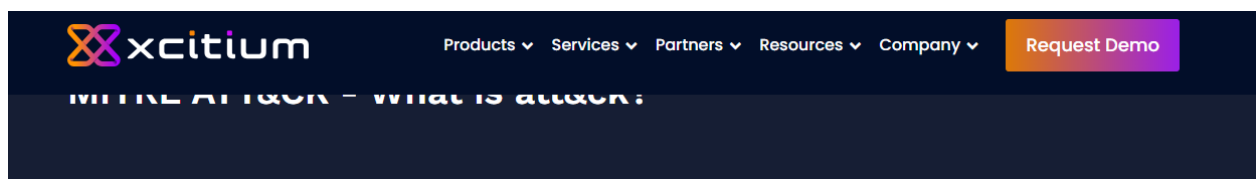


Introduction

MITRE's ATT&CK Matrix is a critical resource in the field of cybersecurity, providing comprehensive data on tactics and techniques used by threat actors. While commonly associated with blue team (defensive) activities, the matrix's utility extends to red teamers and purple teamers. This report delves into specific aspects of the ATT&CK Matrix.

1. **Question:** Besides Blue Teamers, who else will use the ATT&CK Matrix? **Answer:** Red Teamers. They use it for attack simulation.



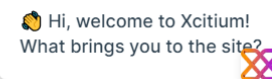
What is att&ck? MITRE ATT&CK is a framework, collection of data matrices, and assessment tool established by MITRE Corporation to assist organizations in understanding their security readiness and identifying gaps in their defenses.

With the answer to what is att&ck, the MITRE ATT&CK Framework, which was created in 2013, utilizes observations to document targeted attack methods, tactics, and techniques. As new vulnerabilities and attack surfaces emerge, they are introduced to the ATT&CK framework. The MITRE ATT&CK framework [EDR](#) and its matrices have grown into an industry standard for both knowledge and restoration tools regarding attacker behavior in recent years.

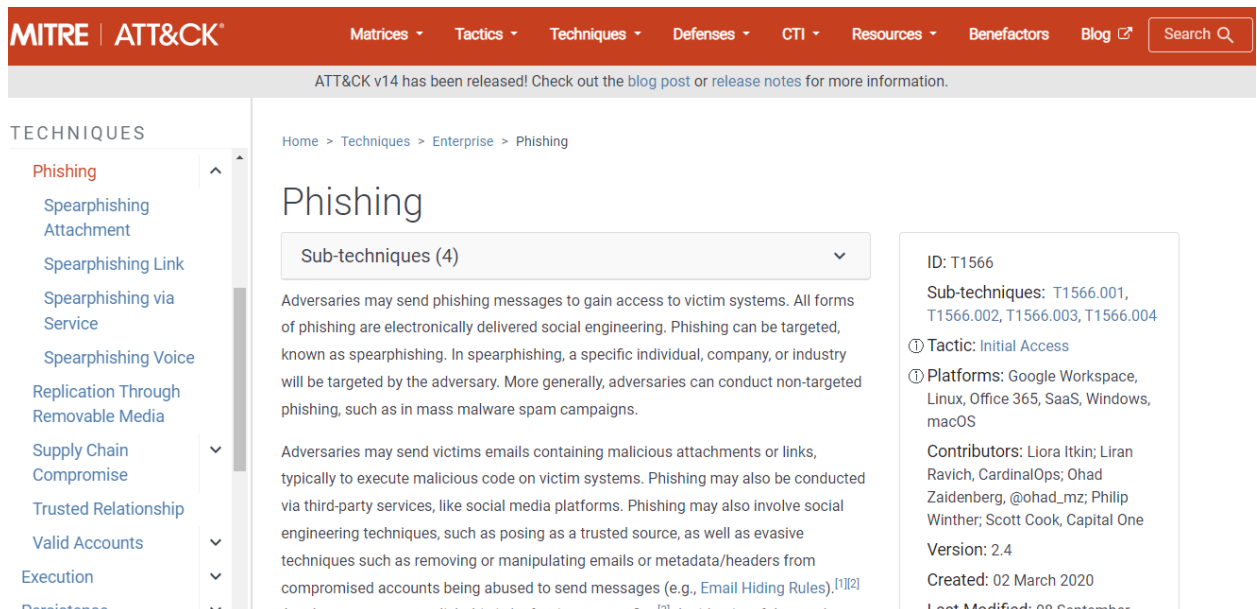
What is att&ck? - Who Uses MITRE ATT&CK and Why?

With the query to what is att&ck, a wide range of IT and security professionals use ATT&CK matrices, including red teamers who play the role of attacker or competitor, security product development engineers, threat hunters, threat intelligence teams, and risk management professionals.

What is att&ck and its use? The MITRE ATT&CK framework is used as a blueprint by red teamers to help uncover attack surfaces and vulnerabilities in corporate systems and



2. **Question:** What is the ID for Technique? **Answer:** T1566. T1566 is identified as phishing in the MITRE ATT&CK framework.



The screenshot shows the MITRE ATT&CK website. The top navigation bar includes links for Matrices, Tactics, Techniques, Defenses, CTI, Resources, Benefactors, and a Blog. A search bar is on the right. Below the navigation bar, a banner announces the release of ATT&CK v14. The left sidebar lists various techniques, with 'Phishing' highlighted. The main content area is titled 'Phishing' and includes a dropdown for 'Sub-techniques (4)'. The text describes phishing as electronically delivered social engineering. A right-hand box provides metadata for T1566, including its ID, sub-techniques, tactic, platforms, contributors, version, creation date, and last modification date.

MITRE | ATT&CK®

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

ATT&CK v14 has been released! Check out the [blog post](#) or [release notes](#) for more information.

TECHNIQUES

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

Home > Techniques > Enterprise > Phishing

Phishing

Sub-techniques (4) ▾

Adversaries may send phishing messages to gain access to victim systems. All forms of phishing are electronically delivered social engineering. Phishing can be targeted, known as spearphishing. In spearphishing, a specific individual, company, or industry will be targeted by the adversary. More generally, adversaries can conduct non-targeted phishing, such as in mass malware spam campaigns.

Adversaries may send victims emails containing malicious attachments or links, typically to execute malicious code on victim systems. Phishing may also be conducted via third-party services, like social media platforms. Phishing may also involve social engineering techniques, such as posing as a trusted source, as well as evasive techniques such as removing or manipulating emails or metadata/headers from compromised accounts being abused to send messages (e.g., [Email Hiding Rules](#)).^{[1][2]} Another way to accomplish this is by forging an email's^[3] the identity of the sender.

ID: T1566

Sub-techniques: T1566.001, T1566.002, T1566.003, T1566.004

① Tactic: Initial Access

① Platforms: Google Workspace, Linux, Office 365, SaaS, Windows, macOS

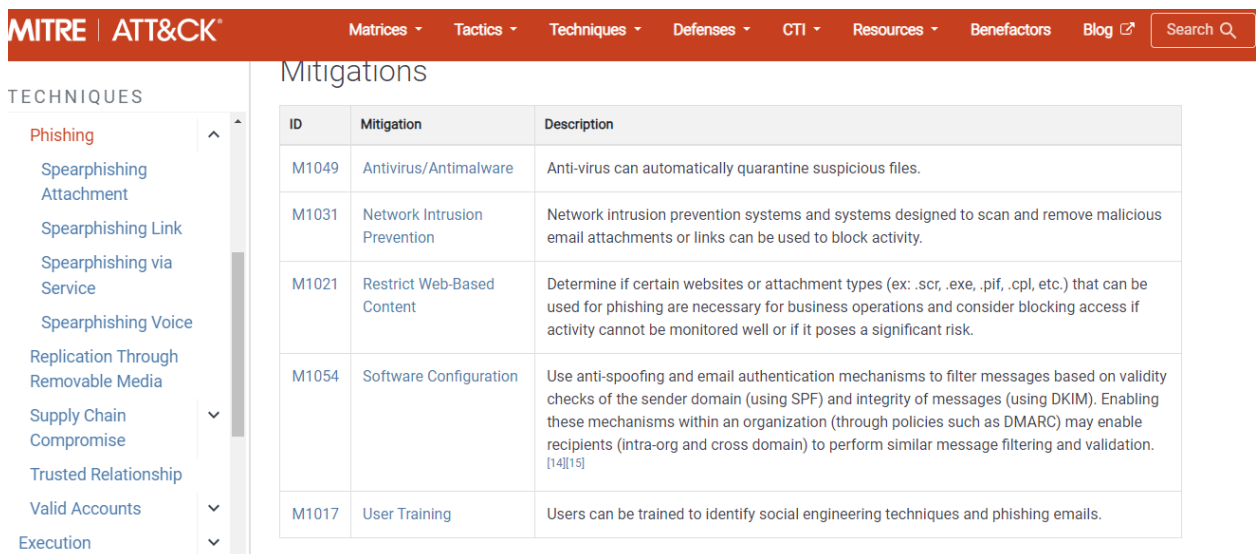
Contributors: Liora Itkin; Liran Ravich, CardinalOps; Ohad Zaidenberg, @ohad_mz; Philip Winther; Scott Cook, Capital One

Version: 2.4

Created: 02 March 2020

Last Modified: 08 September

3. **Question:** What mitigation covers identifying social engineering techniques based on T1566? **Answer:** User Training. Educating users on recognizing and responding to social engineering tactics is essential in mitigating spear-phishing attacks.



