VirusTotal

Analyse suspicious files, domains, IPs and URLs to detect malware and other breaches, automatically share them with the security community.

URL: https://www.virustotal.com/

Analyze the report

1. **Detection:** This tab provides a list of third-party security vendors and their detection verdicts on an artifact. Detection verdicts include: malicious, suspicious, unsafe, and others. Notice how many security vendors have reported this hash as malicious and how many have not.
2. **Details**: This tab provides additional information extracted from a static analysis of the IoC. Notice the additional hashes associated with this malware like MD5, SHA-1, and more.
3. **Relations**: This tab contains information about the network connections this malware has made with URLs, domain names, and IP addresses. The **Detections** column indicates how many vendors have flagged the URL or IP address as malicious.
4. **Behavior**: This tab contains information related to the observed activity and behaviors of an artifact after executing it in a controlled environment, such as a sandboxed environment. A sandboxed environment is an isolated environment that allows a file to be executed and observed by analysts and researchers. Information about the malware's behavioral patterns is provided through sandbox reports. Sandbox reports include information about the specific actions the file takes when it's executed in a sandboxed environment, such as registry and file system actions, processes, and more. Notice the different types of tactics and techniques used by this malware and the files it created.

> *“* ***Pro tip****: Sandbox reports are useful in understanding the behavior of a file, but they might contain information that is not relevant to the analysis of the file. By default, VirusTotal shows all sandbox reports in the Behavior tab. You can select individual sandbox reports to view. This is helpful because you can view the similarities and differences between reports so that it's easier to identify which behaviors are likely to be associated with the file.*

Determine whether the file is malicious

- The **Vendors' ratio** is the metric widget displayed at the top of the report. This number represents how many security vendors have flagged the file as malicious over all. A file with a high number of vendor flags is more likely to be malicious.

- The **Community Score** is based on the collective inputs of the VirusTotal community. The community score is located below the vendor's ratio and can be displayed by hovering your cursor over the red **X**. A file with a negative community score is more likely to be malicious.
- Under the **Detection** tab, the **Security vendors' analysis** section provides a list of detections for this file made by security vendors, like antivirus tools. Vendors who *have not* identified the file as malicious are marked with a checkmark. Vendors who *have* flagged the file as malicious are marked with an exclamation mark. Files that are flagged as malicious might also include the name of the malware that was detected and other additional details about the file. This section provides insights into a file's potential maliciousness.

Review these three sections to determine if there is a consistent assessment of the file's potential maliciousness such as: a high vendors' ratio, a negative community score, and malware detections in the security vendors' analysis section.

Screenshots

61 / 74

Community Score -209

61/74 security vendors flagged this file as malicious

Reanalyze Similar More

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

bfsvc.exe

Size 430.00 KB | Last Analysis Date 14 hours ago | EXE

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

DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 28+

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	Cybereason	Malicious.e29b71

