

<https://infosecwriteups.com/mitre-tryhackme-room-writeup-walkthrough-by-md-amiruddin-5dbafe52f594>



Md Amiruddin Mart 20

MITRE | Tryhackme Room Writeup/Walkthrough | By Md Amiruddin

This room will discuss the various resources MITRE has made available for the cybersecurity community.

Room Link : <https://tryhackme.com/room/mitre>

Task 1 : Introduction to MITRE

For those that are new to the cybersecurity field, you probably never heard of MITRE. Those of us that have been around *might* only associate MITRE with CVEs ([Common Vulnerabilities and Exposures](#)) list, which is one resource you'll probably check when searching for an exploit for a given vulnerability. But 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.

From [Mitre.org](#): *"At MITRE, we solve problems for a safer world. Through our federally funded R&D centers and public-private partnerships, we work across government to tackle challenges to the safety, stability, and well-being of our nation."*

In this room, we will focus on other projects/research that the US-based non-profit MITRE Corporation has created for the cybersecurity community, specifically:

- ATT&CK® (**A**dversarial **T**actics, **T**echniques, **a**nd **C**ommo
n **K**nowledge) Framework
- CAR (**C**yber **A**nalYTics **R**epository) Knowledge Base
- ENGAGE (sorry, not a fancy acronym)
- D3FEND (**D**etection, **D**enial,
and **D**isruption Framework **E**mpowering Network **D**efense
)
- AEP (**A**TT&**C**K **E**mulation **P**lans)

Task 2 : Basic Terminology



Before diving in, let's briefly discuss a few terms that you will often hear when dealing with the framework, threat intelligence, etc.

APT is an acronym for **A**dvanced **P**ersistent **T**hreat. This can be considered a team/group (***threat group***), or even country (***nation-state group***), that engages in long-term attacks against organizations and/or countries. The term 'advanced' can be misleading as it will tend to cause us to believe that each APT group all have some super-weapon, e.i. a zero-day exploit, that they use. That is not the case. As we will see a bit later, the techniques these APT groups use are quite common and can be detected with the right implementations in place. You can view FireEye's current list of APT groups [here](#).

TTP is an acronym for **T**actics, **T**echniques, and **P**rocedures, but what does each of these terms mean?

- The **Tactic** is the adversary's goal or objective.
- The **Technique** is how the adversary achieves the goal or objective.
- The **Procedure** is how the technique is executed.

If that is not that clear now, don't worry. Hopefully, as you progress through each section, TTPs will make more sense.

Task 3 : ATT&CK® Framework



What is the ATT&CK® framework?

According to the [website](#), “MITRE ATT&CK® is a globally-accessible knowledge base of adversary tactics and techniques based on real-world observations.” In 2013, 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. This started with an internal project known as FMX (**Fort Meade Experiment**). Within this project, selected security professionals were tasked to emulate 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.

The ATT&CK® framework has grown and expanded throughout the years. One notable expansion was that the framework focused solely on the Windows platform but has expanded to cover other platforms, such as macOS and Linux. The framework is heavily contributed to by many sources, such as security researchers and threat intelligence reports. Note this is not only a tool for blue teamers. The tool is also useful for red teamers.

If you haven't done so, navigate to the ATT&CK® [website](#).

Direct your attention to the bottom of the page to view the **ATT&CK® Matrix for Enterprise**. Across the top of the matrix, there are 14 categories. Each category contains the techniques an adversary could use to perform the tactic. The

categories cover the seven-stage Cyber Attack Lifecycle (credit Lockheed Martin for the Cyber Kill Chain).

Essential Framework for the Cyber Risk Analyst

ATT&CK Matrix for Enterprise

layout: side

show sub-techniques

hide sub-techniques

Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 12 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 16 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 19 techniques	Exfiltration 9 techniques	Impact 12 techniques
---------------------------------	--------------------------------------	--------------------------------	----------------------------	------------------------------	---------------------------------------	----------------------------------	------------------------------------	----------------------------	----------------------------------	-----------------------------	--------------------------------------	------------------------------	-------------------------

(ATT&CK Matrix v11.2)

Under **Initial Access**, there are 9 techniques. Some of the techniques have sub-techniques, such as Phishing.

