

VirusTotal



March 2024
DEEPAK RAWAT

Virus Total

1.Introduction:

1. VirusTotal Overview:

- **VirusTotal** is a comprehensive online service that aggregates and analyzes files, URLs, domains, and IP addresses to detect and identify malicious content.
- It provides a wealth of information by scanning submitted files and URLs using multiple antivirus engines, threat intelligence feeds, and other security tools.
- As a SOC analyst, you'll find it invaluable for threat hunting, incident response, and overall security investigations.

2. Key Features and Benefits:

- **Threat Intelligence Aggregation:** VirusTotal collects data from various sources, making it a one-stop-shop for threat intelligence.
- **File and URL Scanning:** Upload files or submit URLs to check for malware, suspicious behavior, and reputation scores.
- **Crowdsourced Threat Reputation:** Access community-contributed Yara rules, IDS signatures, and other threat indicators.
- **Integration with Cortex XSOAR:**
 - **Cortex XSOAR**, developed by Palo Alto Networks, is a leading Security Orchestration, Automation, and Response (SOAR) platform.
 - Together, VirusTotal and Cortex XSOAR enhance your SOC capabilities.
 - Here's how:
 - **Orchestration:** Create custom threat feeds in Cortex XSOAR and perform live IoC matching.
 - **Early Detection:** Leverage VirusTotal's threat reputation data for files, domains, IPs, and URLs.
 - **Triage Process:** Prioritize SOC alerts based on severity and threat categories.
 - **EDR Integration:** Feed relevant and undetected threats identified with VirusTotal YARA into your EDR platform.
 - **Custom IOC Feeds:** You can even create your own VirusTotal Livehunt rules and integrate them into XSOAR.

Explore the **four XSOAR VirusTotal content packs** to find the right fit for your needs.

While reviewing the alert of a SIEM or other security solution, you may have noticed a suspicious file and want to analyze it. To view the file analysis results of different AV companies, you can upload the file on VirusTotal and find out if AV products detect this file as malicious.

* Please note that uploaded files can be downloaded by premium VirusTotal users. Because of this if you suspect that file may have contains sensitive informations, you shouldn't upload to VirusTotal.



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

FILE

URL

SEARCH

Choose file

42 / 58

Community Score

42 security vendors and 6 sandboxes flagged this file as malicious

415ba65e21e8de9196462b10dd17ab81d75b3e315759ecced5ea8f5812000c1b3bcthf8ct.dll

calls-urmi create-ole doc executes-dropped-file hide-app macros obfuscated

242.53 KB

Size

2022-06-29 07:28:56 UTC

a moment ago

DOC

DETECTION

DETAILS

RELATIONS

BEHAVIOR

COMMUNITY

Security Vendors' Analysis

Acronis (Static ML)	① Suspicious	Ad-Aware	① VB_Heur_EmoDldr.28.3F4FCF67.Gen
AhnLab-V3	① Downloader/DOC.Emotet.S1279	ALYac	① Trojan.Downloader.DOC.Gen
Arcabit	① VB_Heur_EmoDldr.28.3F4FCF67.Gen	Avast	① SNH.Script [Dropper]
AVG	① SNH.Script [Dropper]	Avira (no cloud)	① W97M/Agent.2957911
BitDefender	① VB_Heur_EmoDldr.28.3F4FCF67.Gen	ClamAV	① Doc.Downloader.Generic-9420931-0
Comodo	① Malware@#8qgf69dcj6x9	Cynet	① Malicious (score: 99)
Cyren	① W97M/Downldr.IE.gen/Eldorado	DrWeb	① Exploit.Siggen2.25228
Elastic	① Malicious (High Confidence)	Emsisoft	① Trojan-Downloader.Macro.Generic.AM (A)

<https://www.virustotal.com/gui/file/415ba65e21e8de9196462b10dd17ab81d75b3e315759ecced5ea8f5812000c1b>

In order to interpret the results in more detail, it is necessary to look at various areas. In the image below, it is stated that 42 of 58 security companies have detected this file as malicious.



In the section with tags, there is information about how the file is classified. For example, it was stated that the file we uploaded contains "macro" and was "obfuscated".



Detection:

In the Detection section, you can view the label with which the vendors marked the file as malicious.

