Investigate a Suspicious Hash File

Scenario

You are a level one security operations center (SOC) analyst at a financial services company. You have received an alert about a suspicious file being downloaded on an employee's computer.

You investigate this alert and discover that the employee received an email containing an attachment. The attachment was a password-protected spreadsheet file. The spreadsheet's password was provided in the email. The employee downloaded the file, then entered the password to open the file. When the employee opened the file, a malicious payload was then executed on their computer.

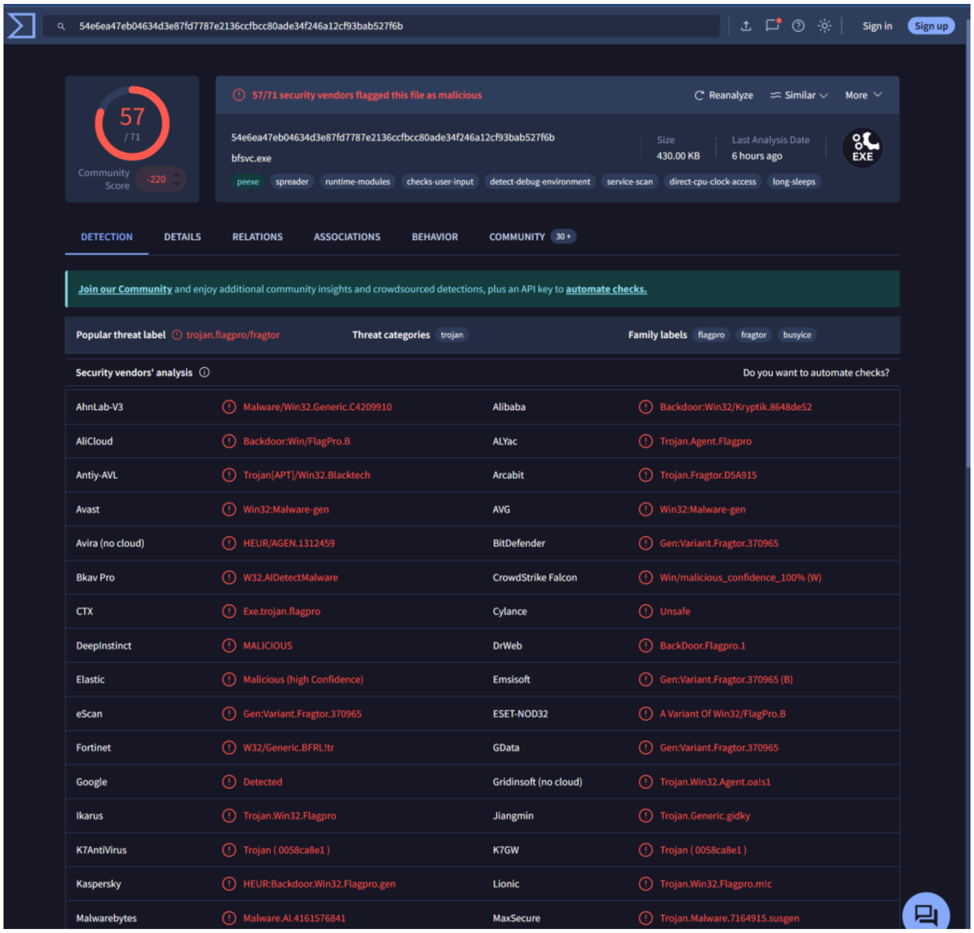
You retrieve the malicious file and create a SHA256 hash of the file. You might recall from a previous course that a hash function is an algorithm that produces a code that can't be decrypted. Hashing is a cryptographic method used to uniquely identify malware, acting as the file's unique fingerprint.

Now that you have the file hash, you will use VirusTotal to uncover additional IoCs that are associated with the file.

Response

The file hash has been reported as malicious by over 50 vendors. The community score is -220. Upon further investigation, this file hash is known as the malware Flagpro, which has been commonly used by the advanced threat actor BlackTech.

Using the Pyramid of Pain, we can list attributes as Indicators of compromise.