Initial Access

9 techniques

Drive-by Compromise	
Exploit Public-Facing Application	
External Remote Services	
Hardware Additions	
Phishing (3)	
Replication Through Removable Media	
Supply Chain Compromise (3)	
Trusted Relationship	
Valid Accounts (4)	

If we click on the gray bar to the right, a new layer appears listing the sub-techniques.

	Spearphishing Attachment
Phishing (3)	Spearphishing Link
	Spearphishing via Service

To get a better understanding of this technique and its associated sub-techniques, click on Phishing.

We have been directed to a page dedicated to the technique known as Phishing and all related information regarding the technique, such as a brief description, **Procedure Examples**, and **Mitigations**.

Phishing

Sub-techniques (3)

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 or to gather credentials for use of **Valid Accounts**. Phishing may also be conducted via third-party services, like social media platforms.

You can alternatively resort to using the Search feature to retrieve all associated information regarding a given technique, sub-technique, and/or group.

phishing|

Phishing: Technique T1566 - Enterprise

Phishing: 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 spearphish...

Phishing: Spearphishing Attachment, Sub-technique T1566.001 - Enterprise

Phishing: Spearphishing Attachment Adversaries may send spearphishing emails with a malicious attachment in an attempt to gain access to victim systems. Spearphishing attachment is a specific varian...

Phishing: Spearphishing via Service, Sub-technique T1566.003 - Enterprise

Phishing: Spearphishing via Service Adversaries may send spearphishing messages via third-party services in an attempt to gain access to victim systems. Spearphishing via service is a specific varia...

Phishing: Spearphishing Link, Sub-technique T1566.002 - Enterprise

Phishing: Spearphishing Link Adversaries may send spearphishing emails with a malicious link in an attempt to gain access to victim systems. Spearphishing with a link is a specific variant of spearp...

Phishing for Information, Technique T1598 - Enterprise

Phishing for Information Before compromising a victim, adversaries may send phishing messages to elicit sensitive information that can be used during targeting. Phishing for information is an attempt...