DETECTION	DETAILS	RELATIONS	BEHAVIOR	COMMUNITY
Security Vendors' Analysis				
Acronis (Static ML)	① Suspicious		Ad-Aware	① VB.Heur.EmoDldr.28.3F4FCF67.Gen
AhnLab-V3	① Downloader.DOC.Emotet.S1279		ALYac	① Trojan.Downloader.DOC.Gen
Arcabit	① VB.Heur.EmoDldr.28.3F4FCF67.Gen		Avast	① SNH.Script [Dropper]
AVG	① SNH.Script [Dropper]		Avira (no cloud)	① W97M/Agent.2957911
BitDefender	① VB.Heur.EmoDldr.28.3F4FCF67.Gen		ClamAV	① Doc.Downloader.Generic-9420931-0
Comodo	① Malware@#8qgf69dcj6x9		Cynet	① Malicious (score: 99)
Cyren	① W97M/Downldr.IE.gen/Eldorado		DrWeb	① Exploit.Siggen2.25228
Elastic	① Malicious (high Confidence)		Emsisoft	① Trojan-Downloader.Macro.Generic.AM (A)

Details:

Here you can find some basic information about the file and details about its VirusTotal history. For example, the "Basic Properties" area contains file hash information and more.

Basic Properties	
MD5	ac596d282e2f9b1501d66fce5a451f00
SHA-1	44398f4b11de435005b32523ed4d31006a10ab98
SHA-256	415ba65e21e8de9196462b10dd17ab81d75b3e315759ecced5ea8f5812000c1b
Vhash	806de0b58934ed6fca886ea337e6a568
SSDEEP	3072:j6yw1MgpQIBhGVb6esLbTh8YuyDRBFIdGkq+BsyFu+powKvIkIHgIEWPsl/aTyT9GkxqyNpowKE
TLSH	T18E341AE255D3DB7AE503C63B7695EEBC307B8C0028125617A99637EF2D3903C484F69A
File type	MS Word Document
Magic	CDF V2 Document, Little Endian, Os: Windows, Version 6.2, Code page: 1252, Title: Eum., Author: Ambre Meyer, Template: Normal.dotm, Revision Number: 1, Name of Creating Application: Microsoft Office Word, Create Time/Date: Wed Aug 19 11:41:00 2020, Last Saved Time/Date: Wed Aug 19 11:41:00 2020, Number of Pages: 1, Number of Words: 4, Number of Characters: 25, Security: 0
TrID	Microsoft Word document (52.6%)
TrID	Microsoft Word document (old ver.) (33.3%)
TrID	Generic OLE2 / Multistream Compound (14%)
File size	242.53 KB (248346 bytes)

In the "History" field, there are the dates of the first and last analysis of the file in VirusTotal.

History ⓘ

Creation Time	2020-08-20 11:41:00 UTC
First Seen In The Wild	2020-06-11 13:11:51 UTC
First Submission	2020-08-20 11:58:19 UTC
Last Submission	2020-08-20 12:02:04 UTC
Last Analysis	2022-06-29 07:28:56 UTC

As a SOC Analyst, you can draw very important conclusions from this field. For example, there is a phishing attack on your institution and you analyze the attachment in the email. After you upload the file to VirusTotal, if you see that this file has been analyzed before you, you can draw the conclusion that this malware was not written specifically for your institution. (Not exactly, but more likely.)

Similarly, if you come across a file that has been analyzed before, you can understand that this attack was done on different institutions.

Relations:

This is the tab that shows detailed information about the domain, IP, URL, and other files that the suspicious file in your hand communicates with. The data shown here is scanned by security vendors within VirusTotal and you can see the results.

