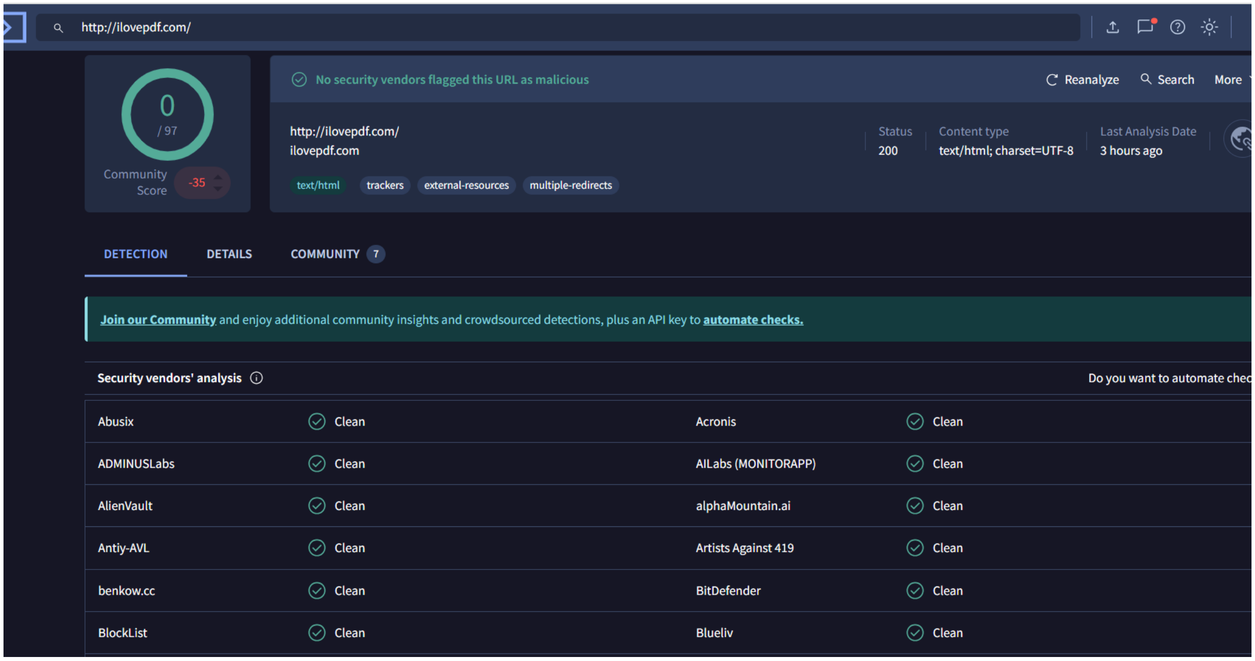
Scanning Hashes/Files using the VirusTotal

First, I'll scan a URL that I commonly use for converting documents, and notice most vendor detections have marked it clean:



http://ilovepdf.com/

0 / 97

Community Score -35

No security vendors flagged this URL as malicious

Reanalyze · Search · More

http://ilovepdf.com/
ilovepdf.com

text/html · trackers · external-resources · multiple-redirects

Status: 200 · Content type: text/html; charset=UTF-8 · Last Analysis Date: 3 hours ago