The screenshot shows the MITRE ATT&CK website's 'Mitigations' page. The top navigation bar is identical to the previous screenshot. The left sidebar lists techniques, with 'Phishing' highlighted. The main content area is titled 'Mitigations' and contains a table with three columns: ID, Mitigation, and Description. The table lists five mitigations: M1049 (Antivirus/Antimalware), M1031 (Network Intrusion Prevention), M1021 (Restrict Web-Based Content), M1054 (Software Configuration), and M1017 (User Training).

MITRE | ATT&CK®

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

TECHNIQUES

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

Mitigations

ID	Mitigation	Description
M1049	Antivirus/Antimalware	Anti-virus can automatically quarantine suspicious files.
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.

4. **Question:** What are the data sources for Detection of T1566? **Answer:** Application Log, File, Network Traffic. These data sources are key in identifying signs of spear-phishing attempts, such as unusual network traffic or file access patterns.

MITRE ATT&CK [®]		Matrices ▾	Tactics ▾	Techniques ▾	Defenses ▾	CTI ▾	Resources ▾	Benefactors	Blog ↗	Se
TECHNIQUES										
Phishing ^										
Spearphishing										
Attachment										
Spearphishing Link										
Spearphishing via Service										
Spearphishing Voice										
Replication Through Removable Media										
Supply Chain Compromise ▾										
Trusted Relationship ▾										
Valid Accounts ▾										
Execution ▾										
Persistence ▾										
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. 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.							
DS0022	File	File Creation	Monitor for newly constructed files from a phishing messages to gain access to victim systems.							
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							

5. **Question:** What groups have used spear-phishing in their campaigns? **Answer:** Axiom, Gold SOUTHFIELD. These groups are known to employ spear-phishing, highlighting the

technique's prevalence among sophisticated threat actors.

The screenshot shows the MITRE ATT&CK website. The left sidebar lists various 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, and Persistence. The main content area is titled 'Procedure Examples' and contains a table with four rows of examples. Below this, there is a 'Mitigations' section with a table listing two mitigation techniques: M1049 (Antivirus/Antimalware) and M1031 (Network Intrusion).

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]}

ID	Mitigation	Description
M1049	Antivirus/Antimalware	Anti-virus can automatically quarantine suspicious files.
M1031	Network Intrusion	Network intrusion prevention systems and systems designed to scan and remove malicious

6. **Question:** What are the associated groups with Axiom? **Answer:** Group 72. Group 72 is linked to Axiom, indicating possible shared tactics or collaborative efforts.

The screenshot shows the MITRE ATT&CK website for the Axiom group. The left sidebar lists various groups under the 'Axiom' category, including BackdoorDiplomacy, BITTER, BlackOasis, BlackTech, Blue Mockingbird, Bouncing Golf, BRONZE BUTLER, Carbanak, Chimera, Cleaver, Cobalt Group, Confucius, and CopyKittens. The main content area is titled 'Axiom' and contains a description of the group. To the right of the description is a box with metadata: ID: G0001, Associated Groups: Group 72, Version: 2.0, Created: 31 May 2017, and Last Modified: 20 March 2023. Below this, there is a section titled 'Associated Group Descriptions' with a table listing Group 72. At the bottom, there is a section titled 'Techniques Used' with a table listing various techniques.

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]}

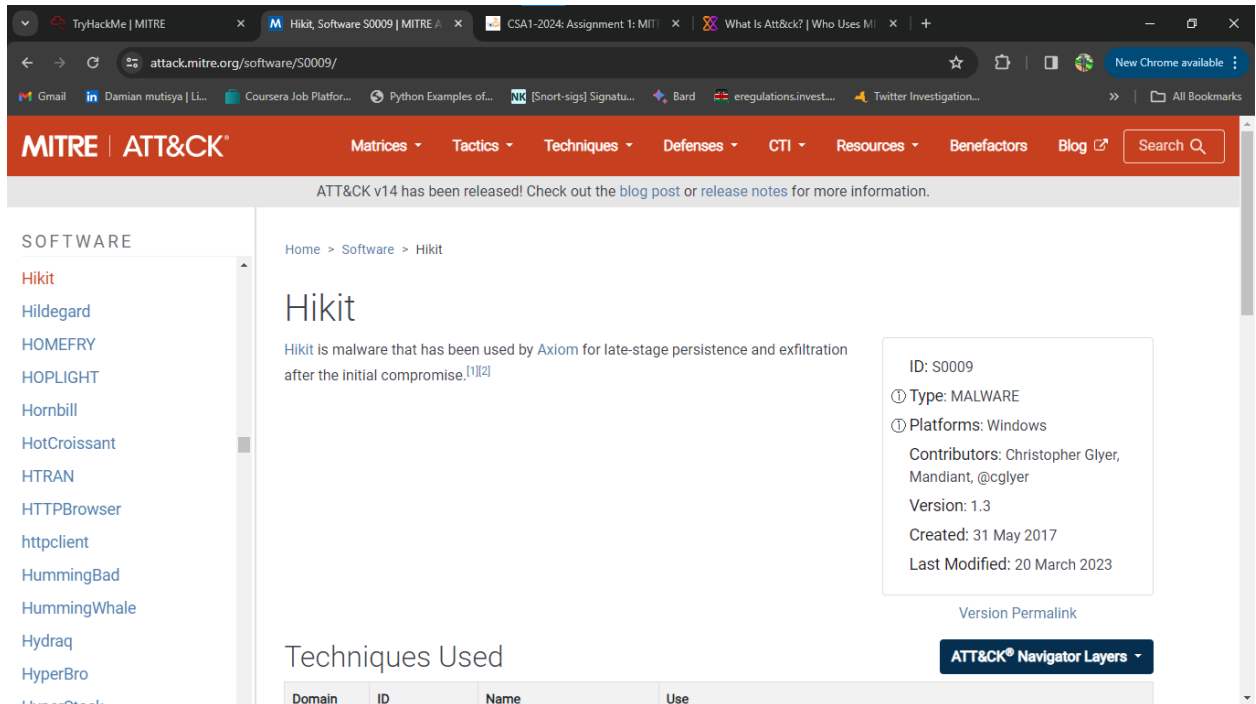
ID: G0001
① Associated Groups: Group 72
Version: 2.0
Created: 31 May 2017
Last Modified: 20 March 2023
[Version Permalink](#)

Name	Description
Group 72	[4]

Domain	ID	Name	Use
--------	----	------	-----

7. **Question:** What software is associated with Axiom that lists phishing as a technique?

Answer: Hikit. Hikit malware, used by Axiom, signifies advanced persistent threats involving phishing for long-term access and data exfiltration.



8. **Question:** What is the description of Hikit? **Answer:** Hikit is malware used by Axiom for late-stage persistence and exfiltration after initial compromise. This description underscores Hikit's role in maintaining stealth and extracting information post-

compromise.

The screenshot shows the MITRE ATT&CK website interface. The browser's address bar displays `attack.mitre.org/software/S0009/`. The page header includes the MITRE ATT&CK logo and navigation links for Matrices, Tactics, Techniques, Defenses, CTI, Resources, Benefactors, and a Blog. A notification banner at the top states: "ATT&CK v14 has been released! Check out the [blog post](#) or [release notes](#) for more information."

The main content area is titled "Hikit" and includes a breadcrumb trail: "Home > Software > Hikit". The description states: "Hikit is malware that has been used by [Axiom](#) for late-stage persistence and exfiltration after the initial compromise.^{[1][2]}".

A metadata box on the right provides the following details:

- ID: S0009
- Type: MALWARE
- Platforms: Windows
- Contributors: Christopher Glyer, Mandiant, @cglyer
- Version: 1.3
- Created: 31 May 2017
- Last Modified: 20 March 2023

Below the metadata box, there is a "Version Permalink" link and an "ATT&CK® Navigator Layers" button.

