VirusTotal IoC Analysis Activity – Pyramid of Pain

# Activity Overview

In this activity, you analyze an artifact using VirusTotal and capture details about its related indicators of compromise using the Pyramid of Pain. This exercise uses the SHA256 hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b.

## Scenario Summary

As a level one SOC analyst at a financial services company, you've received an alert related to a suspicious file. The employee opened a password-protected spreadsheet from an email, triggering a malicious payload. You retrieved the file and created its SHA256 hash, which you used in VirusTotal for further investigation.

# Investigation Summary

SHA256 Hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Timeline of Events:

1:11 p.m.: Email with attachment received

1:13 p.m.: File downloaded and opened

1:15 p.m.: Unauthorized executables created

1:20 p.m.: IDS alert triggered

## Maliciousness Determination

Based on VirusTotal's analysis, this file is determined to be malicious. Reasons include a high number of vendors flagging the file, a negative community score, and malware detections in the vendor analysis section.

# Indicators of Compromise (IoCs) – Pyramid of Pain

|  |  |
| --- | --- |
| Indicator Type | Example |
| Hash value | MD5: 5d41402abc4b2a76b9719d911017c592 |
| IP address | 45.77.123.12 |
| Domain name | malicious-domain.net |
| Network/Host Artifact | Created file: C:\Users\Public\system32.exe |
| Tool | Uses 'PowerShell' to download additional payloads |
| Tactics, Techniques, Procedures (TTPs) | Execution via Scripting: T1059 |

# Conclusion

This exercise demonstrated how VirusTotal and the Pyramid of Pain framework can help identify and analyze IoCs in a real-world alert scenario. Leveraging threat intelligence and contextual analysis significantly improves an organization’s ability to detect and respond to malicious activity.