DETECTION · DETAILS · COMMUNITY 7

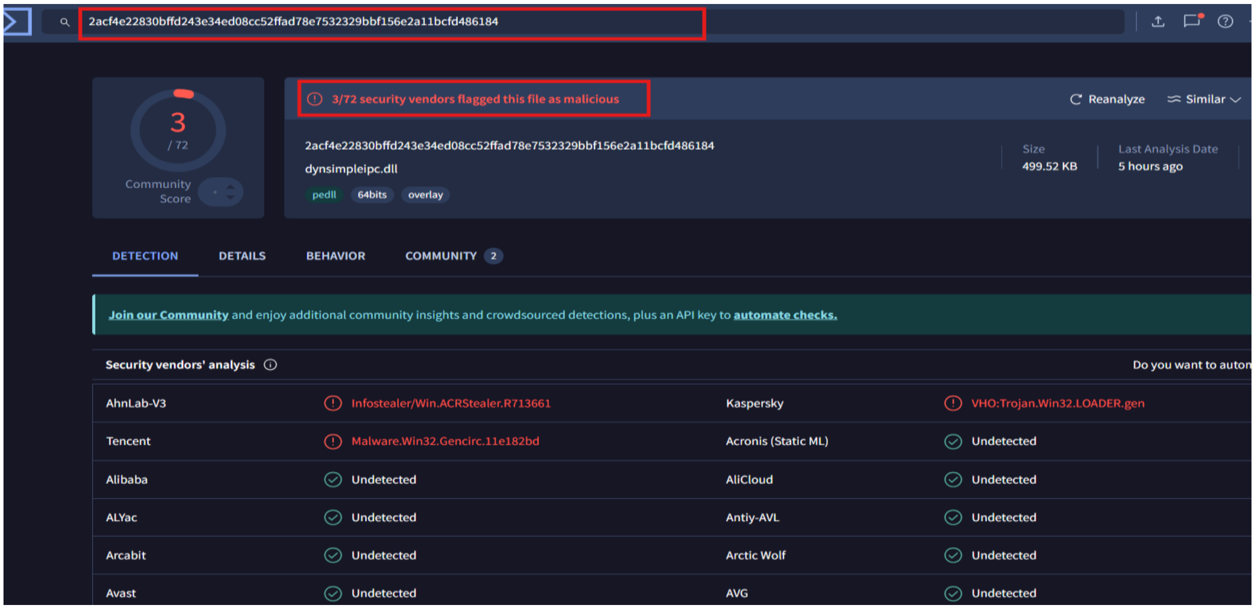
Join our Community and enjoy additional community insights and crowdsourced detections, plus an API key to automate checks.

Security vendors' analysis ⓘ · Do you want to automate chec

Abusix	✓ Clean	Acronis	✓ Clean
ADMINUSLabs	✓ Clean	AILabs (MONITORAPP)	✓ Clean
AlienVault	✓ Clean	alphaMountain.ai	✓ Clean
Antiy-AVL	✓ Clean	Artists Against 419	✓ Clean
benkow.cc	✓ Clean	BitDefender	✓ Clean
BlockList	✓ Clean	Blueliv	✓ Clean

Vendor ratio being 0/97 vendors have identified any suspicious or malicious data on the url.

Now I'll grab a malware sample SHA Hash (from MalwareBazaar) to scan, right away it shows 3 vendors flagged the hash as malicious using trojan malware:



2acf4e22830bffd243e34ed08cc52ffad78e7532329bbf156e2a11bcfd486184

3 / 72

Community Score

3/72 security vendors flagged this file as malicious

Reanalyze · Similar

2acf4e22830bffd243e34ed08cc52ffad78e7532329bbf156e2a11bcfd486184
dynsimpleipc.dll

pedll · 64bits · overlay

Size: 499.52 KB · Last Analysis Date: 5 hours ago

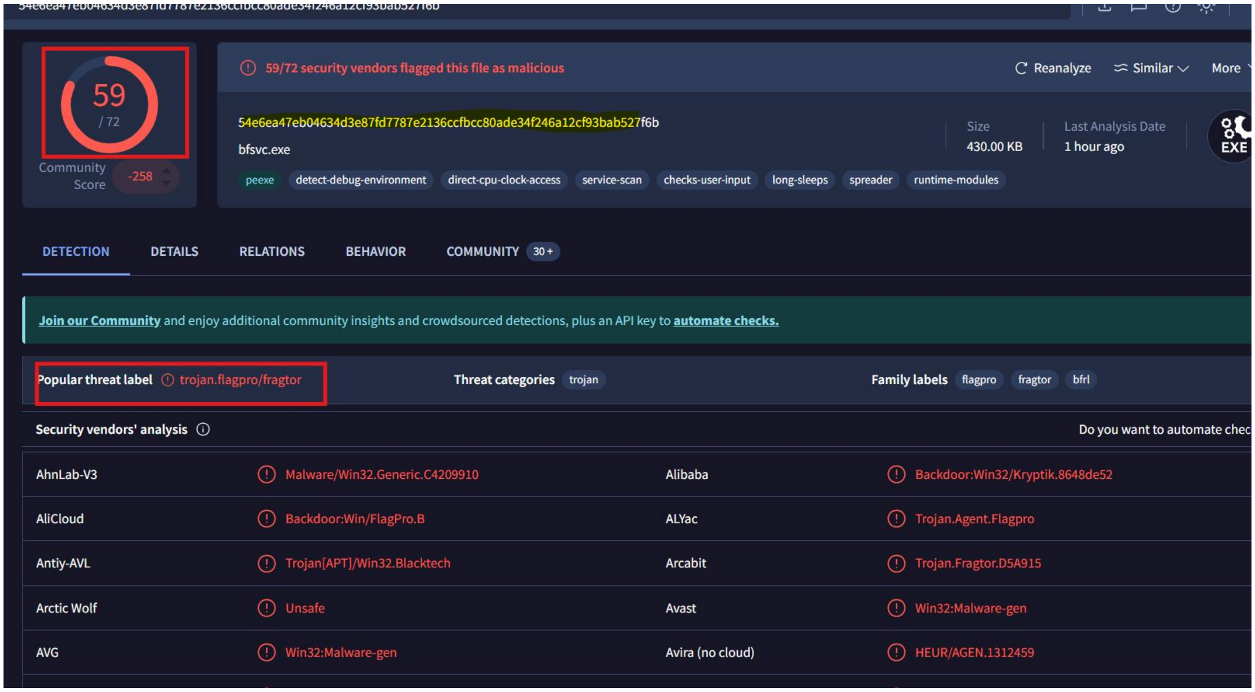
DETECTION · DETAILS · BEHAVIOR · COMMUNITY 2

