Analysis of Files and URLs for malicious content and IoCs using VirusTotal, Utilizing the Pyramid of Pain Framework

---

Incident Report

Date: May 13, 2023	**Entry:** 175-A2
Description	Investigating a suspicious file hash. This incident occurred in the **Detection and Analysis** phase. The scenario put me in the place of a security analyst at a SOC investigating a suspicious file hash. After the suspicious file was detected by the security systems in place, I had to perform deeper analysis and investigation to determine if the alert signified a real threat.
Tool(s) used	• VirusTotal An investigative tool that analyzes files and URLs for malicious content such as viruses, worms, trojans, and more. It's a very helpful tool to use if you want to quickly check if an indicator of compromise like a website or file has been reported as malicious by others in the cybersecurity community. I used VirusTotal to analyze a file hash, which was reported as malicious.
The 5 W's	● **Who**: An unknown malicious actor ● **What**: An email sent to an employee contained a malicious file attachment with the SHA-256 file hash of 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b ● **Where**: An employee's computer at a financial services company ● **When**: At 1:20 p.m., an alert was sent to the organization's SOC after the intrusion detection system detected the file ● **Why**: An employee was able to download and execute a malicious file attachment via e-mail.
Additional notes	How can this incident be prevented in the future? Should we consider improving security awareness training so that employees are careful with what they click on?

The activity is about analyzing an artifact using VirusTotal, a threat intelligence platform, and capturing details about its indicators of compromise (IoCs) using the Pyramid of Pain. It involves investigating a suspicious file downloaded on an employee's computer, retrieving its hash, and using VirusTotal to gather more information about the file, such as detection verdicts, related IoCs, and behavioral patterns.

Details about the alert include a file hash and a timeline of the event:

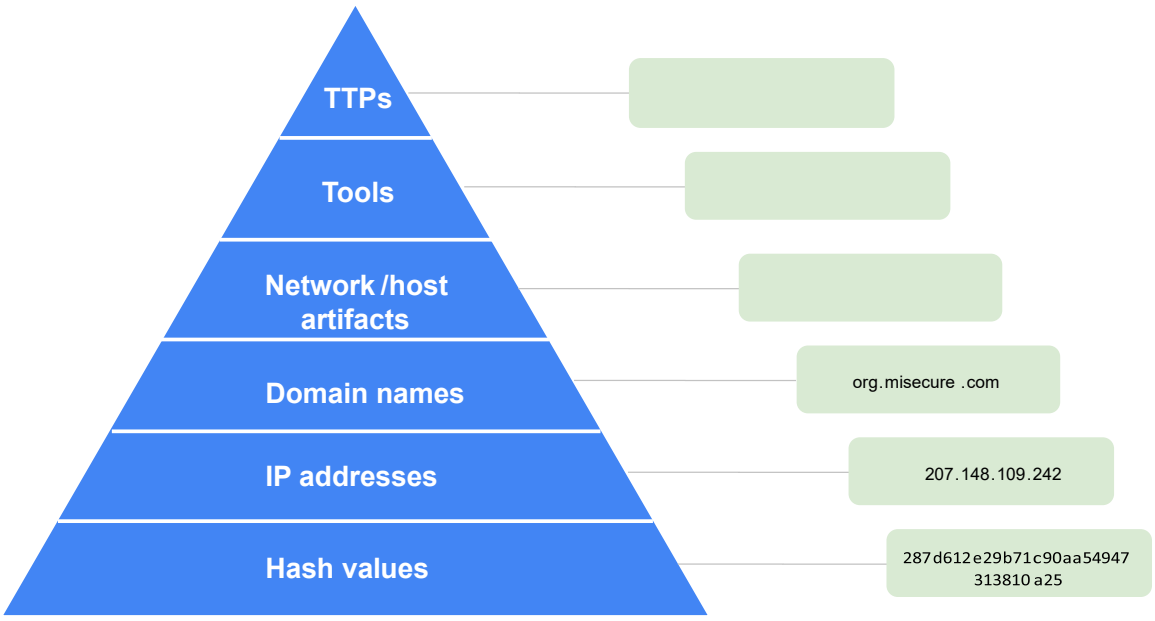
SHA256 file hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Timeline of the events leading up to this alert:

- **1:11 p.m.:** An employee receives an email containing a file attachment.
- **1:13 p.m.:** The employee successfully downloads and opens the file.
- **1:15 p.m.:** Multiple unauthorized executable files are created on the employee's computer.
- **1:20 p.m.:** An intrusion detection system detects the executable files and alerts the SOC.

The file hash has been reported as malicious by over 50 vendors. Upon further investigation, this file hash is known as the malware Flagpro, which has been commonly used by the advanced threat actor BlackTech.

Utilizing the Pyramid of Pain Framework



In this lab, I learned how to effectively use VirusTotal as a security analyst to gain insights into potential security incidents. I gained skills in:

- Utilizing VirusTotal to analyze files, domains, URLs, and IP addresses for malicious content.
- Understanding the importance of shared threat intelligence from the global cybersecurity community.
- Assessing detection verdicts from multiple security vendors to evaluate the maliciousness of a file.
- Identifying and documenting different types of IoCs, such as hash values, IP addresses, domain names, network/host artifacts, tools, and tactics/techniques/procedures (TTPs).
- Analyzing sandbox reports to gain insights into the behavioral patterns and actions of malware.
- Using the Pyramid of Pain framework to categorize and prioritize IoCs based on their difficulty for malicious actors to evade detection or mitigate.

Overall, this activity enhanced my skills in investigating security incidents, leveraging threat intelligence platforms, and making informed decisions based on the analysis of IoCs. It emphasized the importance of using multiple sources of information, staying updated with the latest security trends, and continuously learning to improve detection capabilities.