61 / 74

Community Score -209

61/74 security vendors flagged this file as malicious

Reanalyze Similar More

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

bfsvc.exe

Size 430.00 KB | Last Analysis Date 14 hours ago | EXE

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

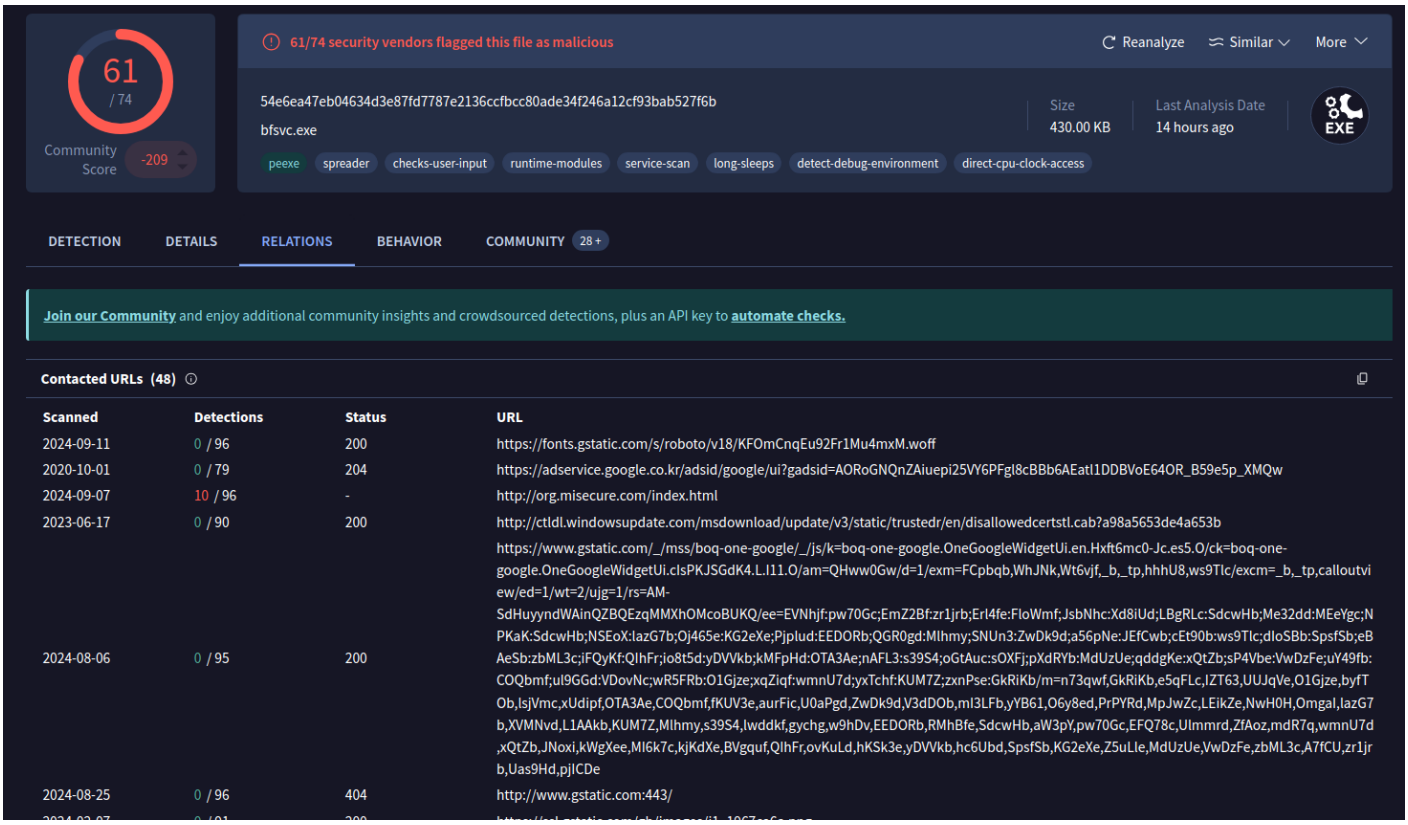
DETECTION DETAILS RELATIONS BEHAVIOR COMMUNITY 28+

