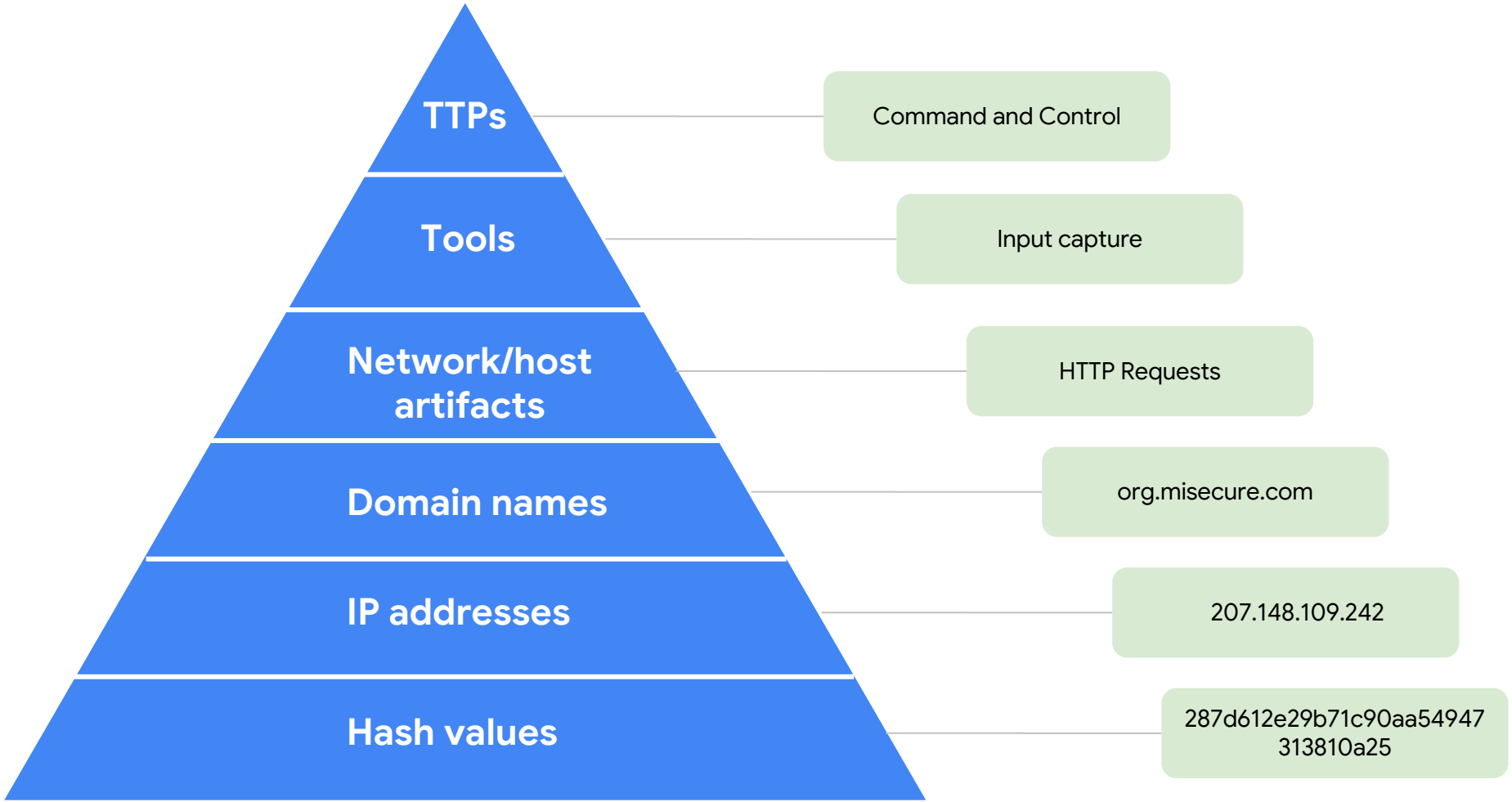
Has this file hash been reported as malicious? Explain why or why not.

The file hash has been reported as malicious by over 50 vendors. Upon further investigation, this file hash is known as the malware Flagpro, which has been commonly used by the advanced threat actor BlackTech.


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
287d612e29b71c90aa54947313810a25

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Sign in

57 / 72

Community Score -231

57/72 security vendors flagged this file as malicious

Reanalyze Similar More

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

bfsvc.exe

peexe service-scan spreader checks-user-input runtime-modules detect-debug-environment long-sleeps direct-cpu-clock-access

Size 430.00 KB

Last Analysis Date 3 hours ago

EXE

DETECTION DETAILS RELATIONS ASSOCIATIONS BEHAVIOR COMMUNITY 30+

Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.flagpro/fragtor

Threat categories trojan

Family labels flagpro fragtor busyice

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Malware/Win32.Generic.C4209910	Alibaba	Backdoor:Win32/Kryptik.8648de52
ALYac	Trojan.Agent.Flagpro	Antiy-AVL	Trojan[APT]/Win32.Blacktech
Arcabit	Trojan.Fragtor.D5A915	Avast	Win32:Malware-gen
AVG	Win32:Malware-gen	Avira (no cloud)	HEUR/AGEN.1312459