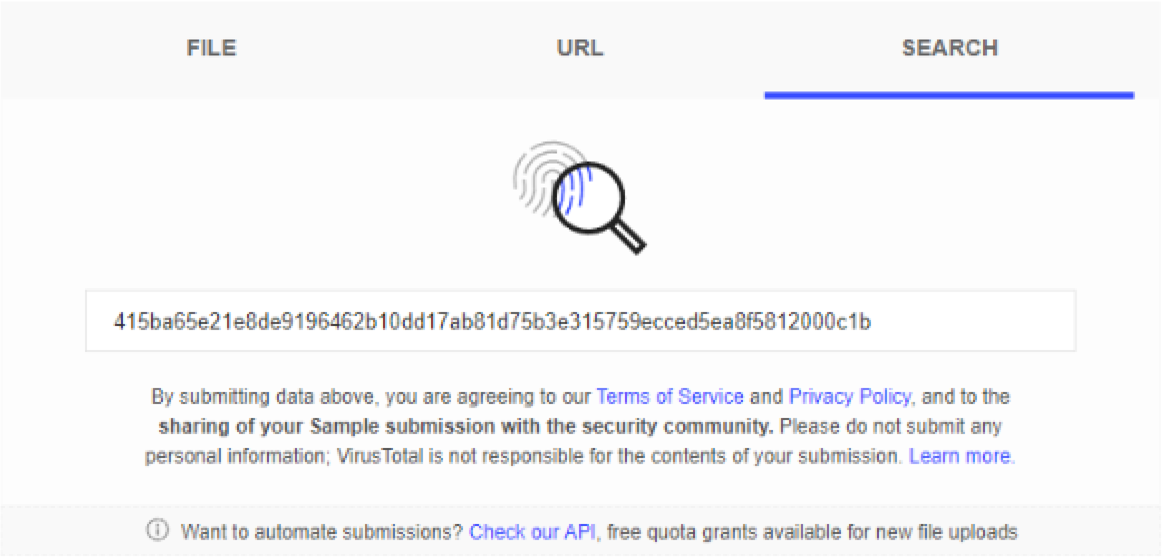
Searching for IOCs

By: Ryan Stewart

Searching for IOC

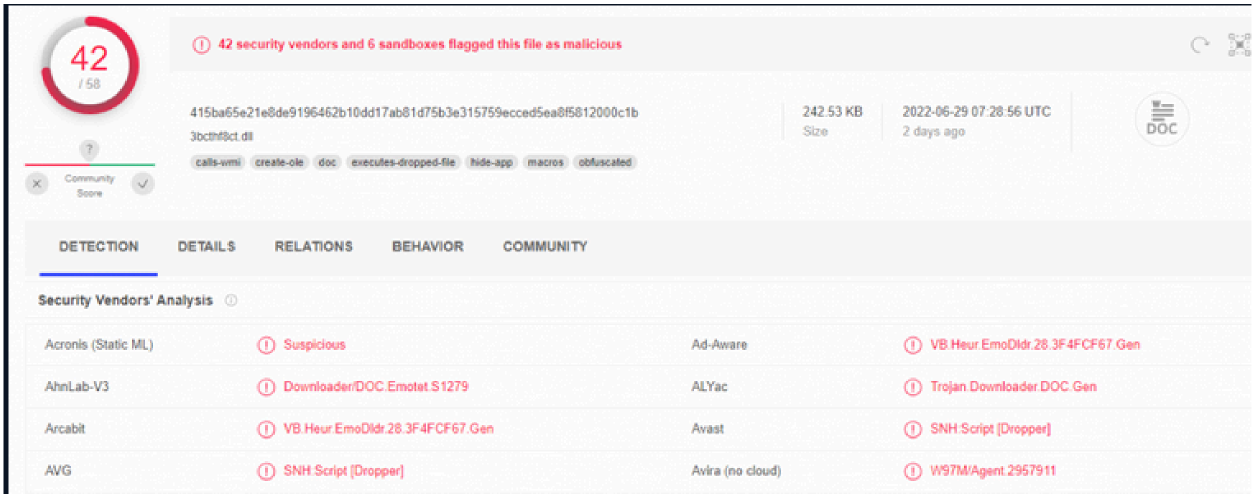
Throughout an investigation, you may come across various IOCs (Indicators of Compromise). To gather more information about these IOCs, you can utilize the "**Search**" section on VirusTotal. For instance, by entering the hash value of a suspicious file in the search bar, you can access historical analysis results and other relevant data, if available.



415ba65e21e8de9196462b10dd17ab81d75b3e315759ecced5ea8f5812000c1b

By submitting data above, you are agreeing to our Terms of Service and Privacy Policy, and to the **sharing of your Sample submission with the security community.** Please do not submit any personal information; VirusTotal is not responsible for the contents of your submission. Learn more.