The "Techniques Used" section features a table with the following columns: Domain, ID, Name, and Use.

Domain	ID	Name	Use
--------	----	------	-----

9. **Question:** Which group slightly overlaps with Axiom? **Answer:** Winnti Group. This overlap suggests shared techniques or objectives between Axiom and the Winnti Group.

The screenshot shows the MITRE ATT&CK website in a web browser. The URL is attack.mitre.org/groups/G0001/. The page title is "Axiom". The breadcrumb trail is "Home > Groups > Axiom". The main content area describes Axiom as a suspected Chinese cyber espionage group that has targeted the aerospace, defense, government, manufacturing, and media sectors since at least 2008. It mentions a degree of overlap between Axiom and Winnti Group. A sidebar on the left lists various groups, including Axiom, BackdoorDiplomacy, BITTER, BlackOasis, BlackTech, Blue Mockingbird, Bouncing Golf, BRONZE BUTLER, Carbanak, Chimera, Cleaver, Cobalt Group, Confucius, and CorelKitten. A metadata box on the right shows the ID: G0001, Associated Groups: Group 72, Version: 2.0, Created: 31 May 2017, and Last Modified: 20 March 2023. A "Version Permalink" link is also present. Below the main description, there is a section titled "Associated Group Descriptions" with a table showing the relationship between Axiom and Group 72.

Name	Description
Group 72	[4]

10. **Question:** How many techniques are attributed to this group? **Answer:**15. This number reflects the group's diverse arsenal of tactics and their sophisticated approach to cyber

operations.

Techniques Used			
Domain	ID	Name	Use
Enterprise	T1583	.002 Acquire Infrastructure: DNS Server	Axiom has acquired dynamic DNS services for use in the targeting of intended victims. ^[4]
		.003 Acquire Infrastructure: Virtual Private Server	Axiom has used VPS hosting providers in targeting of intended victims. ^[4]
Enterprise	T1560	Archive Collected Data	Axiom has compressed and encrypted data prior to exfiltration. ^[4]
Enterprise	T1584	.005 Compromise Infrastructure: Botnet	Axiom has used large groups of compromised machines for use as proxy nodes. ^[4]
Enterprise	T1005	Data from Local System	Axiom has collected data from a compromised network. ^[4]
Enterprise	T1001	.002 Data Obfuscation: Steganography	Axiom has used steganography to hide its C2 communications. ^[4]
Enterprise	T1189	Drive-by Compromise	Axiom has used watering hole attacks to gain access. ^[4]
Enterprise	T1546	.008 Event Triggered Execution: Accessibility Features	Axiom actors have been known to use the Sticky Keys replacement within RDP sessions to obtain persistence. ^[4]
Enterprise	T1190	Exploit Public-Facing Application	Axiom has been observed using SQL injection to gain access to systems. ^{[4][5]}
Enterprise	T1203	Exploitation for Client Execution	Axiom has used exploits for multiple vulnerabilities including CVE-2014-0322, CVE-2012-4792, CVE-2012-1689, and CVE-2012-3893. ^[4]
Enterprise	T1003	OS Credential Dumping	Axiom has been known to dump credentials. ^[4]
Enterprise	T1566	Phishing	Axiom has used spear phishing to initially compromise victims. ^{[4][6]}
Enterprise	T1563	.002 Remote Service Session Hijacking: RDP Hijacking	Axiom has targeted victims with remote administration tools including RDP. ^[4]
Enterprise	T1021	.001 Remote Services: Remote Desktop Protocol	Axiom has used RDP during operations. ^[4]
Enterprise	T1553	Subvert Trust Controls	Axiom has used digital certificates to deliver malware. ^[4]
Enterprise	T1078	Valid Accounts	Axiom has used previously compromised administrative accounts to escalate privileges. ^[4]

11. **Question:** What tactic has an ID of TA0003? **Answer:** Persistence. TA0003 refers to tactics used by adversaries to maintain their foothold within a target's network.

MITRE | ATT&CK

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

ATT&CK v14 has been released! Check out the [blog post](#) or [release notes](#) for more information.

TACTICS

Enterprise

Reconnaissance

Resource Development

Initial Access

Execution

Persistence

Privilege Escalation

Defense Evasion

Credential Access

Discovery

Lateral Movement

Collection

Command and Control

Exfiltration

Impact

Home > Tactics > Enterprise > Persistence

Persistence

The adversary is trying to maintain their foothold.

Persistence consists of techniques that adversaries use to keep access to systems across restarts, changed credentials, and other interruptions that could cut off their access. Techniques used for persistence include any access, action, or configuration changes that let them maintain their foothold on systems, such as replacing or hijacking legitimate code or adding startup code.

ID: TA0003

Created: 17 October 2018

Last Modified: 19 July 2019

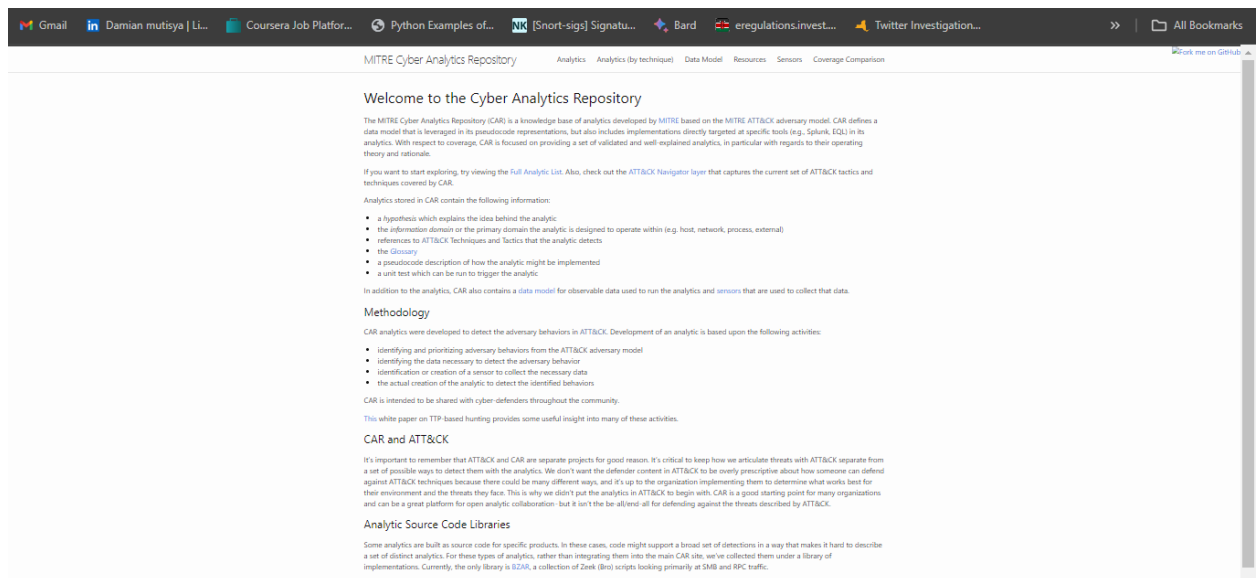
Version Permalink

Techniques: 20

ID	Name	Description
T1098	Account Manipulation	Adversaries may manipulate accounts to maintain and/or elevate access to victim systems. Account manipulation may consist of any action that preserves or modifies adversary access to a compromised account, such as modifying credentials or permission groups. These actions could also include account activity designed to subvert security policies, such as performing iterative password updates to bypass password duration policies and preserve the life of compromised credentials.
T1099	Additional Cloud	Adversaries may add adversary-controlled credentials to a cloud account to maintain persistent access to

12. **Question:** What is the name of the library of Zeek scripts? **Answer:** BZAR. BZAR

(Bro/Zeek ATT&CK-based Analytics and Reporting) is a collection of scripts enhancing network analysis with respect to ATT&CK techniques.



13. **Question:** What is the technique for running executables with the same hash but different names? **Answer:** Masquerading. it involves altering executable files to evade detection

while retaining malicious functionality.

