https://documentation.wazuh.com/3.0/user-manual/capabilities/virustotal-scan/what-is-virustotal.html

What is VirusTotal?

VirusTotal is an online service that analyzes files and URLs enabling the detection of viruses, worms, trojans and other kinds of malicious content using antivirus engines and website scanners. It also can be used to detect false positives.

VirusTotal is a free service with numerous features that make its use very interesting, for our purpose we can highlight the following:

- VirusTotal stores all the analyses it performs, this means that we can search for a report using the hash of the file that we are interested in. In other words, sending that hash to the VirusTotal engine we can find out if that file has been scanned by VirusTotal and analyze its report.
- On the other hand, VirusTotal provides an API that allows us to access the information generated by VirusTotal without the need of using the HTML website interface. This API is subjected to its Terms of Service, which are discussed in the following section.

Features:

VirusTotal was founded in 2004 as a free service that analyzes files and URLs for viruses, worms, trojans and other kinds of malicious content. The goal is to make the internet a safer place through collaboration between members of the antivirus industry, researchers and end users of all kinds. Fortune 500 companies, governments and leading security companies are all part of the VirusTotal community, which has grown to over 500,000 registered users.

VT Web Interface

API

VT Intelligence

VT Hunting

VT Graph

Web interface:

Any user can upload files, URLs and search for free through the web interface.

Searching

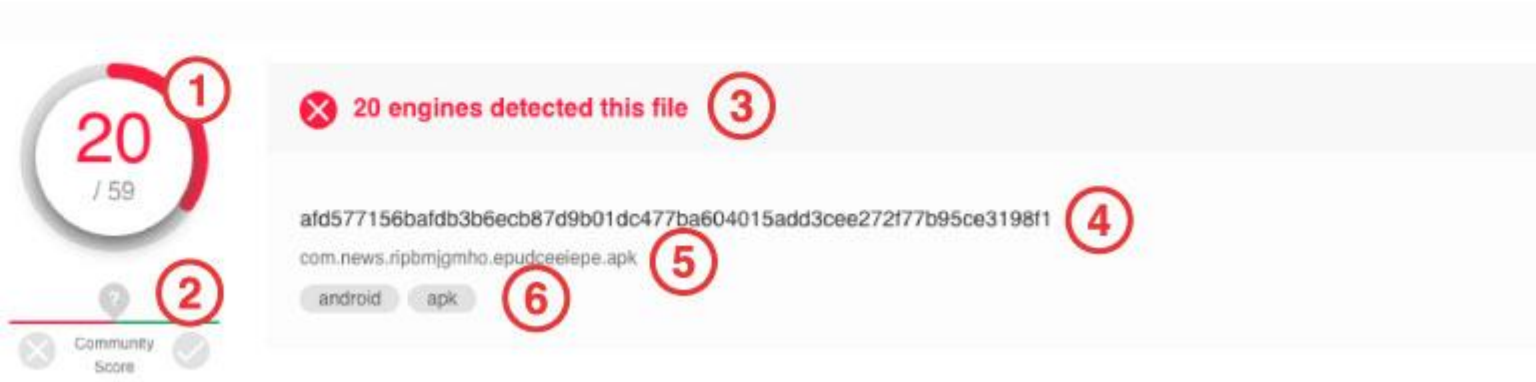
The search feature is free and available to any user. Every time a scan is requested by users, VirusTotal stores the analyses and report. This allows users to query for reports given an MD5, SHA1, SHA256 or URL and render them without having to resubmit the items (whether URLs or files) for scanning. VirusTotal also allows you to search through the comments that users have posted on files and URLs, inspect our passive DNS data, and retrieve threat intelligence details regarding domains and IP addresses.

How to search?- https://support.virustotal.com/hc/en-us/articles/115002739245-Searching

Understanding the reports:

File reports Summary

When you scan a file or search for a file given its hash, you'll see a report that looks like this:



20 engines detected this file

afd577156bafdb3b6ecb87d9b01dc477ba604015add3cee272f77b95ce3198f1

com.news.ripbmjgmho.epudceeiepe.apk

1) and 3) The total number of VirusTotal partners who consider this file harmful out of the total number of partners who reviewed the file.

2) The reputation of the given URL as determined by VirusTotal's Community. Users sometimes vote on files and URLs submitted to VirusTotal, these users in turn have a reputation themselves, the *community score* condenses the votes performed on a given item weighted by the reputation of the users that casted these votes. Negative (red) scores indicate maliciousness, whereas positive (green) scores reflect harmlessness. The higher the absolute number, the more that you may trust a given score. You can read more about this at: https://support.virustotal.com/hc/en-us/sections/115000737185-Community

