

Scenario

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.

Steps

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](https://www.virustotal.com). 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:** 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.

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 5: Enter the file hash into VirusTotal

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 goals. 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.