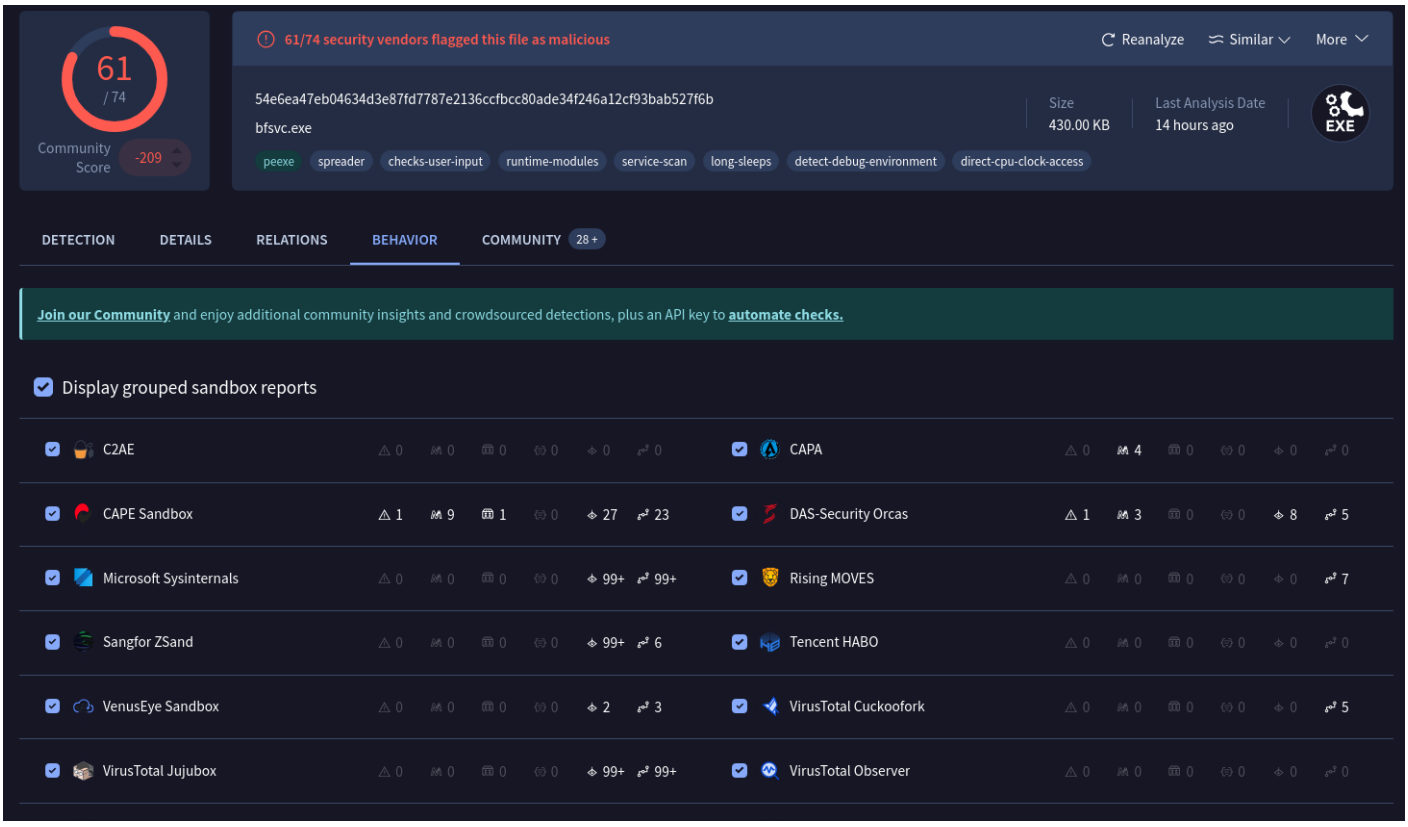
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