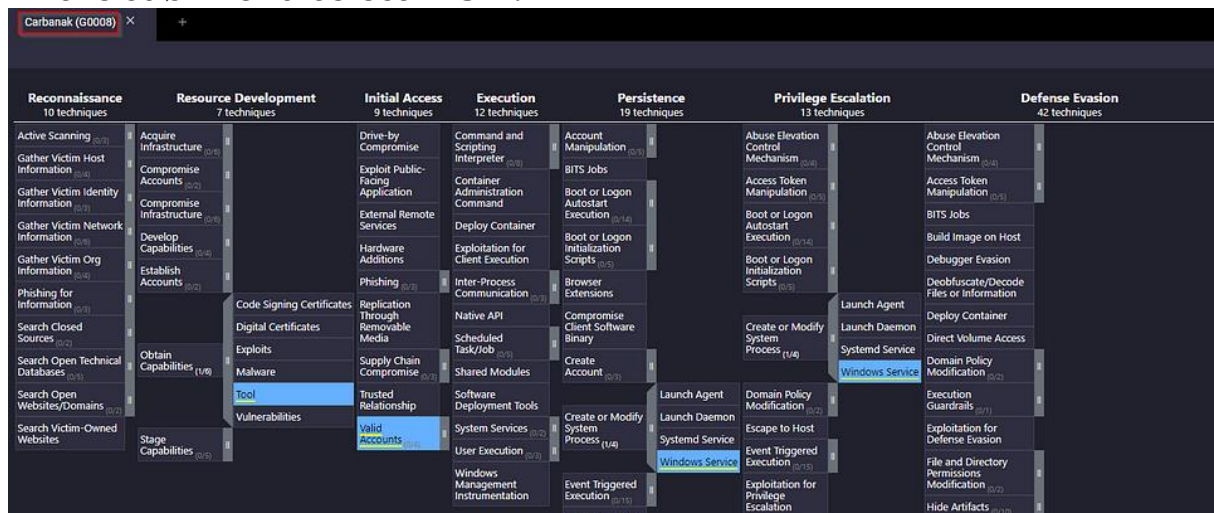
load more results

Lastly, the same data can be viewed via the **MITRE ATT&CK® Navigator**: *“The ATT&CK® Navigator is designed to provide basic navigation and annotation of ATT&CK® matrices, something that people are already doing today in tools like Excel. We’ve designed it to be simple and generic — you can use the Navigator to visualize your defensive coverage, your red/blue team planning, the frequency of detected techniques, or anything else you want to do.”*

You can access the Navigator view when visiting a group or tool page. The ATT&CK® Navigator Layers button will be available.

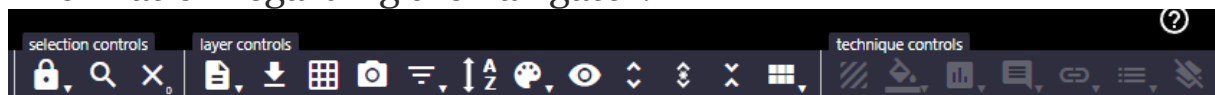
ATT&CK® Navigator Layers ▾

In the sub-menu select **view**.



Let's get acquainted with this tool. Click [here](#) to view the ATT&CK® Navigator for Carbanak.

At the top left, there are 3 sets of controls: **selection controls**, **layer controls**, and **technique controls**. I encourage you to inspect each of the options under each control to get familiar with them. The question mark at the far right will provide additional information regarding the navigator.



To summarize, we can use the ATT&CK Matrix to map a threat group to their tactics and techniques. There are various methods the search can be initiated.

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.

Answer the questions below :

1. Besides blue teamers, who else will use the ATT&CK Matrix?
A. red teamers
2. What is the ID for this technique?
A. T1566
3. Based on this technique, what mitigation covers identifying social engineering techniques?
A. User Training
4. What are the data sources for Detection? (format: source1,source2,source3 with no spaces after commas)
A. Application Log,File,Network Traffic
5. What groups have used spear-phishing in their campaigns? (format: group1,group2)
A. Axiom,GOLD SOUTHFIELD
6. Based on the information for the first group, what are their associated groups?
A. Group 72
7. What software is associated with this group that lists phishing as a technique?
A. Hikit
8. What is the description for this software?
A. 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?
A. Winnti Group
10. How many techniques are attributed to this group?
A. 15

Task 4 : CAR Knowledge Base

[Cyber Analytics Repository](#)

The official definition of **CAR** is “*The MITRE Cyber Analytics Repository (CAR) is a knowledge base of analytics developed by*

MITRE based on the MITRE ATT&CK® adversary model. 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. With respect to coverage, CAR is focused on providing a set of validated and well-explained analytics, in particular with regards to their operating theory and rationale.”

Instead of further attempting to explain what CAR is, let's dive in. With our newly acquired knowledge from the previous section, we should feel comfortable and understand the information that CAR is providing to us.

Let's begin our journey by reviewing [CAR-2020-09-001: Scheduled Task — File Access](#).

Upon visiting the page, we're given a brief description of the analytic and references to ATT&CK (**technique**, **sub-technique**, and **tactic**).

MITRE Cyber Analytics Repository

CAR-2020-09-001: Scheduled Task - FileAccess

In order to gain persistence, privilege escalation, or remote execution, an adversary may use the Windows Task Scheduler to schedule a command to be run at a specified time, date, and even host. Task Scheduler stores tasks as files in two locations - C:\Windows\Tasks (legacy) or C:\Windows\System32\Tasks. Accordingly, this analytic looks for the creation of task files in these two locations.

Technique	Subtechnique(s)	Tactic(s)
Scheduled Task/Job	Scheduled Task	Execution, Persistence, Privilege Escalation

We're also provided with Pseudocode and a query on how to search for this specific analytic within Splunk. A pseudocode is a plain,

human-readable way to describe a set of instructions or algorithms that a program or system will perform.

