**MITRE**

MITRE research 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.

What MITRE does:

* ATT&CK*®* (**A**dversarial **T**actics, **T**echniques, **and** **C**ommon **K**nowledge) Framework
* CAR (**C**yber **A**nalytics **R**epository) Knowledge Base
* ENGAGE
* D3FEND (**D**etection, **D**enial, and **D**isruption **F**ramework **E**mpowering **N**etwork **D**efense)
* AEP (**A**TT&CK **E**mulation **P**lans)

**APT**

**APT** is an acronym for **Advanced Persistent Threat**. 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.

**TTP**

TTP is an acronym for **Tactics, Techniques, and Procedures,** 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.

**ATT&CK**

"MITRE ATT&CK® is a globally accessible knowledge base of adversary tactics and techniques based on real-world observations."

#### THM Questions

*Besides blue teamers, who else will use the ATT&CK Matrix?*

Red Teamers

*What is the ID for this technique?*

T1566

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

User Training

*What are the data sources for Detection?*

Application Log, File, Network Traffic

*What groups have used spear-phishing in their campaigns?*

Axiom, Gold Southfield

*What are their associated groups?*

Group 72

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

Hikit

*What is the description for this software?*

Hikit is malware that has been used by Axiom for late-stage persistence and exfiltration after the initial compromise.

*This group overlaps with?*

Winnti Group

*How many techniques are attributed to this group?*

15

#### …

**CAR**

"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."

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.

**Implementations**

* Pseudocode - Windows task file creation (Pseudocode, CAR native)
* 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)
* LogPoint search - Windows task file creation (Logpoint, LogPoint native)

#### THM Questions

*For the above analytic, what is the pseudocode a representation of?*

CAR-2020-09-001

*What tactic has an ID of TA0003?*

**Persistence**

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

**BZAR**

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

**Masquerading**

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

**Unit Tests**

#### …

**MITRE Engage**

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.

* **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)

#### THM Questions

*Under Prepare, what is ID SAC0002?*

**Persona Creation**

*What is the name of the resource to aid you with the engagement activity from the previous question?***PERSONA PROFILE WORKSHEET** *Which engagement activity baits a specific response from the adversary?***Lures**

*What is the definition of Threat Model?***A risk assessment that models organizational strengths and weaknesses**

#### …

**MITRE D3FEND**

Per the [**D3FEND**](https://d3fend.mitre.org/) website, this resource is "*A knowledge graph of cybersecurity countermeasures.*"

#### THM Questions

*Question 1: What is the first MITRE ATT&CK technique listed in the ATT&CK Lookup dropdown?*

**Answer: Data Obfuscation**

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

**Outbound Internet Network Traffic**

#### ***…***

**ATT&CK Emulation Plans**

The **[Center of Threat-Informed Defense](https://mitre-engenuity.org/ctid/" \t "_blank)** (**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

**Adversary Emulation Library & ATT&CK**®**Emulations Plans**

The [**Adversary Emulation Library**](https://medium.com/mitre-engenuity/introducing-the-all-new-adversary-emulation-plan-library-234b1d543f6b) 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**](https://github.com/center-for-threat-informed-defense/adversary_emulation_library) currently available: [**APT3**](https://attack.mitre.org/resources/adversary-emulation-plans/), [**APT29**](https://github.com/center-for-threat-informed-defense/adversary_emulation_library/tree/master/apt29), and [**FIN6**](https://github.com/center-for-threat-informed-defense/adversary_emulation_library/tree/master/fin6).

#### THM Questions

Question 1: In Phase 1 for the APT3 Emulation Plan, what is listed first?

Answer: C2 Setup

Question 2: Under Persistence, what binary was replaced with cmd.exe?

Answer: sethc.exe

Question 3: Examining APT29, what  C2 frameworks are listed in Scenario 1 Infrastructure? (format: tool1,tool2)

Answer: Pupy,Metasploit Framework

Question 4: What C2 framework is listed in Scenario 2 Infrastructure?

