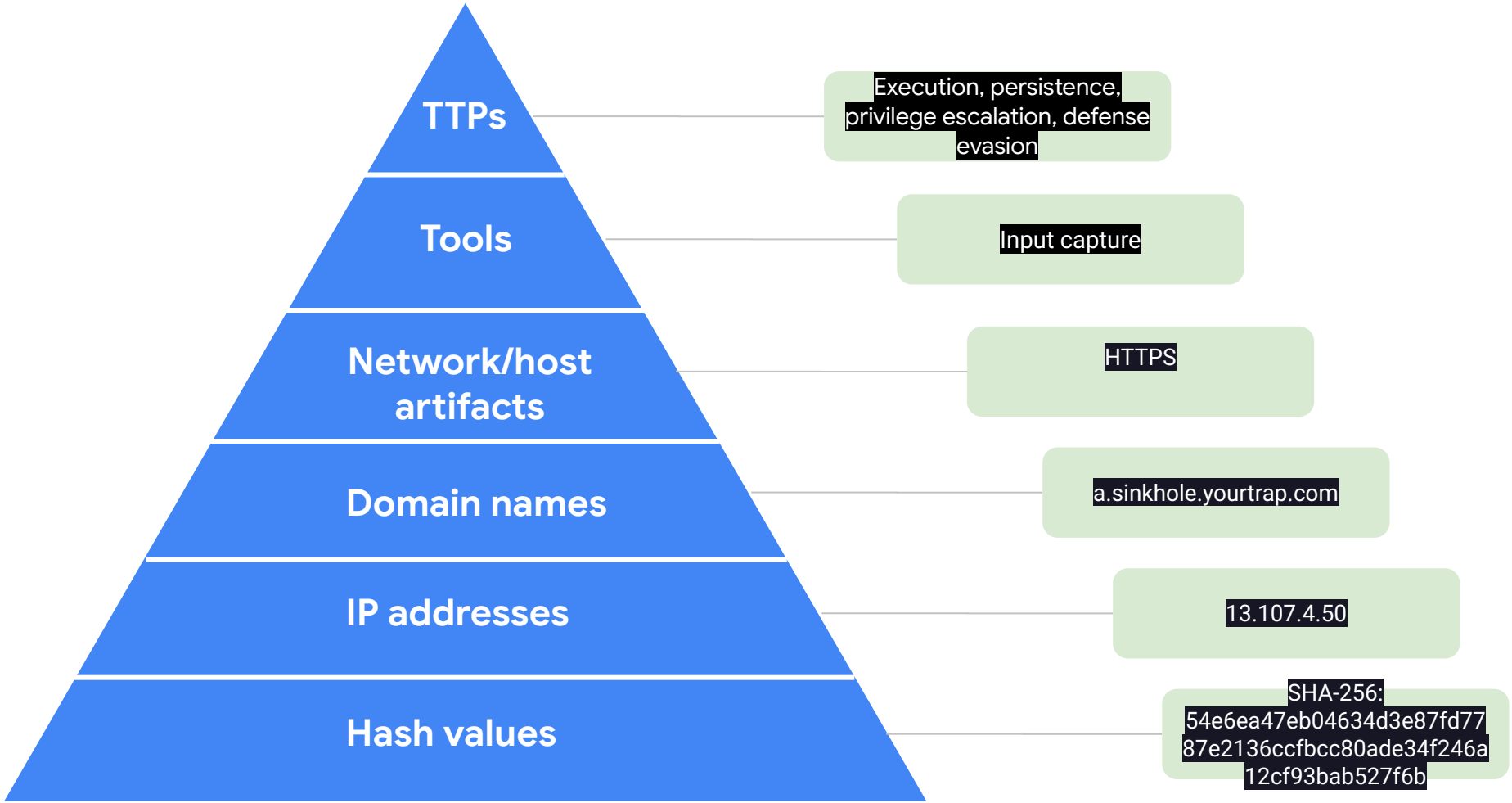
Has this file been identified as malicious? Explain why or why not.

This file has been identified malicious by 59/72 security vendors. This number is daily high making this file seem malicious. Additionally, this file has a community score of -247, which says that VirusTotal community identify this file as malicious. The popular threat label for this file is flagpro that is used by BlackTech.


TTPs
Tools
Network/host artifacts
Domain names
IP addresses
Hash values
Execution, persistence, privilege escalation, defense evasion
Input capture
HTTPS
a.sinkhole.yourtrap.com
13.107.4.50
SHA-256: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b