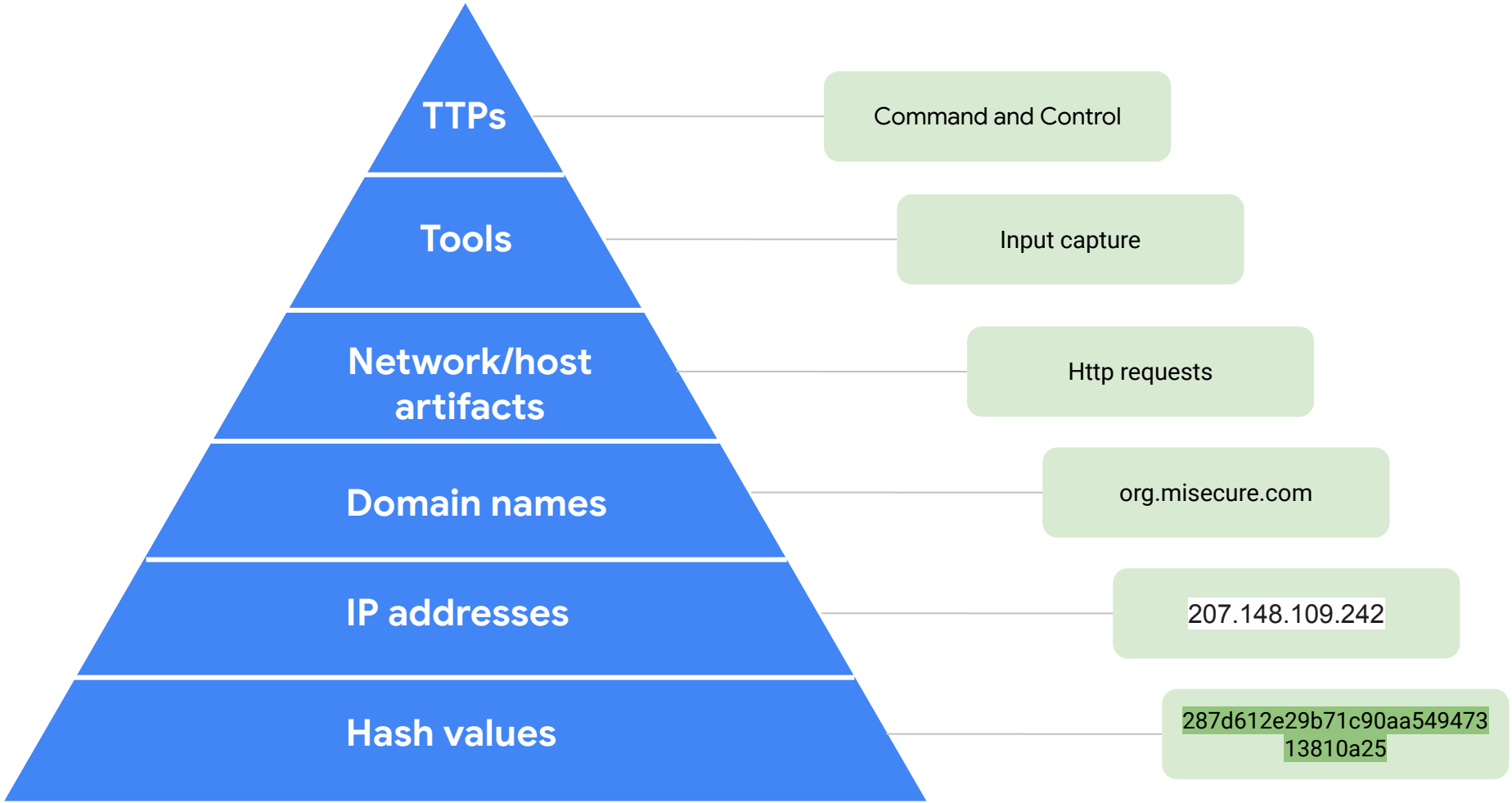
Has this file been identified as malicious? Explain why or why not.

The file has been confirmed as malicious by over 50 vendors and identified as a well-known threat categorized under the **Trojan family**, specifically recognized as **Flagpro**. This malware has been frequently associated with the activities of **BlackTech**, an advanced threat actor group known for its sophisticated campaigns targeting organizations across various industries.


TTPs
Tools
Network/host artifacts
Domain names
IP addresses
Hash values
Command and Control
Input capture
Http requests
org.misecure.com
207.148.109.242
287d612e29b71c90aa549473 13810a25