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

Security vendors' analysis ⓘ · Do you want to auton

AhnLab-V3	ⓘ Infostealer/Win.ACRStealer.R713661	Kaspersky	ⓘ VHO:Trojan.Win32.LOADER.gen
Tencent	ⓘ Malware.Win32.Gencirc.11e182bd	Acronis (Static ML)	✓ Undetected
Alibaba	✓ Undetected	AliCloud	✓ Undetected
ALYac	✓ Undetected	Antiy-AVL	✓ Undetected
Arcabit	✓ Undetected	Arctic Wolf	✓ Undetected
Avast	✓ Undetected	AVG	✓ Undetected

Here’s another hash example, 59 vendors marked malicious, known as the malware “flagpro”:



59/72 security vendors flagged this file as malicious

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

bfsvc.exe

Size 430.00 KB

Last Analysis Date 1 hour ago

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

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

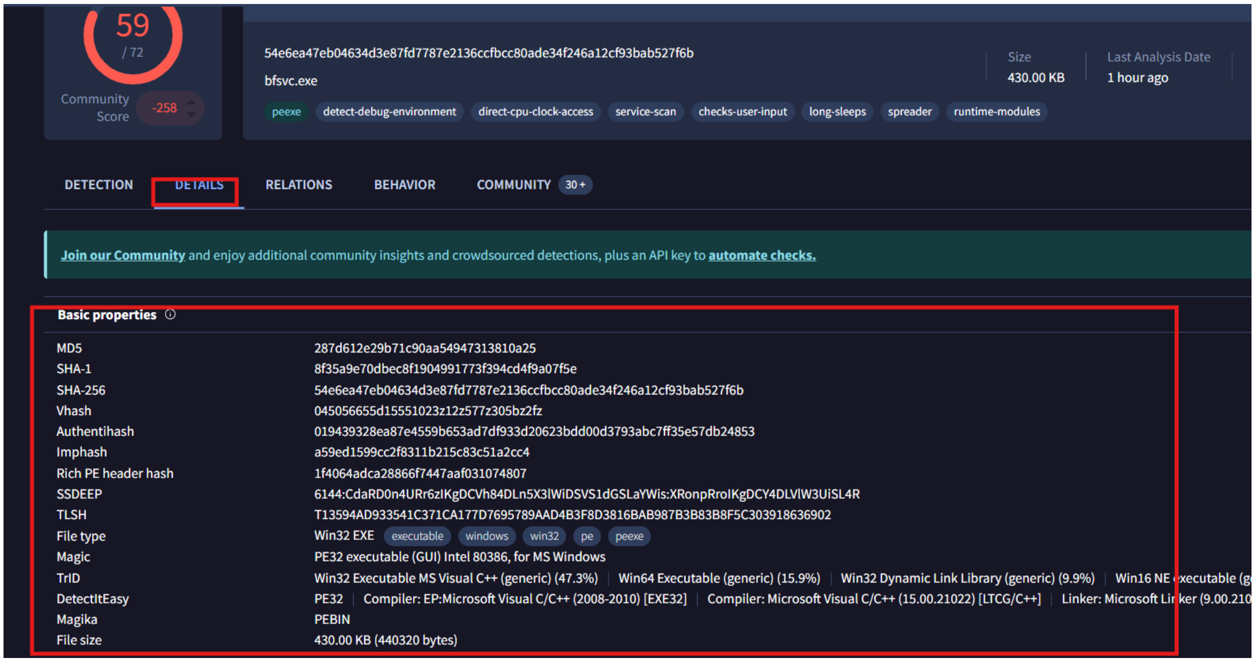
