

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.

The screenshot shows the VirusTotal interface for a file with hash 54e6e47eb04634d3e87fd7787e2136ccfbcc80adc34f246a12c93bab527f6b. The file is identified as bfwc.exe, 430.00 KB, and was analyzed 36 minutes ago. A red circle with the number 58 indicates that 58 out of 71 security vendors flagged this file as malicious. The file is categorized as a Trojan (trojan.flagpro/fragtor) and is associated with several threat labels including flagpro, fragtor, and bbf. The security vendors' analysis table shows detections from AhnLab-V3, AliCloud, Antiy-AVL, Arctic Wolf, and others, all identifying the file as malicious.

54e6e47eb04634d3e87fd7787e2136ccfbcc80adc34f246a12c93bab527f6b

58 / 71
Community Score -258

58/71 security vendors flagged this file as malicious

Reanalyze Similar More

54e6e47eb04634d3e87fd7787e2136ccfbcc80adc34f246a12c93bab527f6b
bfwc.exe
Size 430.00 KB
Last Analysis Date 36 minutes ago
EXE

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

DETECTION DETAILS RELATIONS 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 bbf

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/APT1/Win32.Blacktech	Arcabit	Trojan.Fragtor.D5A915
Arctic Wolf	Unsafe	Avast	Win32:Malware-gen
BK	Win32:Malware-gen	Avira (opencloud)	Win32:Malware-gen

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:
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a1
2cf93bab527f6b