Investigating a File Hash with Virustotal

Project description

This simulation project puts the performer, **Maheswar Reddy Avula**, into the position of a L1 SOC Analyst for a financial services company. Responsibilities include investigating a file hash to determine if it is harmless or malicious.

Scenario:

An alert is generated regarding a suspicious file on an employee's workstation. The 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.

The **SHA256 filehash** is determined to be:

54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b

Enter the file hash into virustotal

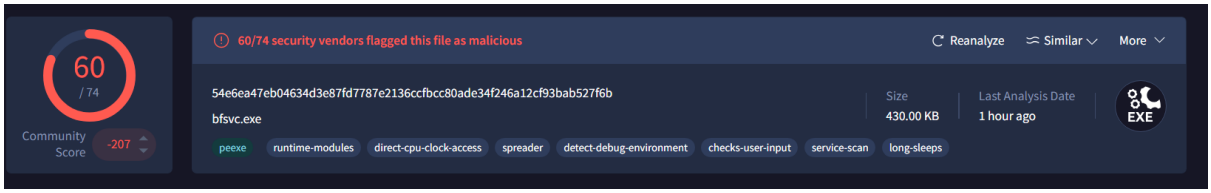
Direction: The analyst must submit the hash into Virustotal to investigate it.

The filehash is entered into the Virustotal website search as follows:

Analyze Virustotal report

Direction: The analyst must analyze the report generated by Virustotal.

The report is generated and the overview is observed.



Next, the following tabs are explained:

1. **Detection:**

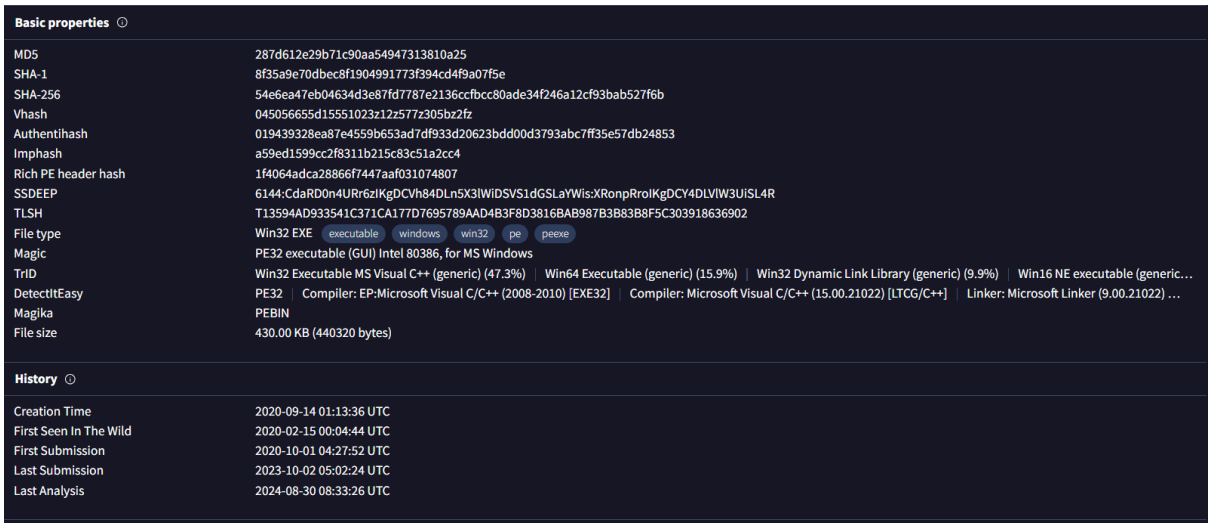
Popular threat label	trojan.flagpro/fragtor	Threat categories	trojan	Family labels	flagpro, fragtor, busyice

Security vendors' analysis — Do you want to automate checks?

AhnLab-V3	Malware/Win32.Generic.C4209910	Alibaba	Backdoor:Win32/Kryptik.8648de52
ALYac	Trojan.Agent.Flagpro	Arcabit	Trojan.Fragtor.D5A915
Avast	Win32:Malware-gen	AVG	Win32:Malware-gen
Avira (no cloud)	HEUR/AGEN.1312459	BitDefender	Gen:Variant.Fragtor.370965
BitDefenderTheta	Gen:NN.ZexaF.36812.Au0@a0!5WTfi	Bkav Pro	W32.AIDetectMalware
CrowdStrike Falcon	Win/malicious_confidence_100% (W)	Cybereason	Malicious.e29b71
Cylance	Unsafe	Cynet	Malicious (score: 99)
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

It is observed that most security vendors have flagged this file as malicious.

