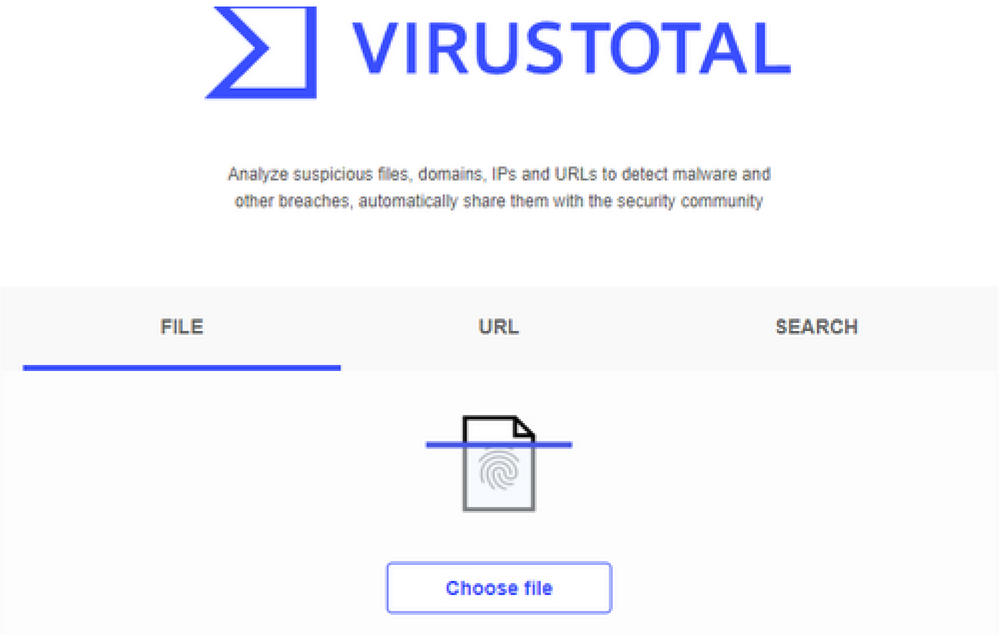
LetsDefend

File Analysis with VirusTotal

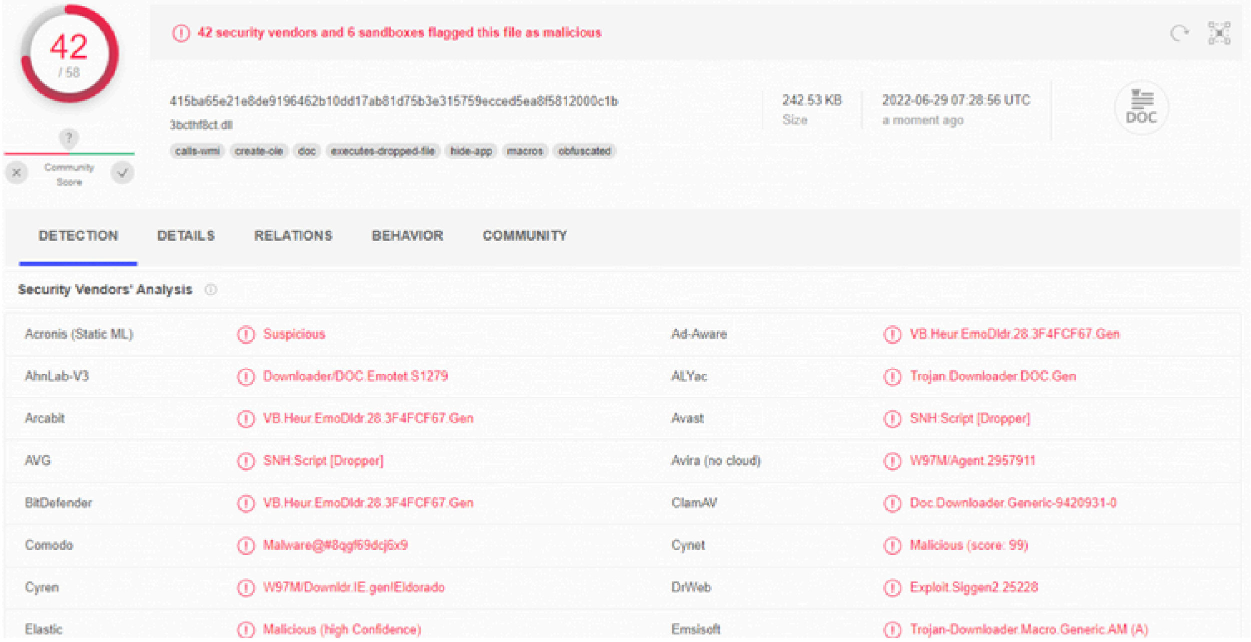
By: Ryan Stewart

When examining alerts from a Security Information and Event Management (SIEM) system or another security solution, you might come across a suspicious file that requires analysis. To access diverse file analysis results from various antivirus (AV) companies, consider uploading the file to VirusTotal. This service checks if AV products identify the file as malicious.

* It is **important** to be aware that premium VirusTotal users have the capability to download uploaded files. Consequently, exercise caution and **refrain** from uploading files that may contain sensitive information, as a precautionary measure.