Splunk search - Windows task file creation (Splunk, Sysmon native)

This Splunk search looks for any files created under the Windows tasks directories.

```
index=__your_sysmon_index__ EventCode=11 Image!="C:\\WINDOWS\\system32\\svchost.exe" (TargetFilename="C:\\Windows\\System32\\Tasks\\*" OR TargetFilename="C:\\Windows\\Tasks\\*")
```

Note the reference to Sysmon. If you're not familiar with Sysmon, check out the Sysmon [room](#).

To take full advantage of CAR, we can view the [Full Analytic List](#) or the [CAR ATT&CK® Navigator layer](#) to view all the analytics.

Full Analytic List Analytics

Analytic List (by date added)

Analytic	ATT&CK Techniques	Implementations	Applicable Platform(s)
----------	-------------------	-----------------	------------------------

In the Full Analytic List view, we can see what implementations are available for any given analytic at a single glance, along with what OS platform it applies to.

CAR ATTACK Navigator

ATT&CK Analytic Coverage - CAR					
Initial Access 9 techniques	Execution 10 techniques	Persistence 18 techniques	Privilege Escalation 13 techniques	Defense Evasion 36 techniques	Credential Access 14 techniques
Drive-by Compromise	Command and Scripting Interpreter (2/9)	Account Manipulation (2/2)	Abuse Elevation Control Mechanism (1/9)	Abuse Elevation Control Mechanism (1/9)	Adversary-in-the-Middle (2/2)
Exploit Public-Facing Application	Exploitation for Client Execution	BITS Jobs	Access Token Manipulation (2/5)	Access Token Manipulation (2/5)	Brute Force (2/4)
External Remote Services	Inter-Process Communication (1/2)	Boot or Logon Autostart Execution (3/15)	Boot or Logon Autostart Execution (3/15)	BITS Jobs	Credentials from Password Stores (2/5)
Hardware Additions	Native API	Boot or Logon Initialization Scripts (1/5)	Boot or Logon Initialization Scripts (1/5)	Deobfuscate/Decode Files or Information	Exploitation for Credential Access
Phishing (2/2)	Scheduled Task/Job (2/5)	Browser Extensions	Create or Modify System Process (1/4)	Direct Volume Access	Forced Authentication
Replication Through Removable Media	Shared Modules	Compromise Client Software Binary	Domain Policy Modification (2/2)	Domain Policy Modification (2/2)	Forge Web Credentials (1/2)
Supply Chain Compromise (2/5)	Software Deployment Tools	Create Account (1/2)	Escape to Host	Execution Guardrails (2/7)	Input Capture (2/4)
Trusted Relationship	System Services (2/2)	Create or Modify System Process (1/4)	Event Triggered Execution (6/15)	Exploitation for Defense Evasion	Modify Authentication Process (2/4)
Valid Accounts (2/3)	User Execution (1/2)	Event Triggered Execution (6/15)	Exploitation for Privilege Escalation	File and Directory Permissions Modification (2/2)	Network Sniffing
	Windows Management Instrumentation	External Remote Services	Hijack Execution Flow (6/11)	Hide Artifacts (1/9)	OS Credential Dumping (3/9)
		Hijack Execution Flow (6/11)	Process Injection (2/11)	Hijack Execution Flow (6/11)	Steal or Forge Kerberos Tickets (2/4)
		Modify Authentication Process (2/4)	Scheduled Task/Job (2/5)	Impair Defenses (2/7)	Steal Web Session Cookie
		Office Application Startup (2/6)	Valid Accounts (2/3)	Indicator Removal on Host (3/9)	Two-Factor Authentication Interception
		Pre-OS Boot (2/5)		Indirect Command Execution	Unsecured Credentials (2/5)
		Scheduled Task/Job (2/5)		Masquerading (2/2)	
		Server Software Component (1/4)		Modify Authentication Process (2/4)	
				Modify Registry	

(The techniques highlighted in purple are the analytics currently in CAR)

Let's look at another analytic to see a different implementation, [CAR-2014-11-004: Remote PowerShell Sessions](#).

