Contents

[**MITRE** 1](#_Toc129430795)

[APT 2](#_Toc129430796)

[TTP 2](#_Toc129430797)

[ATT&CK 2](#_Toc129430798)

[CAR 3](#_Toc129430799)

[Implementations 3](#_Toc129430800)

[MITRE Engage 3](#_Toc129430801)

[MITRE D3FEND 4](#_Toc129430802)

[ATT&CK Emulation Plans 4](#_Toc129430803)

[ATT&CK and Threat Intelligence 5](#_Toc129430804)

[**MISP** 6](#_Toc129430805)

[What does MISP support? 7](#_Toc129430806)

[Feeds & Taxonomies 7](#_Toc129430807)

[Tagging 8](#_Toc129430808)

[**RED TEAM THREAT INTEL** 9](#_Toc129430809)

[**UNIFIED KILL CHAIN** 12](#_Toc129430810)

[Threat Modelling 12](#_Toc129430811)

[Phase: In (Initial Foothold) 13](#_Toc129430812)

[Phase: Through(Network Propagation) 16](#_Toc129430813)

[Phase: Out (Actin on Objectives) 17](#_Toc129430814)

## **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.

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, **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."

*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)

*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)

*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.*"

*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).

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.

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**

**Room Objectives**

We will be covering the following areas within the room:

* Introduction to MISP and why it was developed.
* Use cases MISP can be applied to
* Core features and terminologies.
* Dashboard Navigation.
* Event Creation and Management.
* Feeds and Taxonomies.

[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.

Information sharing follows a distributed model, with supported closed, semi-private, and open communities (public). 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.

*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 axonomies 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.

*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. The red cell can leverage CTI from an offensive perspective to assist in adversary emulation.

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,

1. Threat Group
2. Kill Chain Phase
3. Tactic
4. 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 centers 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
2. **Weaponization**:
   * Command and Scripting Interpreter
     + PowerShell
     + Python
     + VBA
   * User executed malicious attachments
3. **Delivery**:
   * Exploit Public-Facing Applications
   * Spearphishing
4. **Exploitation**:
   * Registry modification
   * Scheduled tasks
   * Keylogging
   * Credential dumping
5. **Installation**:
   * Ingress tool transfer
   * Proxy usage
6. **Command & Control:** 
   * Web protocols (HTTP/HTTPS)
   * DNS
7. **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**

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

* C2 Traffic
  + User Agents
  + Ports, Protocols
  + Listener Profiles
* 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.

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 and what function they serve in the environment. For example, is the system critical to normal operations, and is a system holding sensitive information like payment info or addresses?
2. Assessing what vulnerabilities and weaknesses these systems and applications may have and how they could be potentially exploited
3. Creating a plan of action to secure these systems and applications from the vulnerabilities highlighted
4. Putting in policies to prevent these vulnerabilities from occurring again where possible (for example, implementing a software development life cycle (SDLC) for an application or training employees on phishing awareness).

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.

The UKC states that there are 18 phases to an attack: Everything from reconnaissance to data exfiltration and understanding an attacker's motive. These phases have been grouped together in this room into a few areas of focus for brevity, which will be detailed in the remaining tasks.

|  |  |
| --- | --- |
| **Benefits of the Unified Kill Chain (UKC) Framework** | **How do Other Frameworks Compare?** |
| Modern (released in 2017, updated in 2022). | Some frameworks, such as MITRE’s were released in 2013, when the cybersecurity landscape was very different. |
| The UKC is extremely detailed (18 phases). | Other frameworks often have a small handful of phases. |
| The UKC covers an entire attack - from reconnaissance, exploitation, post-exploitation and includes identifying an attacker's motivation. | Other frameworks cover a limited amount of phases. |
| The UKC highlights a much more realistic attack scenario. Various stages will often re-occur. For example, after exploiting a machine, an attacker will begin reconnaissance to pivot another system. | Other frameworks do not account for the fact that an attacker will go back and forth between the various phases during an attack. |

### Phase: In (Initial Foothold)

**Reconnaissance (**[**MITRE Tactic TA0043**](https://attack.mitre.org/tactics/TA0043/)**)**

This phase of the UKC describes techniques that an adversary employs to gather information relating to their target. This can be achieved through means of passive and active reconnaissance. The information gathered during this phase is used all throughout the later stages of the UKC (such as the initial foothold).

