Activity Overview

In this activity, you'll analyze an artifact using VirusTotal and capture details about its related indicators of compromise using the Pyramid of Pain.

Previously, you were introduced to the concept of the Pyramid of Pain, which is used to understand the different types of **indicators of compromise** (**IoCs**). Remember, an IoC is observable evidence that suggests signs of a potential security incident. The Pyramid of Pain describes the relationship between IoCs and the level of difficulty that malicious actors experience when the IoCs are blocked by security teams.

VirusTotal is one of many tools that security analysts use to identify and respond to security incidents. **VirusTotal** is a service that allows anyone to analyze suspicious files, domains, URLs, and IP addresses for malicious content. Through crowdsourcing, VirusTotal gathers and reports on threat intelligence from the global cybersecurity community. This helps security analysts determine which IoCs have been reported as malicious. As a security analyst, you can take advantage of shared threat intelligence to learn more about threats and help improve detection capabilities.

Important Note: *Data uploaded to VirusTotal will be publicly shared with the entire VirusTotal community. Be careful of what you submit, and make sure you do not upload personal information.*

Scenario

Review the following scenario. Then complete the step-by-step instructions.

You are a level one security operations center (SOC) analyst at a financial services company. You have received an alert about a suspicious file being downloaded on an employee's computer.

You investigate this alert and discover that the employee received an email containing an attachment. The attachment was a password-protected spreadsheet file. The spreadsheet's password was provided in the email. The employee downloaded the file, then entered the password to open the file. When the employee opened the file, a malicious payload was then executed on their computer.

You retrieve the malicious file and create a SHA256 hash of the file. You might recall from a previous course that a **hash function** is an algorithm that produces a code that can't be decrypted. Hashing is a cryptographic method used to uniquely identify malware, acting as the file's unique fingerprint.

Now that you have the file hash, you will use VirusTotal to uncover additional IoCs that are associated with the file.

Step 1: Review the details of the alert

The following information contains details about the alert that will help you complete this activity. The details include a file hash and a timeline of the event. Keep these details for reference as you proceed to the next steps.

SHA256 file hash:
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Here is a 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 sends out an alert to the SOC.

Step 2: Enter the file hash into VirusTotal

Go to the VirusTotal website. Click **SEARCH**, enter the SHA256 file hash in the search box, and press enter. The SHA256 file hash is listed in Step 2 of this activity.

Note*: For the purpose of this activity, you'll focus on evaluating VirusTotal results. However, no single tool can detect all types of malicious activity. Security analysts will often use a combination of other tools to carefully evaluate the results of a scan before making a decision about the file.*

Step 3: Analyze the VirusTotal report

Once you've retrieved VirusTotal's report on the file hash, take some time to examine the report details. You can start by exploring the following tabs:

1. **Detection:** This tab provides a list of third-party security vendors and their detection verdicts on an artifact. Detection verdicts include: malicious, suspicious, unsafe, and others. Notice how many security vendors have reported this hash as malicious and how many have not.
2. **Details**: This tab provides additional information extracted from a static analysis of the IoC. Notice the additional hashes associated with this malware like MD5, SHA-1, and more.

3. **Relations**: This tab contains information about the network connections this malware has made with URLs, domain names, and IP addresses. The **Detections** column indicates how many vendors have flagged the URL or IP address as malicious.

4. **Behavior**: This tab contains information related to the observed activity and behaviors of an artifact after executing it in a controlled environment, such as a sandboxed environment. A sandboxed environment is an isolated environment that allows a file to be executed and observed by analysts and researchers. Information about the malware's behavioral patterns is provided through sandbox reports. Sandbox reports include information about the specific actions the file takes when it's executed in a sandboxed environment, such as registry and file system actions, processes, and more. Notice the different types of tactics and techniques used by this malware and the files it created.

Pro tip*: Sandbox reports are useful in understanding the behavior of a file, but they might contain information that is not relevant to the analysis of the file. By default, VirusTotal shows all sandbox reports in the Behavior tab. You can select individual sandbox reports to view. This is helpful because you can view the similarities and differences between reports so that it's easier to identify which behaviors are likely to be associated with the file.*

Step 4: Determine whether the file is malicious

Review the VirusTotal report to determine whether the file is malicious. The following sections will be helpful to review before making this determination:

- The **Vendors' ratio** is the metric widget displayed at the top of the report. This number represents how many security vendors have flagged the file as malicious over all. A file with a high number of vendor flags is more likely to be malicious.
- The **Community Score** is based on the collective inputs of the VirusTotal community. The community score is located below the vendor's ratio and can be displayed by hovering your cursor over the red **X**. A file with a negative community score is more likely to be malicious.
- Under the **Detection** tab, the **Security vendors' analysis** section provides a list of detections for this file made by security vendors, like antivirus tools. Vendors who *have not* identified the file as malicious are marked with a checkmark. Vendors who *have* flagged the file as malicious are marked with an exclamation mark. Files that are flagged as malicious might also include the name of the malware that was detected and other additional details about the file. This section provides insights into a file's potential maliciousness.

Review these three sections to determine if there is a consistent assessment of the file's potential maliciousness such as: a high vendors' ratio, a negative community score, and malware detections in the security vendors' analysis section.

In the first slide of your **Pyramid of Pain template**, indicate whether this file is malicious. Then, explain your reasoning based on your findings.