Under Implementations, a pseudocode is provided and an EQL version of the pseudocode. EQL (pronounced as 'equal'), and it's an acronym for Event Query Language. EQL can be utilized to query, parse, and organize Sysmon event data. You can read more about this [here](#).

Eql, EQL native

EQL version of the above pseudocode.

```
process where subtype.create and
  (process_name == "wsmpovhost.exe" and parent_process_name == "svchost.exe")
```

To summarize, CAR is a great place for finding analytics that takes us further than the Mitigation and Detection summaries in the ATT&CK® framework. This tool is not a replacement for ATT&CK® but an added resource.

Answer the questions below :

1. For the above analytic, what is the pseudocode a representation of?
A. splunk search
2. What tactic has an ID of TA0003?
A. Persistence
3. What is the name of the library that is a collection of Zeek (BRO) scripts?
A. BZAR
4. What is the name of the technique for running executables with the same hash and different names?
A. Masquerading

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

Task 5 : MITRE Engage

MITRE ENGAGE

Per the website, “**MITRE Engage** is a framework for planning and discussing adversary engagement operations that empowers you to engage your adversaries and achieve your cybersecurity goals.”

MITRE Engage is considered an **Adversary Engagement Approach**. This is accomplished by the implementation of **Cyber Denial** and **Cyber Deception**.

With **Cyber Denial** we prevent the adversary’s ability to conduct their operations and with **Cyber Deception** we intentionally plant artifacts to mislead the adversary.

The Engage website provides a [starter kit](#) to get you ‘started’ with the Adversary Engagement Approach. The starter kit is a collection of whitepapers and PDFs explaining various checklists, methodologies, and processes to get you started.

As with MITRE ATT&CK, Engage has its own matrix. Below is a visual of the **Engage Matrix**.

INTRODUCING THE ENGAGE MATRIX!								
Prepare	Expose		Affect			Elicit		Understand
Plan	Collect	Detect	Prevent	Direct	Disrupt	Reassure	Motivate	Analyze
Cyber Threat Intelligence	API Monitoring	Introduced Vulnerabilities	Baseline	Attack Vector Migration	Isolation	Application Diversity	Application Diversity	After-Action Review
Engagement Environment	Network Monitoring	Lures	Hardware Manipulation	Email Manipulation	Lures	Artifact Diversity	Artifact Diversity	Cyber Threat Intelligence
Gating Criteria	Software Manipulation	Malware Detonation	Isolation	Introduced Vulnerabilities	Network Manipulation	Burn-In	Information Manipulation	Threat Model
Operational Objective	System Activity Monitoring	Network Analysis	Network Manipulation	Lures	Software Manipulation	Email Manipulation	Introduced Vulnerabilities	
Persona Creation			Security Controls	Malware Detonation		Information Manipulation	Malware Detonation	
Storyboarding				Network Manipulation		Network Diversity	Network Diversity	
Threat Model				Peripheral Management		Peripheral Management	Personas	
				Security Controls		Pocket Litter		
				Software Manipulation				

(Source: <https://engage.mitre.org>)

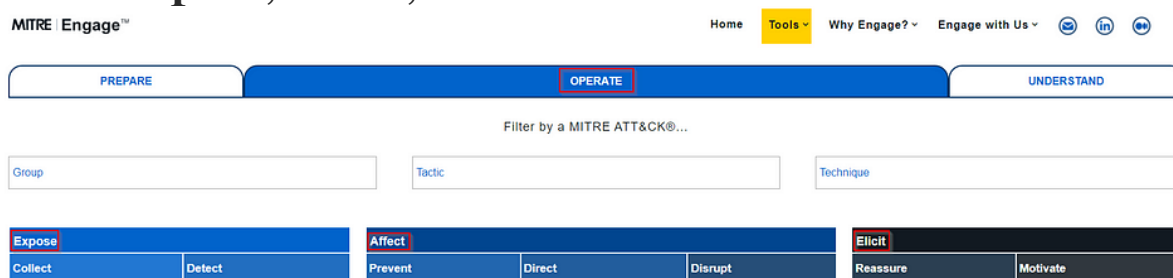
Let's quickly explain each of these categories based on the information on the Engage website.