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



42 security vendors and 6 sandboxes flagged this file as malicious

415ba65e21e8de9196462b10dd17ab81d75b3e315759ecced5ea8f5812000c1b
3bcthf8ct.dll
calls-wmi create-ole doc executes-dropped-file hide-app macros obfuscated

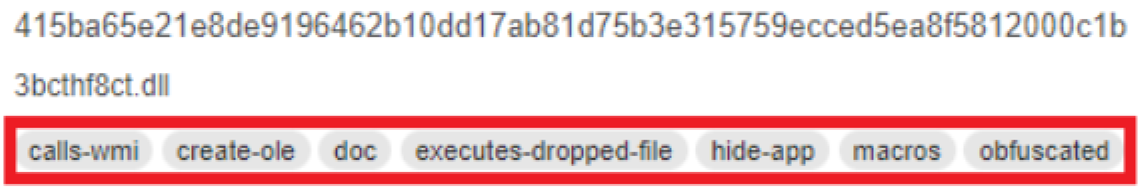
242.53 KB
Size

2022-06-29 07:28:56 UTC
a moment 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
BitDefender	VB.Heur.EmoDldr.28.3F4FCF67.Gen	ClamAV	Doc.Downloader.Generic-9420931-0
Comodo	Malware@#8qgf69dcj6x9	Cynet	Malicious (score: 99)
Cyren	W97M/Downldr.IE.gen!Eldorado	DrWeb	Exploit.Siggen2.25228
Elastic	Malicious (high Confidence)	Emsisoft	Trojan-Downloader.Macro.Generic.AM (A)

- 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.