MITRE Cyber Analytics Repository					
Analytics Analytics (by technique) Data Model Resources Sensors Coverage Comparison					
Analytics					
Analytic List (sortable)					
ID	Name	Submission Date	ATT&CK Techniques	Implementations	Applicable Platforms
CAR-2013-01-002	Autorun Differences	January 25 2013	<ul style="list-style-type: none"> Create or Modify System Process Scheduled Task/Job 		Windows
CAR-2013-01-003	SMB Events Monitoring	January 25 2013	<ul style="list-style-type: none"> Data from Network Shared Drive Remote Services 	Pseudocode	N/A
CAR-2013-02-003	Processes Spawning cmd.exe	February 05 2013	<ul style="list-style-type: none"> Command and Scripting Interpreter 	Dnif, Logpoint, Pseudocode	Windows
CAR-2013-02-008	Simultaneous Logins on a Host	February 18 2013	<ul style="list-style-type: none"> Valid Accounts 	Pseudocode	Windows, Linux, macOS
CAR-2013-02-012	User Logged in to Multiple Hosts	February 27 2013	<ul style="list-style-type: none"> Valid Accounts 		Windows, Linux, macOS
CAR-2013-03-001	Reg.exe called from Command Shell	March 28 2013	<ul style="list-style-type: none"> Query Registry Modify Registry 	Dnif, Pseudocode	Windows
CAR-2013-04-002	Quick execution of a series of suspicious commands	April 11 2013	<ul style="list-style-type: none"> Account Discovery OS Credential Dumping 	Dnif, Logpoint, Pseudocode, Sigma	Windows, Linux, macOS
CAR-2013-05-002	Suspicious Run Locations	May 07 2013	<ul style="list-style-type: none"> Masquerading 	Dnif, Logpoint, Pseudocode, Sigma	Windows
CAR-2013-05-003	SMB Write Request	May 13 2013	<ul style="list-style-type: none"> Lateral Tool Transfer Remote Services 	Pseudocode	Windows, Linux, macOS
CAR-2013-05-004	Execution with AT	May 13 2013	<ul style="list-style-type: none"> Scheduled Task/Job 	Dnif, Eql, Logpoint, Pseudocode, Splunk	Windows
CAR-2013-05-005	SMB Copy and Execution	May 13 2013	<ul style="list-style-type: none"> Remote Services Valid Accounts 	Pseudocode	Windows, Linux, macOS
CAR-2013-05-009	Running executables with same hash and different	May 23 2013	<ul style="list-style-type: none"> Masquerading 	Dnif, Logpoint, Sigma, Splunk	Windows, Linux, macOS

14. **Question:** What additional information does CAR-2013-05-004 provide? **Answer:** Unit Tests. Unit Tests are provided to help analysts validate and ensure coverage for specific

<code>process</code>	<code>create</code>	<code>command_line</code>
<code>process</code>	<code>create</code>	<code>exe</code>

Implementations

Pseudocode

Instances of the process `@t.exe` running imply the querying or creation of tasks. Although the command_line is not essential for the analytic to run, it is critical when identifying the command that was scheduled.

```
process = search Process::Create
at = filter process where (exe == "at.exe")
output at
```

Splunk Sysmon native

Splunk version of the above pseudocode.

```
index=_your_sysmon_index__ Inago="C:\Windows\*\*(lat.exe)"(stats values(Command_Line) as "Command Lines" by ComputerName)
```

Eql EQL native

EQL version of the above pseudocode.

```
process where subtype::create and process_name == "at.exe"
```

Dnif Sysmon native

DNIF version of the above pseudocode.

```
_fetch * from event where $logname=4NDX3G-SYSMON AND $eventID=1 AND $app=at.exe limit 100
```

Logpoint, LogPoint native

LogPoint version of the above pseudocode.

```
nom _id=4AndbxSysmon event_id=1 Inago=="lat.exe"
```

Unit Tests

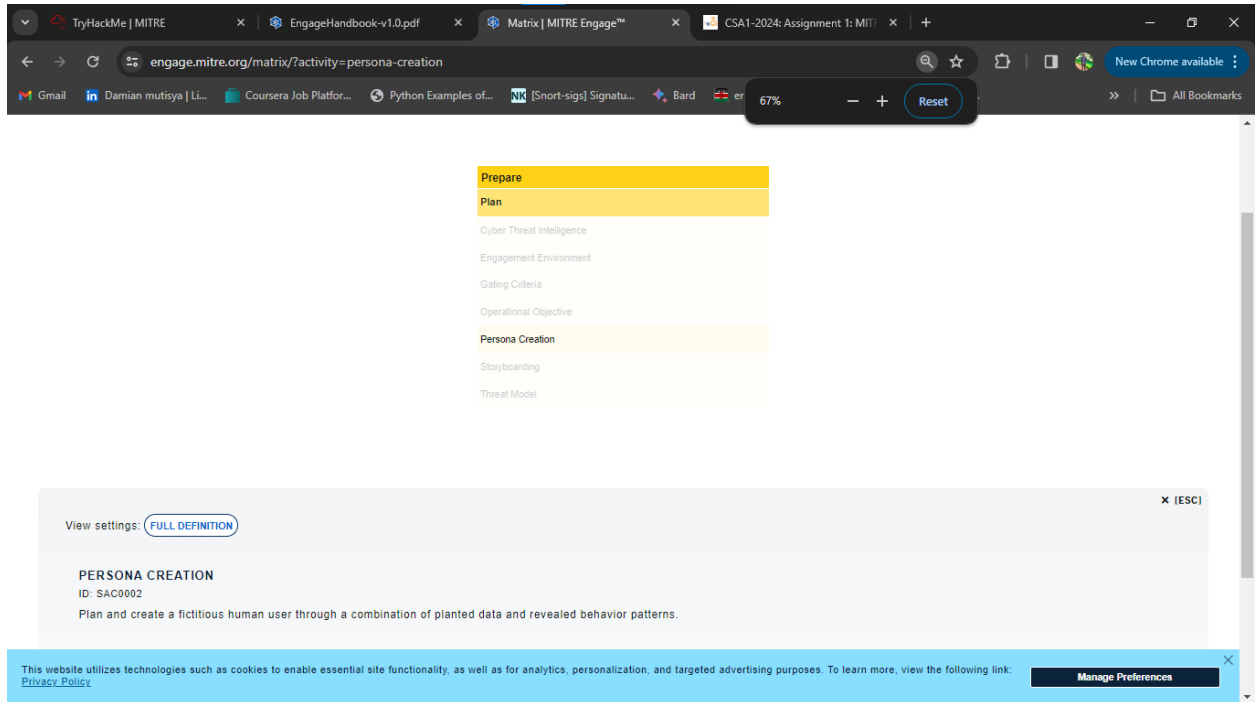
Test Case 1

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 /delete" where you replace "1" with the job ID output in step 2a above.

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

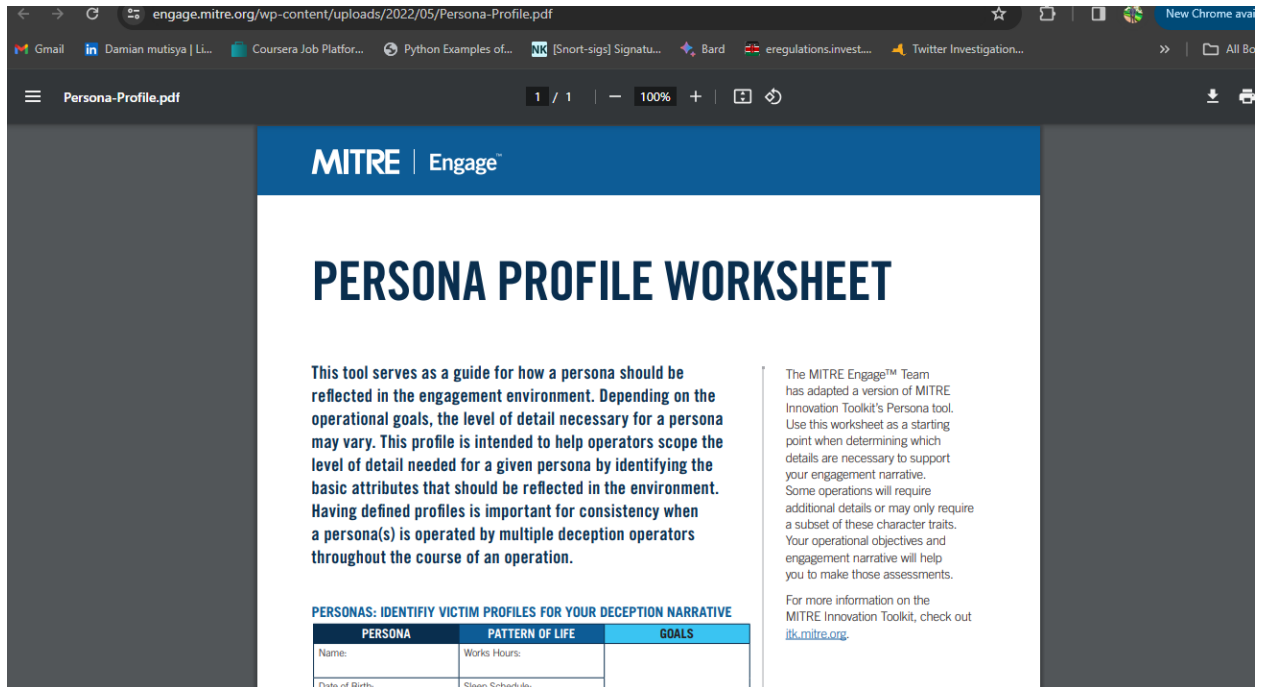
simulations.