2. Details



Basic properties

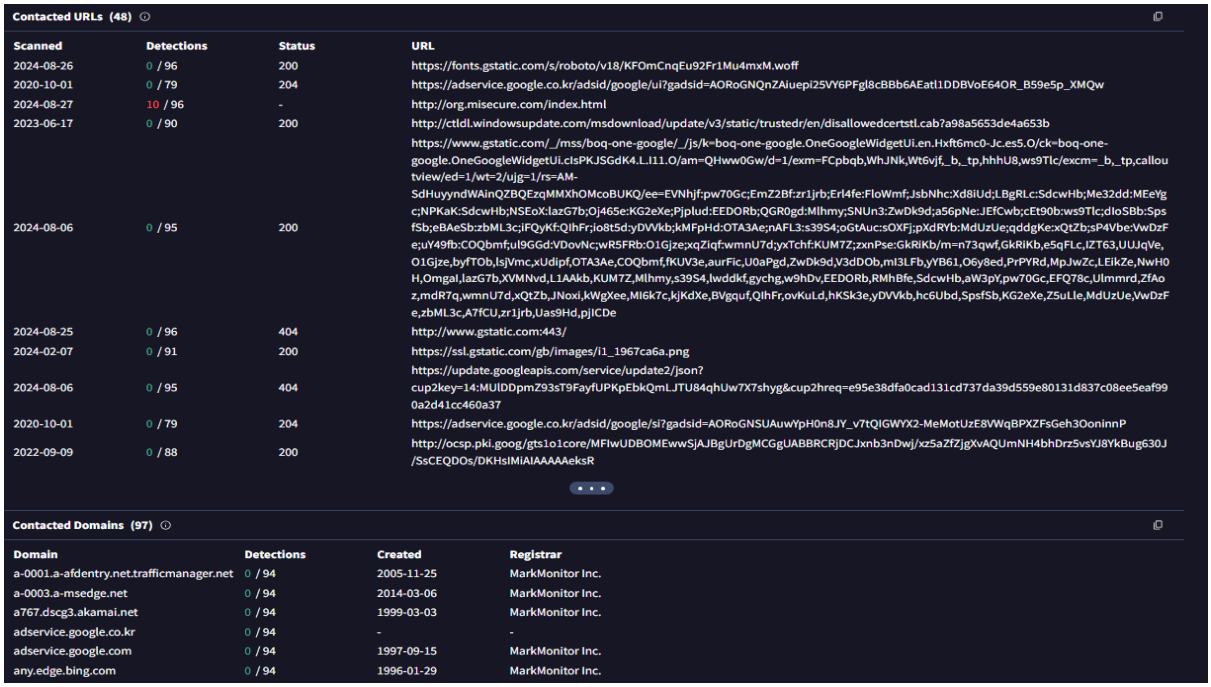
MD5	287d612e29b71c90aa54947313810a25
SHA-1	8f35a9e70dbec8f1904991773f394cd4f9a07f5e
SHA-256	54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b
Vhash	045056655d15551023z12z577z305bz2fz
Authentihash	019439328ea87e4559b653ad7df933d20623bdd00d3793abc7ff35e57db24853
Imphash	a59ed1599cc2f8311b215c83c51a2cc4
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 (generic…
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) …
Magika	PEBIN
File size	430.00 KB (440320 bytes)

History

Creation Time	2020-09-14 01:13:36 UTC
First Seen In The Wild	2020-02-15 00:04:44 UTC
First Submission	2020-10-01 04:27:52 UTC
Last Submission	2023-10-02 05:02:24 UTC
Last Analysis	2024-08-30 08:33:26 UTC

Additional details like associated hashes, history etc. are observed.

2. Relations



Contacted URLs (48)

Scanned	Detections	Status	URL
2024-08-26	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
2024-08-27	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.cIsPKJSGdK4.L.I11.O/am=QHww0Gw/d=1/exm=FCpbqb,WhJNk,Wt6vjf,_b,_tp,hhhU8,ws9Tlc/excm=_b,_tp,callouttview/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:Mlhmy;SNUn3:ZwDk9d;a56pNe:JEfCwb;cEt90b:ws9Tlc;dIoSBb:SpsfSb;eBAeSb:zbML3c;iFQyKf:QIhFr;io8t5d:yDVkb;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,ml3LFb,yYB61,O6y8ed,PrPYRd,MpJwZc,LEikZe,NwH0H,Omgal,lazG7b,XVMNvd,L1AAkb,KUM7Z,Mlhmy,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,Z5uLIe,MdUzUe,VwDzFe,zbML3c,A7fCU,zr1jrb,Uas9Hd,pjICDe
2024-08-25	0 / 96	404	http://www.gstatic.com:443/
2024-02-07	0 / 91	200	https://ssl.gstatic.com/gb/images/i1_1967ca6a.png
2024-08-06	0 / 95	404	https://update.googleapis.com/service/update2/json?cup2key=14:MUlDDpmZ93sT9FayfUPKpEbkQmLJTU84qhUw7X7shyg&cup2hreq=e95e38dfa0cad131cd737da39d559e80131d837c08ee5eaf990a2d41cc460a37
2020-10-01	0 / 79	204	https://adservice.google.co.kr/adsid/google/si?gadsid=AORoGNSUAuwYpH0n8JY_v7tQIGWYX2-MeMotUzE8VWqBPXZFsGeh3OoninnP
2022-09-09	0 / 88	200	http://ocsp.pki.goog/gts1o1core/MFIwUDBOMEwwSjAJBgUrDgMCGgUABBRCRjDCJxnb3nDwj/xz5aZfZjgXvAQUmNH4bhDrz5vsYJ8YkBug630J/SsCEQDOs/DKHsIMiAIAAAAAeksR