- **Prepare** the set of operational actions that will lead to your desired outcome (input)
- **Expose** adversaries when they trigger your deployed deception activities
- **Affect** adversaries by performing actions that will have a negative impact on their operations
- **Elicit** information by observing the adversary and learn more about their modus operandi (TTPs)
- **Understand** the outcomes of the operational actions (output)

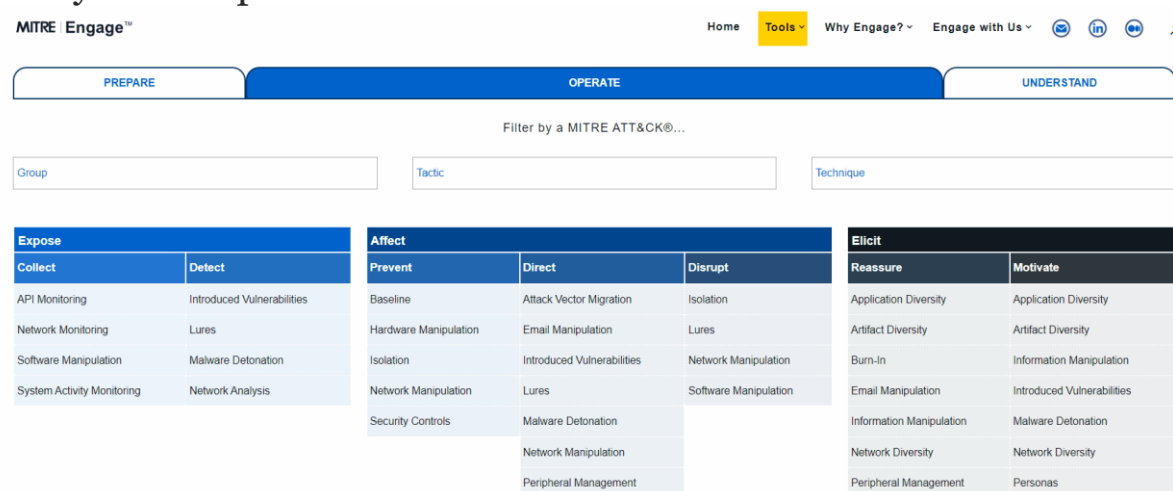
Refer to the [Engage Handbook](#) to learn more.

You can interact with the [Engage Matrix Explorer](#). We can filter by information from [MITRE ATT&CK](#).

Note that by default the matrix focuses on **Operate**, which entails **Expose**, **Affect**, and **Elicit**.



You can click on **Prepare** or **Understand** if you wish to focus solely on that part of the matrix.



That should be enough of an overview. We'll leave it to you to explore the resources provided to you on this website.

Before moving on, let's practice using this resource by answering the questions below.

Answer the questions below :

1. Under Prepare, what is ID SAC0002?
A. Persona Creation
2. What is the name of the resource to aid you with the engagement activity from the previous question?
A. PERSONA PROFILE WORKSHEET
3. Which engagement activity baits a specific response from the adversary?
A. Lures
4. What is the definition of Threat Model?
A. A risk assessment that models organizational strengths and weaknesses

Task 6 : MITRE D3FEND

[D3FEND](#)

What is this MITRE resource? Per the [D3FEND](#) website, this resource is “*A knowledge graph of cybersecurity countermeasures.*”

D3FEND is still in beta and is funded by the Cybersecurity Directorate of the NSA.

D3FEND stands for **D**etection, **D**enial, and **D**isruption **F**ramework **E**mpowering **N**etwork **D**efense.

At the time of this writing, there are 408 artifacts in the D3FEND matrix. See the below image.