Information gathered from this phase can include:

* Discovering what systems and services are running on the target, this is beneficial information in the weaponisation and exploitation phases of this section.
* Finding contact lists or lists of employees that can be impersonated or used in either a social engineering or phishing attack.
* Looking for potential credentials that may be of use in later stages,  such as pivoting or initial access.
* Understanding the network topology and other networked systems can be used to pivot too.

**Weaponization (**[**MITRE Tactic TA0001**](https://attack.mitre.org/tactics/TA0001/)**)**

This phase of the UKC describes the adversary setting up the necessary infrastructure to perform the attack. For example, this could be setting up a command and control server, or a system capable of catching reverse shells and delivering payloads to the system.

**Social Engineering (**[**MITRE Tactic TA0001**](https://attack.mitre.org/tactics/TA0001/)**)**

This phase of the UKC describes techniques that an adversary can employ to manipulate employees to perform actions that will aid in the adversaries attack. For example, a social engineering attack could include:

* Getting a user to open a malicious attachment.
* Impersonating a web page and having the user enter their credentials.
* Calling or visiting the target and impersonating a user (for example, requesting a password reset) or being able to gain access to areas of a site that the attacker would not previously be capable of (for example, impersonating a utility engineer).

**Exploitation (**[**MITRE Tactic TA0002**](https://attack.mitre.org/tactics/TA0002/)**)**

This phase of the UKC describes how an attacker takes advantage of weaknesses or vulnerabilities present in a system. The UKC defines "Exploitation" as abuse of vulnerabilities to perform code execution. For example:

* Uploading and executing a reverse shell to a web application.
* Interfering with an automated script on the system to execute code.
* Abusing a web application vulnerability to execute code on the system it is running on.

**Persistence (**[**MITRE Tactic TA0003**](https://attack.mitre.org/tactics/TA0003/)**)**

This phase of the UKC is rather short and simple. Specifically, this phase of the UKC describes the techniques an adversary uses to maintain access to a system they have gained an initial foothold on. For example:

* Creating a service on the target system that will allow the attacker to regain access.
* Adding the target system to a Command & Control server where commands can be executed remotely at any time.
* Leaving other forms of backdoors that execute when a certain action occurs on the system (i.e. a reverse shell will execute when a system administrator logs in).

**Defence Evasion (**[**MITRE Tactic TA0005**](https://attack.mitre.org/tactics/TA0005/)**)**

The "Defence Evasion" section of the UKC is one of the more valuable phases of the UKC. This phase specifically is used to understand the techniques an adversary uses to evade defensive measures put in place in the system or network. For example, this could be:

* Web application firewalls.
* Network firewalls.
* Anti-virus systems on the target machine.
* Intrusion detection systems.

This phase is valuable when analysing an attack as it helps form a response and better yet - gives the defensive team information on how they can improve their defence systems in the future.

**Command & Control (**[**MITRE Tactic TA0011**](https://attack.mitre.org/tactics/TA0011/)**)**

The "Command & Control" phase of the UKC combines the efforts an adversary made during the "Weaponization" stage of the UKC to establish communications between the adversary and target system.

An adversary can establish command and control of a target system to achieve its action on objectives. For example, the adversary can:

* Execute commands.
* Steal data, credentials and other information.
* Use the controlled server to pivot to other systems on the network.

**Pivoting (**[**MITRE Tactic TA0008**](https://attack.mitre.org/tactics/TA0008/)**)**

"Pivoting" is the technique an adversary uses to reach other systems within a network that are not otherwise accessible (for example, they are not exposed to the internet). There are often many systems in a network that are not directly reachable and often contain valuable data or have weaker security.

For example, an adversary can gain access to a web server that is publically accessible to attack other systems that are within the same network (but are not accessible via the internet).

