Pyramid of Pain Malware Analysis – VirusTotal Investigation

Objective

The goal of this lab was to perform a malware investigation using VirusTotal and map the results to the Pyramid of Pain framework. This exercise simulated the work of a SOC (Security Operations Center) analyst investigating a real-world phishing incident involving a malicious file attachment.

Scenario Overview

As a Level 1 SOC Analyst at a financial services organization, I received an alert indicating that a suspicious file was downloaded onto an employee's workstation. The investigation revealed that the employee had opened a password-protected spreadsheet which executed a malicious payload.

Time	Event
1:11 p.m.	Employee receives email with attachment
1:13 p.m.	Employee opens the password-protected spreadsheet
1:15 p.m.	Malicious executables are created on the system
1:20 p.m.	IDS detects activity and sends an alert to the SOC

Tools & Methodology

• Tool Used: VirusTotal
• Technique: Hash-based threat intelligence lookup
• SHA-256 Hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
• Framework Used: Pyramid of Pain

Investigation Process

Step 1: VirusTotal Analysis – Entered the provided SHA-256 hash into VirusTotal's search bar to retrieve a report on the file's reputation.

Step 2: Reviewing Detection Metrics – Vendor ratio ~32/69 flagged the file as malicious; community score was negative. Malware family: Flagpro / BlackTech Trojan.

Step 3: Behavioral and Network Analysis – Observed process injection, registry modification, and file creation in the sandbox environment; outbound HTTP requests to known malicious

domains.

Indicators of Compromise (IoCs)

IoC Type	Example	Description
File Hashes	SHA-256: 54e6ea47...f6b SHA-1: 8f35a9e70dbec8f1904991773f394cd4f9a07f5e MD5: 287d612e29b71c90aa54947313810a25	Unique identifiers for the malicious sample
IP Address	207.148.109.242	Contacted C2 (Command & Control) server
Domain	org.misecure.com	Associated malicious domain
Network Artifact	Outbound HTTP requests via port 80	Network behavior consistent with exfiltration attem
Tool Used	curl (for simulated HTTP generation)	Triggered traffic for packet analysis
TTPs	Registry modifications, file system manipulation, process injection	MITRE ATT&CK: T1055 (Process Injection), T105

Pyramid of Pain Mapping

IoC Type	Example	Adversary Pain Level	Impact on Threat Actor
Hash	SHA-256 file hash	Low	Easily changed by recompiling malware
IP/Domain	207.148.109.242 / org.misecure.com	Moderate	Requires infrastructure changes
TTPs (Behavioral)	Registry modification, process injection	High	Forces attacker to modify tactics and code b

Analysis & Determination

Based on the VirusTotal results, the file was confirmed malicious by over thirty reputable antivirus vendors. Community feedback, sandbox analysis, and network behaviors confirmed it as a Flagpro/BlackTech Trojan. These results were mapped to the Pyramid of Pain to determine which IoCs provide the highest disruption potential.

Cybersecurity Relevance

This investigation demonstrated real-world SOC skills in threat intelligence analysis, IoC correlation, behavioral analysis, and use of the Pyramid of Pain to strengthen detection and mitigation strategies.

Key Takeaway

This lab reinforced proficiency in using VirusTotal for malware intelligence, extracting and categorizing IoCs, applying MITRE ATT&CK; and Pyramid of Pain frameworks, and making data-driven decisions for malware classification and defense.