DEFEND™

A knowledge graph of cybersecurity countermeasures

0.10.0-BETA-2

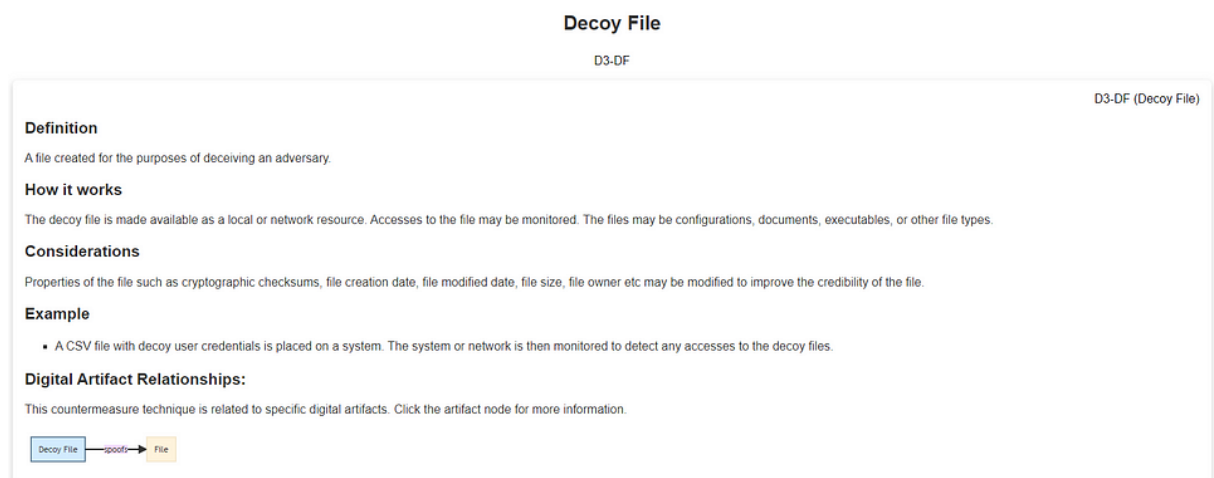
ATT&CK Lookup

Search D3FEND's 408 Artifacts

D3FEND Lookup

Harden				Detect						Isolate		Deceive		Evict		
Application Hardening	Credential Hardening	Message Hardening	Platform Hardening	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	Process Eviction

Let's take a quick look at one of the D3FENDs artifacts, such as **Decoy File**.



The screenshot shows the D3FEND artifact page for "Decoy File". The page is titled "Decoy File" and "D3-DF". It contains the following sections:

- Definition**: A file created for the purposes of deceiving an adversary.
- How it works**: The decoy file is made available as a local or network resource. Accesses to the file may be monitored. The files may be configurations, documents, executables, or other file types.
- Considerations**: Properties of the file such as cryptographic checksums, file creation date, file modified date, file size, file owner etc may be modified to improve the credibility of the file.
- Example**: A CSV file with decoy user credentials is placed on a system. The system or network is then monitored to detect any accesses to the decoy files.
- Digital Artifact Relationships**: This countermeasure technique is related to specific digital artifacts. Click the artifact node for more information.

At the bottom, there is a diagram showing a "Decoy File" node connected to a "File" node.

As you can see, you're provided with information on what is the technique (**definition**), how the technique works (**how it works**), things to think about when implementing the technique (**considerations**), and how to utilize the technique (**example**).

Note, as with other MITRE resources, you can filter based on the ATT&CK matrix.

Since this resource is in beta and will change significantly in future releases, we won't spend that much time on D3FEND.

The objective of this task is to make you aware of this MITRE resource and hopefully you'll keep an eye on it as it matures in the future.

We will still encourage you to navigate the website a bit by answering the questions below.

Answer the questions below :

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

A. Data Obfuscation

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

A. Outbound Internet Network Traffic

Task 7 : ATT&CK® Emulation Plans

If these tools provided to us by MITRE are not enough, under [MITRE ENGENUITY](#), we have **CTID**, the **Adversary Emulation Library**, and **ATT&CK® Emulation Plans**.

