

**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**

Command and Control

**Tools**

Input capture

**Network/host  
artifacts**

HTTP Requests

**Domain names**

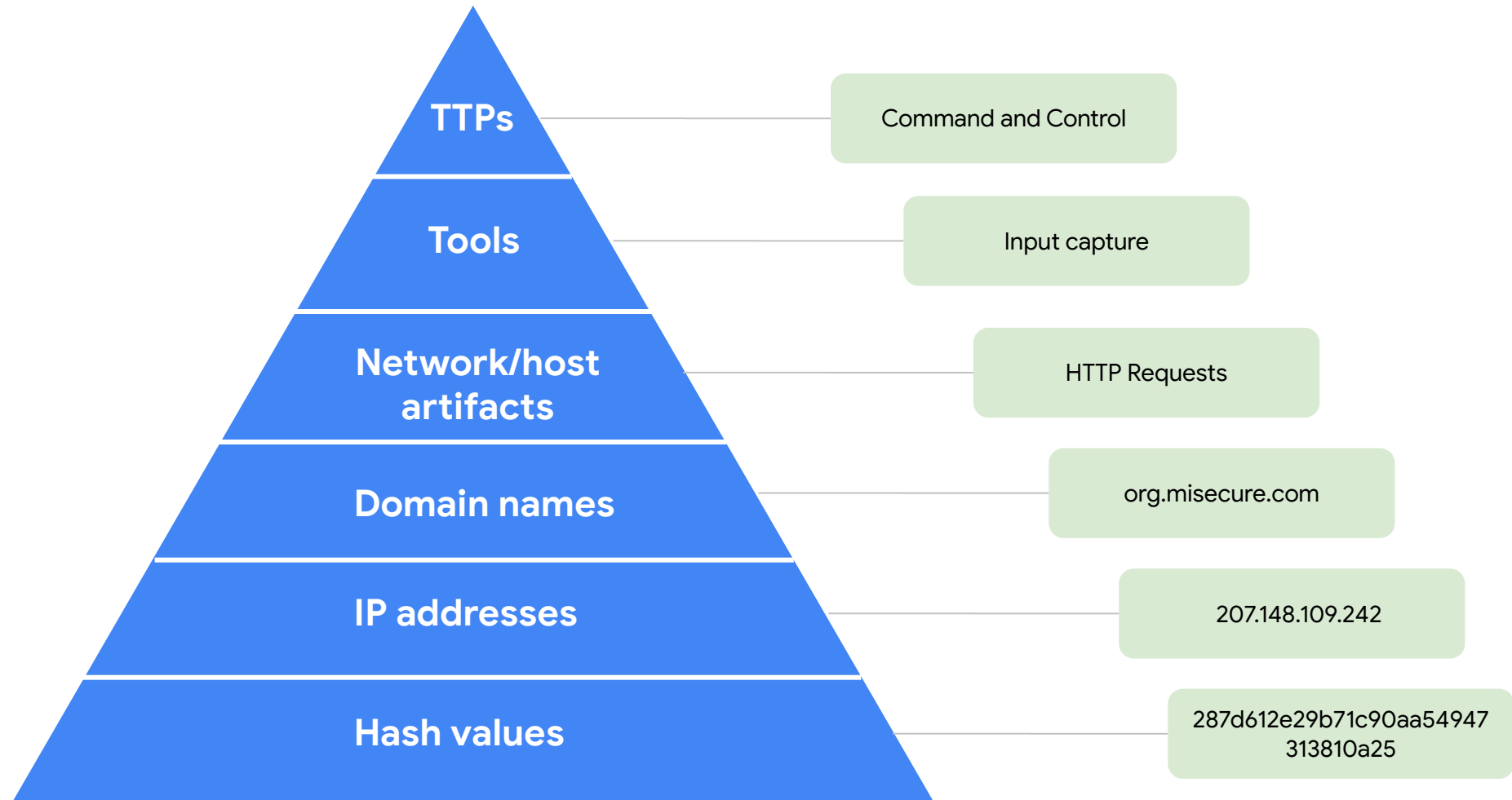
org.misecure.com

**IP addresses**

207.148.109.242

**Hash values**

287d612e29b71c90aa54947  
313810a25





54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b



Sign in

Sign up



Community Score

57 security vendors and 3 sandboxes flagged this file as malicious

Reanalyze

Similar

More

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

bfsvc.exe

Size

430.00 KB

Last Analysis Date

3 hours ago



peexe

runtime-modules

detect-debug-environment

long-sleeps

direct-cpu-clock-access

checks-user-input

spreader

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY 24 +

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

ALYac

Trojan.Agent.Flagpro

Antiy-AVL

Trojan[APT]/Win32.Blacktech