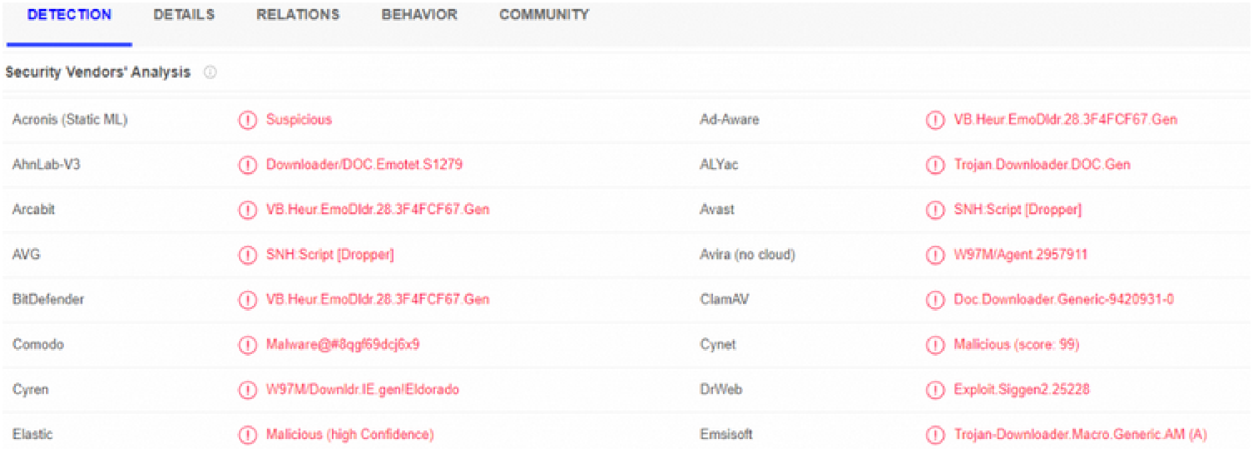


415ba65e21e8de9196462b10dd17ab81d75b3e315759ecced5ea8f5812000c1b
3bcthf8ct.dll
calls-wmi create-ole doc executes-dropped-file hide-app macros obfuscated

- 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.

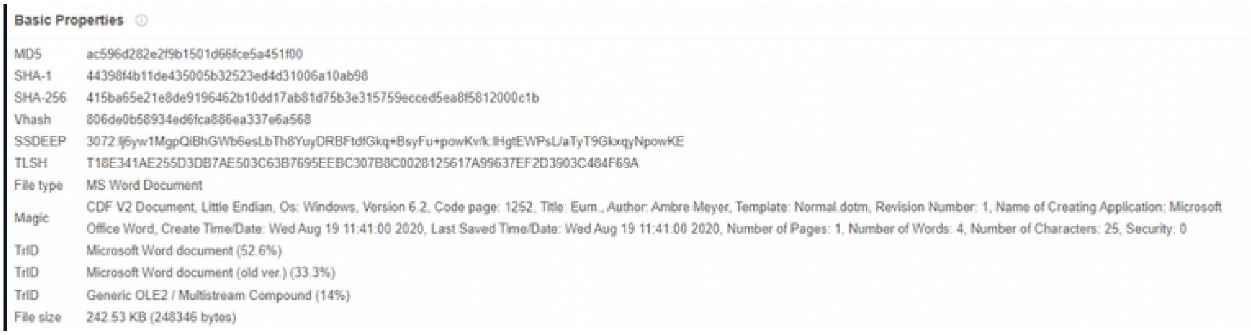


Security Vendors' Analysis

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
BitDefender	VB.Heur.EmoDldr.28.3F4FCF67.Gen	ClamAV	Doc.Downloader.Generic-9420931-0
Comodo	Malware@#8qgf69dcj6x9	Cynet	Malicious (score: 99)
Cyren	W97M/Downldr.IE.gen!Eldorado	DrWeb	Exploit.Siggen2.25228
Elastic	Malicious (high Confidence)	Emsisoft	Trojan-Downloader.Macro.Generic.AM (A)

Details

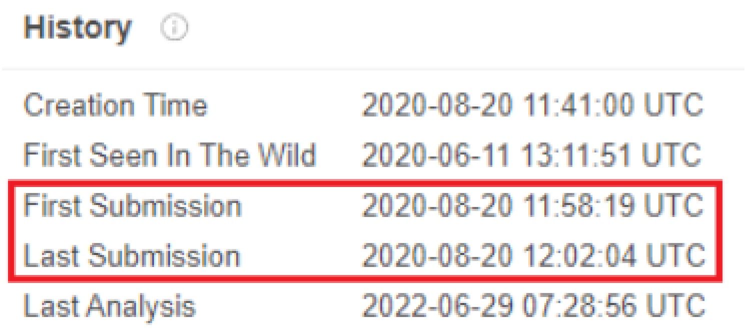
Here you can find some basic information about the file and details about its VirusTotal history. For example, the “Basic Properties” area contains file hash information and more.