Contacted Domains (97)

Domain	Detections	Created	Registrar
a-0001.a-afdentry.net.trafficmanager.net	0 / 94	2005-11-25	MarkMonitor Inc.
a-0003.a-msedge.net	0 / 94	2014-03-06	MarkMonitor Inc.
a767.dscg3.akamai.net	0 / 94	1999-03-03	MarkMonitor Inc.
adservice.google.co.kr	0 / 94	-	-
adservice.google.com	0 / 94	1997-09-15	MarkMonitor Inc.
any.edge.bing.com	0 / 94	1996-01-29	MarkMonitor Inc.

The network connections this malware has made with URLs, domain names, and IP addresses etc. are observed.

3. Behavior

The file's behavior in multiple sandbox environments is observed and a summary is generated.

Determine whether file is Malicious

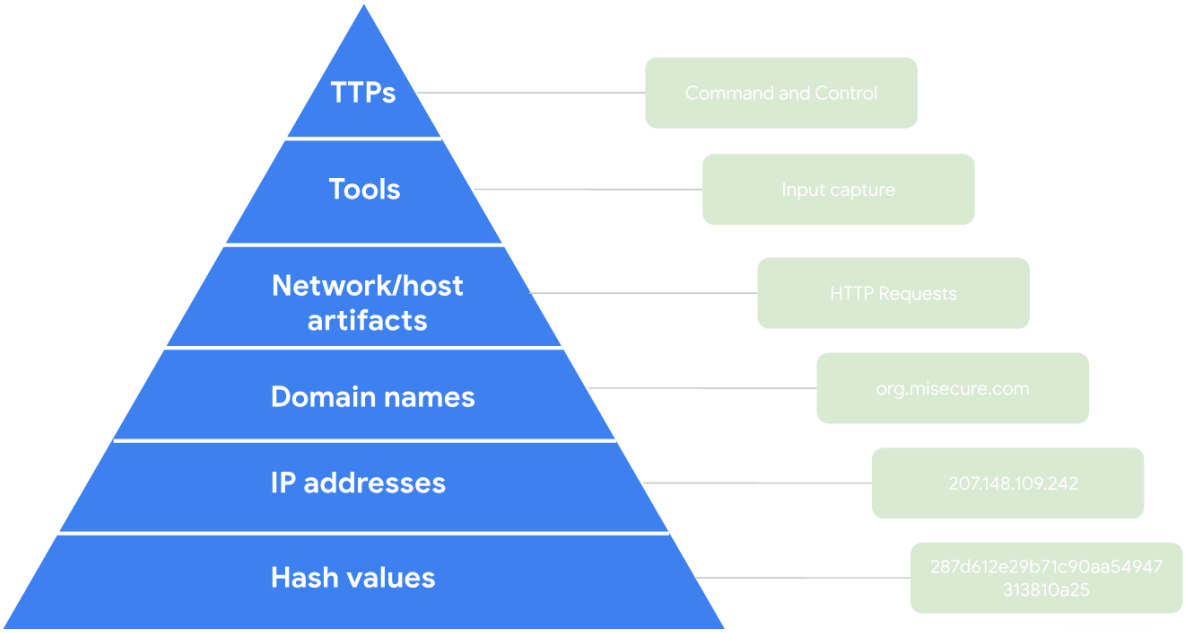
Direction: The analyst must determine if the file is malicious or hamless.

Based on the Virustotal summary and all the tabs giving more details, it is concluded that the file is definitely malicious by nature. The investigation reveals that the file hash is known as malware Flagpro, commonly used by Blacktech, an advance threat actor.

Draft a Pyramid of Pain for this malware

Direction: The analyst must complete the investigation by drafting a Pyramid of Pain diagram for the malware detected.

Based on the investigation, the following Pyramid of Pain diagram is made:



Links for reference:

- https://www.virustotal.com/gui/file/54e6ea47eb04634d3e87fd7787e2136ccfbcc80ade34f246a12cf93bab527f6b/detection

Summary

The file hash was submitted to Virustotal and investigated thoroughly. The file was determined to be malicious. All tasks were successfully completed in accordance with the directions given by the organization.