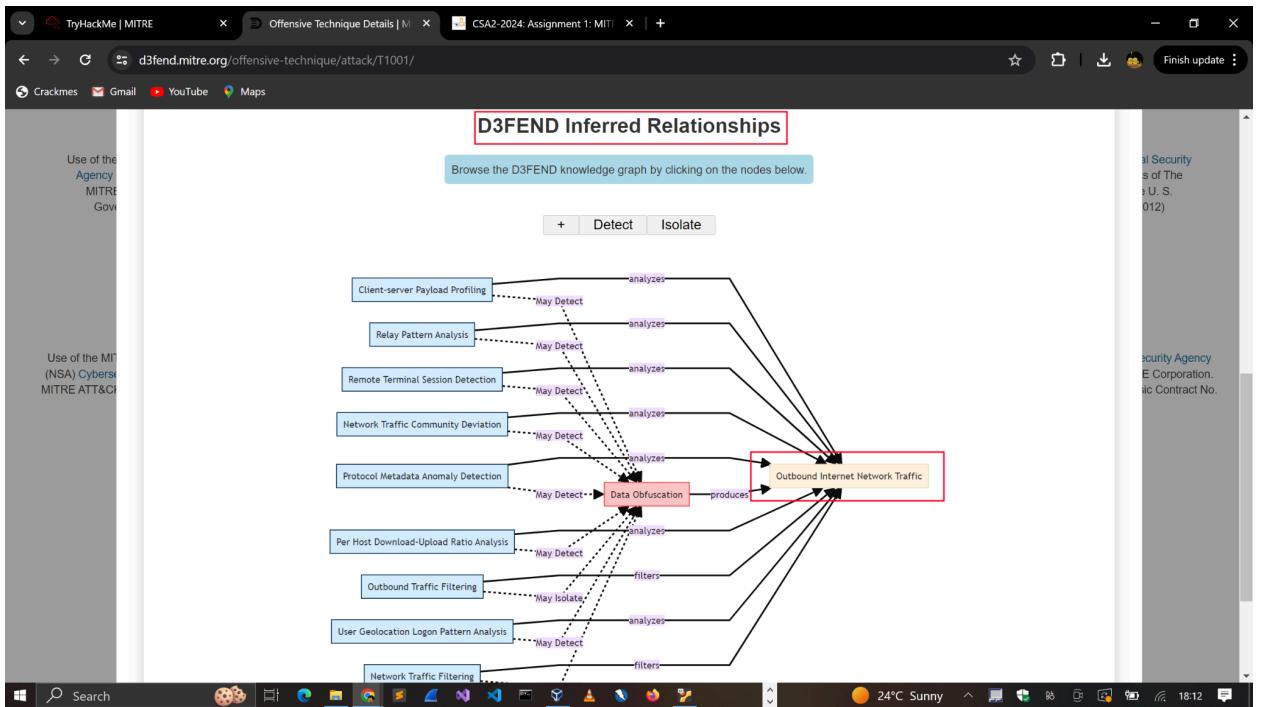
From Mitre Engage > Prepare tab > Threat model, a threat model is defined as a risk assessment that models organizational strengths and weaknesses.

MITRE DEFEND

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

The screenshot shows a web browser window with three tabs: "TryHackMe | MITRE", "D3FEND Matrix | MITRE D3FEND", and "CSA2-2024: Assignment 1: MITRE". The main content area is titled "DEFEND™" and "A knowledge graph of cybersecurity countermeasures 0.15.0". It features a search bar "Search D3FEND's 679 Artifacts" and a table titled "ATT&CK Lookup". The table has columns for "File Analysis", "Identifier Analysis", "Message Analysis", "Network Traffic Analysis", "Platform Monitoring", "Process Analysis", "User Behavior Analysis", "Execution Isolation", "Network Isolation", and "Decoy Environment". A dropdown menu is open over the first row of the table, showing a list of ATT&CK techniques: T1001.001 - Junk Data, T1001.002 - Steganography, T1001.003 - Protocol Impersonation, T1002 - Data Compressed, T1003 - OS Credential Dumping, T1003.001 - LSASS Memory, T1003.002 - Security Account Manager, T1003.003 - NTDS, T1003.004 - LSA Secrets, T1003.005 - Cached Domain Credentials, T1003.006 - DCSync, T1003.007 - Proc Filesystem, T1003.008 - /etc/passwd and /etc/shadow, T1004 - Winlogon Helper DLL, T1005 - Data from Local System, and T1006 - Direct Volume Access. The first item, T1001.001 - Junk Data, is highlighted with a red box.

