# Investigate a suspicious file hash

# 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.

**Details of Alert:**

**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.

**Analysis of Hash File can be done using below metrics in details tab:**

* 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

**Pyramid of Pain:** It captures the relation between Indicators of Compromise(IOC) and level of difficulty the malicious actors experience with IOC. Below are the 6 IOC and steps to determine them from Virus total Service

* **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** sectionin 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.

Sample for pyramid of painA blue pyramid with white text

Description automatically generated

Sample of Virus Total:

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

Observations:

There are over 55 security vendors that are compromised with -67 of community score which shows that this file hash has malware and many community members have categorized the file as Flagpro malware, a well-known malware used by advanced threat actors.