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.

***Note**: Use the incident handler's journal you started in a previous activity to take notes during the activity and keep track of your findings.*

***Note**: You might recall creating SHA256 hashes in the lab activity on hash values from a previous course.*

Step-By-Step Instructions

Follow the instructions to complete the activity. Then, go to the next course item to compare your work to a completed exemplar.

Step 1: Access the template

To use the template for this course item, click the link below and select *Use Template*.

Link to template: Pyramid of Pain

OR

If you don't have a Google account, you can download the template directly from the following attachment.

Pyramid of Pain
PPTX File

Step 2: 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 3: 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 4: Analyze the VirusTotal report

1.
2.
3.
4.

Step 5: Determine whether the file is malicious

-

-
-

Step 6: Fill in the template with additional indicators of compromise

-
-
-
-
-
-

What to Include in Your Response

Be sure to include the following points in the template of your completed activity:

- A statement explaining whether the file hash is malicious
- Three different types of indicators of compromise