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

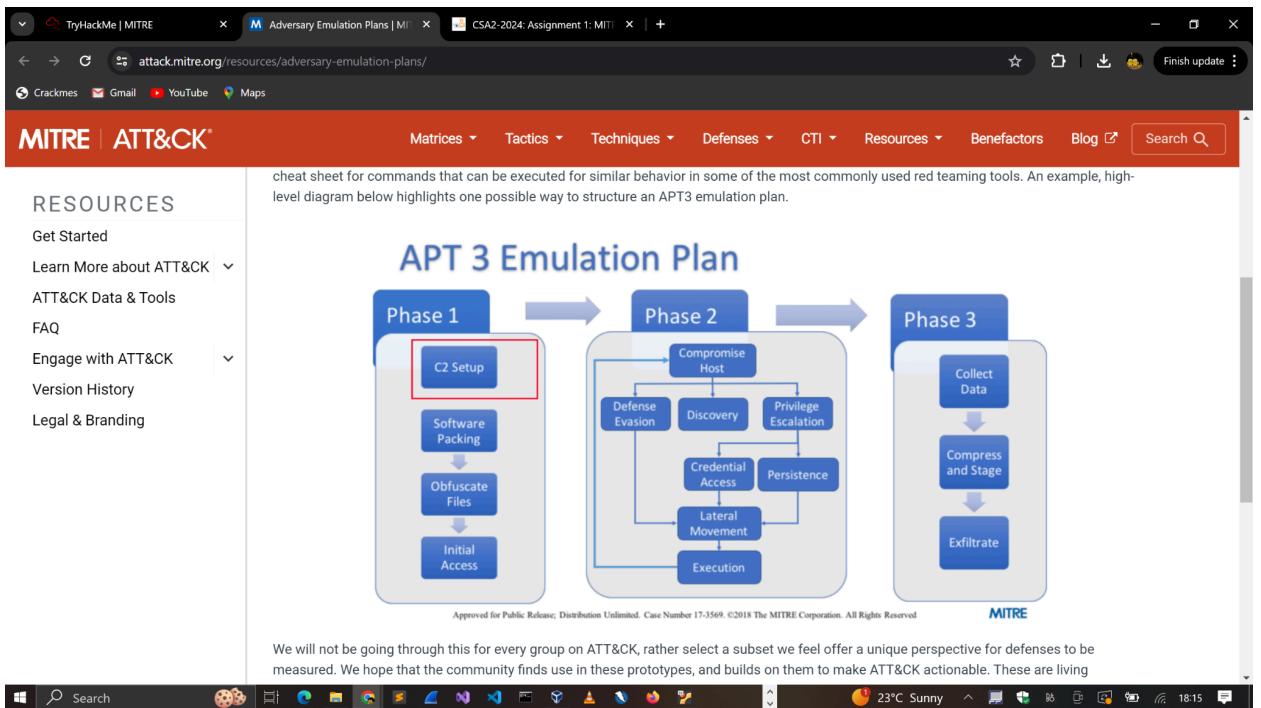


ATT&CK Emulation Plans

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

- 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 shows a PDF document titled "APT3_Adversary_Emulation_Plan.pdf" open in a browser-based PDF viewer. The document contains a diagram titled "3.2.1.3 Persistence" which lists several persistence techniques: Accessibility Features (ATTACK:T1015), Start Folder (ATTACK:T1060), New Service (ATTACK:T1050), SchTasks (ATTACK:T1053), and Legitimate Credentials (ATTACK:T1078). A callout box highlights the "Accessibility Features" entry. Below the diagram, a note states: "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].". A recommendation follows: "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 browser interface includes tabs for "TryHackMe | MITRE", "Adversary Emulation Plans | MITRE", and "APT3_Adversary_Emulation_Plan.pdf". The address bar shows the URL "chrome-extension://efaidnbmnnibpcapcglclefindmkaj/https://attack.mitre.org/docs/APT3_Adversary_Emulation_Plan.pdf". The bottom of the screen shows a Windows taskbar with various icons and system status information.