Basic Properties

MD5	ac596d282e2f9b1501d66fce5a451f00
SHA-1	44398f4b11de435005b32523ed4d31006a10ab98
SHA-256	415ba65e21e8de9196462b10dd17ab81d75b3e315759ecced5ea8f5812000c1b
Vhash	806de0b58934ed6fca886ea337e6a568
SSDEEP	3072:Ij6yw1MgpQiBhGWb6esLbTh8YuyDRBFtdfGkq+BsyFu+powKv/k:IHgtEWPsL/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

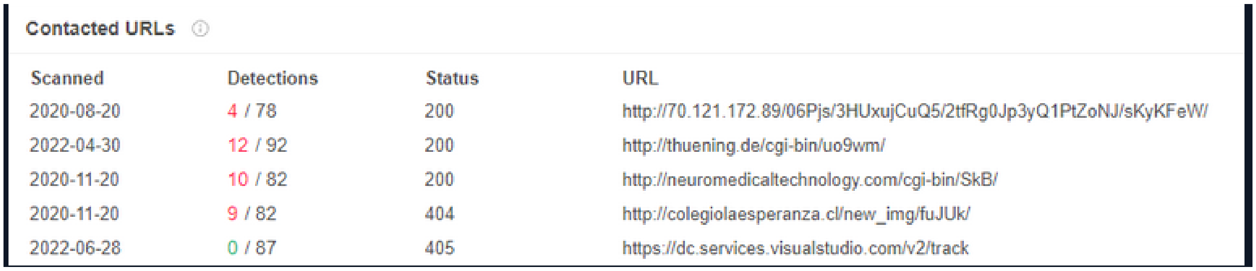
Creation Time	2020-08-20 11:41:00 UTC
First Seen In The Wild	2020-06-11 13:11:51 UTC
First Submission	2020-08-20 11:58:19 UTC
Last Submission	2020-08-20 12:02:04 UTC
Last Analysis	2022-06-29 07:28:56 UTC

As a **Security Operations Center** (SOC) Analyst, deriving crucial insights from this information is paramount. For instance, in the case of a phishing attack targeting your institution, when analyzing the email attachment, uploading it to VirusTotal may reveal prior analyses. If you discover that the file has been scrutinized previously, it suggests that the malware was not crafted specifically for your institution (though not definitively, but with a higher likelihood).

Likewise, encountering a file with a history of analysis indicates that the same attack has targeted other institutions, providing valuable context and aiding in understanding the broader scope of the threat.

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.



