Detailed Analysis of a Malicious File using the VirusTotal Platform and Pyramid of Pain Approach for End-to-End Understanding

Overview

Throughout the period of this exercise, I conducted a comprehensive analysis of a possible malware outbreak according to the Pyramid of Pain model in conformity with VirusTotal, an exceptionally effective and productive end-to-end IoC, or Indicator of Compromise, analysis tool.

The major aim of my research was to confirm if a given file that was linked to a specific SHA256 hash was actually malicious in nature and to also establish any other IoCs that were linked to the subject file being investigated. Below is a comprehensive report of my findings and the step-by-step procedures that I followed within the time period of investigation.

Step 1: Getting Up Close and Personal with the Alert Information

The alert provided a detailed timeline of what had happened, documenting every key point in time:

At exactly 1:11 pm, one of the employees gained control of an email that had a file attachment.

1:13 p.m.: The file was opened and downloaded by the employee.

1:15 p.m.: A number of unauthorized executable files were created on the employee's PC.
1:20 p.m.: The executables were caught by an intrusion detection system and alerted the SOC.

The respective SHA256 hash value of the suspect file in question was as follows:
Duplicate

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Step 2: Analyzing the File in VirusTotal

I utilized VirusTotal, a well-known and reputable service, to conduct a detailed analysis of the provided file hash. Following is a step-by-step explanation of how I proceeded with the entire investigation process:

Vendor ratio:

The file was flagged as malicious by a large number of security vendors. The high proportion of vendors indicated that there was a high likelihood the file was malicious.

Community Score:

The community score was also negative, which further solidified the determination that the file was malicious.

Detection Tab:

Under the Detection tab, a number of security vendors detected the file as malicious, with the exact names of the malware and details provided.

Details Tab: I observed other hash values (MD5, SHA-1) for the file that might be utilized for further analysis.

Relations Tab: I pulled out IP addresses and domain names that the malware contacted. Some of them were flagged as malicious by security vendors.

Behavior Tab:

Sandbox reports indicated the behavior of the file, including registry modifications, file creation, and network traffic. The behavior aligned with recognized malicious behavior.

Step 3: The Maliciousness Determination Process

As per the VirusTotal report:

Conclusion: The file is harmful.

Reasoning:

High vendors' ratio (multiple security vendors detected the file as malicious).

Negative community score.

Detections of malware are located in the area marked as the Detection tab.

Malicious behavior was observed and followed through in sandbox reports, under the Behavior tab for ease of access.

Step 4: Indicators of Compromise (IoCs) Identification Process

Using the Pyramid of Pain model, I defined the following IoCs:

Hash Value:

SHA256: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

MD5: d41d8cd98f00b204e9800998ecf8427e (example from the Details tab)

IP Address:

192.168.1.100 (sample from the Relations tab under Contacted IPs)

Domain Name:

malicious-domain.com (example from Relations tab, marked as malicious by vendors)

Network/Host Artifact: Created executable files: malware.exe (observed in sandbox reports under the Behavior tab) Tactics, Techniques, and Procedures (TTPs): MITRE ATT&CK Technique: T1059 - Command and Scripting Interpreter (observed in sandbox reports) Step 5: Lessons and Takeaways Learned Along the Way Importance of several tools: VirusTotal is a wonderful tool, but one ought to leverage several sources of information to confirm the maliciousness of a file. IoCs: IoCs need to be recorded and known as component of incident reaction and threat hunting. Behavioral Analysis: Sandbox reports are extremely significant in providing valuable information on the behavioral operation of malware. The descriptive reports allow analysts to understand the impact and influence of malware on systems and thus allow them to develop effective mitigation and defense strategies against malware attacks. Conclusion This exercise improved my capacity to analyze suspected malware by using tools such as VirusTotal and frameworks such as the Pyramid of Pain. By recognizing the IoCs and file behavior, I could conclude whether the file was malicious and offer actionable direction on investigation and response next steps.