Assessment

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.