Family labels flagpro fragtor bfrl

Security vendors' analysis

Do you want to automate chec

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

By drilling into the Details, Relations, & Behavior tab, I’m able to see more details about the file like hash values, IPs, domains, etc.:



54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

bfsvc.exe

Size 430.00 KB

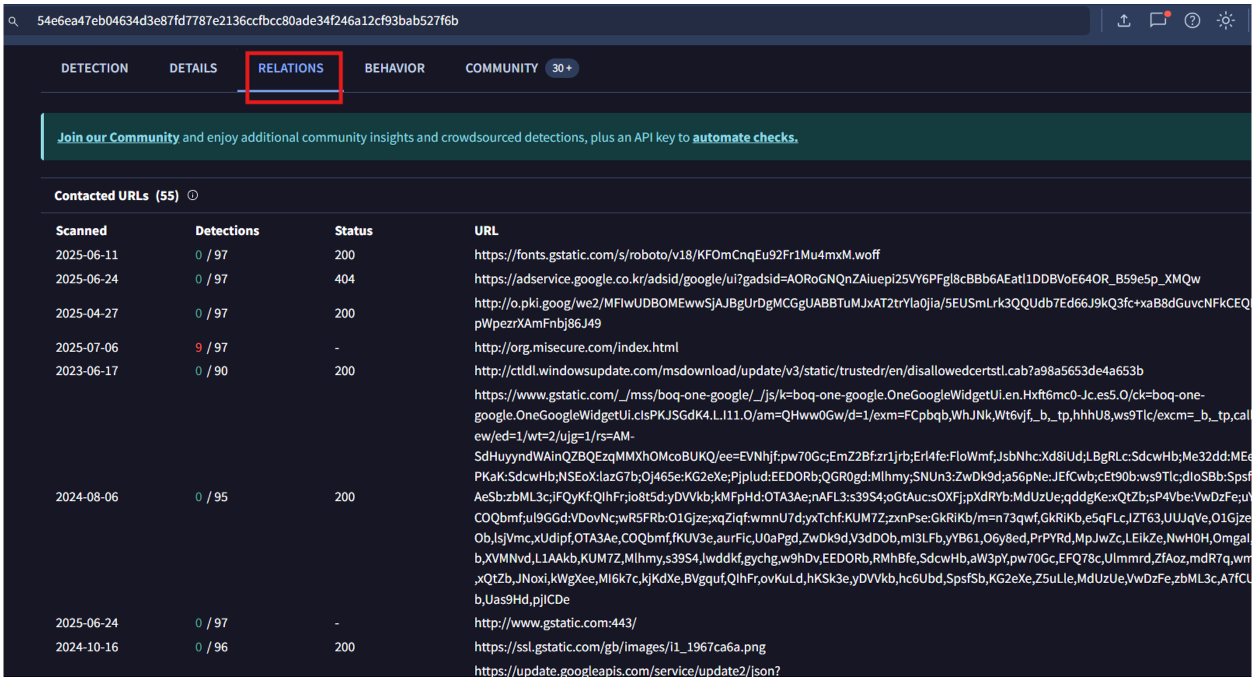
Last Analysis Date 1 hour ago

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

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:XRonpRroIKgDCY4DLVlW3UiSL4R
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 (g
DetectItEasy	PE32 | Compiler: EP:Microsoft Visual C/C++ (2008-2010) [EXE32] | Compiler: Microsoft Visual C/C++ (15.00.21022) [LTCG/C++] | Linker: Microsoft Linker (9.00.210
Magika	PEBIN
File size	430.00 KB (440320 bytes)