CTID

MITRE formed an organization named The [Center of Threat-Informed Defense](#) (CTID). This organization consists of various companies and vendors from around the globe. Their objective is to conduct research on cyber threats and their TTPs and share this research to improve cyber defense for all.

Some of the companies and vendors who are participants of CTID:

- AttackIQ (founder)
- Verizon
- Microsoft (founder)
- Red Canary (founder)
- Splunk

Per the website, “Together with Participant organizations, we cultivate solutions for a safer world and advance threat-informed defense with open-source software, methodologies, and frameworks. By expanding upon the MITRE ATT&CK knowledge base, our work expands the global understanding of cyber adversaries and their tradecraft with the public release of data sets critical to better understanding adversarial behavior and their movements.”

Adversary Emulation Library & ATT&CK® Emulations Plans

The [Adversary Emulation Library](#) is a public library making adversary emulation plans a free resource for blue/red teamers. The library and the emulations are a contribution from CTID. There are several [ATT&CK® Emulation Plans](#) currently available: [APT3](#), [APT29](#), and [FIN6](#). The emulation plans are a step-by-step guide on how to mimic the specific threat group. If any of the C-Suite were to ask, “how would we fare if APT29 hits us?” This can easily be answered by referring to the results of the execution of the emulation plan.

Review the emulation plans to answer the questions below.
Answer the questions below :

1. In Phase 1 for the APT3 Emulation Plan, what is listed first?
A. C2 Setup
2. Under Persistence, what binary was replaced with cmd.exe?
A. sethc.exe
3. Examining APT29, what C2 frameworks are listed in Scenario 1 Infrastructure? (format: tool1,tool2)
A. Pupy, Metasploit Framework
4. What C2 framework is listed in Scenario 2 Infrastructure?
A. 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)
P.A.S., S0598

Task 8 : ATT&CK® and Threat Intelligence

Threat Intelligence (TI) or Cyber Threat Intelligence

(CTI) is the information, or TTPs, attributed to the adversary. By using threat intelligence, as defenders, we can make better decisions regarding the defensive strategy. Large corporations might have an in-house team whose primary objective is to gather threat intelligence for other teams within the organization, aside from using threat intel already readily available. Some of this threat intel can be open source or through a subscription with a vendor, such as [CrowdStrike](#). In contrast, many defenders wear multiple hats (roles) within some organizations, and they need to take time from their other tasks to focus on threat intelligence. To cater to the latter, we'll work on a scenario of using ATT&CK® for threat intelligence. The goal of threat intelligence is to make the information actionable.

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. Answer the questions below :

1. What is a group that targets your sector who has been in operation since at least 2013?
A. 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?
A. Cloud Accounts
3. What tool is associated with the technique from the previous question?
A. Ruler
4. Per the detection tip, what should you be detecting? (format: phrase1 or phrase2)
A. abnormal or malicious behavior
5. What platforms does the technique from question #2 affect?
A. Azure AD, Google Workspace, IaaS, Office 365, SaaS

Task 9 : Conclusion

In this room, we explored tools/resources that MITRE has provided to the security community. The room's goal was to expose you to these resources and give you a foundational knowledge of their uses. Many vendors of security products and security teams across the globe consider these contributions from MITRE invaluable in the day-to-day efforts to thwart evil. The more information we have as defenders, the better we are equipped to fight back. Some of you might be looking to transition to become a SOC analyst, detection engineer, cyber threat analyst, etc. these tools/resources are a must to know.

As mentioned before, though, this is not only for defenders. As red teamers, these tools/resources are useful as well. Your objective is to mimic the adversary and attempt to bypass all the controls in place within the environment. With these resources, as the red teamer, you can effectively mimic a true adversary and communicate your findings in a common language that both sides can understand. In a nutshell, this is known as **purple teaming**.

Answer the questions below :

- 1. Read the above
- A. No answer needed

Thankyou For Reading.