Answer: PoshC2

Question 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)

Answer: P.A.S.,S0598

#### …

**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**](https://www.crowdstrike.com). 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.

#### THM Questions

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

Answer: APT33

Question 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?

Answer: Cloud Accounts

Question 3: What tool is associated with the technique from the previous question?

Answer: Ruler

Question 4: Per the detection tip, what should you be detecting? (format: phrase1 or phrase2)

Answer: abnormal or malicious behavior

Question 5: What platforms does the technique from question #2 affect?

Answer: Azure AD, Google Workspace, IaaS, Office 365, SaaS

#### …

**MISP**

[**MISP (Malware Information Sharing Platform)**](https://www.misp-project.org/) is an open-source threat information platform that facilitates the collection, storage and distribution of threat intelligence and Indicators of Compromise (IOCs) related to malware, cyber attacks, financial fraud or any intelligence within a community of trusted members.

Additionally, the threat information can be distributed and consumed by Network Intrusion Detection Systems (NIDS), log analysis tools and Security Information and Event Management Systems (SIEM).

**MISP is effectively useful for the following use cases:**

* **Malware Reverse Engineering**: Sharing of malware indicators to understand how different malware families function.
* **Security Investigations:** Searching, validating and using indicators in investigating security breaches.
* **Intelligence Analysis:** Gathering information about adversary groups and their capabilities.
* **Law Enforcement:**Using indicators to support forensic investigations.
* **Risk Analysis:**Researching new threats, their likelihood and occurrences.
* **Fraud Analysis:** Sharing of financial indicators to detect financial fraud.

**What does MISP support?**

MISP provides the following core functionalities:

* **IOC database:** This allows for the storage of technical and non-technical information about malware samples, incidents, attackers and intelligence.
* **Automatic Correlation:** Identification of relationships between attributes and indicators from malware, attack campaigns or analysis.
* **Data Sharing:** This allows for sharing of information using different models of distributions and among different MISP instances.
* **Import & Export Features:** This allows the import and export of events in different formats to integrate other systems such as NIDS, HIDS, and OpenIOC.
* **Event Graph:** Showcases the relationships between objects and attributes identified from events.
* **API support:** Supports integration with own systems to fetch and export events and intelligence.

The following terms are commonly used within MISP and are related to the functionalities described above and the general usage of the platform:

* **Events:** Collection of contextually linked information.
* **Attributes:** Individual data points associated with an event, such as network or system indicators.
* **Objects:** Custom attribute compositions.
* **Object References:** Relationships between different objects.
* **Sightings:** Time-specific occurrences of a given data point or attribute detected to provide more credibility.
* **Tags:** Labels attached to events/attributes.
* **Taxonomies:** Classification libraries are used to tag, classify and organise information.
* **Galaxies:** Knowledge base items used to label events/attributes.
* **Indicators:** Pieces of information that can detect suspicious or malicious cyber activity.

#### THM Questions

*3.1 How many distribution options does MISP provide to share threat information?*

Answer: 4

*3.2 Which user has the role to publish events?*

Answer: *organisation admin*

#### …

**Feeds & Taxonomies**

Feeds are resources that contain indicators that can be imported into MISP and provide attributed information about security events. These feeds provide analysts and organisations with continuously updated information on threats and adversaries and aid in their proactive defence against attacks.

MISP Feeds provide a way to:

* Exchange threat information.
* Preview events along with associated attributes and objects.
* Select and import events to your instance.
* Correlate attributes identified between events and feeds.

A taxonomy is a means of classifying information based on standard features or attributes. On MISP, taxonomies are used to categorise events, indicators and threat actors based on tags that identify them.

Analysts can use taxonomies to:

* Set events for further processing by external tools such as [VirusTotal](https://virustotal.com/).
* Ensure events are classified appropriately before the Organisation Admin publishes them.
* Enrich intrusion detection systems' export values with tags that fit specific deployments.

Taxonomies are expressed in machine tags, which comprise three vital parts:

* **Namespace:** Defines the tag's property to be used.
* **Predicate:** Specifies the property attached to the data.
* **Value:** Numerical or text details to map the property.

