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

This file is malicious since it has a high vendors' ratio 58 out of 72 and -95 community score. Majority of vendors had flagged this file as trojan flagpro.

SHA256 file hash:
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

58 / 72

Community Score

58/72 security vendors and 3 sandboxes flagged this file as malicious

Reanalyze | Similar | More

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

bfsvc.exe

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

Size: 430.00 KB

Last Modification Date: 3 hours ago

EXE

DETECTION | DETAILS | RELATIONS | BEHAVIOR | TELEMETRY | COMMUNITY 25+

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

Popular threat label trojan.flagpro/fragtor

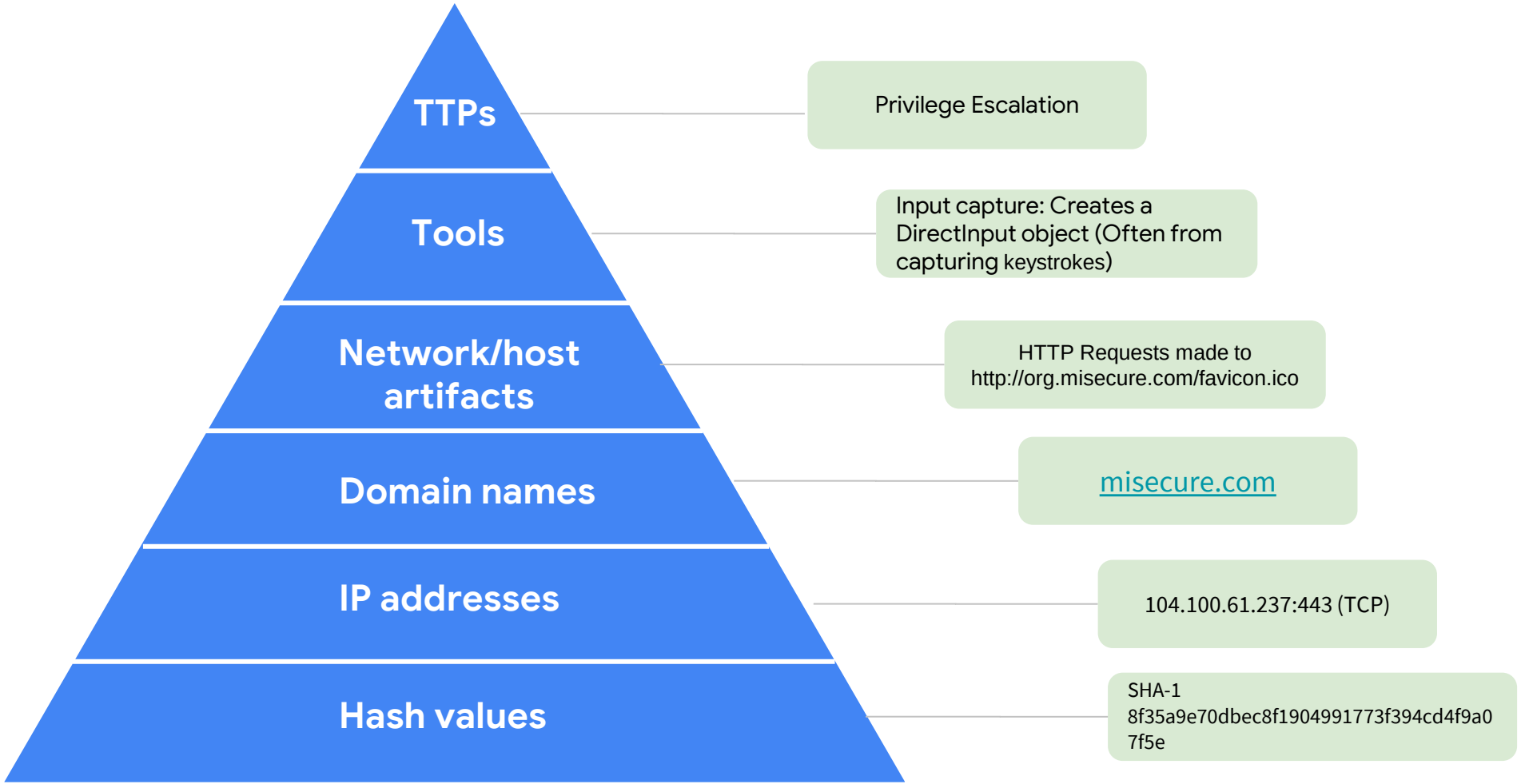
Threat categories trojan

Family labels flagpro | fragtor | busyice

Security vendors' analysis

Do you want to automate checks?

AhnLab-V3	Malware/Win32.Generic.C4209910	Alibaba	Backdoor:Win32/Flagpro.59f5de24
AliCloud	Suspicious	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	BitDefender	Gen:Variant.Fragtor.370965
BitDefenderTheta	Gen:NN.ZexaF.36802.Au0@a0!5WTfi	Bkav Pro	W32.Common.BFF1CCFD
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason	Malicious.e29b71
Cylance	Unsafe	Cynet	Malicious (score: 99)
DeepInstinct	MALICIOUS	DrWeb	BackDoor.Flagpro.1
Elastic	Malicious (high Confidence)	Emsisoft	Gen:Variant.Fragtor.370965 (B)


TTPs
Tools
Network/host artifacts
Domain names
IP addresses
Hash values
Privilege Escalation
Input capture: Creates a DirectInput object (Often from capturing keystrokes)
HTTP Requests made to http://org.misecure.com/favicon.ico
misecure.com
104.100.61.237:443 (TCP)
SHA-1
8f35a9e70dbec8f1904991773f394cd4f9a07f5e