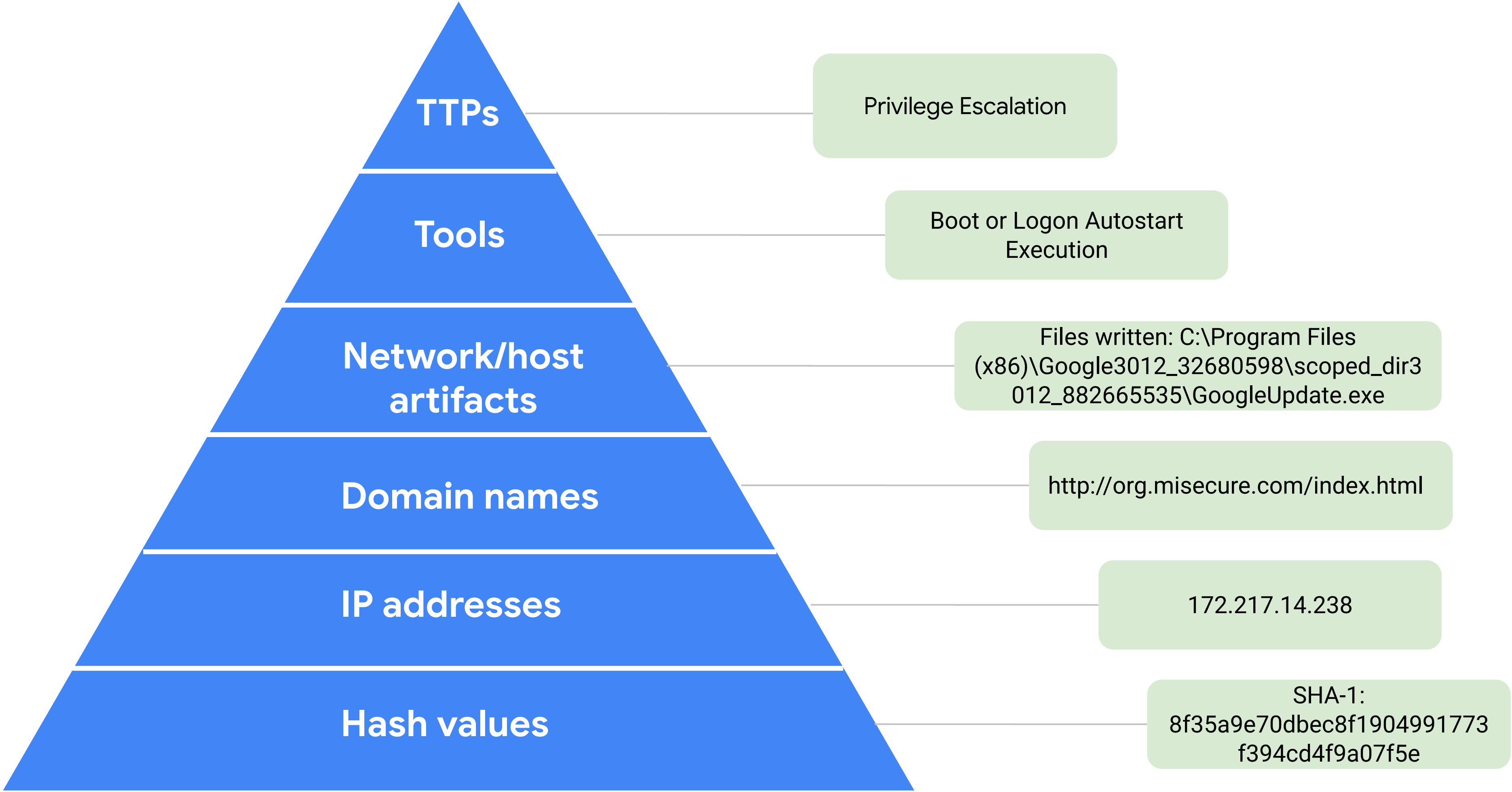
Has this file been identified as malicious? Explain why or why not.

The file associated with SHA-256 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b is malicious based on the vendors’ ratio as it is significantly high (over 60 vendors reported this file as malicious) while the community scores are very low (negative range). These indicators along with the security vendor’s analysis strongly point to a trojan horse.



TTPs — Privilege Escalation

Tools — Boot or Logon Autostart Execution

Network/host artifacts — Files written: C:\Program Files (x86)\Google3012_32680598\scoped_dir3012_882665535\GoogleUpdate.exe

Domain names — http://org.misecure.com/index.html

IP addresses — 172.217.14.238

Hash values — SHA-1: 8f35a9e70dbec8f1904991773f394cd4f9a07f5e