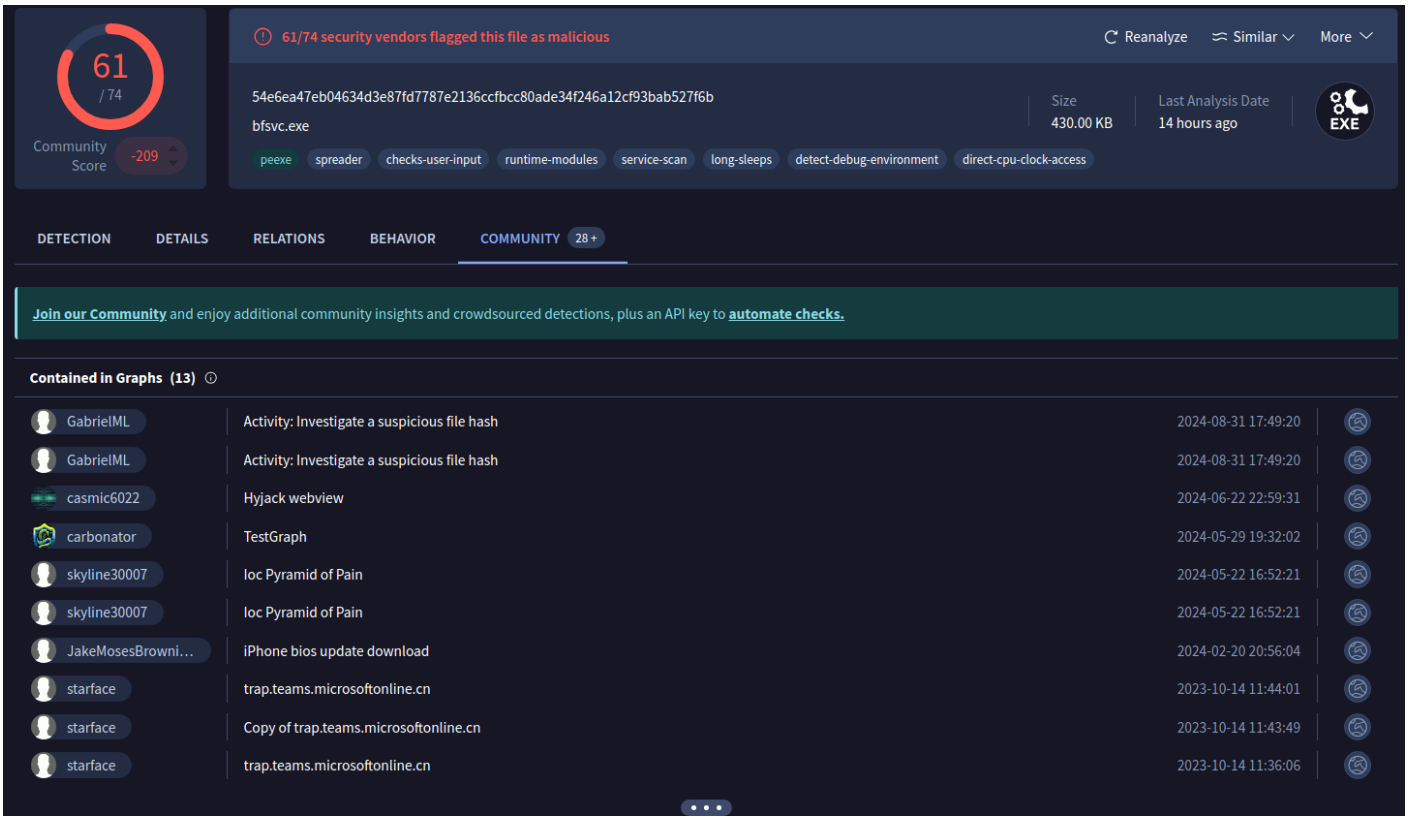
Basic properties

MD5	287d612e29b71c90aa54947313810a25
SHA-1	8f35a9e70dbec8f1904991773f394cd4f9a07f5e
SHA-256	54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
Vhash	045056655d15551023z12z577z305bz2fz
Authentihash	019439328ea87e4559b653ad7df933d20623bdd00d3793abc7ff35e57db24853
Imphash	a59ed1599cc2f8311b215c83c51a2cc4
Rich PE header hash	1f4064adca28866f7447aaf031074807
SSDEEP	6144:CdaRD0n4URr6zIKgDCVh84DLn5X3lWiDSVS1dGSLaYWis:XRonpRroIKgDCY4DLVIW3UiSL4R
TLSH	T13594AD933541C371CA177D7695789AAD4B3F8D3816BAB987B3B83B8F5C303918636902
File type	Win32 EXE executable windows win32 pe peexe
Magic	PE32 executable (GUI) Intel 80386, for MS Windows
TrID	Win32 Executable MS Visual C++ (generic) (47.3%) | Win64 Executable (generic) (15.9%) | Win32 Dynamic Link Library (generic) (9.9%) | Win16 NE executable (generic) (7…
DetectItEasy	PE32 | Compiler: EP:Microsoft Visual C/C++ (2008-2010) [EXE32] | Compiler: Microsoft Visual C/C++ (15.00.21022) [LTCG/C++] | Linker: Microsoft Linker (9.00.21022) | To…
Magika	PEBIN
File size	430.00 KB (440320 bytes)