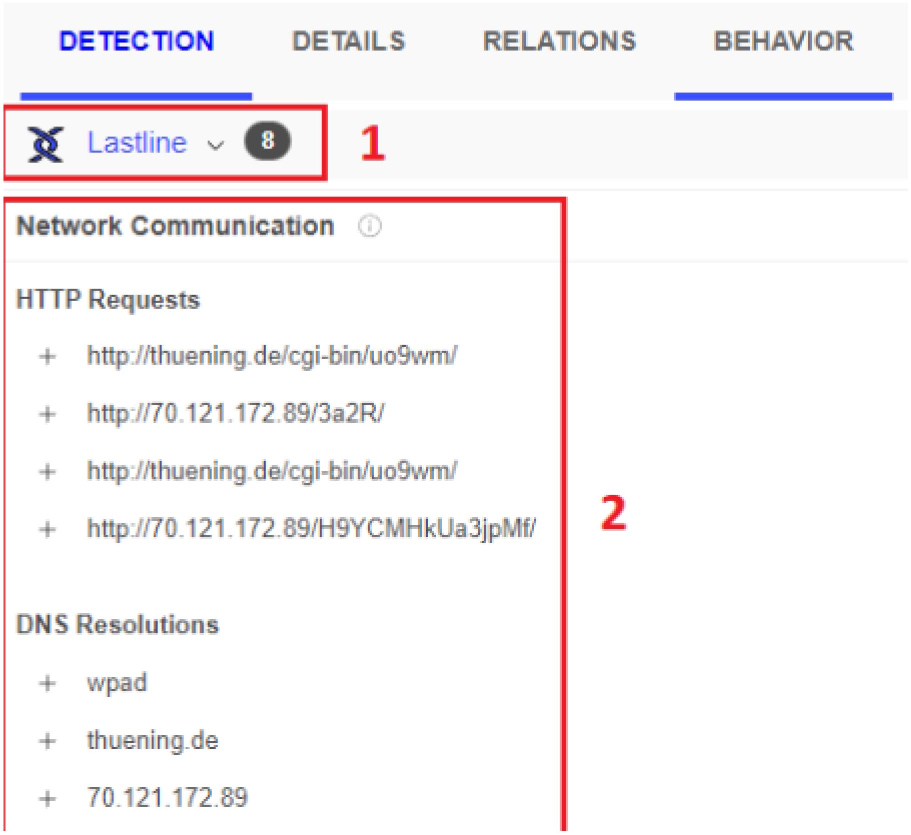
Contacted URLs

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.



Network Communication

HTTP Requests

- http://thuening.de/cgi-bin/uo9wm/
- http://70.121.172.89/3a2R/
- http://thuening.de/cgi-bin/uo9wm/
- http://70.121.172.89/H9YCMHkUa3jpMf/

DNS Resolutions

- wpad
- thuening.de
- 70.121.172.89

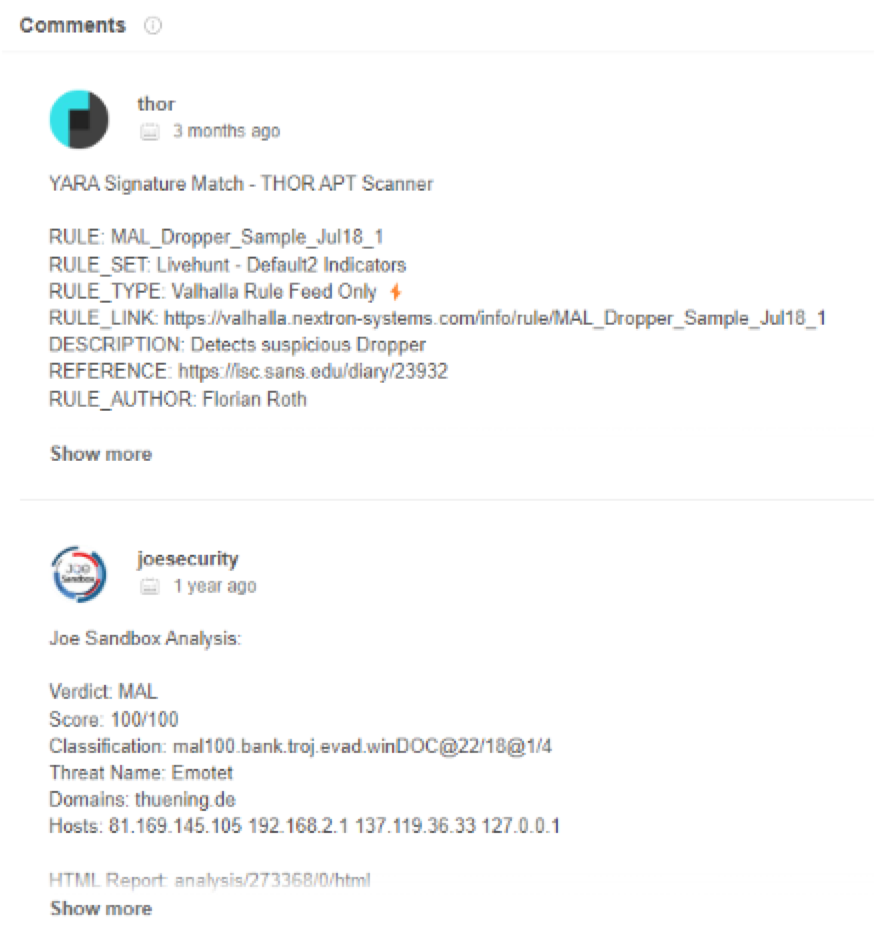
In section 1, you can specify which manufacturer you want to see the results of.

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.nextron-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.