### Phase: Through(Network Propagation)

This phase follows a successful foothold being established on the target network. An attacker would seek to gain additional access and privileges to systems and data to fulfil their goals. The attacker would set up a base on one of the systems to act as their pivot point and use it to gather information about the internal network.

**Pivoting** ([MITRE Tactic TA0008](https://attack.mitre.org/tactics/TA0008/))

Once the attacker has access to the system, they would use it as their staging site and a tunnel between their command operations and the victim’s network. The system would also be used as the distribution point for all malware and backdoors at later stages.

#### **Discovery** ([MITRE Tactic TA0007](https://attack.mitre.org/tactics/TA0007/))

The adversary would uncover information about the system and the network it is connected to. Within this stage, the knowledge base would be built from the active user accounts, the permissions granted, applications and software in use, web browser activity, files, directories and network shares, and system configurations.

#### **Privilege Escalation** ([MITRE Tactic TA0004](https://attack.mitre.org/tactics/TA0004/))

Following their knowledge-gathering, the adversary would try to gain more prominent permissions within the pivot system. They would leverage the information on the accounts present with vulnerabilities and misconfigurations found to elevate their access to one of the following superior levels:

* SYSTEM/ ROOT.
* Local Administrator.
* A user account with Admin-like access.
* A user account with specific access or functions.

#### **Execution** ([MITRE Tactic TA0002](https://attack.mitre.org/tactics/TA0002/))

Recall when the adversary set up their attack infrastructure. Once the attacker has access to the system, they would use it as their staging site and a tunnel between their command operations and the victim’s network. The system would also be used as the distribution point for all malware and backdoors at later stages. and weaponised payloads? This is where they deploy their malicious code using the pivot system as their host. Remote trojans, C2 scripts, malicious links and scheduled tasks are deployed and created to facilitate a recurring presence on the system and uphold their persistence.

#### **Credential Access** ([MITRE Tactic TA0006](https://attack.mitre.org/tactics/TA0006/))

Working hand in hand with the Privilege Escalation stage, the adversary would attempt to steal account names and passwords through various methods, including keylogging and credential dumping. This makes them harder to detect during their attack as they would be using legitimate credentials.

**Lateral Movement** ([MITRE Tactic TA0008](https://attack.mitre.org/tactics/TA0008/))

With the credentials and elevated privileges, the adversary would seek to move through the network and jump onto other targeted systems to achieve their primary objective. The stealthier the technique used, the better.

### Phase: Out (Actin on Objectives)

This phase wraps up the journey of an adversary’s attack on an environment, where they have critical asset access and can fulfil their attack goals. These goals are usually geared toward compromising the confidentiality, integrity and availability (CIA) triad.

#### **Collection** [MITRE Tactic (TA0009)](https://attack.mitre.org/tactics/TA0009/)

**After all the hunting for access and assets, the adversary will be seeking to gather all the valuable data of interest. This, in turn, compromises the confidentiality of the data and would lead to the next attack stage – Exfiltration. The main target sources include drives, browsers, audio, video and email.**

**Exfiltration (**[**MITRE Tactic TA0010**](https://attack.mitre.org/tactics/TA0010/)**)**

To elevate their compromise, the adversary would seek to steal data, which would be packaged using encryption measures and compression to avoid any detection. The C2 channel and tunnel deployed in the earlier phases will come in handy during this process.

#### **Impact** ([MITRE Tactic TA0040](https://attack.mitre.org/tactics/TA0040/))

If the adversary seeks to compromise the integrity and availability of the data assets, they would manipulate, interrupt or destroy these assets. The goal would be to disrupt business and operational processes and may involve removing account access, disk wipes, and data encryption such as ransomware, defacement and denial of service (DoS) attacks.

#### **Objectives**

With all the power and access to the systems and network, the adversary would seek to achieve their strategic goal for the attack.

For example, if the attack was financially motivated, they may seek to encrypt files and systems with ransomware and ask for payment to release the data. In other instances, the attacker may seek to damage the reputation of the business, and they would release private and confidential information to the public.