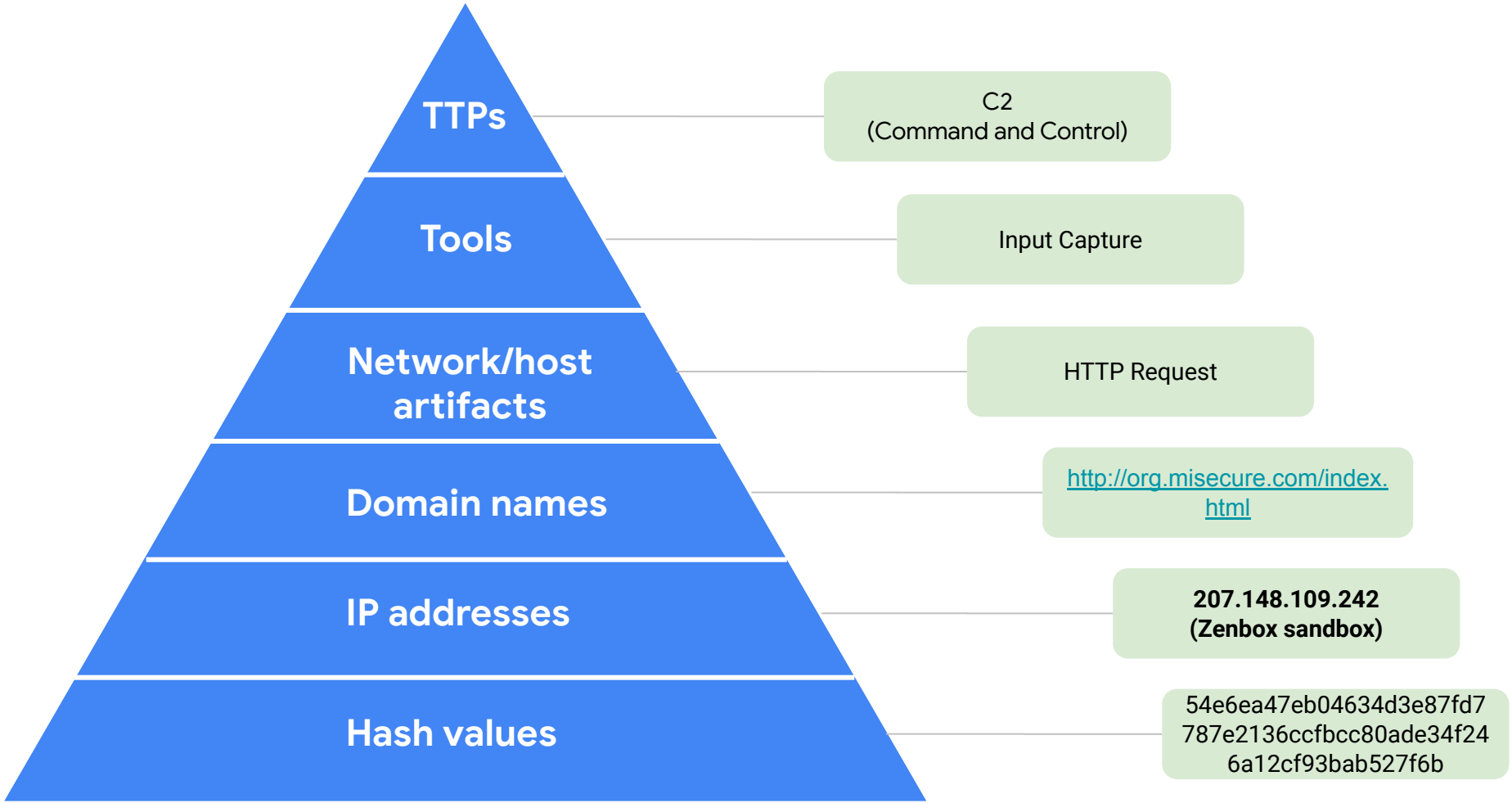
Has this file been identified as malicious? Explain why or why not.

This file has been flagged by 80.281% as a threat and it has been labeled trojan.flagpro/jaik. The file has been considered a Trojan. It is named flagpro which was widely used by BlackTech.

- 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.
- Domain names: org.misecure.com is reported as a malicious contacted domain under the Relations tab in the VirusTotal 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.


TTPs
Tools
Network/host artifacts
Domain names
IP addresses
Hash values
C2 (Command and Control)
Input Capture
HTTP Request
http://org.misecure.com/index.html
207.148.109.242 (Zenbox sandbox)
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b