History


61
/ 74
Community Score
-209
61/74 security vendors flagged this file as malicious
Reanalyze
Similar
More
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
bfsvc.exe
peexe
spreader
checks-user-input
runtime-modules
service-scan
long-sleeps
detect-debug-environment
direct-cpu-clock-access
Size
430.00 KB
Last Analysis Date
14 hours ago
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 28+
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Contacted URLs (48)
Scanned
Detections
Status
URL
2024-09-11
0 / 96
200
https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxM.woff
2020-10-01
0 / 79
204
https://adservice.google.co.kr/adsid/google/ui?gadsid=AORoGNQnZAiuepi25VY6PFgl8cBBb6AEatl1DDBVoE64OR_B59e5p_XMQw
2024-09-07
10 / 96
-
http://org.misecure.com/index.html
2023-06-17
0 / 90
200
http://ctldl.windowsupdate.com/msdownload/update/v3/static/trustedr/en/disallowedcertstl.cab?a98a5653de4a653b
2024-08-06
0 / 95
200
https://www.gstatic.com/_/mss/boq-one-google/_/js/k=boq-one-google.OneGoogleWidgetUi.en.Hxft6mc0-Jc.es5.O/ck=boq-one-google.OneGoogleWidgetUi.clsPKJSGdK4.L.I11.O/am=QHww0Gw/d=1/exm=FCpbqb,WhJNk,Wt6vjf,_b,_tp,hhhU8,ws9Tlc/excm=_b,_tp,calloutview/ed=1/wt=2/ujg=1/rs=AM-SdHuyyndWAinQZBQEzqMMXhOMcoBUKQ/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEeYgc;NPKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:MIhmy;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;uY49fb:COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:wmnU7d;yxTchf:KUM7Z;zxnPse:GkRiKb/m=n73qwf,GkRiKb,e5qFLc,IZT63,UUJqVe,O1Gjze,byfTOb,lsjVmc,xUdipf,OTA3Ae,COQbmf,fKUV3e,aurFic,U0aPgd,ZwDk9d,V3dDOb,mI3LFb,yYB61,O6y8ed,PrPYRd,MpJwZc,LEikZe,NwH0H,Omgal,lazG7b,XVMNvd,L1AAkb,KUM7Z,MIhmy,s39S4,lwddkf,gychg,w9hDv,EEDORb,RMhBfe,SdcwHb,aW3pY,pw70Gc,EFQ78c,Ulmmrd,ZfAoz,mdR7q,wmnU7d,xQtZb,JNoxi,kWgXee,MI6k7c,kjKdXe,BVgquf,QIhFr,ovKuLd,hKSk3e,yDVVkb,hc6Ubd,SpsfSb,KG2eXe,Z5uLle,MdUzUe,VwDzFe,zbML3c,A7fCU,zr1jrb,Uas9Hd,pjICDe
2024-08-25
0 / 96
404
http://www.gstatic.com:443/


61
/ 74
Community Score
-209
61/74 security vendors flagged this file as malicious
Reanalyze
Similar
More
54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
bfsvc.exe
peexe
spreader
checks-user-input
runtime-modules
service-scan
long-sleeps
detect-debug-environment
direct-cpu-clock-access
Size
430.00 KB
Last Analysis Date
14 hours ago
EXE
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY 28+
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.
Display grouped sandbox reports
C2AE
CAPA
CAPE Sandbox
DAS-Security Orcas
Microsoft Sysinternals
Rising MOVES
Sangfor ZSand
Tencent HABO
VenusEye Sandbox
VirusTotal Cuckoofork
VirusTotal Jujubox
VirusTotal Observer



Revision #3
Created 14 September 2024 09:52:32 by Admin
Updated 14 September 2024 10:07:00 by Admin