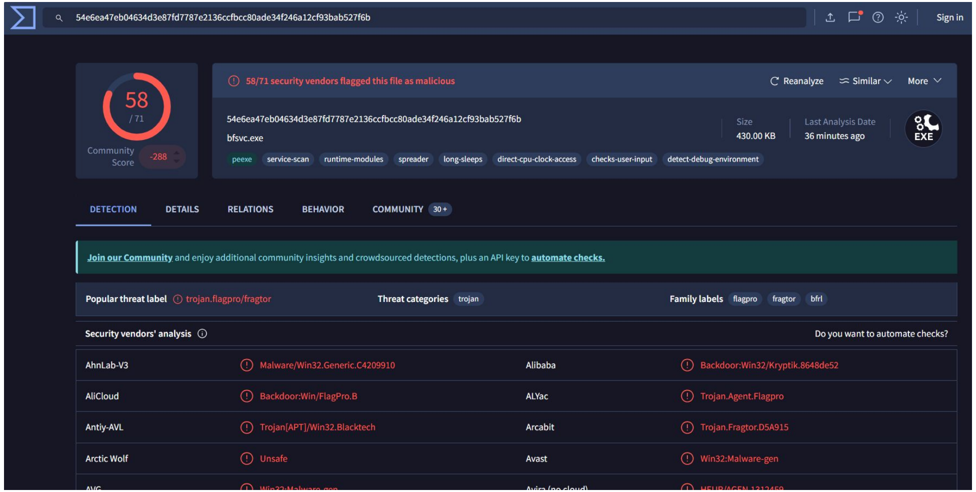
SHA256 file hash: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Here is a timeline of the events leading up to this alert:

- **1:11 p.m.:** An employee receives an email containing a file attachment.
- **1:13 p.m.:** The employee successfully downloads and opens the file.
- **1:15 p.m.:** Multiple unauthorized executable files are created on the employee's computer.
- **1:20 p.m.:** An intrusion detection system detects the executable files and sends out an alert to the SOC.

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



58/71 security vendors flagged this file as malicious

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
bfsvc.exe
peexe service-scan runtime-modules spreader long-sleeps direct-cpu-clock-access checks-user-input detect-debug-environment

Size
430.00 KB

Last Analysis Date
36 minutes ago

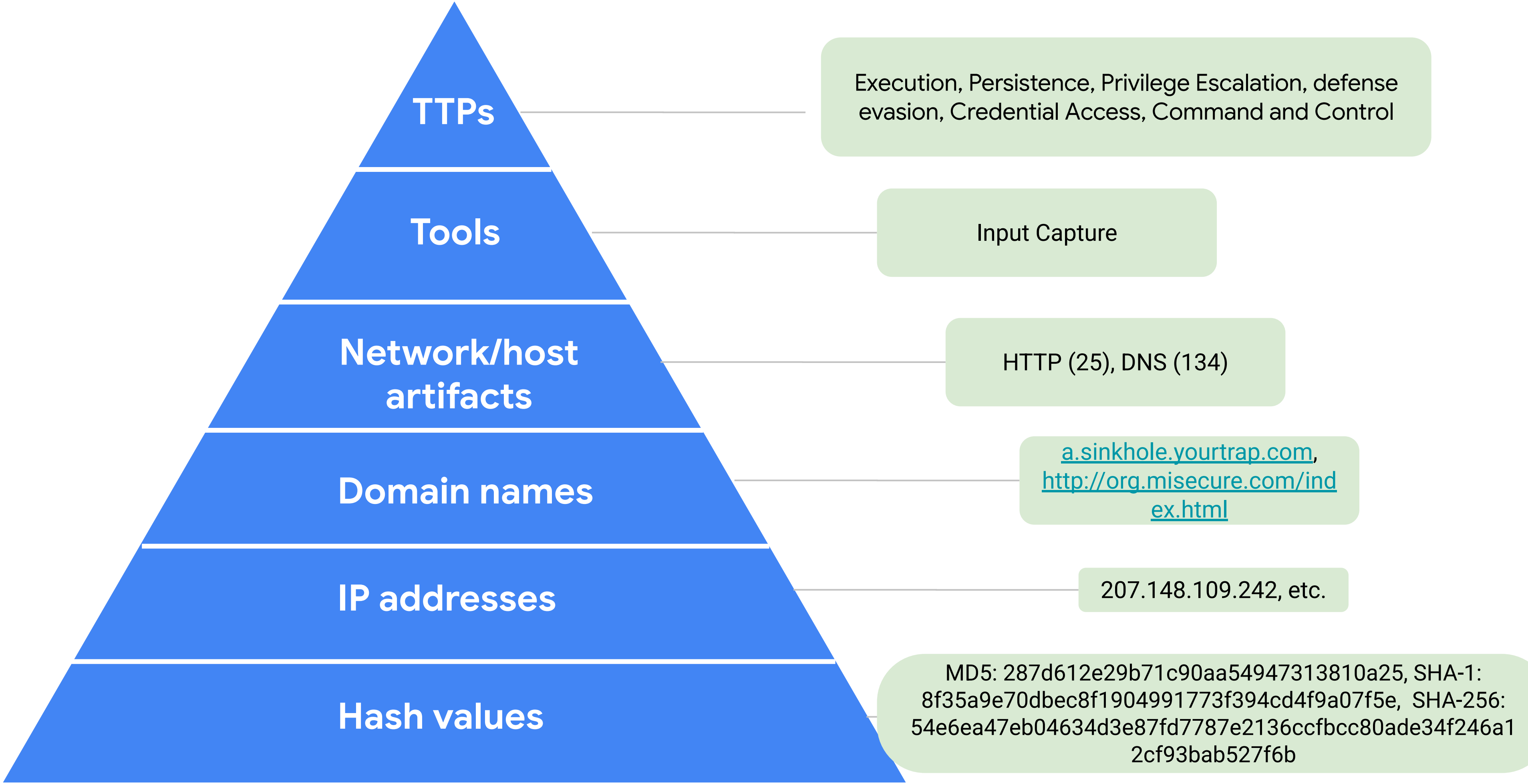
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Popular threat label trojan.flagpro/fragtor   Threat categories trojan   Family labels flagpro fragtor bfrl

Security vendors' analysis   Do you want to automate checks?

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

VirusTotal was used to look at the file (https://www.virustotal.com/). Based on the results of the file hash using the tool's search function, the file is malicious. It seems to be signed by Microsoft (unverified) and labeled as a Boot File Service Utility. It is used in multiple different backdoors and Trojans.



TTPs

Execution, Persistence, Privilege Escalation, defense evasion, Credential Access, Command and Control

Tools

Input Capture

Network/host artifacts

HTTP (25), DNS (134)

Domain names

a.sinkhole.yourtrap.com, http://org.misecure.com/index.html

IP addresses

207.148.109.242, etc.

Hash values

MD5: 287d612e29b71c90aa54947313810a25, SHA-1: 8f35a9e70dbec8f1904991773f394cd4f9a07f5e, SHA-256: 54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b