Contacted URLs ⓘ

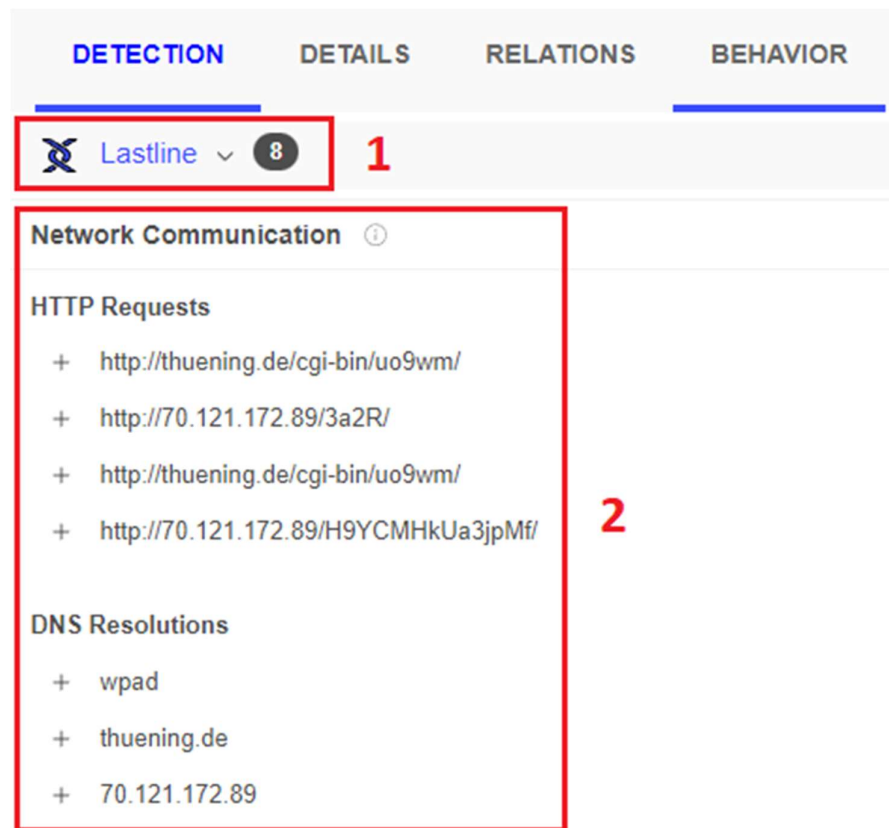
Scanned	Detections	Status	URL
2020-08-20	4 / 78	200	http://70.121.172.89/06Pjs/3HUxujCuQ5/2tfRg0Jp3yQ1PtZoNJ/sKyKFeW/
2022-04-30	12 / 92	200	http://thuening.de/cgi-bin/uo9wm/
2020-11-20	10 / 82	200	http://neuromedicaltechnology.com/cgi-bin/SkB/
2020-11-20	9 / 82	404	http://colegiolaesperanza.cl/new_img/fuJUk/
2022-06-28	0 / 87	405	https://dc.services.visualstudio.com/v2/track

You can usually use this tab to check for a suspicious address that the file is communicating with. At the same time, you can detect suspicious communication activities faster by viewing its reputation with the "Detections" score. There is an important point to note: new generation malware does not always exhibit the same behavior. They try to bypass security solutions by taking different actions in different systems. For this reason, the addresses you display in the relations tab may not give the entire list that the malware wants to communicate with, you should be aware that this list may be incomplete.

Behavior:

What determines whether a file is malicious is its activities. In the "Behavior" tab, you can see that different manufacturers list the activities that the scanned file has done. Among

these activities, you may encounter many behaviors such as network connections, DNS queries, file reading/deletion, registry actions, and process activities.



In section 1, you can specify which manufacturer you want to see the results of. Section 2 contains the activities performed by the scanned file. For example, if you look at the image above, you can see that the file makes four HTTP requests and a few DNS queries.

IMPORTANT NOTE: As we mentioned earlier, today's malware may not always exhibit the same behavior. For example, malware that cannot communicate with the command and control center (CC) may not activate itself. If the command and control center of the malware you want to analyze is not active, dynamic and static analyzes may not yield a clear result. In such cases, you should find old analysis reports made in environments such as VirusTotal and examine the behavior as in the "Behavior" tab.

Community:

You can see the comments added by the community in this area. Sometimes, there are those who share important details about how the suspicious file was obtained, what needs

to be considered during the analysis, or undetected. For this reason, checking the "Community" tab can be of great benefit.