54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

57 / 71

Community Score -220

57/71 security vendors flagged this file as malicious

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

bfsvc.exe

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

Size: 430.00 KB

Last Analysis Date: 6 hours ago

EXE

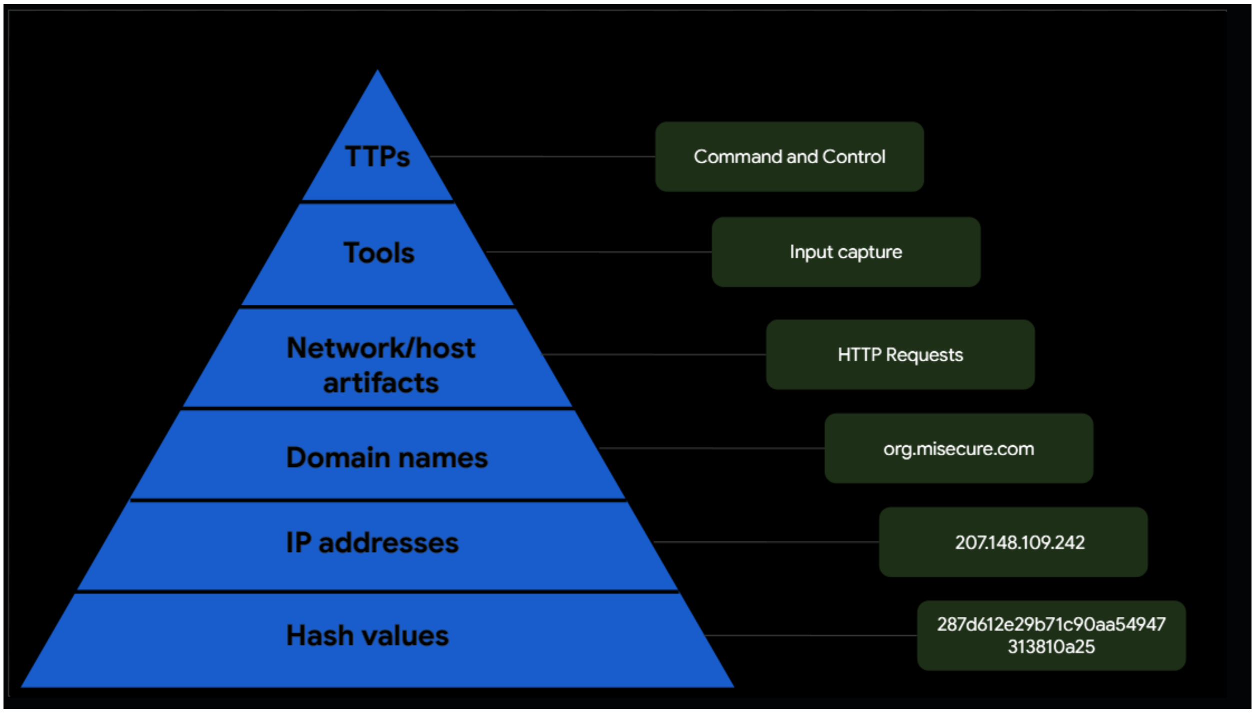
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

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
AliCloud	Backdoor:Win/FlagPro.B	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
Bkav Pro	W32.AIDetectMalware	CrowdStrike Falcon	Win/malicious_confidence_100% (W)
CTX	Exe.trojan.flagpro	Cylance	Unsafe
DeepInstinct	MALICIOUS	DrWeb	BackDoor.Flagpro.1
Elastic	Malicious (high Confidence)	Emsisoft	Gen:Variant.Fragtor.370965 (B)
eScan	Gen:Variant.Fragtor.370965	ESET-NOD32	A Variant Of Win32/FlagPro.B
Fortinet	W32/Generic.BFRL!tr	GData	Gen:Variant.Fragtor.370965
Google	Detected	Gridinsoft (no cloud)	Trojan.Win32.Agent.oa!s1
Ikarus	Trojan.Win32.Flagpro	Jiangmin	Trojan.Generic.gidky
K7AntiVirus	Trojan (0058ca8e1)	K7GW	Trojan (0058ca8e1)
Kaspersky	HEUR:Backdoor.Win32.Flagpro.gen	Lionic	Trojan.Win32.Flagpro.m!c
Malwarebytes	Malware.AI.4161576841	MaxSecure	Trojan.Malware.7164915.susgen


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