ⓘ Want to automate submissions? Check our API, free quota grants available for new file uploads



42 security vendors and 6 sandboxes flagged this file as malicious

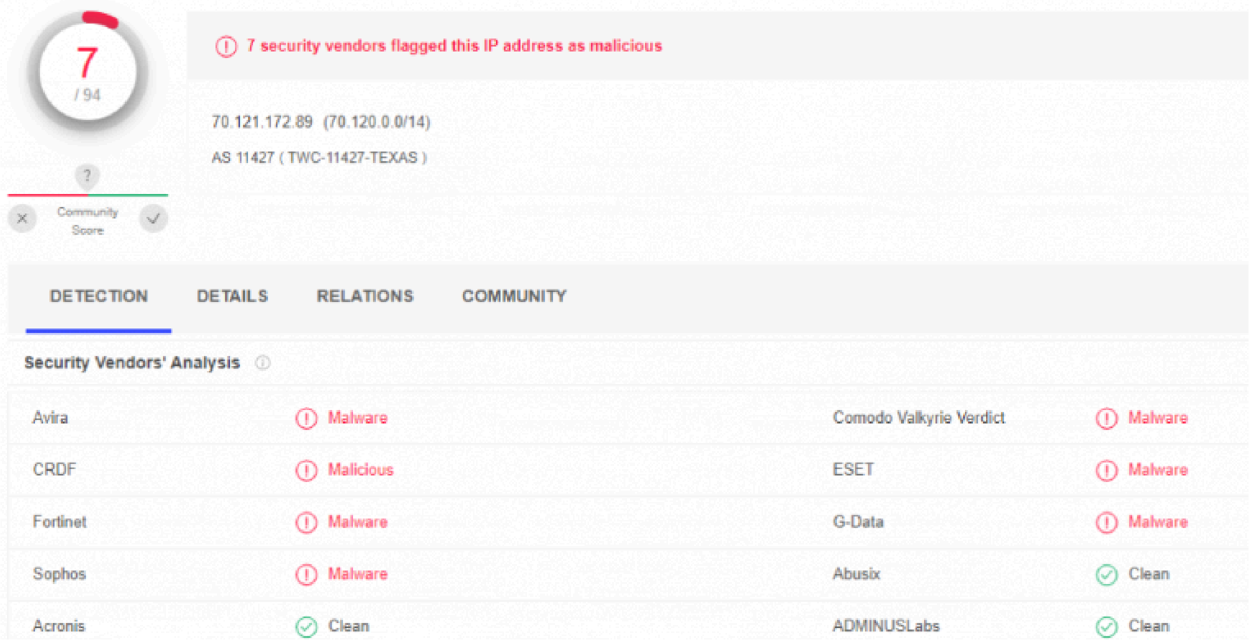
415ba65e21e8de9196462b10dd17ab81d75b3e315759ecced5ea8f5812000c1b
3bcthf8ct.dll

242.53 KB
Size

2022-06-29 07:28:56 UTC
2 days ago

Security Vendors' Analysis

Acronis (Static ML)	Suspicious	Ad-Aware	VB.Heur.EmoDldr.28.3F4FCF67.Gen
AhnLab-V3	Downloader/DOC.Emotet.S1279	ALYac	Trojan.Downloader.DOC.Gen
Arcabit	VB.Heur.EmoDldr.28.3F4FCF67.Gen	Avast	SNH:Script [Dropper]
AVG	SNH:Script [Dropper]	Avira (no cloud)	W97M/Agent.2957911



