Red Team Threat Intelligence

Introduction

Threat Intelligence (TI) or Cyber Threat Intelligence (CTI) is the information, or TTPs (Tactics, Techniques, and Procedures), 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.

Learning Objectives

- Understand the basics of threat intelligence and how it can be applied to red team engagements.
- Learn how to create a threat-intel-driven campaign.
- Use frameworks to understand concepts and leverage threat intelligence.

What is Threat Intelligence?

Expanding upon task 1, CTI can be consumed (to taken action upon data) by collecting IOCs (Indicators of Compromise) and TTPs commonly distributed and maintained by ISACs (Information and Sharing Analysis Centers). Intelligence platforms and frameworks also aid in the consumption of CTI, primarily focusing on an overarching timeline of all activities.

Note: The term ISAC is used loosely in the threat intelligence landscape and often refers to a threat intelligence platform.

Traditionally, defenders use threat intelligence to provide context to the ever-changing threat landscape and quantify findings. IOCs are quantified by traces left by adversaries such as domains, IPs, files, strings, etc. The blue team can utilize various IOCs to build detections and analyze behavior. From a red team perspective, you can think of threat intelligence as the red team's analysis of the blue team's ability to properly leverage CTI for detections.

In this room, we will be focusing on APT (Advanced Persistent Threat) activity and how to leverage their documented TTPs. The next task will detail the specifics of threat intelligence and its significance to the red team.

Applying Threat Intelligence to the Red Team

As previously mentioned, the red team will leverage CTI to aid in adversary emulation and support evidence of an adversary's behaviors.

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

Once a targeted adversary is selected, the goal is to identify all TTPs categorized with that chosen adversary and map them to a known cyber kill chain. This concept is covered further in the next task.

Leveraging TTPs is used as a planning technique rather than something a team will focus on during engagement execution. Depending on the size of the team, a CTI team or threat intelligence operator may be employed to gather TTPs for the red team. During the execution of an engagement, the red team will use threat intelligence to craft tooling, modify traffic and behavior, and emulate the targeted adversary. This concept is covered further in task 5.

Overall the red team consumes threat intelligence to analyze and emulate the behaviors of adversaries through collected TTPs and IOCs.

The TIBER-EU Framework

TIBER-EU (Threat Intelligence-based Ethical Red 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, "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."

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

This framework encompasses a best practice rather than anything actionable from a red team perspective.

There are several public white papers and documents if you are interested in reading about this framework further,

- https://www.ecb.europa.eu/pub/pdf/other/ecb.tiber_eu_framework.en.pdf
- https://www.crest-approved.org/membership/tiber-eu/

TTP Mapping

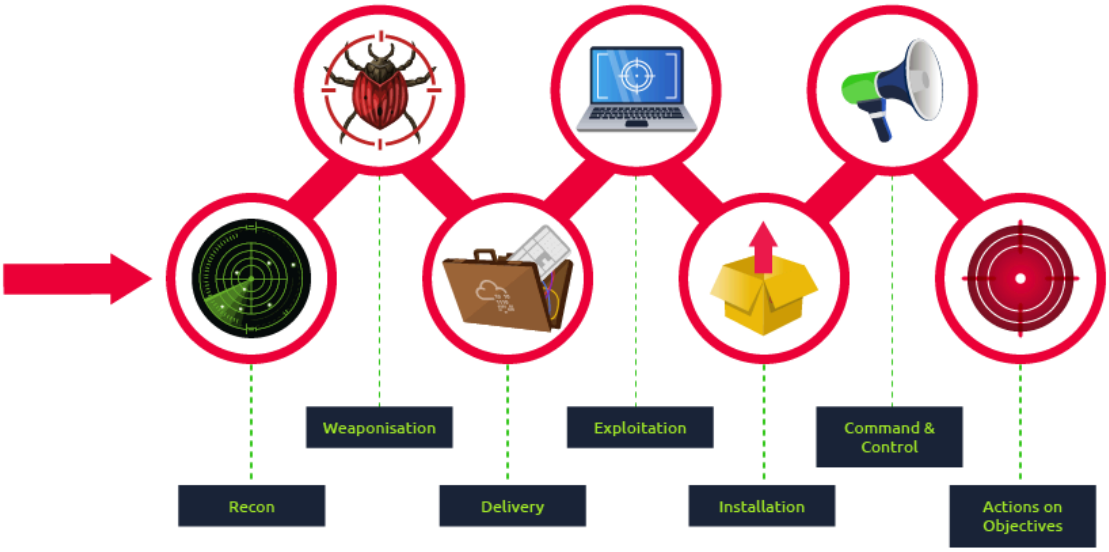
TTP Mapping is employed by the red cell to map adversaries' collected TTPs to a standard cyber kill chain. Mapping TTPs to a kill chain aids the red team in planning an engagement to emulate an adversary.

To begin the process of mapping TTPs, an adversary must be selected as the target. An adversary can be chosen based on,

1. Target Industry
2. Employed Attack Vectors
3. Country of Origin
4. Other Factors

As an example for this task, we have decided to use APT 39, a cyber-espionage group run by the Iranian ministry, known for targeting a wide variety of industries.

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

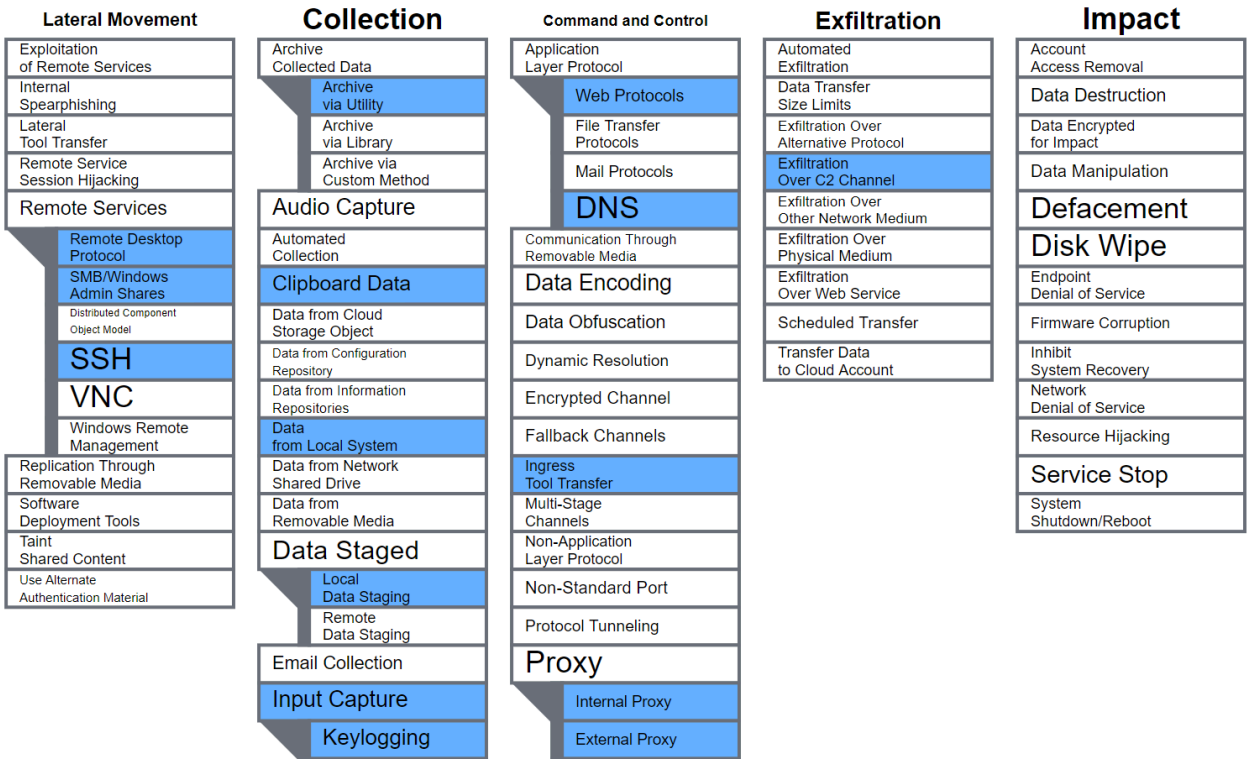


The first cyber framework we will be collecting TTPs from is MITRE ATT&CK. If you are not familiar with MITRE ATT&CK, it provides IDs and descriptions of categorized TTPs. For more information about MITRE and how to use ATT&CK, check out the MITRE room.

ATT&CK provides a basic summary of a group's collected TTPs. We can use ATT&CK Navigator to help us visualize each TTP and categorize its place in the kill chain. Navigator visualizes the ATT&CK chain with the adversaries' designated TTPs highlighted under the corresponding sub-section.

To use the ATT&CK Navigator: navigate to the groups summary page, next to "Techniques Used," navigate to "ATT&CK Navigator Layers," from the dropdown navigate to "view." An ATT&CK Navigator layer should have opened with the selected group's TTPs highlighted in a new tab.

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. <u>Reconnaissance:</u>
    a. No identified TTPs, use internal team methodology
2. <u>Weaponization:</u>
    a. Command and Scripting Interpreter
        i. PowerShell
        ii. Python
        iii. VBA
    b. User executed malicious attachments
3. <u>Delivery:</u>
    a. Exploit Public-Facing Applications
    b. Spearphishing
4. <u>Exploitation:</u>
    a. Registry modification
    b. Scheduled tasks
    c. Keylogging
    d. Credential dumping
5. <u>Installation:</u>
    a. Ingress tool transfer
    b. Proxy usage
6. <u>Command & Control:</u>

    a. Web protocols (HTTP/HTTPS)
    b. DNS
7. Actions on Objectives:
    a. Exfiltration over C2

MITRE ATT&CK will do most of the work needed, but we can also supplement threat intelligence information with other platforms and frameworks. Another example of a TTP framework is OST Map.

OST Map provides a visual map to link multiple threat actors and their TTPs.

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

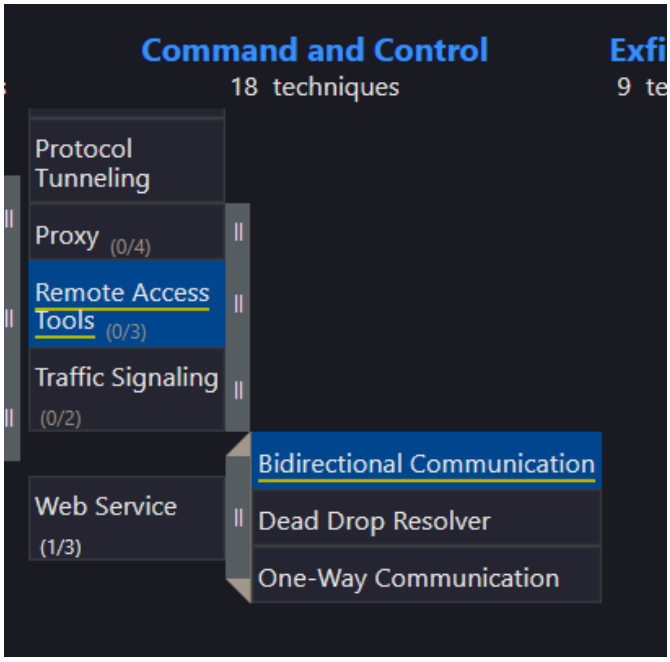
****

Answer the questions below:

Read the above and use MITRE ATT&CK Navigator to answer the questions below using a Carbanak layer.

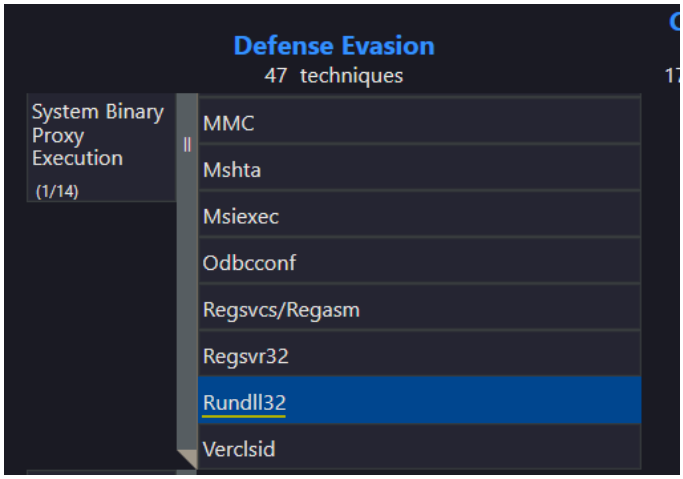
No Answer Needed

How many Command and Control techniques are employed by Carbanak?



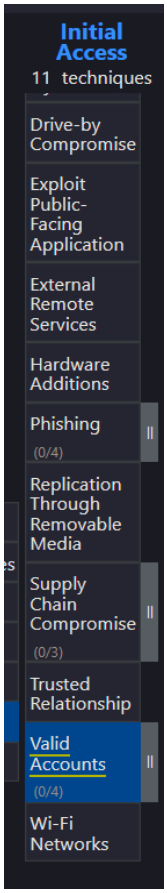
Answer: 2

What signed binary did Carbanak use for defense evasion?



Answer: Rundll32

What Initial Access technique is employed by Carbanak?



Answer: Valid Accounts

****

Other Red Team Applications of CTI

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

The first behavioral use of CTI we will showcase is C2 (Command & Control) traffic manipulation. A red team can use CTI to identify adversaries' traffic and modify their C2 traffic to emulate it.

An example of a red team modifying C2 traffic based on gathered CTI is malleable profiles. A malleable profile allows a red team operator to control multiple aspects of a C2's listener traffic.

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

Intelligence and tools gathered from behavioral threat intelligence can aid a red team in preparing the specific tools they will use to action planned TTPs.

Creating a Threat Intelligence Driven Campaign

A threat-intel-driven campaign will take all knowledge and topics previously covered and combine them to create a well-planned and researched campaign.

The task flow in this room logically follows the same path you would take as a red team to begin planning a campaign,

1. Identify framework and general kill chain
2. Determine targeted adversary
3. Identify adversary's TTPs and IOCs
4. Map gathered threat intelligence to a kill chain or framework
5. Draft and maintain needed engagement documentation
6. Determine and use needed engagement resources (tools, C2 modification, domains, etc.)

In this task, we will be walking through a red team's thought process from beginning to end of planning a threat-intel-driven campaign.

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

To begin working through this task, download the required resources and launch the static site attached to this task.

Your team has already decided to use the Lockheed Martin cyber kill chain to emulate APT 41 as the adversary that best fits the client's objectives and scope.
****
Answer the questions below:

Open the provided ATT&CK Navigator layer and identify matched TTPs to the cyber kill chain. Once TTPs are identified, map them to the cyber kill chain in the static site.
To complete the challenge, you must submit one technique name per kill chain section.

Once the chain is complete and you have received the flag, submit it below.
The answers are:

- Weaponization: Powershell
- Delivery: Spearphishing Attachment
- Exploitation: External Remote Services

- Installation: BITS Jobs
- C2: DNS
- Actions on Objectives: Keylogging

Answer: THM{7HR347_1N73L_12_4w35om3}

Answer questions below relating to needed engagement resources.

What web shell is APT 41 known to use?

ID	Name	References	Techniques
S0073	ASPXSpy	[2]	Server Software Component: Web Shell

Answer: ASPXspy

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

Enterprise	T1105	Ingress Tool Transfer	APT41 used certutil to download additional files.[9][4][3] APT41 downloaded post-exploitation tools such as Cobalt Strike via command shell following initial access.[8] APT41 has uploaded Procdump and NATBypass to a staging directory and has used these tools in follow-on activities.[10]

Answer: certutil

What tool does APT 41 use to mine and monitor SMS traffic?

S0443	MESSAGETAP	[14][4]	Archive Collected Data: Archive via Custom Method, Automated Collection, Data Staged: Local Data Staging, Deobfuscate/Decode Files or Information, File and Directory Discovery, Indicator Removal: File Deletion, Network Sniffing, System Network Connections Discovery

Answer: MESSAGETAP

****