**Tagging**

Information from feeds and taxonomies, tags can be placed on events and attributes to identify them based on the indicators or threats identified correctly. Tagging allows for effective sharing of threat information between users, communities and other organisations using MISP to identify various threats.

**The minimal subset of Tags**

The following tags can be considered a must-have to provide a well-defined event for distribution:

* [**Traffic Light Protocol:**](https://www.first.org/tlp/) Provides a colour schema to guide how intelligence can be shared.
* **Confidence:** Provides an indication as to whether or not the data being shared is of high quality and has been vetted so that it can be trusted to be good for immediate usage.
* **Origin:** Describes the source of information and whether it was from automation or manual investigation.
* **Permissible Actions Protocol:** An advanced classification that indicates how the data can be used to search for compromises within the organisation.

#### THM Questions

*5.1 What event ID has been assigned to the PupyRAT event?*

Go to home and click on List events. In the filter search box type in PupyRat

Answer: 1146

*5.2 The event is associated with the adversary gaining \_\_\_\_\_\_ into organisations.*

Look at the tags the find the answer

Answer: Remote Access

*5.3 What IP address has been mapped as the PupyRAT C2 Server*

Scroll down in the event and look for ip-dst

Answer: 89.107.62.39

*5.4 From the Intrusion Set Galaxy, what attack group is known to use this form of attack?*

Answer: Magic Hound

*5.5 There is a taxonomy tag set with a Certainty level of 50. Which one is it?*

Click on Event actions -> list taxonomies -> search for certainty

Answer: OSINT

#### …

**RED TEAM THREAT INTEL**

**Threat Intelligence (TI)** or **Cyber Threat Intelligence (CTI)** is the information, or TTPs (**T**actics, **T**echniques, and **P**rocedures), attributed to an adversary, commonly used by defenders to aid in detection measures.

CTI can be consumed (to taken action upon data) by collecting IOCs (**I**ndicators **o**f **C**ompromise) and TTPs commonly distributed and maintained by [ISACs (**I**nformation and **S**haring **A**nalysis **C**enters)](https://tryhackme.com/room/introtoisac). Intelligence platforms and frameworks also aid in the consumption of CTI, primarily focusing on an overarching timeline of all activities.

To aid in consuming CTI and collecting TTPs, red teams will often use threat intelligence platforms and frameworks such as **MITRE ATT&CK**, **TIBER-EU**, and **OST Map**.

These cyber frameworks will collect known TTPs and categorize them based on varying characteristics such as:

* Threat Group
* Kill Chain Phase
* Tactic
* Objective/Goal

**TIBER-EU** (**T**hreat **I**ntelligence-**b**ased **E**thical **R**ed Teaming) is a common framework developed by the European Central Bank that centres around the use of threat intelligence.

From the [ECB TIBER-EU white paper](https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf), "The Framework for Threat Intelligence-based Ethical Red Teaming (TIBER-EU) enables European and national authorities to work with financial infrastructures and institutions (hereafter referred to collectively as 'entities') to put in place a programme to test and improve their resilience against sophisticated cyber attacks."

A screenshot of a video game

Description automatically generated with medium confidence

The main difference between this framework and others is the "Testing" phase that requires threat intelligence to feed the red team's testing.

We will use the Lockheed Martin cyber kill chain as our standard cyber kill chain to map TTPs.

Icon

Description automatically generated with medium confidence

Going through the Navigator layer, we can assign various TTPs we want to employ during the engagement. Below is a compiled kill chain with mapped TTPs for **APT39**.