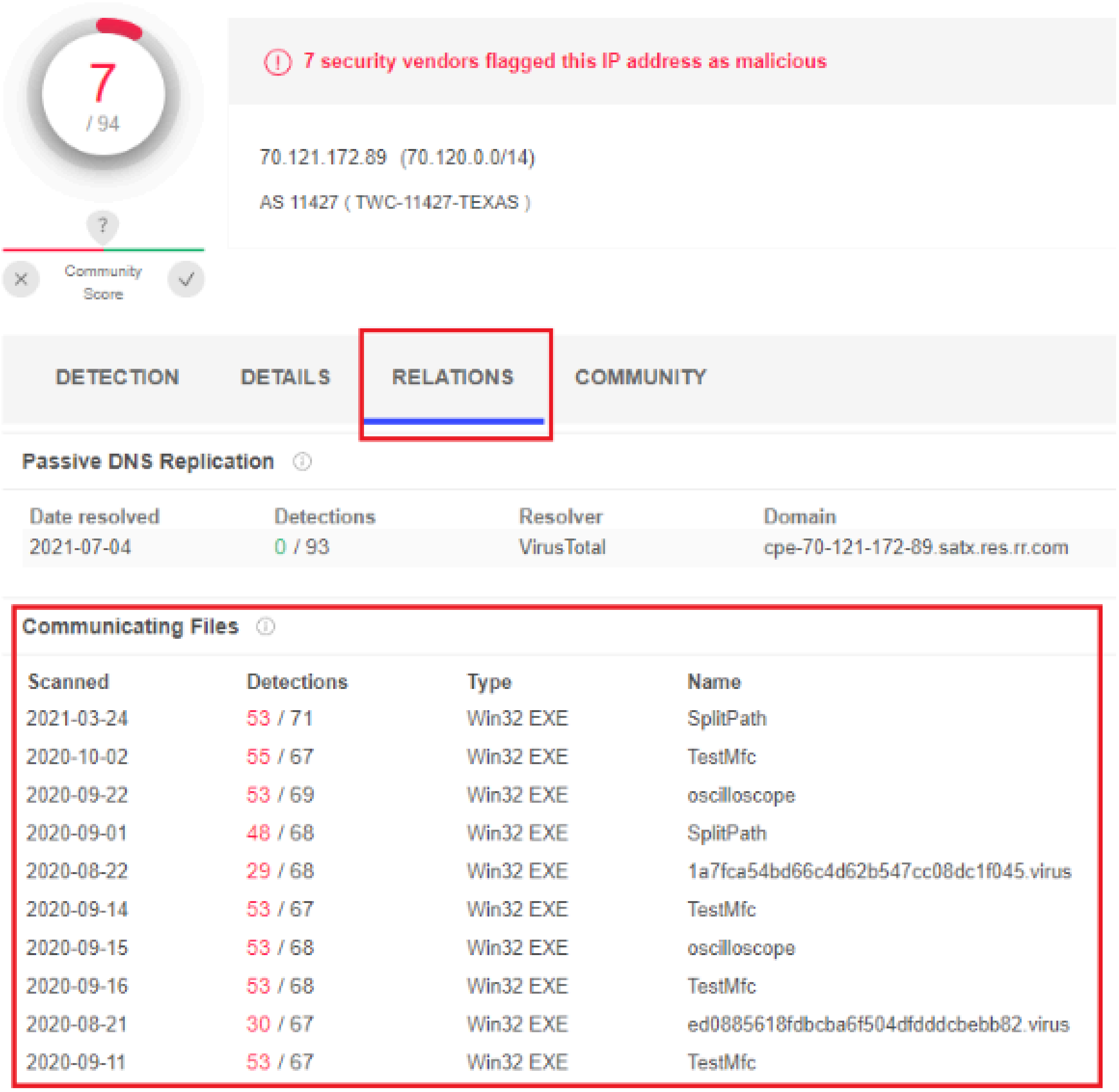
7 security vendors flagged this IP address as malicious

70.121.172.89 (70.120.0.0/14)
AS 11427 (TWC-11427-TEXAS)

Security Vendors' Analysis

Avira	Malware	Comodo Valkyrie Verdict	Malware
CRDF	Malicious	ESET	Malware
Fortinet	Malware	G-Data	Malware
Sophos	Malware	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean

When we uploaded a file, we could see the IP addresses that the malware was connecting to in the "**Relations**" tab. This is also true for the opposite. By searching the IP address, you can find the files related to the IP address in the "**Relations**" tab. We can get more ideas by looking at the scores of the files. If we look at the image below, we can understand that the IP address we are looking for is related to files such as “**SplitPath**”, and “**TestMfc**”.



ⓘ 7 security vendors flagged this IP address as malicious

70.121.172.89 (70.120.0.0/14)

AS 11427 (TWC-11427-TEXAS)

Passive DNS Replication

Date resolved	Detections	Resolver	Domain
2021-07-04	0 / 93	VirusTotal	cpe-70-121-172-89.satx.res.rr.com

Communicating Files

Scanned	Detections	Type	Name
2021-03-24	53 / 71	Win32 EXE	SplitPath
2020-10-02	55 / 67	Win32 EXE	TestMfc
2020-09-22	53 / 69	Win32 EXE	oscilloscope
2020-09-01	48 / 68	Win32 EXE	SplitPath
2020-08-22	29 / 68	Win32 EXE	1a7fca54bd66c4d62b547cc08dc1f045.virus
2020-09-14	53 / 67	Win32 EXE	TestMfc
2020-09-15	53 / 68	Win32 EXE	oscilloscope
2020-09-16	53 / 68	Win32 EXE	TestMfc
2020-08-21	30 / 67	Win32 EXE	ed0885618fdbcba6f504dfdddcbebb82.virus
2020-09-11	53 / 67	Win32 EXE	TestMfc