16. **Question:** What is the resource for Persona Creation? **Answer:** Persona Profile

Worksheet. This worksheet aids in developing detailed and plausible personas for various

cyber engagements.



17. **Question:** Which engagement activity baits a specific response from the adversary?

Answer. Lures. Lures are tactics designed to entice or provoke specific actions or

responses from adversaries.

The screenshot shows the MITRE Engage Matrix website in a web browser. The URL is engage.mitre.org/matrix?activity=lures. The page displays a matrix of activities categorized into three main sections: Expose, Affect, and Elicit. The 'Lures' activity is highlighted in the 'Affect' section under the 'Direct' category. Below the matrix, there is a detailed view of the 'LURES' activity, including its ID (EAC0005) and a description: 'Deceptive systems and artifacts intended to serve as decoys, breadcrumbs, or bait to elicit a specific response from the adversary.'

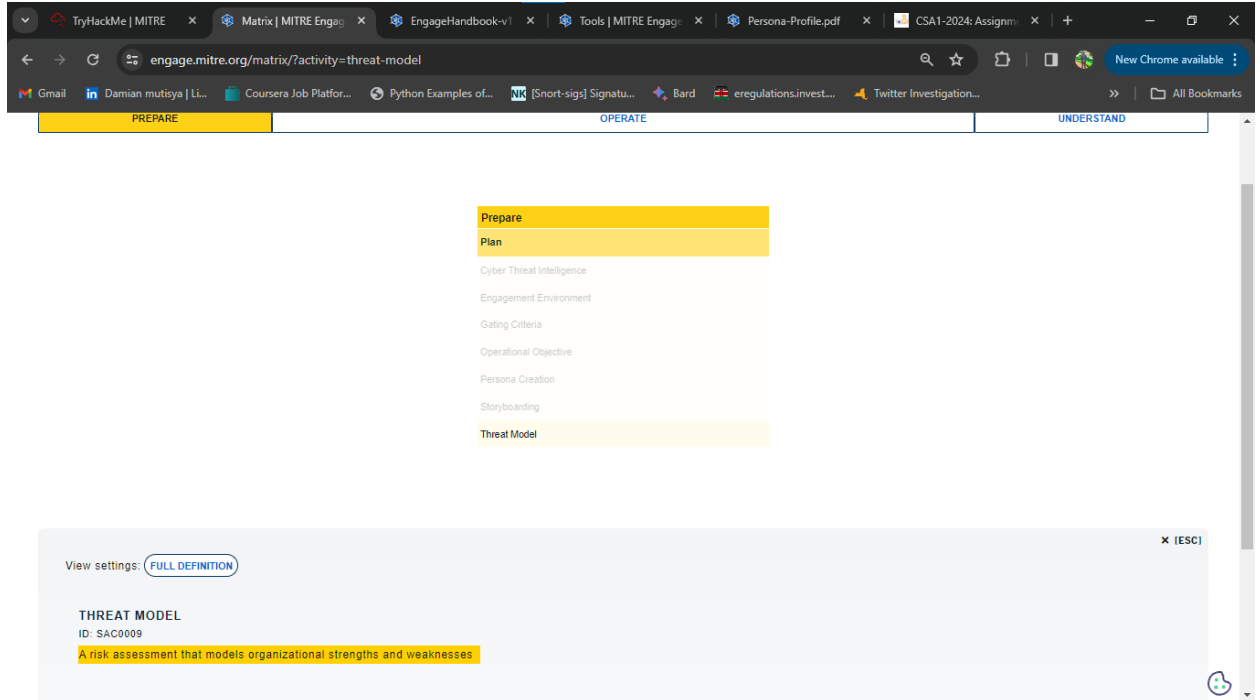
Expose		Affect			Elicit	
Collect	Detect	Prevent	Direct	Disrupt	Reassure	Motivate
API Monitoring	Introduced Vulnerabilities	Baseline	Attack Vector Migration	Isolation	Application Diversity	Application Diversity
Network Monitoring	Lures	Hardware Manipulation	Email Manipulation	Lures	Artifact Diversity	Artifact Diversity
Software Manipulation	Malware Detonation	Isolation	Introduced Vulnerabilities	Network Manipulation	Burn-In	Information Manipulation
System Activity Monitoring	Network Analysis	Network Manipulation	Lures	Software Manipulation	Email Manipulation	Introduced Vulnerabilities
		Security Controls	Malware Detonation		Information Manipulation	Malware Detonation
			Network Manipulation		Network Diversity	Network Diversity
			Peripheral Management		Peripheral Management	Personas
			Security Controls		Pocket Litter	
			Software Manipulation			

View settings: [FULL DEFINITION](#) [REFERENCES](#) [ADVERSARY VULNERABILITIES](#) ✕ [ESC]

LURES
ID: EAC0005
Deceptive systems and artifacts intended to serve as decoys, breadcrumbs, or bait to elicit a specific response from the adversary.

18. **Question:** What is the definition of Threat Model? **Answer:** A risk assessment that models organizational strengths and weaknesses. Threat Modeling is a systematic

approach to identifying and assessing potential threats to an organization.



19. **Question:** What is the first MITRE ATT&CK technique listed in the dropdown?

Answer: Data Obfuscation. This technique involves disguising data to hide malicious

activity, underscoring the complexity of modern cyber threats

The screenshot shows the D3FEND Matrix website. On the left, there is a list of artifacts under the heading "MITRE". The artifact "T1001.001 - Junk Data" is selected. On the right, there is a matrix of countermeasures organized into columns: Detect, Isolate, Deceive, and Evict. Each column contains a list of specific countermeasures. For example, under "Detect", there are "File analysis", "Identifier Analysis", "Message Analysis", "Network Traffic Analysis", "Platform Monitoring", "Process Analysis", "User Behavior Analysis", "Execution Isolation", "Network Isolation", "Decoy Environment", "Decoy Object", "Credential Eviction", and "File Eviction".

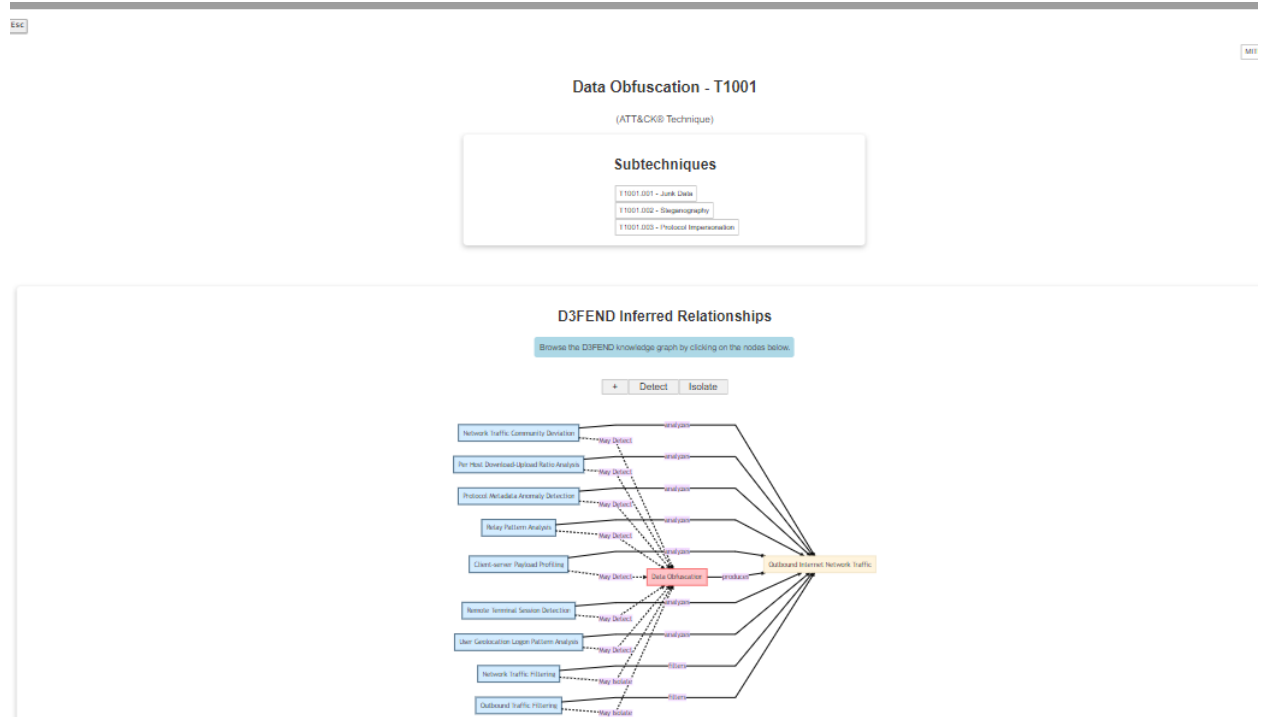
MITRE Lookup	Search D3FEND's 618 Artifacts	D3FEND Lookup
T1001 - Data Obfuscation		
T1001.001 - Junk Data		
T1001.002 - Steganography		
T1001.003 - Protocol Impersonation		
T1002 - Data Compressed		
T1003 - OS Credential Dumping		
T1003.001 - LSASS Memory		
T1003.002 - Security Account Manager		
T1003.003 - 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		
T1006 - Direct Volume Access		