Comments ⓘ



thor

3 months ago

YARA Signature Match - THOR APT Scanner

RULE: MAL_Dropper_Sample_Jul18_1

RULE_SET: Livehunt - Default2 Indicators

RULE_TYPE: Valhalla Rule Feed Only ⚡

RULE_LINK: https://valhalla.nexttron-systems.com/info/rule/MAL_Dropper_Sample_Jul18_1

DESCRIPTION: Detects suspicious Dropper

REFERENCE: <https://isc.sans.edu/diary/23932>

RULE_AUTHOR: Florian Roth

Show more



joesecurity

1 year ago

Joe Sandbox Analysis:

Verdict: MAL

Score: 100/100

Classification: mal100.bank.troj.evad.winDOC@22/18@1/4

Threat Name: Emotet

Domains: thuening.de

Hosts: [81.169.145.105](#) [192.168.2.1](#) [137.119.36.33](#) [127.0.0.1](#)

HTML Report: [analysis/273368/0/html](#)

Show more

In general, we talked about why you should look at which areas after uploading and scanning a file. This way you can better interpret VirusTotal outputs.


Scanning URLs with VirusTotal

You can analyze URL addresses as well as file analysis in VirusTotal. All you have to do is query the relevant address from the URL section.

FILE

URL

SEARCH



By submitting data above, you are agreeing to our [Terms of Service](#) and [Privacy Policy](#), and to the sharing of your URL 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

In the rest of the article, the malicious address “`thuening[.]de[/]cgi-bin/uo9wm/`” will be examined. (Do not directly access this address as it is a malicious address. You can follow the lesson by clicking the VirusTotal link below that we provided.)

12

/ 92

?

Community Score

12 security vendors flagged this URL as malicious

http://thuening.de/cgi-bin/uo9wm/

thuening.de

200

Status

text/html

Content Type

2022-04-30 20:40:20 UTC

2 months ago

DETECTION

DETAILS

LINKS

COMMUNITY

Security Vendors' Analysis

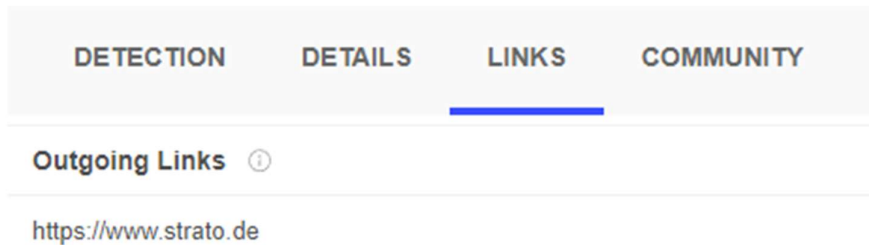
alphaMountain.ai	Malicious	Avira	Malware
BitDefender	Malware	Comodo Valkyrie Verdict	Phishing
Emsisoft	Malware	ESET	Malware
Fortinet	Malware	G-Data	Malware
Kaspersky	Malware	SCUMWARE.org	Malware
Sophos	Phishing	Webroot	Malicious
Forcepoint ThreatSeeker	Suspicious	Abusix	Clean
Acronis	Clean	ADMINUSLabs	Clean

<https://www.virustotal.com/gui/url/2bcbc32b84d5d2f6ca77e99232134947377302e7eeee77555672e57f81cd9428>

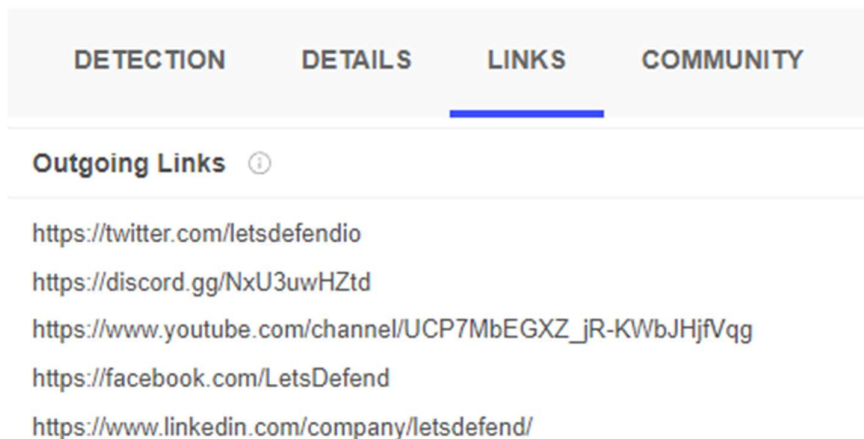
We encounter a similar interface as in file analysis. You can review the previous article for Detection and Details, it will be continued with the Links tab without explaining the same fields again.

