A screenshot of a computer

Description automatically generated

1. **Malicious Nature of the File:** The file hash is detected by multiple security vendors and sandboxes as malicious, indicated by the high community score of 56/70. The popular threat label associated with it is "trojan.flagpro/frgator," which categorizes the file as a trojan, a type of malicious software that disguises itself as legitimate.
2. **Indicators of Compromise (IoCs):**
   * **Hash Value:** The SHA256 hash given in the report 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b itself is an IoC. Additional hash values like the MD5 or SHA1 for this file would also serve as IoCs if provided within the report.
   * **IP Addresses and Domain Names:** The report might list associated IP addresses and domain names the malware has contacted. This specific screenshot does not display them, but they would typically be found in the "Relations" or "Details" tabs.
   * **Network/Host Artifacts:** The terms "spreader," "long sleeps," "detect-debug-environment," "checks-user-input," and "runtime-modules" suggest behaviors or artifacts indicative of the malware's operation within a network or host system. These could include specific registry keys, file paths, or network traffic signatures associated with the malware.
   * **Tools:** The report labels such as "Backdoor.Win32.Flagpro," "Trojan.Agent.Flagpro," and "Trojan.Fragtor" suggest specific tools or payloads used by the attackers that are encapsulated within the malware.
   * **Tactics, Techniques, and Procedures (TTPs):** The behaviors mentioned (like "spreader" and "detect-debug-environment") hint at the TTPs the malware employs. To detail the TTPs, one would refer to the MITRE ATT&CK framework for a more precise mapping of the malware's behavior to known attack patterns.

Given the provided information, these are the types of IoCs you would include in the Pyramid of Pain template. Remember, each IoC should be categorized based on its type, and the template should reflect both the nature of the IoCs and their relationship to the difficulty experienced by adversaries when these are mitigated by security teams.

security analysts would look for other IoCs such as:

* **IP Addresses:** Any IP addresses that the malware communicates with, which can be found in the Relations or Details tabs of the full VirusTotal report.
* **Domain Names:** Any domain names that the malware is associated with, which are often listed in the Relations tab of the full report and can be indicators of the command-and-control servers or other infrastructure used by the attackers.
* **Tools:** Specific malware families or tools used in the attack, which can sometimes be inferred from the labels provided by the security vendors in the report, like "Backdoor.Win32.Flagpro."