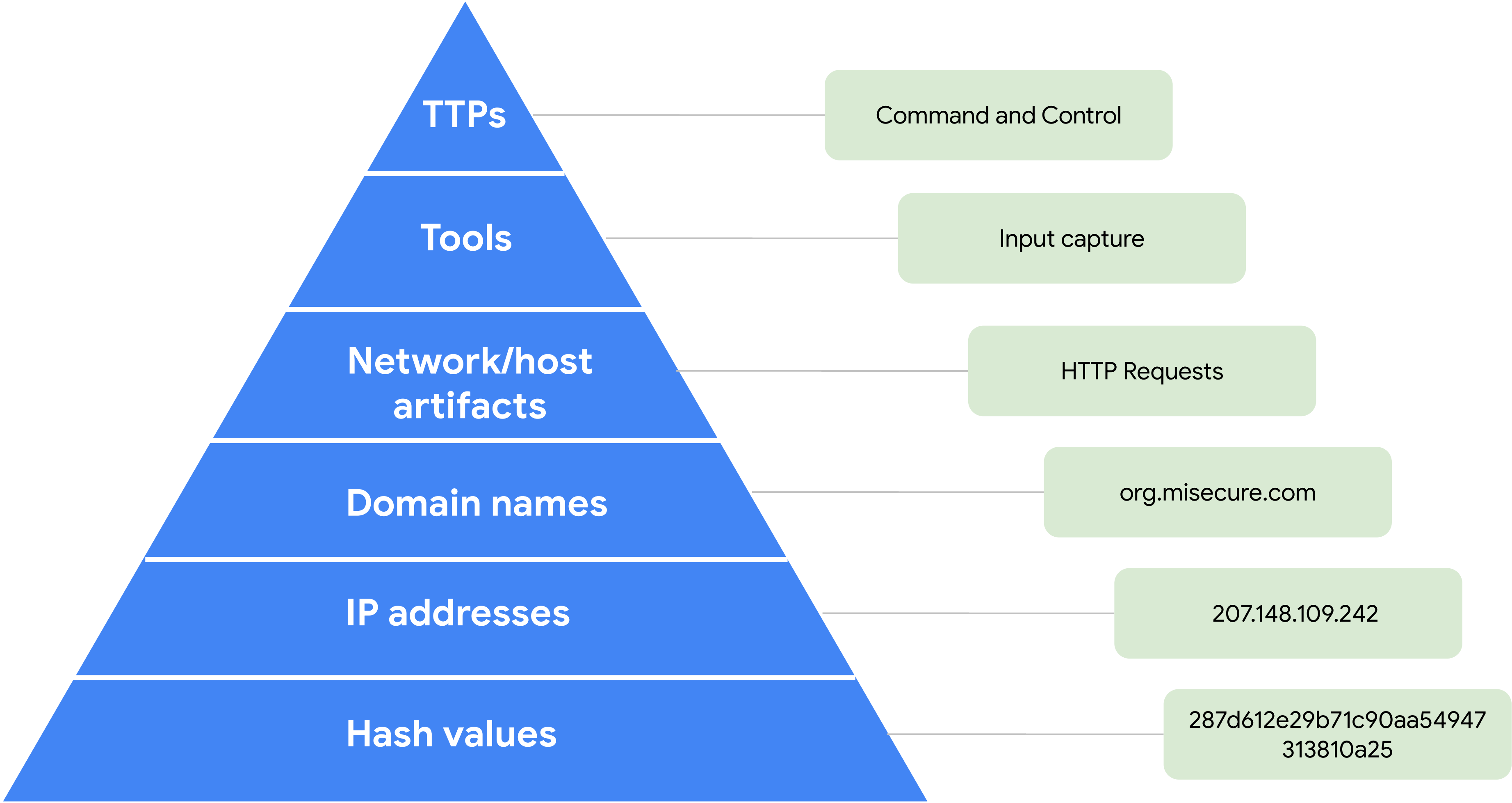
Has this file been identified as malicious? Explain why or why not.

The file hash has been flagged as malicious by over 50 vendors. Further investigation reveals it as the malware Flagpro, commonly associated with the advanced threat group BlackTech.



TTPs

Command and Control

Tools

Input capture

Network/host
artifacts

HTTP Requests

Domain names

org.misecure.com

IP addresses

207.148.109.242

Hash values

287d612e29b71c90aa54947
313810a25