

To pass this course item, you must receive 100%, or 1 out of 1 point, by completing the activity. You can learn more about the graded and practice items in the [course overview](#).



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

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 5: 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.

Note: The Vendors' ratio is based on security vendors' detections and vendors might not always detect malicious files. The Community Score is based on the opinions and insights from the VirusTotal community. If a file's scores are low, it doesn't necessarily mean that the file is safe. It is recommended to use multiple sources of information when evaluating files.

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

After you've explored the sections in the VirusTotal report, you will uncover additional IoCs that are associated with the file according to the VirusTotal report.

Identify *three* indicators of compromise (IoCs) that are associated with this file hash using the tabs in the VirusTotal report. Then, enter the IoCs into their respective sections in the Pyramid of Pain template.

Indicators of compromise are valuable sources of information for security professionals because they are used to identify malicious activity. You can choose to identify any three of the six types of IoCs found in the Pyramid of Pain:

- Hash value: Hashes convert information into a unique value that can't be decrypted. Hashes are often used as unique references to files involved in an intrusion. In this activity, you used a SHA256 hash as the artifact for this investigation. Find another hash that's used to identify this malware and enter it beside the Hash values section in the Pyramid of Pain template. You can use the Details tab to help you identify other hashes.
- IP address: Find an IP address that this malware contacted and enter it beside the IP addresses section in the Pyramid of Pain template. You can locate IP addresses in the Relations tab under the Contacted IP addresses section or in the Behavior tab under the IP Traffic section.
- Domain name: Find a domain name that this malware contacted and enter it beside the Domain names section in the Pyramid of Pain template. You can find domain name information under the Relations tab. You might encounter benign domain names. Use the Detections column to identify domain names that have been reported as malicious.
- Network artifact/host artifact: Malware can create network-related or host-related artifacts on an infected system. Find a network-related or host-related artifact that this malware created and enter it beside the Network/host artifacts section in the Pyramid of Pain template. You can find this information from the sandbox reports under the Behavior tab or from the Relations tab.
- Tools: Attackers can use tools to achieve their goal. Try to find out if this malware has used any tool. Then, enter it beside the Tools section in the Pyramid of Pain template.
- Tactics, techniques, and procedures (TTPs): TTPs describe the behavior of an attacker. Using the sandbox reports from the Behavior tab, find the list of tactics and techniques used by this malware as identified by MITRE ATT&CK® and enter it beside the TTPs section in the Pyramid of Pain template.

Note: VirusTotal reports can contain legitimate domains and IP addresses that are not considered malicious.

Pro tip: To learn more about a section in VirusTotal, hover your cursor over the information icon to display information on what that section includes.

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

Activity Exemplar: Investigate a suspicious file hash

Here is a completed exemplar along with an explanation of how the exemplar fulfills the expectations for the activity.

Completed Exemplar

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

Link to exemplar: [Investigation findings](#)

OR

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

[Investigation findings](#)

[PPTX File](#)

Assessment of Exemplar

Compare the exemplar to your completed activity. Review your work using each of the criteria in the exemplar. What did you do well? Where can you improve? Use your answers to these questions to guide you as you continue to progress through the course.

Note: *The exemplar represents one of many possible ways to complete this activity. Yours will likely differ depending on which IoCs you have identified and listed. What's important is that your activity captures some details of the file hash investigation including related IoCs and verification of the file as malicious.*

Step 1: The exemplar provides a clear and brief summary of the file hash by using the information found under the **Detection** tab. The **Community Score** and the **Security vendors' analysis** listed in the VirusTotal report provide insight into the file. Over fifty security vendors have flagged this file as malicious. Additionally, multiple vendors have categorized the file as Flagpro malware, a well-known malware used by advanced threat actors.

Step 2: The exemplar also identifies different types of IoCs using the VirusTotal report. While the exemplar provides an example for each field in the pyramid, your activity only has to include *three* IoC examples. Using the information found in the **Details**, **Relations**, and **Behavior** tabs, you'll be able to find additional IoCs that are related to the file such as: a domain names, IP addresses, hash values, network or host artifacts, tools, and tactics, techniques, and procedures (TTPs).

- **Domain names:** org.misecure.com is reported as a malicious contacted domain under the Relations tab in the VirusTotal report.
- **IP address:** 207.148.109.242 is listed as one of many IP addresses under the Relations tab in the VirusTotal report. This IP address is also associated with the org.misecure.com domain as listed in the DNS Resolutions section under the Behavior tab from the Zenbox sandbox report.
- **Hash value:** 287d612e29b71c90aa54947313810a25 is a MD5 hash listed under the Details tab in the VirusTotal report.
- **Network/host artifacts:** Network-related artifacts that have been observed in this malware are HTTP requests made to the org.misecure.com domain. This is listed in the Network Communications section under the Behavior tab from the Venus Eye Sandbox and Rising MOVES sandbox reports.
- **Tools:** Input capture is listed in the Collection section under the Behavior tab from the Zenbox sandbox report. Malicious actors use input capture to steal user input such as passwords, credit card numbers, and other sensitive information.
- **TTPs:** Command and control is listed as a tactic under the Behavior tab from the Zenbox sandbox report. Malicious actors use command and control to establish communication channels between an infected system and their own system.

Key takeaways

In this activity, you determined that a file was malicious using information from a VirusTotal report. You also identified additional indicators of compromise that are associated with this file. As a security analyst, you will use investigative tools like VirusTotal to access threat intelligence from the global cybersecurity community. This helps you add context to investigations and learn more about threats when investigating a possible security incident.