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

The screenshot shows a GitHub repository interface. On the left, there's a sidebar with a 'Files' section showing a tree view of files and folders. The main area displays the content of the 'Infrastructure.md' file under the 'adversary_emulation_library / apt29 / Emulation_Plan / Scenario_1' path. The file content is as follows:

```
adversary_emulation_library / apt29 / Emulation_Plan / Scenario_1 / Infrastructure.md
Preview Code Blame 127 lines (88 loc) · 6.03 KB
Move to the same server

Please note that binary files hosted in Scenario\_1 and Scenario\_2 have been added to password protected zip files. The password for these files is "malware." ↑ Top

Emulation Team Infrastructure

1. Attack Platform: tested and executed on Ubuntu 18.04.3 LTS
    ○ C2 Framework
        □ Pupy
        □ Metasploit Framework
    ○ Chrome Password Dumper
    ○ Sysinternals Suite Zip file
    ○ WebDAV Share

2. Redirector: tested and executed on Ubuntu 18.04.3 LTS
    ○ Socat

3. Windows Attack Platform: Windows 10 x64 version 1903
    ○ Invoke-PSImage
    ○ Python 3
    ○ Powershell
```

A red box highlights the 'C2 Framework' section under point 1.

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

CSA2-2024: Assignment 1: MITRE

Crackmes Gmail YouTube Maps

YARA Rules

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.

23°C Sunny 18:26

TryHackMe | MITRE

adversary_emulation_library/sandworm

CSA2-2024: Assignment 1: MITRE

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

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.

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

The screenshot shows a web browser with multiple tabs open. The active tab is 'Groups | MITRE ATT&CK' at attack.mitre.org/groups/. A search bar at the top contains the word 'aviation'. Below the search bar, a red navigation bar includes links for 'Matrices', 'Tactics', 'Techniques', 'Defenses', 'CTI', 'Resources', 'Benefactors', 'Blog', and 'Search'. The main content area displays a table titled 'GROUPS' with the following data:

Group ID	Group Name	Associated Techniques	Description
G0050	APT32	SeaLotus, OceanLotus, APT-C-00, Canvas Cyclone, BISMUTH	government. While Naikon shares some characteristics with APT30, the two groups do not appear to be exact matches.
G0064	APT33	HOLMIUM, Elfin, 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, TEMP.Reaper, 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. North Korean group definitions are known to have significant overlap,

- 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?
- What tool is associated with the technique from the previous question?

The screenshot shows the MITRE ATT&CK website with the URL attack.mitre.org/groups/G0064/. The left sidebar lists various threat groups, with 'APT33' selected. The main content area displays a table of techniques used by APT33, categorized by platform (Enterprise, ICS). The 'Cloud Accounts' technique (T1078) is highlighted with a red box.

	Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	APT33 has created a scheduled task to execute a .vbe file multiple times a day. ^[4]
APT33	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 Gppassword to gather credentials. ^{[4][6]}
APT37	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]
APT38	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]
APT39	ICS	T0852		Screen Capture	APT33 utilize backdoors capable of capturing screenshots once installed on a system. ^{[7][8]}
				T0853 Scripting	APT33 utilized PowerShell scripts to establish command and control and install files for execution. ^{[9][10]}
APT41	Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	APT33 has created a scheduled task to execute a .vbe file multiple times a day. ^[4]
APT5	Enterprise	T1552	.001	Unsecured Credentials: Credentials In Files	APT33 has used a variety of publicly available tools like LaZagne to gather credentials. ^{[4][6]}
Aquatic Panda	Enterprise	T1204	.001	User Execution: Malicious Link	APT33 has lured users to click links to malicious HTML applications delivered via spearphishing emails. ^{[1][4]}
Axiom	Enterprise	T1078		Valid Accounts	APT33 has used valid accounts for initial access and privilege escalation. ^{[2][6]}
BackdoorDiplomacy	Enterprise	T1078	.004	Cloud Accounts	APT33 has used compromised Office 365 accounts in tandem with Ruler in an attempt to gain control of endpoints. ^[3]
BITTER	ICS	T0852		Screen Capture	APT33 utilize backdoors capable of capturing screenshots once installed on a system. ^{[7][8]}
BlackOasis	ICS	T0853	Scripting		APT33 utilized PowerShell scripts to establish command and control and install files for execution. ^{[9][10]}
BlackTech	Enterprise	T1053	.005	Scheduled Task/Job: Scheduled Task	APT33 has created a scheduled task to execute a .vbe file multiple times a day. ^[4]
Blue Mockingbird	Enterprise	T1552	.001	Unsecured Credentials: Credentials In Files	APT33 has used a variety of publicly available tools like LaZagne to gather credentials. ^{[4][6]}
Bouncing GOLF	Enterprise	T1204	.001	User Execution: Malicious Link	APT33 has lured users to click links to malicious HTML applications delivered via spearphishing emails. ^{[1][4]}

- 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 website with the URL attack.mitre.org/techniques/T1078/004/. The left sidebar lists various techniques under 'Cloud Accounts'. The 'Multi-factor Authentication' technique (M1032) is highlighted with a red box.

	M1036	Account Use Policies	Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges. ^[16]
Cloud Accounts	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]
Execution	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]
Persistence	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.
Privilege Escalation			
Defense Evasion			
Credential Access			
Discovery			
Lateral Movement			
Collection			
Command and Control			
Exfiltration			
Impact			
Mobile			
ICS			

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

The screenshot shows a browser window with four tabs open: 'TryHackMe | MITRE', 'CSA2-2024: Assignment 1: MITRE', 'Valid Accounts: Cloud Accounts', and 'Matrix | MITRE Engage™'. The main content area displays the MITRE ATT&CK framework. A sidebar on the left lists 'TECHNIQUES' under 'Cloud Accounts', including sub-categories like Execution, Persistence, Privilege Escalation, etc. The main content area shows the 'Valid Accounts: Cloud Accounts' page, which includes a sub-section titled 'Other sub-techniques of Valid Accounts (4)'. Below this, there is a detailed description of how valid accounts in cloud environments can be used for various attacks. To the right, there is a summary box with information such as ID: T1078.004, Sub-technique of: T1078, Tactics: Defense Evasion, Persistence, Privilege Escalation, Initial Access, Platforms: Azure AD, Google Workspace, IaaS, Office 365, SaaS, Permissions: Required: Administrator, User, Contributors: Jon Sternstein, Stern Security, Version: 1.7, Created: 13 March 2020, and Last Modified: 29 March 2024.

3. MODULE COMPLETION

Profile link

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

The screenshot shows a browser window for the TryHackMe platform. The address bar shows the URL 'tryhackme.com/r/room/mitre'. The main interface displays a room named 'MITRE' which has been completed. A large 'Congratulations!' message is centered on the screen, accompanied by a small illustration of a castle-like structure with a ladder. Below the message, it says 'You've completed the room! Share this with your friends:' followed by three social sharing buttons for Twitter, Facebook, and LinkedIn. On the left side of the screen, there is a sidebar with navigation links for 'Dashboard', 'Learn', 'Compete', and 'Other'. The main content area also shows a list of tasks completed: 'Task 1 Introduction to MITRE', 'Task 2 Basic Terminology', 'Task 3 ATT&CK® Framework', and 'Task 4 CAR Knowledge Base'. The bottom of the screen shows the Windows taskbar with various pinned icons.

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.