Detect				Isolate	Deceive	Evict						
File analysis	Identifier Analysis	Message Analysis	Network Traffic Analysis	Platform Monitoring	Process Analysis	User Behavior Analysis	Execution Isolation	Network Isolation	Decoy Environment	Decoy Object	Credential Eviction	File Eviction
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	Decoy File	Account Locking	File Removal
Simulated 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	Decoy Network Resource	Authentication Cache Invalidation	Email Removal
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	Decoy Persona	Credential Revoking	
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		Decoy Public Release		
File Hashing	File Hash Reputation Analysis		Passive Certificate Analysis	Peripheral Firmware Verification	Process Self-Modification Detection	Job Function Access Pattern Analysis	Kernel-based Process Isolation	Hierarchical Domain Denylisting		Decoy Session Token		
	IP Reputation Analysis		Client-server Payload Profiling	System Firmware Verification	Process Spam Analysis	Local Account Monitoring	Mandatory Access Control	Homograph Denylisting		Decoy User Credential		
	URL Reputation Analysis		Connection Attempt Analysis	Operating System Monitoring	Process Linkage Analysis	Resource Access Pattern Analysis	System Call Filtering	Forward Resolution IP Denylisting				
								Reverse Resolution				

20. **Question:** In D3FEND Inferred Relationships, what does Data Obfuscation produce?

Answer: Outbound Internet Network Traffic. This indicates that Data Obfuscation

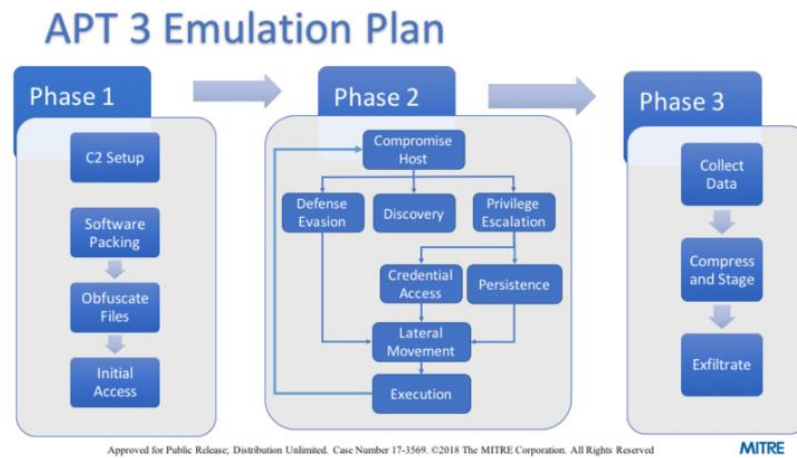
techniques often result in detectable network traffic patterns.



21. **Question:** In the APT3 Emulation Plan's Phase 1, what is listed first? **Answer:** C2 Setup

Command and Control (C2) setup is crucial in establishing communication channels for

controlling compromised systems.



e will not be going through this for every group on ATT&CK, rather select a subset we feel offer a unique perspective for defenses to be measured. e hope that the community finds use in these prototypes, and builds on them to make ATT&CK actionable. These are living documents that can be dated with newer information, format, or changed for other uses. Please reach out to attack@mitre.org for anything relating to these prototypes.

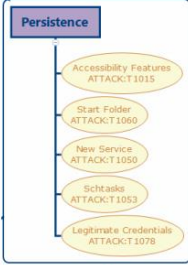
emulation Plan Documents

22. **Question:** Under Persistence, what binary was replaced with cmd.exe? **Answer:** sethc.exe. Replacing system binaries like sethc.exe with cmd.exe is a common

persistence technique, allowing backdoor access.

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

3.2.1.3 Persistence



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/Startup 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.

Figure 5 APT3 Persistence ATT&CK Techniques

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

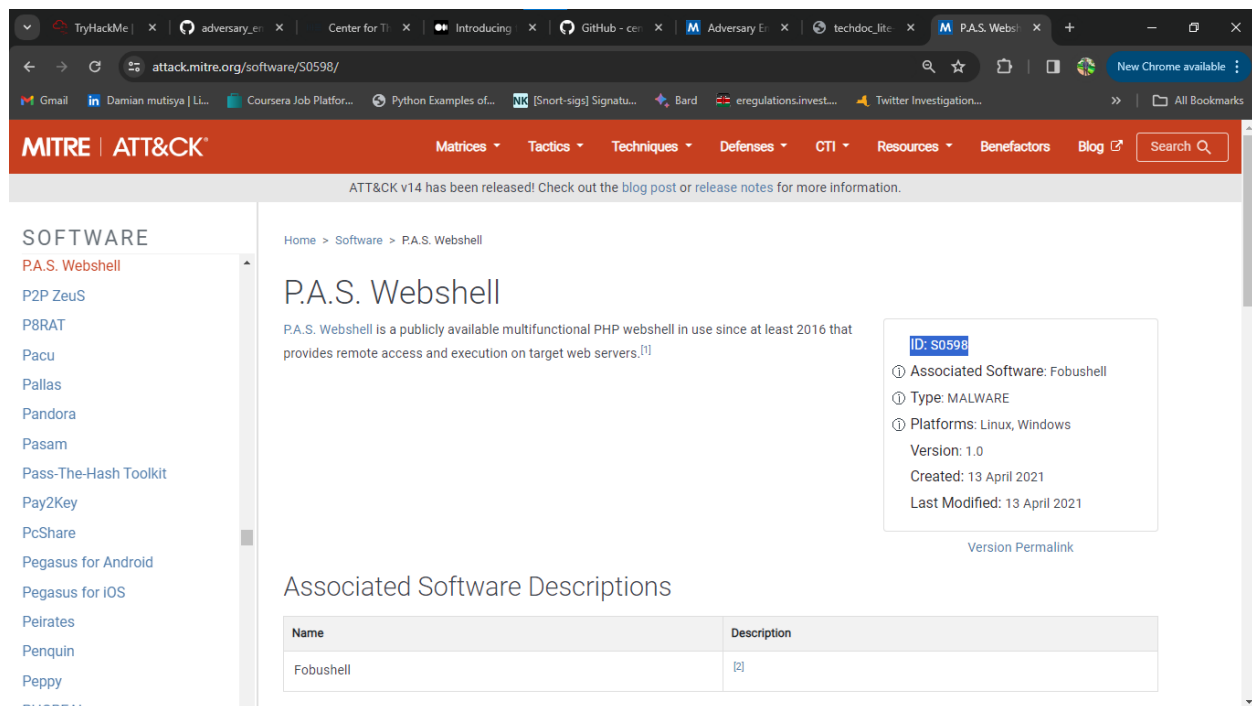
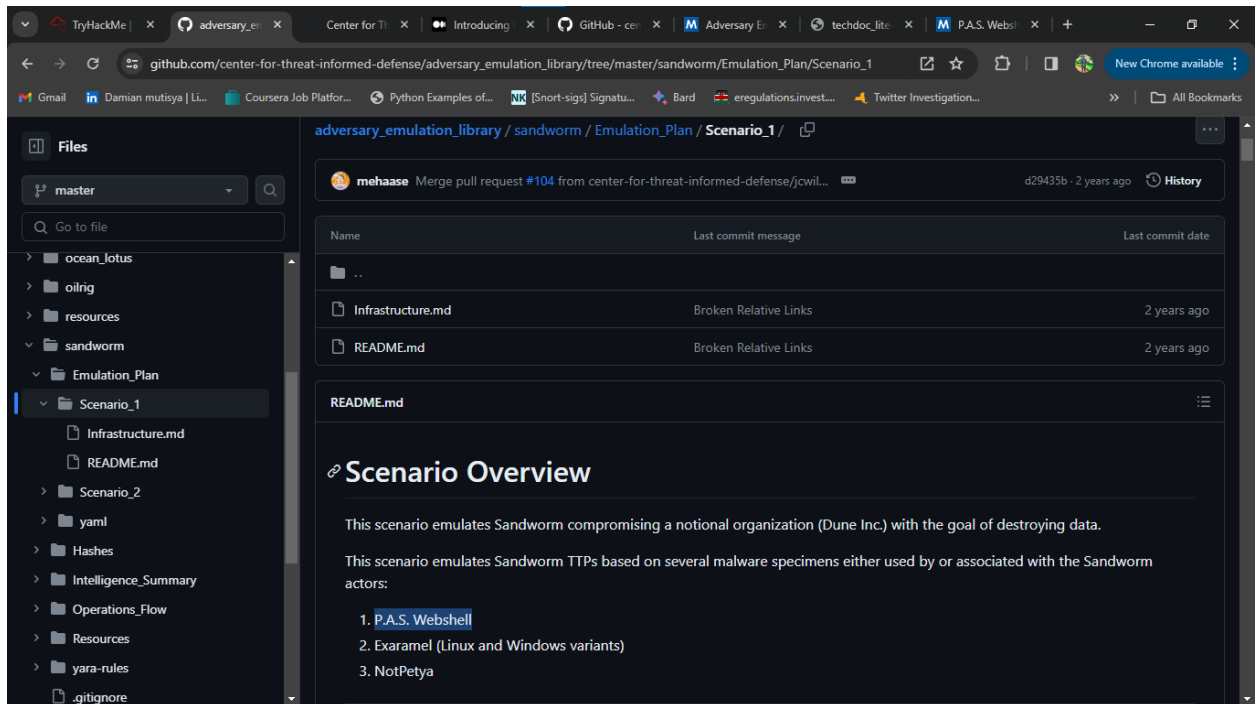
<https://attack.mitre.org/wiki/Technique/T1060>