Links:

It is the part where the links that the URL address leads to outside are listed. If you look at the image below, you can see that the address we scanned is linked to the address in strato[.]de.



When we scan the "letsdefend.io" address, it is seen that there are links to social media accounts.



You can make various inferences with the data you will obtain in this area. For example, even if the URL address does not directly contain harmful content, it may link to harmful addresses, in which case the investigation should continue.

During the investigation, you may receive various IOCs (Indicator of Compromise). To find out more about these IOCs, you can search in the "Search" section of VirusTotal. For example, by searching the hash value of a suspicious file here, you can find historical analysis results or other different data, if any.

As an example, let's search for the SHA256 value "415ba65e21e8de9196462b10dd17ab81d75b3e315759eeced5ea8f5812000c1b".

FILE

URL

SEARCH

415ba65e21e8de9196462b10dd17ab81d75b3e315759eeced5ea8f5812000c1b

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

As can be seen, we are faced with the result of an analysis made in the past.

42

58

42 security vendors and 6 sandboxes flagged this file as malicious

415ba65e21e8de9196462b10dd17ab81d75b3e315759eeced5ea8f5812000c1b

3bctnf8ct.dll

242.53 KB

Size

2022-06-29 07:28:56 UTC

2 days ago

DOC

calls-wmi

create-cle

doc

executes-dropped-file

hide-app

macros

obfuscated

DETECTION

DETAILS

RELATIONS

BEHAVIOR

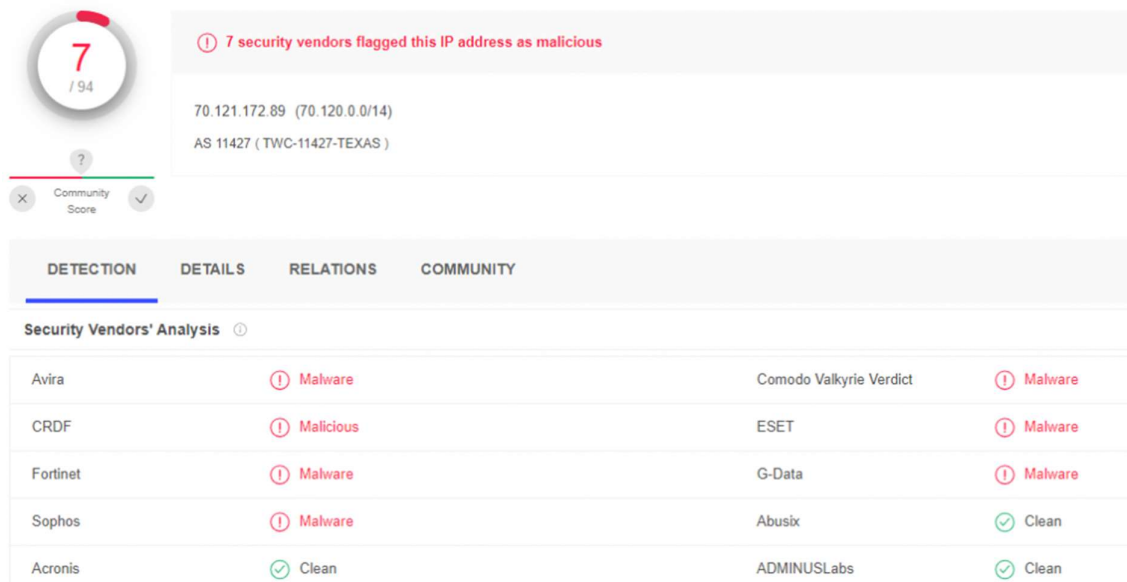
COMMUNITY

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

<https://www.virustotal.com/gui/file/415ba65e21e8de9196462b10dd17ab81d75b3e315759eeced5ea8f5812000c1b>

Or if we want to search for an IP address, we can similarly search and view its reputation.
Example IP address 70[.]121[.]172[.]89



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
/ 94

?

Community Score

7 security vendors flagged this IP address as malicious

70.121.172.89 (70.120.0.0/14)

AS 11427 (TWC-11427-TEXAS)

DETECTION

DETAILS

RELATIONS

COMMUNITY

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

In short, you can view past VirusTotal results and different files, IPs, and URL associations by searching in the “Search” section.