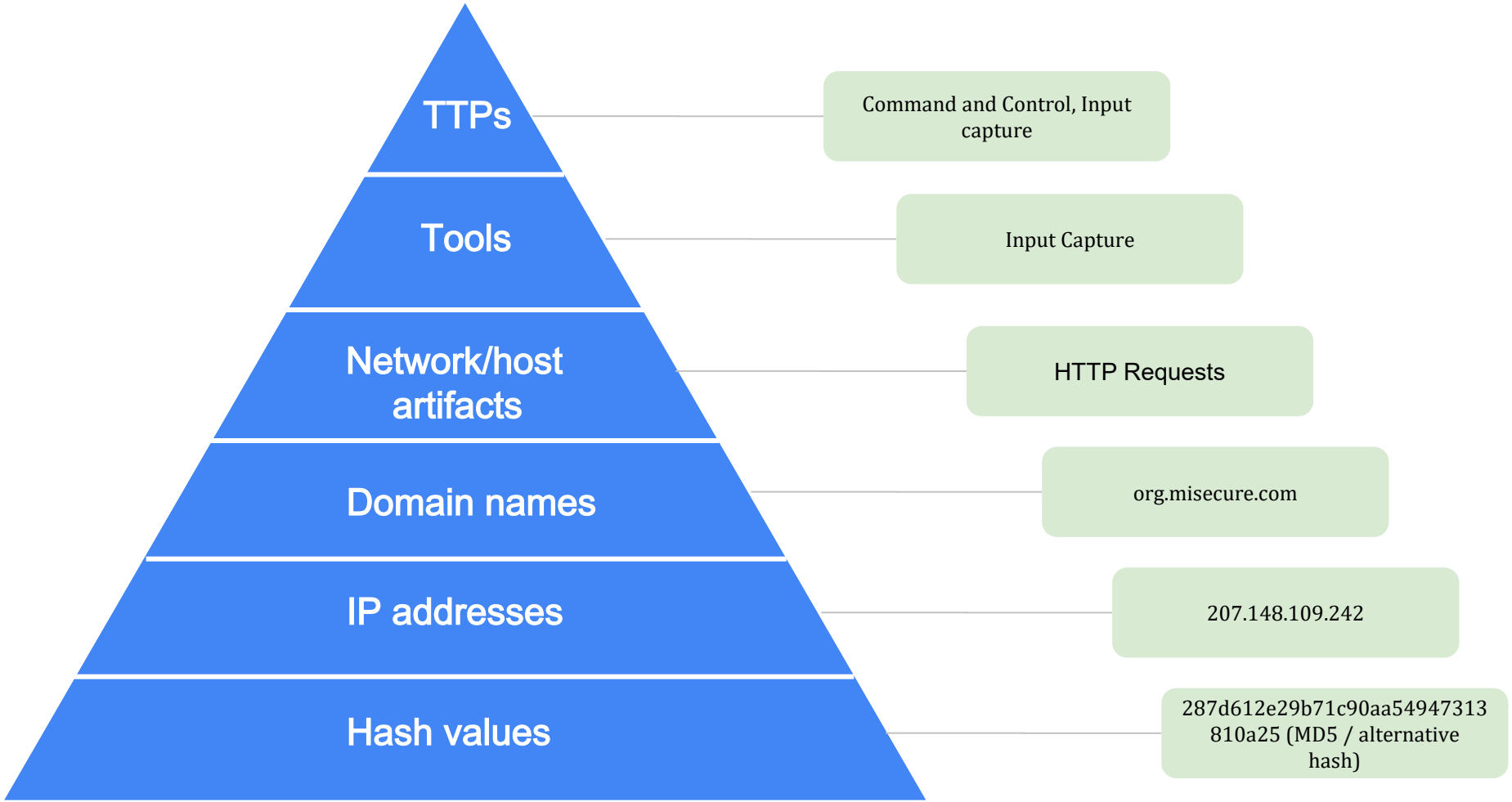
Has this file been identified as malicious? Explain why or why not.

Verdict: Yes, the file hash is malicious.

Reasoning: The VirusTotal scan shows a high Vendor Ratio where 47 out of 65 security vendors flagged the file as malicious. Additionally, it has a strongly negative Community Score (-293) and is identified across multiple engines as a Trojan associated with the FlagPro malware family (commonly linked to the BlackTech threat group).


TTPs
Tools
Network/host artifacts
Domain names
IP addresses
Hash values
Command and Control, Input capture
Input Capture
HTTP Requests
org.misecure.com
207.148.109.242
287d612e29b71c90aa54947313810a25 (MD5 / alternative hash)