1. **Reconnaissance:**

* No identified TTPs, use internal team methodology

1. **Weaponization**:

* Command and Scripting Interpreter
* PowerShell
* Python
* VBA
* User executed malicious attachments

1. **Delivery**:

* Exploit Public-Facing Applications
* Spearphishing

1. **Exploitation**:

* Registry modification
* Scheduled tasks
* Keylogging
* Credential dumping

1. **Installation**:

* Ingress tool transfer
* Proxy usage

1. **Command & Control:**

* Web protocols (HTTP/HTTPS)
* DNS

1. **Actions on Objectives**

* Exfiltration over C2

Other open-source and enterprise threat intelligence platforms can aid red teamers in adversary emulation and TTP mapping, such as,

* **Mandiant Advantage**
* **Ontic**
* **CrowdStrike Falcon**

#### THM Questions

Question: How many Command and Control techniques are employed by Carbanak?  
Answer: 2

Question: What signed binary did Carbanak use for defense evasion?  
Answer: Rundll32

Question: What Initial Access technique is employed by Carbanak?   
Answer: Valid Accounts

#### …

CTI can also be used during engagement execution, emulating the adversary's behavioral characteristics, such as

1. **C2 Traffic**

* User Agents
* Ports, Protocols
* Listener Profiles

1. **Malware and Tooling**

* IOCs
* Behaviors

Information to be implemented in the profile can be gathered from ISACs and collected IOCs or packet captures, including,

* Host Headers
* POST URIs
* Server Responses and Headers

The gathered traffic can aid a red team to make their traffic look similar to the targeted adversary to get closer to the goal of adversary emulation.

The second behavioral use of CTI is analyzing behavior and actions of an adversaries' malware and tools to develop your offensive tooling that emulates similar behaviors or has similar vital indicators.

An example of this could be an adversary using a custom dropper. The red team can emulate the dropper by,

* Identifying traffic
* Observing syscalls and API calls
* Identifying overall dropper behavior and objective
* Tampering with file signatures and IOCs

The hardest part of planning a threat-intel-driven campaign can be mapping two different cyber frameworks. To make this process simpler we have provided a basic table comparing the **Lockheed Martin Cyber Kill Chain** and the **MITRE ATT&CK** framework.

|  |  |
| --- | --- |
| **Cyber Kill Chain** | **MITRE ATT&CK** |
| Recon | Reconnaissance |
| Weaponization | Execution |
| Delivery | Initial Access |
| Exploitation | Initial Access |
| Installation | Persistence / Defense Evasion |
| Command & Control | Command and Control |
| Actions on Objectives | Exfiltration / Impact |

#### THM Questions

Question: Once the chain is complete and you have received the flag, submit it below.  
Answer: THM{7HR347\_1N73L\_12 \_4w35om3}

Question: What web shell is APT 41 known to use?   
Answer: ASPXSpy

Question: What LOLBAS (Living Off The Land Binaries and Scripts) tool does APT 41 use to aid in file transfers?   
Answer: certutil

Question: What tool does APT 41 use to mine and monitor SMS traffic?   
Answer: MESSAGETAPc

#### …

**UNIFIED KILL CHAIN**

Originating from the military, a “Kill Chain” is a term used to explain the various stages of an attack. In the realm of cybersecurity, a “Kill Chain” is used to describe the methodology/path attackers such as hackers or APTs use to approach and intrude a target.

For example, an attacker scanning, exploiting a web vulnerability, and escalating privileges will be a “Kill Chain”.

**Threat Modelling**

Threat modelling, in a cybersecurity context, is a series of steps to ultimately improve the security of a system. Threat modelling is about identifying risk and essentially boils down to:

1. Identifying what systems and applications need to be secured.
2. Assessing what vulnerabilities and weaknesses these systems and applications may have.
3. Creating a plan of action to secure these systems and applications.
4. Putting in policies to prevent these vulnerabilities from occurring again.

To continue from the previous task, the [Unified Kill Chain](https://www.unifiedkillchain.com/assets/The-Unified-Kill-Chain.pdf) published in 2017, aims to complement (**not compete**) with other cybersecurity kill chain frameworks such as Lockheed Martin’s and MITRE’s ATT&CK.

**Benefits of the UKC Framework**

1. Modern
2. UKC is detailed (18 phases) and covers entire attack
3. UKC showcases realistic scenario

**The UKC states that there are 18 phases to an attack**:

