MITRE ENGENUITY | Center for Threat Informed Defense

Lab 1.1: Touring the Adversary Emulation Library

Introduction

Adversary Emulation Plans are one of the primary tools we use to conduct professional adversary emulation engagements.

This lab will help you get familiar with Adversary Emulation Plan contents and structure by touring the Center for Threat Informed Defense (CTID) Adversary Emulation Library.

At the end of this lab, you will be primed with foundational adversary emulation knowledge that will be revisited regularly throughout the course.

Objectives

1. Understand the purpose of the CTID Adversary Emulation Library.
2. Become familiar with Adversary Emulation Plan components and contents.
3. Navigate the CTID Adversary Emulation Library.

Estimated Completion Time

- 30 minutes to 1 hour

Requirements

- This lab can be completed in any modern web browser with Internet access.

Malware Warning

Fundamentally, this course entails executing publicly known adversary TTPs so that we can assess and improve cybersecurity. As a result, many of our tools and resources will likely be flagged malicious by security products. We make every effort to ensure that our adversary emulation content is trusted and safe for the purpose of offensive security testing.

As a precaution, you should not perform these labs on any system that contains sensitive data. Additionally, you should never use capabilities and/or techniques taught in this course without first obtaining explicit written permission from the system/network owner(s).

Walkthrough

Step 1: Access the library

Your first task is to access the CTID Adversary Emulation Library. Open a web browser and navigate to the library using the following URL:

https://github.com/center-for-threat-informed-defense/adversary_emulation_library

You should see a web page that resembles the screenshot below (figure 1).

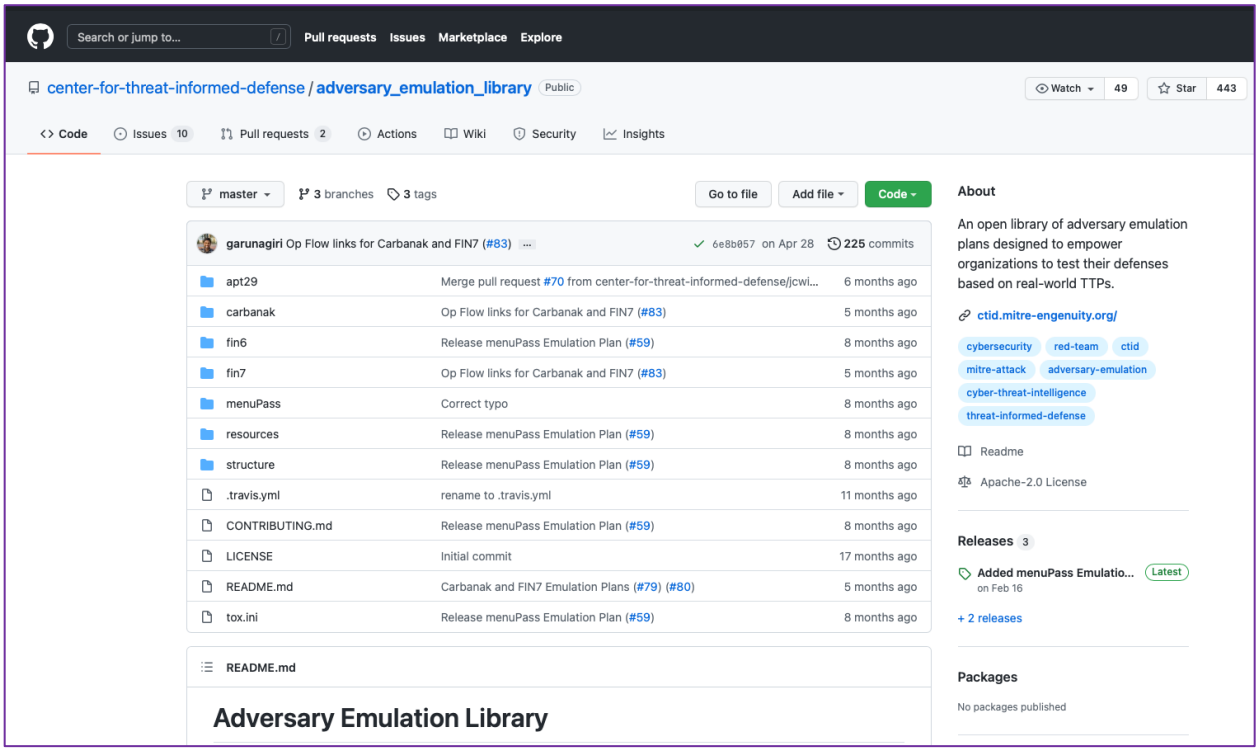


Figure 1. Adversary Emulation Library GitHub Repository

Step 2: Explore the project README

We'll now develop an understanding of the CTID Adversary Emulation Library project's philosophy and general structure.

Click the project README file and take a few minutes to read through its contents (figure 2).[1]

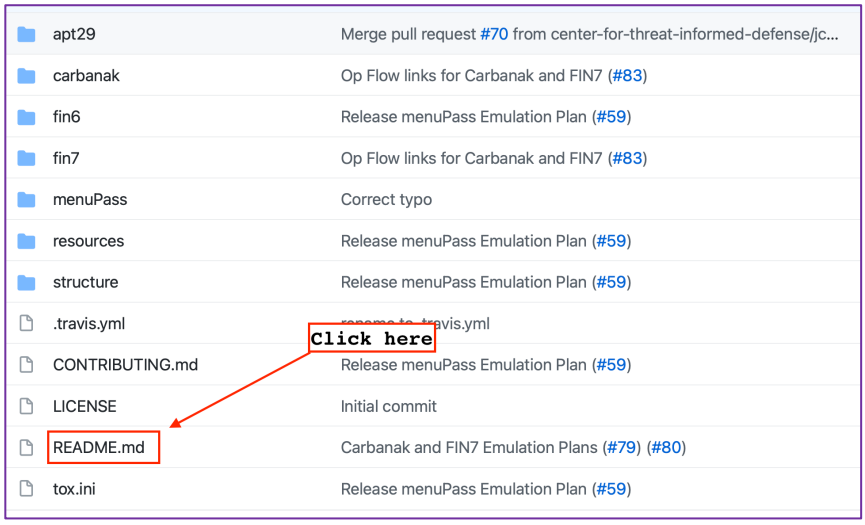
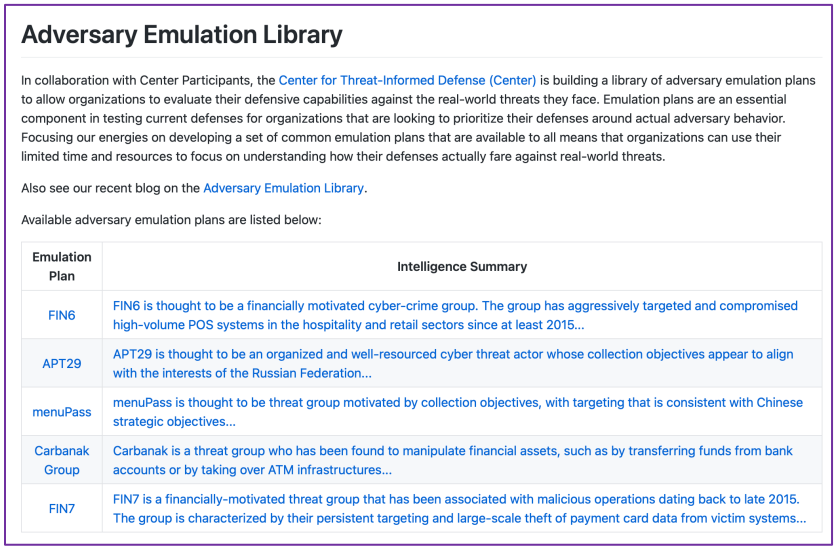


Figure 2. Project README

The project README lists several adversary emulation plans available for your use (figure 3). Are any of these threat actors relevant to your organization?



Adversary Emulation Library

In collaboration with Center Participants, the Center for Threat-Informed Defense (Center) is building a library of adversary emulation plans to allow organizations to evaluate their defensive capabilities against the real-world threats they face. Emulation plans are an essential component in testing current defenses for organizations that are looking to prioritize their defenses around actual adversary behavior. Focusing our energies on developing a set of common emulation plans that are available to all means that organizations can use their limited time and resources to focus on understanding how their defenses actually fare against real-world threats.

Also see our recent blog on the Adversary Emulation Library.

Available adversary emulation plans are listed below:

Emulation Plan	Intelligence Summary
FIN6	FIN6 is thought to be a financially motivated cyber-crime group. The group has aggressively targeted and compromised high-volume POS systems in the hospitality and retail sectors since at least 2015...
APT29	APT29 is thought to be an organized and well-resourced cyber threat actor whose collection objectives appear to align with the interests of the Russian Federation...
menuPass	menuPass is thought to be threat group motivated by collection objectives, with targeting that is consistent with Chinese strategic objectives...
Carbanak Group	Carbanak is a threat group who has been found to manipulate financial assets, such as by transferring funds from bank accounts or by taking over ATM infrastructures...
FIN7	FIN7 is a financially-motivated threat group that has been associated with malicious operations dating back to late 2015. The group is characterized by their persistent targeting and large-scale theft of payment card data from victim systems...

Figure 3. Available Adversary Emulation Plans

[1] README.md is a simple text file in markdown format. README files are commonly used to provide basic documentation about a project, such as its purpose, installation and usage instructions, license information, etc.

Learning Check

Answer the following questions based on the README contents:

1. *Based on the Philosophy section, what is the purpose of the emulation library?*

    a) Stockpile real-world adversary TTPs to defeat the defenders during red team engagements
    b) Empower network defenders to test and tune defensive capabilities against real-world adversary TTPs
    c) Maintain a collection of cyber threat intelligence about real-world adversaries and their TTPs

2. *What is the CTID Emulation Library email address for general inquiries?*

    a) ctid@mitre-engenuity.org
    b) attack@mitre.org
    c) caldera@mitre.org

3. *What is the URL for the web page that provides contributor instructions?*
    a) https://github.com/center-for-threat-informed-defense/adversary_emulation_library
    b) https://github.com/center-for-threat-informed-defense/adversary_emulation_library/blob/master/fin6
    c) https://github.com/center-for-threat-informed-defense/adversary_emulation_library/blob/master/CONTRIBUTING.md

You should now have a good understanding of why the CTID Adversary Emulation Library was created, and its general structure. We'll now shift to exploring an example Adversary Emulation Plan based on the financial cyber-crime group, FIN6.

Step 3: Understand the FIN6 Emulation Plan Components

We're going to explore the FIN6 adversary emulation plan so you can study its components and content. The purpose of this exercise is to prime your understanding as we will execute the FIN6 emulation plan in an upcoming lab.

Navigate to the FIN6 emulation plan directory by clicking the link below:

https://github.com/center-for-threat-informed-defense/adversary_emulation_library/tree/master/fin6

You can also get to the FIN6 emulation plan from the project root directory by clicking the fin6 folder (figure 4).

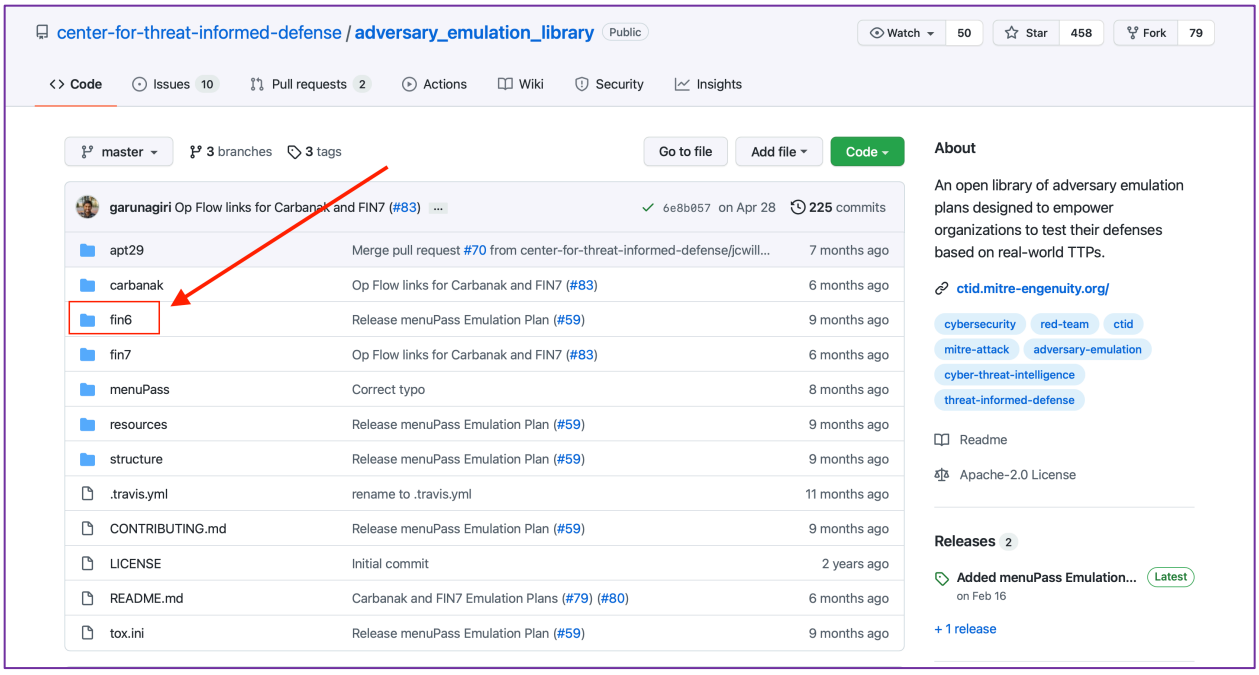


Figure 4. Navigating to the FIN6 Emulation Plan

Take a moment to read through the FIN6 README.

Note that the README provides a link to a video that demonstrates the CTID Emulation Library in action by its original authors; this video is highly recommended to supplement your learning: https://www.youtube.com/watch?v=n5jeGSOyJzY

Also observe the emulation plan components, which can be seen in the FIN6 table of contents (figure 5).

We will step through each of these components to understand their purpose and contents in detail.

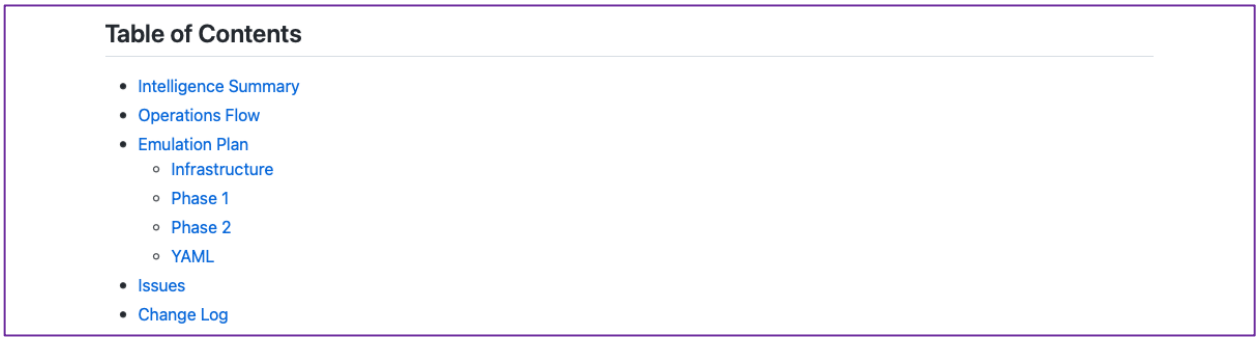


Figure 5. Fin6 Emulation Plan Table of Contents

Step 4: Explore the FIN6 Intelligence Summary

The CTID Adversary Emulation Library provides cyber threat intelligence summaries for each of its emulation plans. The intelligence summaries describe the emulated actor's objectives, targets, and observed TTPs based on publicly available reporting.

We'll learn more about intelligence summaries in a later module; for now, we'll focus on getting familiar with the FIN6 intelligence summary in general terms.

Navigate to the FIN6 intelligence summary at the following link:

https://github.com/maddev-engenuity/adversary_emulation_library/blob/master/fin6/Intelligence_Summary.md

You can also navigate to the intelligence summary from the FIN6 table of contents (figure 6).

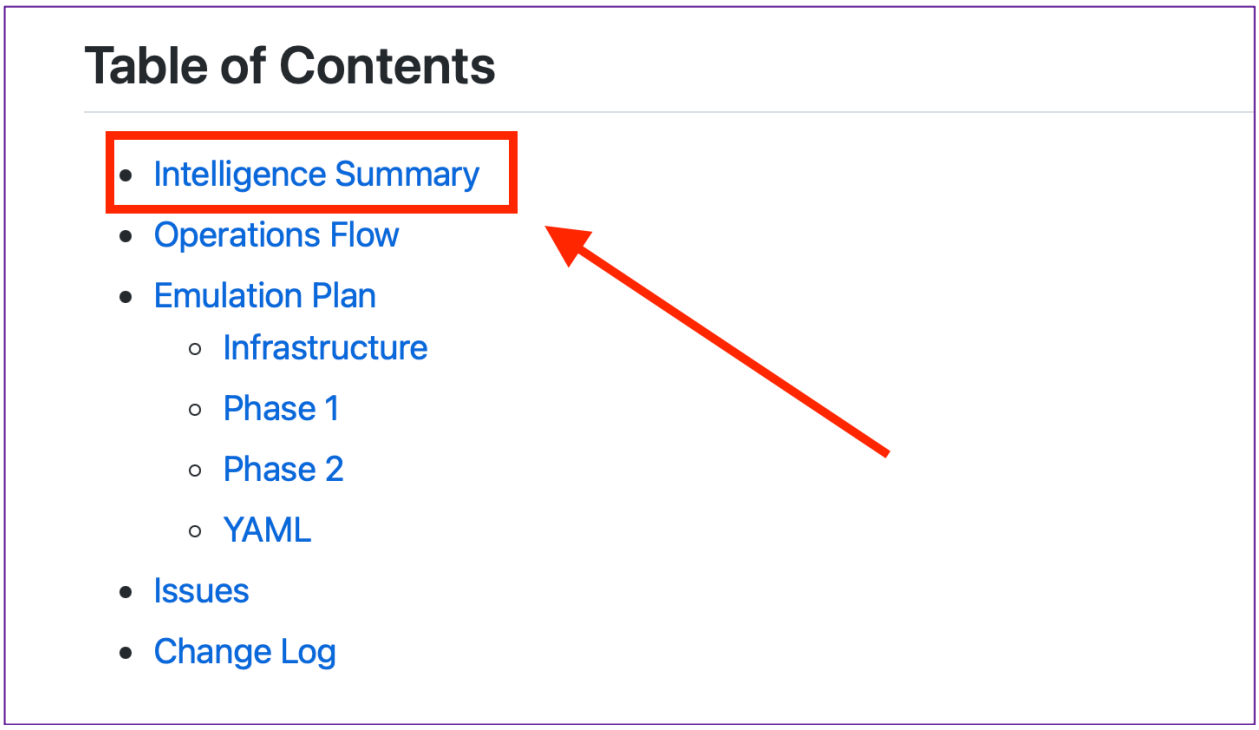


Figure 6. Navigating to the FIN6 Intelligence Summary

After clicking the link, you should be on a page that resembles the following screenshot (figure 7).

Figure 7. FIN6 Intelligence Summary

Read through FIN6 intelligence summary; try to understand FIN6's objectives, target industries, and general TTPs.

Learning Check

Answer the following questions after reading the FIN6 Intelligence Summary:

4. Based on the FIN6 intelligence summary, what is FIN6's primary objective?

    a) Monetize compromised environments via payment card data theft and/or ransomware.
    b) Monetize compromised environments by stealing intellectual property
    c) Gain a strategic advantage over other nations by conducting cyberespionage

5. Based on the FIN6 intelligence summary, what organizations has FIN6 targeted previously? Choose all that apply.

    a) Hospitality
    b) Government
    c) Energy
    d) Retail
    e) Critical Infrastructure

6. Based on the FIN6 intelligence summary, what TTPs has FIN6 used for Initial Access? Choose all that apply.

    a) Supply Chain Compromise
    b) Valid Accounts
    c) External Remote Services
    d) Exploit Public Facing Application
    e) Phishing: Spearphishing Attachment

Step 5: Explore the FIN6 Operations Flow

The Operations Flow page describes how the emulated actor works towards achieving their objectives. The operations flow helps visualize how to logically chain together major steps the emulated actor commonly performs during an operation.

Navigate to the FIN6 Operations Flow page at: https://github.com/maddev-engenuity/adversary_emulation_library/blob/master/fin6/Operations_Flow.md

You can also get to the operations flow from the FIN6 table of contents (figure 8).

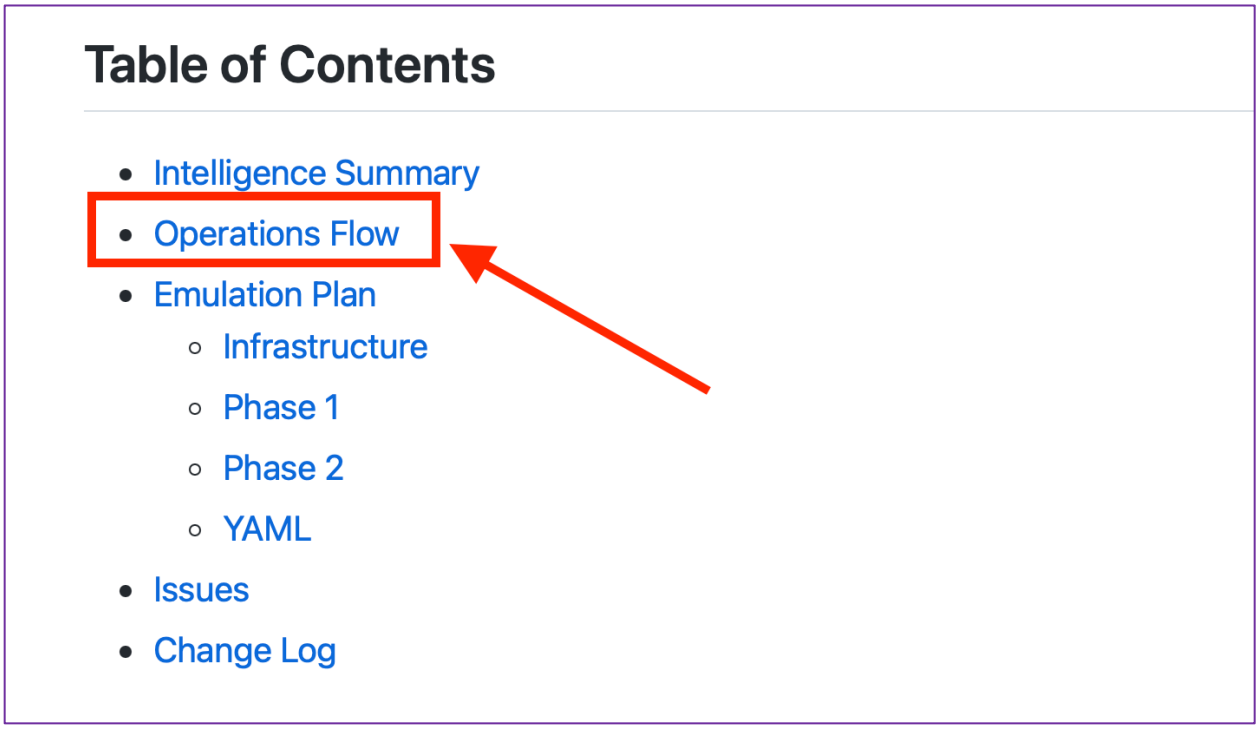


Figure 8. Navigating to the FIN6 Operations Flow

After clicking the link to the Operations Flow, you should see a page resembling the following screenshot (figure 9).

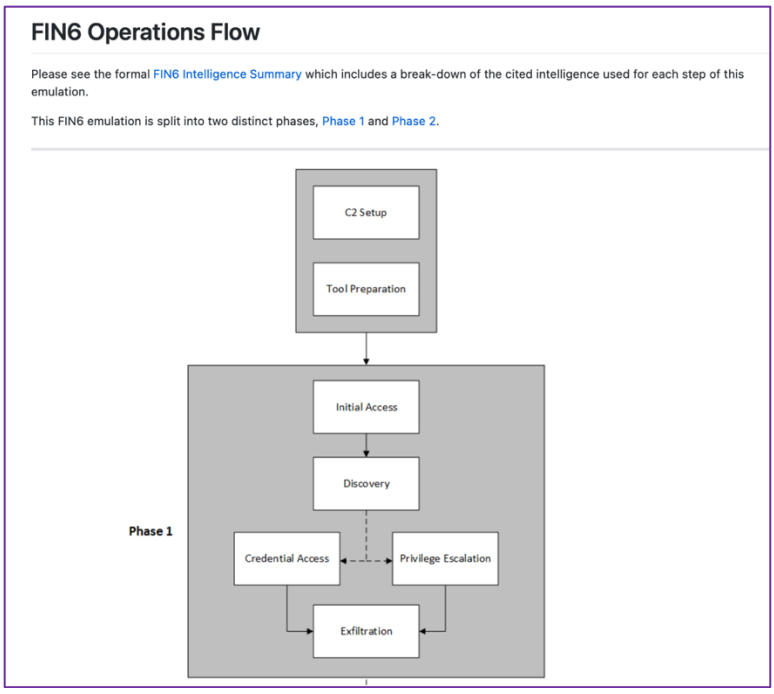


Figure 9. FIN6 Operations Flow

Take a moment to read through the FIN6 Operations Flow content.

Learning Check

Answer the following questions after reading through the Operations Flow page:

7. *What ATT&CK Tactics does FIN6 execute when compromising Point of Sale devices? Choose all that apply.*
   a) Collection
   b) Privilege Escalation
   c) Lateral Movement
   d) Impact
   e) Exfiltration

8. *What ATT&CK tactic or tactics illustrates how FIN6's ransomware tactics differ from point-of-sale intrusions? Choose all that apply.*
   a) Collection
   b) Credential Access
   c) Discovery
   d) Impact
   e) Lateral Movement

Step 6: Explore the FIN6 Adversary Emulation Scenarios

Now that you are familiar with the FIN6 intelligence summary and operations flow, we are going to explore the FIN6 adversary emulation scenarios.

The adversary emulation scenarios provide step-by-step instructions for executing the emulated actor's TTPs, and also provide guidance on how to setup any required tools and/or infrastructure.

Let's look at these scenarios in detail.

Navigate to the FIN6 Emulation Plan folder at:

https://github.com/center-for-threat-informed-defense/adversary_emulation_library/tree/master/fin6/Emulation_Plan

You can also get to this folder from the root of the FIN6 folder by clicking the "Emulation Plan" directory in the GitHub file browser (figure 10).

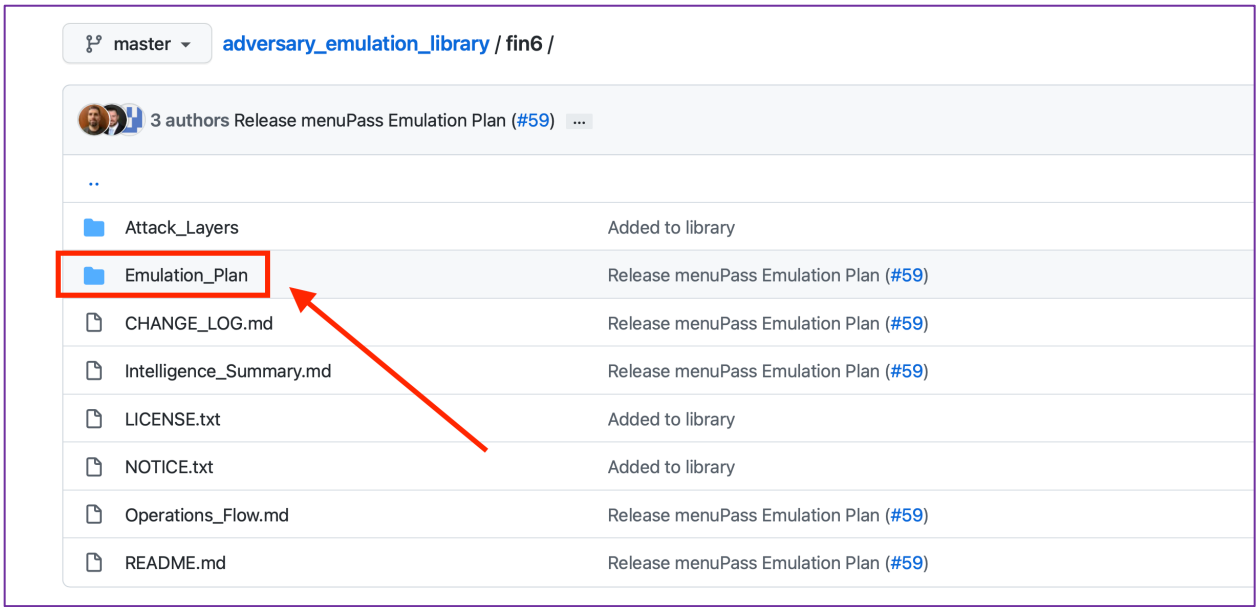


Figure 10. FIN6 Emulation Plan Folder

From the FIN6 Emulation Plan Folder, you should see a page that resembles the following screenshot (figure 11).

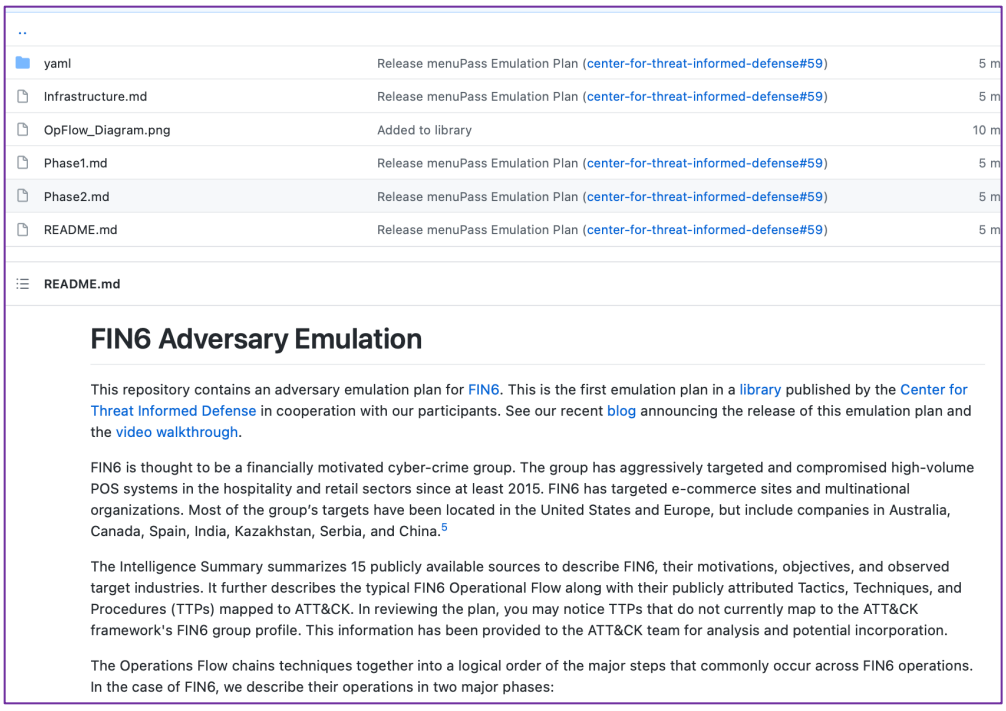


Figure 11. FIN6 Emulation_Plan Files

1. Start by reviewing the contents of `Infrastructure.md`.

- This document provides guidance on tools and infrastructure needed to complete the adversary emulation scenario.
- We will provide streamlined guidance and steps for configuring an environment in which to execute the FIN6 emulation plan in the next lab.

2. Next, skim through the `Phase1.md` file; we're going to execute this scenario in an upcoming lab.
    a. Do you see any TTPs you haven't seen before?

3. Review the machine-readable YAML file, `FIN6.yaml`, located at: https://github.com/center-for-threat-informed-defense/adversary_emulation_library/blob/master/fin6/Emulation_Plan/yaml/FIN6.yaml

- This file is designed to be ingested by an automated adversary emulation framework such as CALDERA. In a future module, we will demonstrate how to execute adversary emulation scenarios automatically.

Lab Summary

During this lab we took a tour of the CTID Adversary Emulation Library.

Some key take-aways from this lab are:

- The CTID Adversary Emulation Library provides example adversary emulation plans that you may use for testing and tuning your defensive capabilities against actor TTPs.
- Adversary emulation plan components commonly include CTI, diagrams, scenarios, and other resources.
- The CTID Adversary Emulation Library is organized by threat actor.

Now that you are familiar with the theory of adversary emulation plans, we are going to put that theory to use in an upcoming lab where we execute the FIN6 "phase 1" adversary scenario.

Learning Check Answer Key

Answer the following questions based on the README contents:

1. *Based on the Philosophy section, what is the purpose of the emulation library?*

    a) Stockpile real-world adversary TTPs to defeat the defenders during red team engagements
    b) Empower network defenders to test and tune defensive capabilities against real-world adversary TTPs
    c) Maintain a collection of cyber threat intelligence about real-world adversaries and their TTPs

2. *What is the CTID Emulation Library email address for general inquiries?*

    a) ctid@mitre-engenuity.org
    b) attack@mitre.org
    c) caldera@mitre.org

3. *What is the URL for the web page that provides contributor instructions?*
    a) https://github.com/center-for-threat-informed-defense/adversary_emulation_library
    b) https://github.com/center-for-threat-informed-defense/adversary_emulation_library/blob/master/fin6

c) https://github.com/center-for-threat-informed-defense/adversary_emulation_library/blob/master/CONTRIBUTING.md

4. Based on the FIN6 intelligence summary, what is FIN6's primary objective?

   a) Monetize compromised environments via payment card data theft and/or ransomware.
   b) Monetize compromised environments by stealing intellectual property
   c) Gain a strategic advantage over other nations by conducting cyberespionage

5. Based on the FIN6 intelligence summary, what organizations has FIN6 targeted previously? Choose all that apply.

   a) Hospitality
   b) Government
   c) Energy
   d) Retail
   e) Critical Infrastructure

6. Based on the FIN6 intelligence summary, what TTPs has FIN6 used for Initial Access? Choose all that apply.

   a) Supply Chain Compromise
   b) Valid Accounts
   c) External Remote Services
   d) Exploit Public Facing Application
   e) Phishing: Spearphishing Attachment

7. *What ATT&CK Tactics does FIN6 execute when compromising Point of Sale devices? Choose all that apply.*
   a) Collection
   b) Privilege Escalation
   c) Lateral Movement
   d) Impact
   e) Exfiltration

8. *What ATT&CK tactic or tactics illustrates how FIN6's ransomware tactics differ from point-of-sale intrusions? Choose all that apply.*
   a) Collection
   b) Credential Access
   c) Discovery
   d) Impact
   e) Lateral Movement