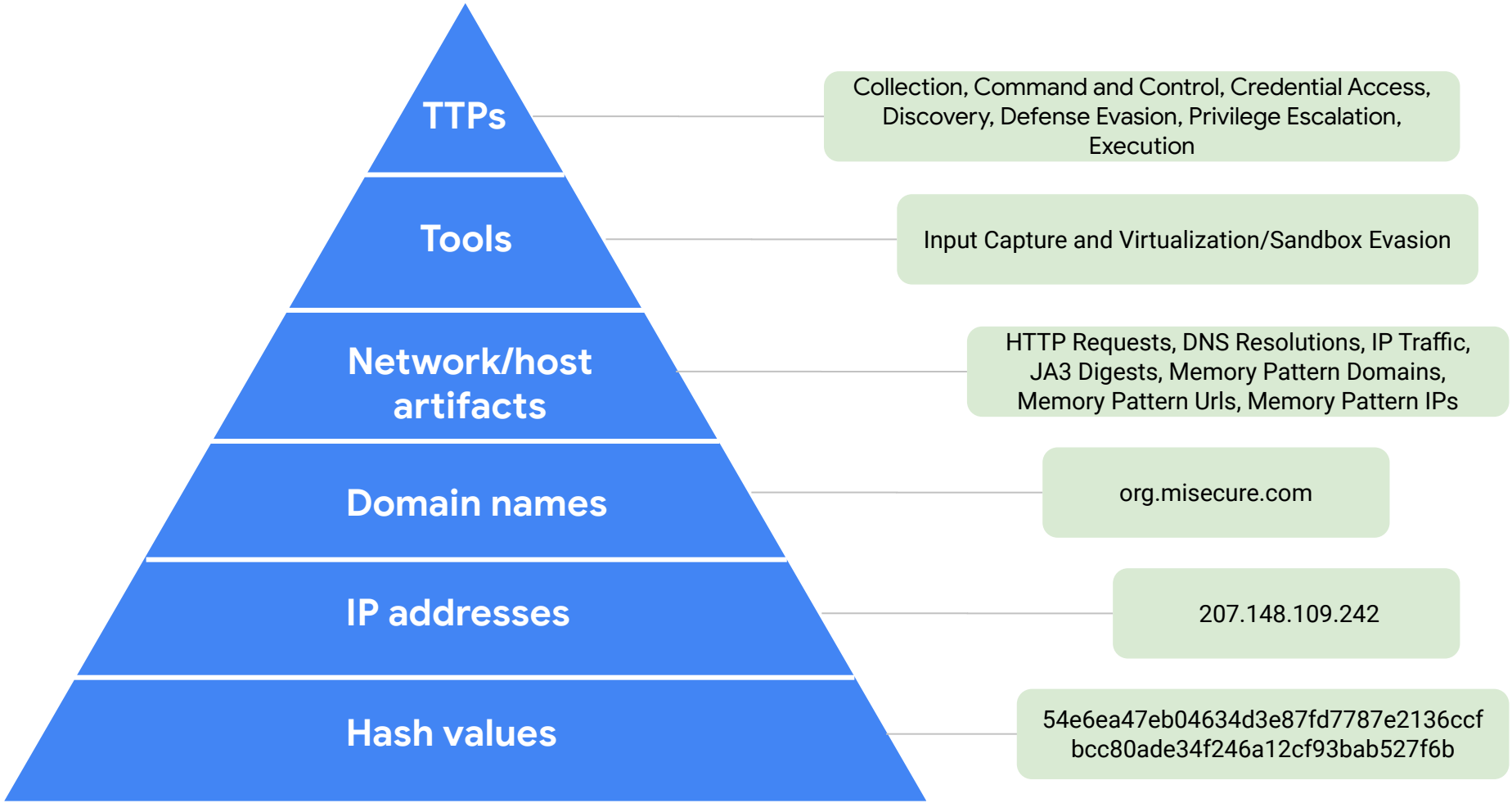
Has this file been identified as malicious? Explain why or why not.

Yes, after checking the file's unique code, most security companies and testing systems found it to be harmful. Specifically, 57 out of 71 security companies and 3 testing systems marked it as dangerous. This code is linked to a well-known malicious program called Flagpro, which is often connected to a skilled hacking group known as BlackTech.

Experts call this program "trojan.flagpro/fragtor." It falls into the category of trojan viruses and has different names like flagpro, fragtor, and busyice.


TTPs
Tools
Network/host artifacts
Domain names
IP addresses
Hash values
Collection, Command and Control, Credential Access, Discovery, Defense Evasion, Privilege Escalation, Execution
Input Capture and Virtualization/Sandbox Evasion
HTTP Requests, DNS Resolutions, IP Traffic, JA3 Digests, Memory Pattern Domains, Memory Pattern Urls, Memory Pattern IPs
org.misecure.com
207.148.109.242
54e6ea47eb04634d3e87fd7787e2136ccf bcc80ade34f246a12cf93bab527f6b