23. **Question:** In APT29, what C2 frameworks are listed in Scenario 1? **Answer:** Pupy, Metasploit Framework: These frameworks provide versatile tools for establishing and maintaining control over compromised systems.

24. **Question:** What C2 framework is listed in Scenario 2 for APT29? **Answer:** PoshC2. PoshC2 is a PowerShell C2 framework used for post-exploitation and lateral movement.

25. **Question:** In the Sandworm Emulation Plan, what webshell is used in Scenario 1? **Answer:** P.A.S., ID: S0598. The use of P.A.S. webshell, identified as S0598, highlights

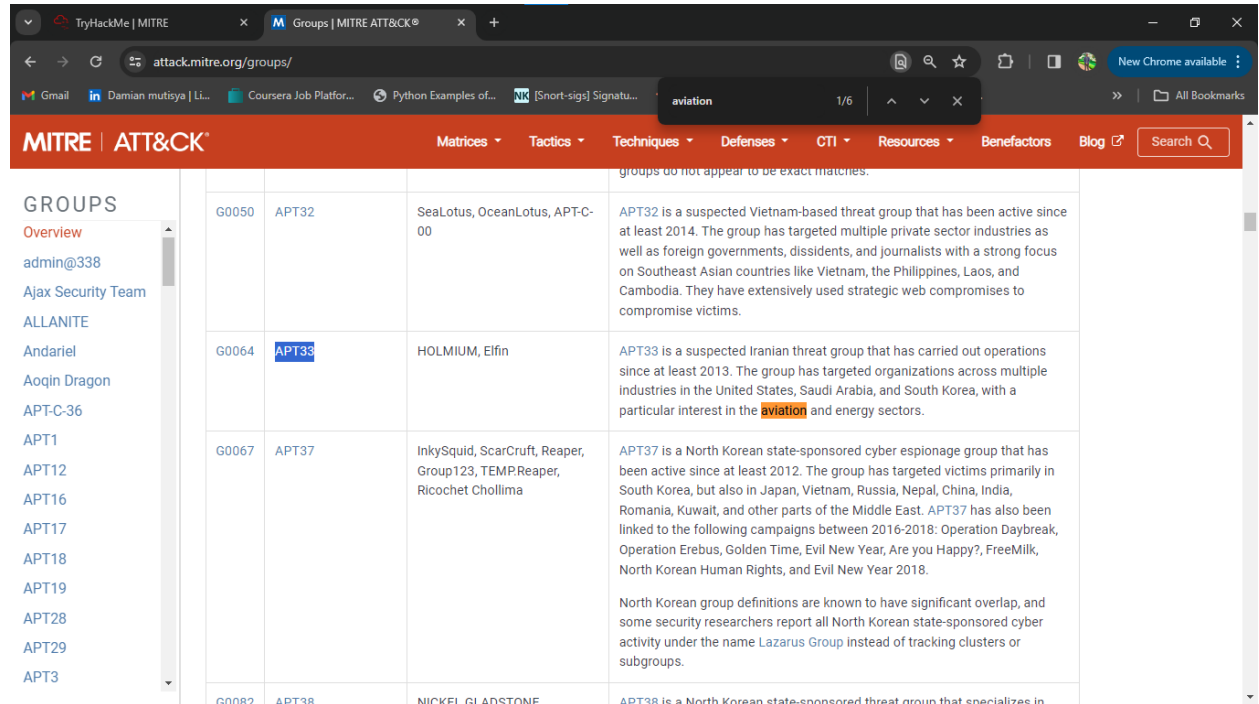
the group's preference for specific web-based exploitation tools.



26. Question: What is a group that targets your sector and has been active since 2013?

Answer: APT33.APT33's long-term activity underscores the need for sustained vigilance

and threat intelligence in the targeted sector.



The screenshot shows the MITRE ATT&CK Groups page. A search bar at the top right contains the text 'aviation'. The page displays a list of groups on the left and a table of results on the right. The table has four columns: ID, Name, Aliases, and Description. The results are filtered to show groups related to 'aviation'.

ID	Name	Aliases	Description
G0050	APT32	SeaLotus, OceanLotus, APT-C-00	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, Elfin	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. North Korean group definitions are known to have significant overlap, and some security researchers report all North Korean state-sponsored cyber activity under the name Lazarus Group instead of tracking clusters or subgroups.
G0082	APT38	NICKEL GLADSTONE	APT38 is a North Korean state-sponsored threat group that specializes in

27. **Question:** For cloud migration, what should be focused on regarding APT33? **Answer:**

Cloud Accounts. As organizations migrate to the cloud, safeguarding cloud accounts

against APT33's known tactics becomes crucial.

The screenshot shows a web browser with multiple tabs open, including 'Intro to C...', 'HackThe...', 'TryHack...', 'Valid Acc...', 'Axiom, G...', 'ATT&CK', 'CYBER SI...', 'CSA1-20...', and 'TryHack...'. The address bar shows the URL 'attack.mitre.org/techniques/T1078/004/'. The page header features the MITRE ATT&CK logo and navigation links: Matrices, Tactics, Techniques, Defenses, CTI, Resources, Benefactors, and Blog. A search bar is also present.

The main content area is titled 'Valid Accounts: Cloud Accounts'. On the left, a sidebar lists various techniques under the heading 'TECHNIQUES', with 'Cloud Accounts' highlighted. The main text describes the technique, stating that valid accounts in cloud environments may allow adversaries to perform actions to achieve Initial Access, Persistence, Privilege Escalation, or Defense Evasion. It mentions that cloud accounts are those created and configured by an organization for use by users, remote support, services, or for administration of resources within a cloud service provider or SaaS application. It also notes that cloud accounts can exist solely in the cloud or be hybrid joined between on-premises systems and the cloud through federation with other identity sources such as Windows Active Directory.

Other sub-techniques of Valid Accounts (4) are listed in a dropdown menu. The text continues: 'Service or user accounts may be targeted by adversaries through Brute Force, Phishing, or various other means to gain access to the environment. Federated accounts may be a pathway for the adversary to affect both on-premises systems and cloud environments.' It also states: 'An adversary may create long lasting Additional Cloud Credentials on a compromised cloud account to maintain persistence in the environment. Such credentials may also be used to bypass security controls such as multi-factor authentication.' Finally, it mentions: 'Cloud accounts may also be able to assume Temporary Elevated Cloud Access or other privileges through various means within the environment. Misconfigurations in role assignments or role assumption policies may allow an adversary to use these mechanisms to leverage permissions outside the intended scope of the account. Such over privileged accounts may be used to harvest sensitive data from online storage accounts and databases through Cloud API or other methods.'