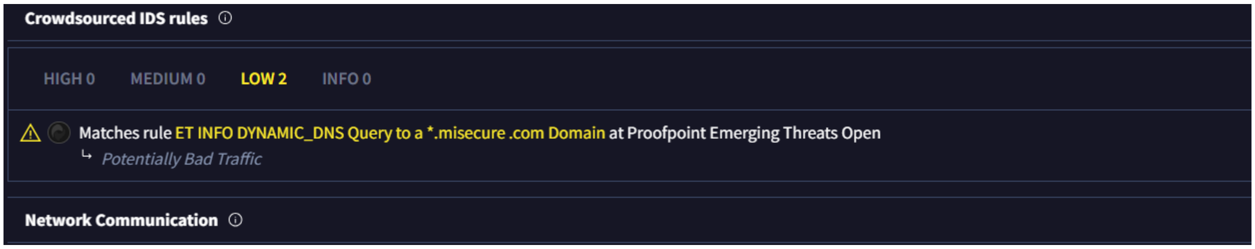


54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

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

Contacted URLs (55)

Scanned	Detections	Status	URL
2025-06-11	0 / 97	200	https://fonts.gstatic.com/s/roboto/v18/KFOmCnqEu92Fr1Mu4mxM.woff
2025-06-24	0 / 97	404	https://adservice.google.co.kr/adsid/google/ui?gadsid=AORoGNQnZAiuepi25VY6PFgl8cBBb6AEatl1DDBVoE64OR_B59e5p_XMQw
2025-04-27	0 / 97	200	http://o.pki.goog/we2/MFIwUDBOMEwwSjAJBgUrDgMCGgUABBTuMJxAT2trYla0jia/5EUSmLrk3QQUdb7Ed66J9kQ3fc+xaB8dGuvcNFkCEQ pWpezrXAmFnbj86J49
2025-07-06	9 / 97	-	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.cIsPKJSGdK4.L.I11.O/am=QHww0Gw/d=1/exm=FCpbqb,WhJNk,Wt6vjf,_b,_tp,hhhU8,ws9Tlc/excm=_b,_tp,call ew/ed=1/wt=2/ujg=1/rs=AM-SdHuyyndWAinQZBQEzqMMXhOMcoBUKQ/ee=EVNhjf:pw70Gc;EmZ2Bf:zr1jrb;Erl4fe:FloWmf;JsbNhc:Xd8iUd;LBgRLc:SdcwHb;Me32dd:MEe PKaK:SdcwHb;NSEoX:lazG7b;Oj465e:KG2eXe;Pjplud:EEDORb;QGR0gd:Mlhmy;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:Spsf AeSb:zbML3c;iFQyKf:QlhFr;io8t5d:yDVVkb;kMFpHd:OTA3Ae;nAFL3:s39S4;oGtAuc:sOXFj;pXdRYb:MdUzUe;qddgKe:xQtZb;sP4Vbe:VwDzFe;uY COQbmf;ul9GGd:VDovNc;wR5FRb:O1Gjze;xqZiqf:wmnU7d;yxTchf:KUM7Z;zxnPse:GkRiKb/m=n73qwf,GkRiKb,e5qFLc,IZT63,UUJqVe,O1Gjze Ob,lsjVmc,xUdipf,OTA3Ae,COQbmf,fKUV3e,aurFic,U0aPgd,ZwDk9d,V3dDOb,mI3LFb,yYB61,O6y8ed,PrPYRd,MpJwZc,LEikZe,NwH0H,OmgaI, b,XVMNvd,L1AAkb,KUM7Z,Mlhmy,s39S4,lwddkf,gychg,w9hDv,EEDORb,RMhBfe,SdcwHb,aW3pY,pw70Gc,EFQ78c,Ulmmrd,ZfAoz,mdR7q,wm ,xQtZb,JNoxi,kWgXee,MI6k7c,kjKdXe,BVgquf,QlhFr,ovKuLd,hKSk3e,yDVVkb,hc6Ubd,SpsfSb,KG2eXe,Z5uLle,MdUzUe,VwDzFe,zbML3c,A7fCU b,Uas9Hd,pjICDe
2025-06-24	0 / 97	-	http://www.gstatic.com:443/
2024-10-16	0 / 96	200	https://ssl.gstatic.com/gb/images/i1_1967ca6a.png
			https://update.googleapis.com/service/update2/json?



Crowdsourced IDS rules

⚠ Matches rule ET INFO DYNAMIC_DNS Query to a *.misecure .com Domain at Proofpoint Emerging Threats Open

↳ *Potentially Bad Traffic*

Network Communication