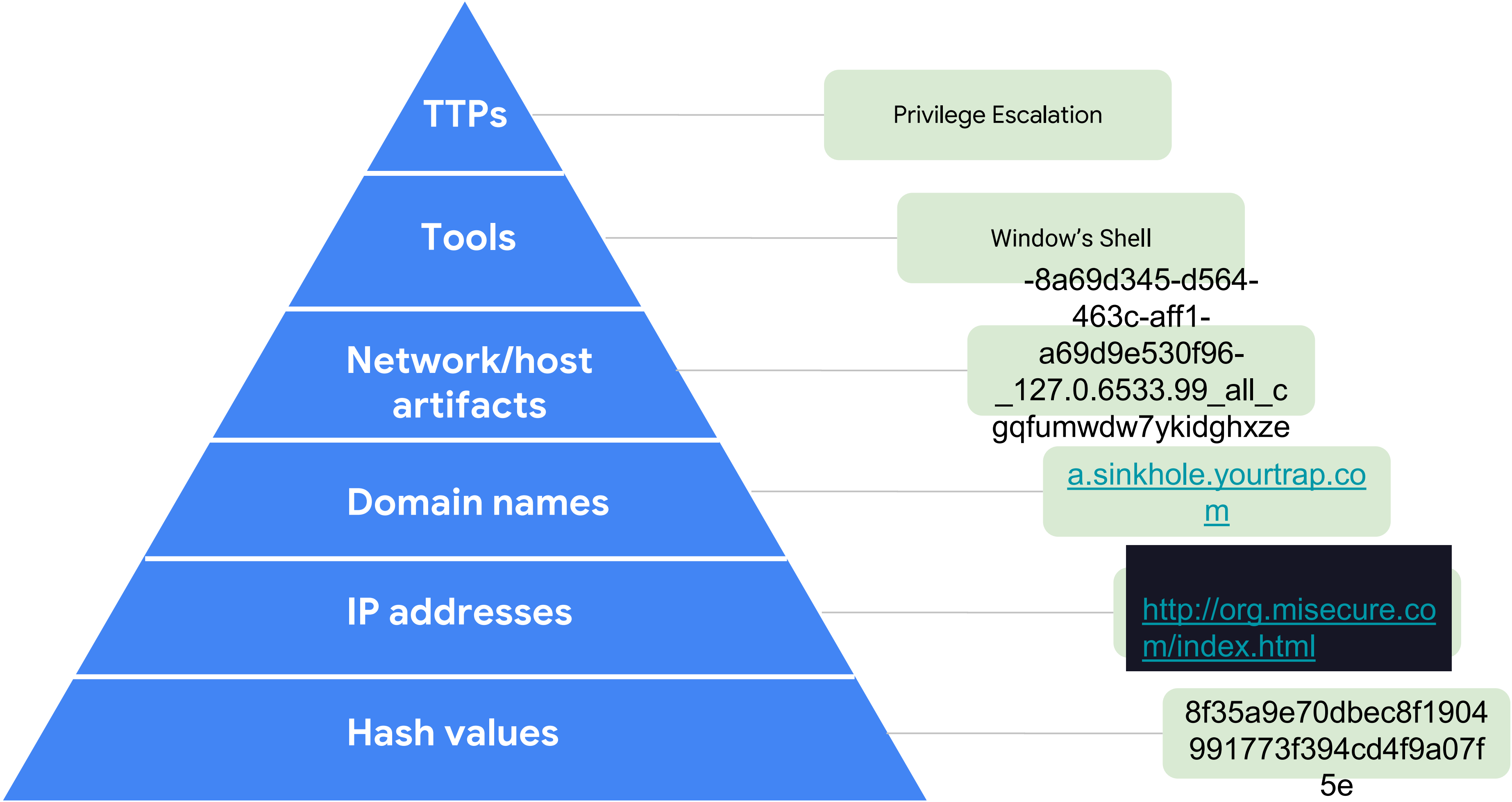
Has this file been identified as malicious? Explain why or why not.

Using an OSINT called VirusTotal to scan the hash of the malicious file I found multiple indicators that the file is in fact malicious in nature. These indicators include a 59/72 security vendor flag for malicious content, a -266 community score, and a popular detected threat label of trojan.flagpro/fragtor. All of these combined would indicate that there is a great chance the file is malicious, but further investigation using other OSINT may be necessary still for confirmation.



TTPs — Privilege Escalation

Tools — Window’s Shell

Network/host artifacts — -8a69d345-d564-463c-aff1-a69d9e530f96-_127.0.6533.99_all_cgqfumwdw7ykidghxze

Domain names — a.sinkhole.yourtrap.com

IP addresses — http://org.misecure.com/index.html

Hash values — 8f35a9e70dbec8f1904991773f394cd4f9a07f5e