On the right side, a box contains the following information:

- 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: 1.6
- Created: 13 March 2020
- Last Modified: 16 October 2023

A 'Version Permalink' link is also provided.

28. **Question:** What tool is associated with APT33 for cloud account exploitation? **Answer:**

Ruler. Ruler is a tool known for its effectiveness in compromising and manipulating

cloud-based services.

The screenshot shows a web browser window with the MITRE ATT&CK website. The URL is attack.mitre.org/software/S0358/. The page title is "Ruler". The left sidebar lists various software tools under the "SOFTWARE" category, including Ruler, RuMMS, RunningRAT, Ryuk, S-Type, S.O.V.A., Saint Bot, Sakula, SamSam, Sardonic, schtasks, SDBbot, SDelete, SeaDuke, Seasalt, and SEASURFER. The main content area for "Ruler" includes a description: "Ruler is a tool to abuse Microsoft Exchange services. It is publicly available on GitHub and the tool is executed via the command line. The creators of Ruler have also released a defensive tool, NotRuler, to detect its usage.^{[1][2]}". A metadata box on the right shows: ID: S0358, Type: TOOL, Platforms: Windows, Office 365, Version: 1.1, Created: 04 February 2019, Last Modified: 22 June 2020. Below this is a "Techniques Used" section with a table. The table has columns: Domain, ID, Name, and Use. It lists two techniques: T1087 (Account Discovery: Email Account) and T1137 (Office Application Startup: Outlook Forms). A "Version Permalink" link and an "ATT&CK Navigator Layers" button are also visible.

MITRE | ATT&CK®

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

ATT&CK v14 has been released! Check out the [blog post](#) or [release notes](#) for more information.

Home > Software > Ruler

Ruler

Ruler is a tool to abuse Microsoft Exchange services. It is publicly available on GitHub and the tool is executed via the command line. The creators of Ruler have also released a defensive tool, NotRuler, to detect its usage.^{[1][2]}

ID: S0358
① Type: TOOL
① Platforms: Windows, Office 365
Version: 1.1
Created: 04 February 2019
Last Modified: 22 June 2020

Version Permalink

ATT&CK® Navigator Layers

Techniques Used

Domain	ID	Name	Use
Enterprise	T1087 .003	Account Discovery: Email Account	Ruler can be used to enumerate Exchange users and dump the GAL. ^[1]
Enterprise	T1137 .003	Office Application Startup: Outlook Forms	Ruler can be used to automate the abuse of Outlook Forms to establish persistence. ^[1]

29. **Question:** For the technique T1566, what mitigation suggests SMS for implementation?

Answer: Multi-factor Authentication. Using SMS as part of Multi-factor Authentication

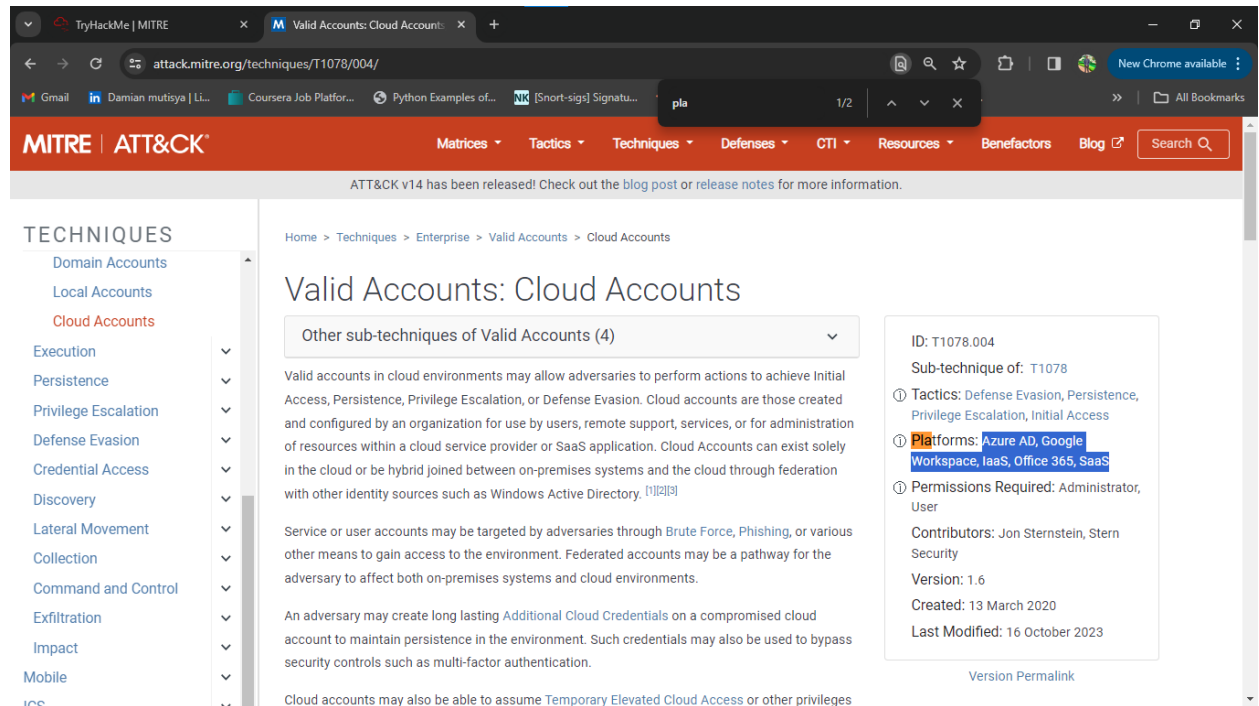
can enhance security by adding an additional layer of verification.

The screenshot shows the MITRE ATT&CK website. The top navigation bar includes links for Matrices, Tactics, Techniques, Defenses, CTI, Resources, Benefactors, and a Blog. A search bar is located on the right. The left sidebar lists various categories under 'TECHNIQUES', with 'Cloud Accounts' highlighted. The main content area is titled 'Mitigations' and contains a table with the following data:

ID	Mitigation	Description
M1036	Account Use Policies	Use conditional access policies to block logins from non-compliant devices or from outside defined organization IP ranges. ^[15]
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. ^[16]
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. ^[16]
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. ^{[17][18][19]} 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. ^[20] Consider using temporary, just-in-time (JIT) privileged access to Azure AD resources rather than permanently assigning privileged roles. ^[19]
M1018	User Account	Periodically review user accounts and remove those that are inactive or unnecessary. Limit the ability for user

30. **Question:** What platforms are affected by Technique T1566? **Answer:** Azure AD, Google Workspace, IaaS, Office 365, SaaS. These platforms, being widely used in

various organizational environments, are common targets for spear-phishing attacks.



Conclusion

The MITRE ATT&CK Matrix is an invaluable tool in the cybersecurity landscape, utilized by various teams for different purposes. The detailed analysis of Technique T1566 and related queries reveal the depth and breadth of the Matrix's application. From understanding specific attack techniques to planning defense strategies, the ATT&CK Matrix serves as a cornerstone for cybersecurity professionals seeking to bolster their defenses and understand the ever-evolving cyber threat landscape.


<https://tryhackme.com/p/Damiano254>

Intro to CHackTheTryHackMeRuler, SolAxiom, GATT&CKCYBERSA1-202TryHackMe

tryhackme.com/p/Damiano254

GmailDamian mutisya | Li...Coursera Job Platfor...Python Examples of...[Snort-sigs] Signatu...Barderegulations.invest...Twitter Investigation...All Bookmarks

TryHackMeDashboardLearnCompeteOtherGo Premium1




453054Rank

5Rooms Complete

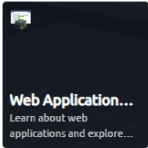
3Level

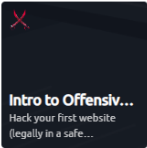
0Badges


Damiano254 [0x3]

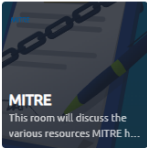
[Get Profile Badge ID](#) [Share Room Badges](#)


Rooms CompleteBadgesCreated RoomsYearly ActivityTickets

**Web Application...**
Learn about web applications and explore...

**Intro to Offensiv...**
Hack your first website (legally in a safe...

**Intro to Digital...**
Learn about digital forensics and related...

**MITRE**
This room will discuss the various resources MITRE h...

**Simple CTF**
Beginner level ctf