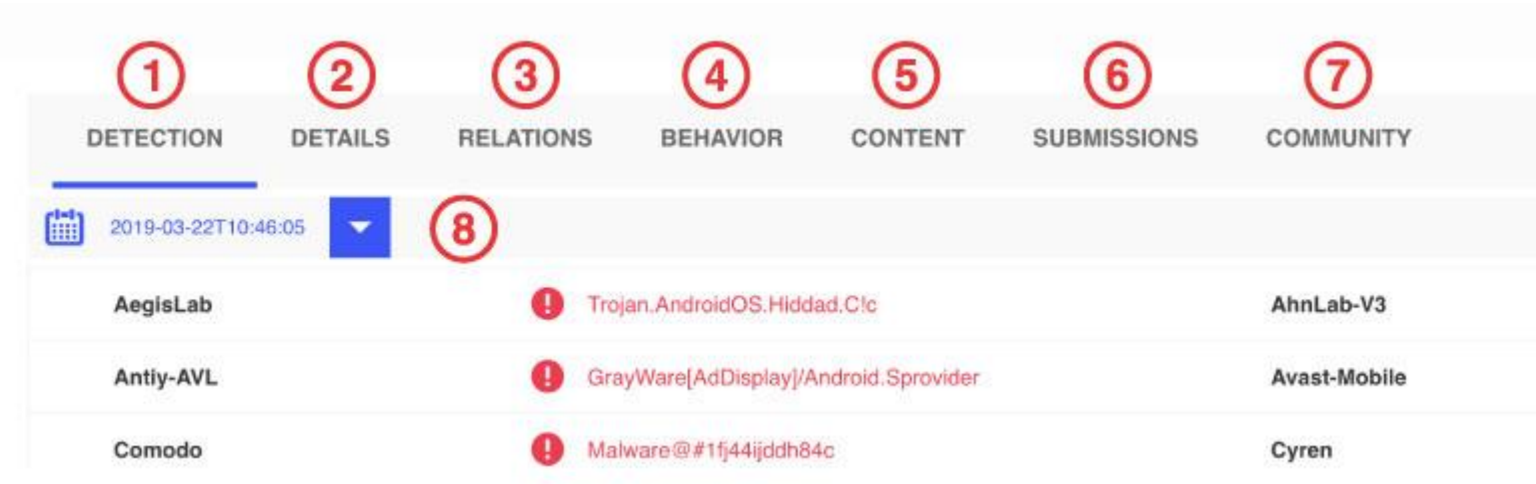
4) SHA-256 (a cryptographic hash function) is a unique way to identify a file and used in the security industry to unambiguously refer to a particular threat.

5) File name of last submission, and access to search by file names.

6) Tags.

7) The date and time (UTC) of the review.

File Reports Details



AegisLab	Trojan.AndroidOS.Hiddad.C!c	AhnLab-V3
Antiy-AVL	GrayWare[AdDisplay]/Android.Sprovider	Avast-Mobile
Comodo	Malware@#1fj44ijddh84c	Cyren

1) A list of each reviewing partner and their findings. Possible findings are:

- Undetected: The given engine does not detect the file as malicious.
- Suspicious: The given engine flags the file as suspicious.
- Unable to process file type: The given engine does not understand the type of file submitted and so will not produce verdicts for it.
- Timeout: The given engine reached VirusTotal's time execution limit when processing the file and so no verdicts were recorded for it.

2) Displays more information about the item being reviewed. For instance, for an Office document file this might list VBA code streams seen in document macros and other file type specific information. Similarly, VirusTotal specific metadata such as first submission and last submission dates, upload file names, etc are also recorded in this section.

3) VirusTotal's backend generates rich relationships: URLs from which a file has been downloaded, whether a given file been seen contained in some other files, what are the parents of a given Portable Executable, domain to IP address mappings over time, etc.

4) The samples submitted to VirusTotal get executed automatically in a controlled (sandboxed) environment and the actions performed are recorded in order to give the analyst a high level overview of what the sample is doing.

Other reports: https://support.virustotal.com/hc/en-us/articles/115002719069-Reports

API

VirusTotal's API lets you upload and scan files, submit and scan URLs, access finished scan reports and make automatic comments on URLs and samples without the need of using the HTML website interface. In other words, it allows you to build simple scripts to access the information generated by VirusTotal.

You can read the full documentation here: API Developer Reference.

VirusTotal Intelligence

VirusTotal Intelligence allows you to search through our dataset in order to identify files that match certain criteria (hash, antivirus detections, metadata, submission file names, file format structural properties, file size, etc.). We could say that it is pretty much like the "Google" of malware.

In order to ease the use of the application we have classified the search queries and modifiers into the following categories:

Retrieving files by hash
Identifying files according to antivirus detections
Search modifiers
Content search (VTGrep)
File similarity search
Multi-similarity searches
URL search modifiers
Domain search modifiers
IP address search modifiers

Ex: Let us get all those PDFs that contain JavaScript and contains an automatic action (perhaps to launch the previous JavaScript):

```
type:pdf tag:autoaction tag:js-embedded
```

What is vt hunting?

VT Hunting is a service that leverages the power of YARA over VirusTotal's dataset, it consists of two different components: Livehunt and Retrohunt.

Livehunt

Livehunt allows you to hook into the stream of files analyzed by VirusTotal and get notified whenever one of them matches a certain rule written in the YARA language.

Livehunt applies your YARA rules to every file analyzed by VirusTotal, both when the file is submitted by some user, and when a file is re-analyzed. The difference between a submission and a re-analysis is that in the former case the user is in possession of the file and is uploading it to VirusTotal, in the latter case some existing file is being analyzed again. A submission always triggers an analysis, but files can be re-analyzed later without being submitted by a user.

If the file is a Portable Executable (PE) packed with some kind of run-time packer, it is unpacked and both the packed and unpacked versions of the file are scanned with YARA. When some file matches one of your rules, a notification is generated with details about the file and the matching rule.

How to do that? https://support.virustotal.com/hc/en-us/articles/360001315437-Livehunt

Retrohunt

Retrohunt allows you to scan all the files sent to VirusTotal in the past 12 months with your YARA rules. A Retrohunt job scans a corpus of more than 420M files (~680TB worth of data) in 3-4 hours and reports you the files that match your rules. Also, you can scan a fixed and smaller corpus composed of about 1 million files that are known to be goodware, which is handy when you are testing your YARA rules, as it can help you to spot false-positives. These jobs usually finish in less than a minute.

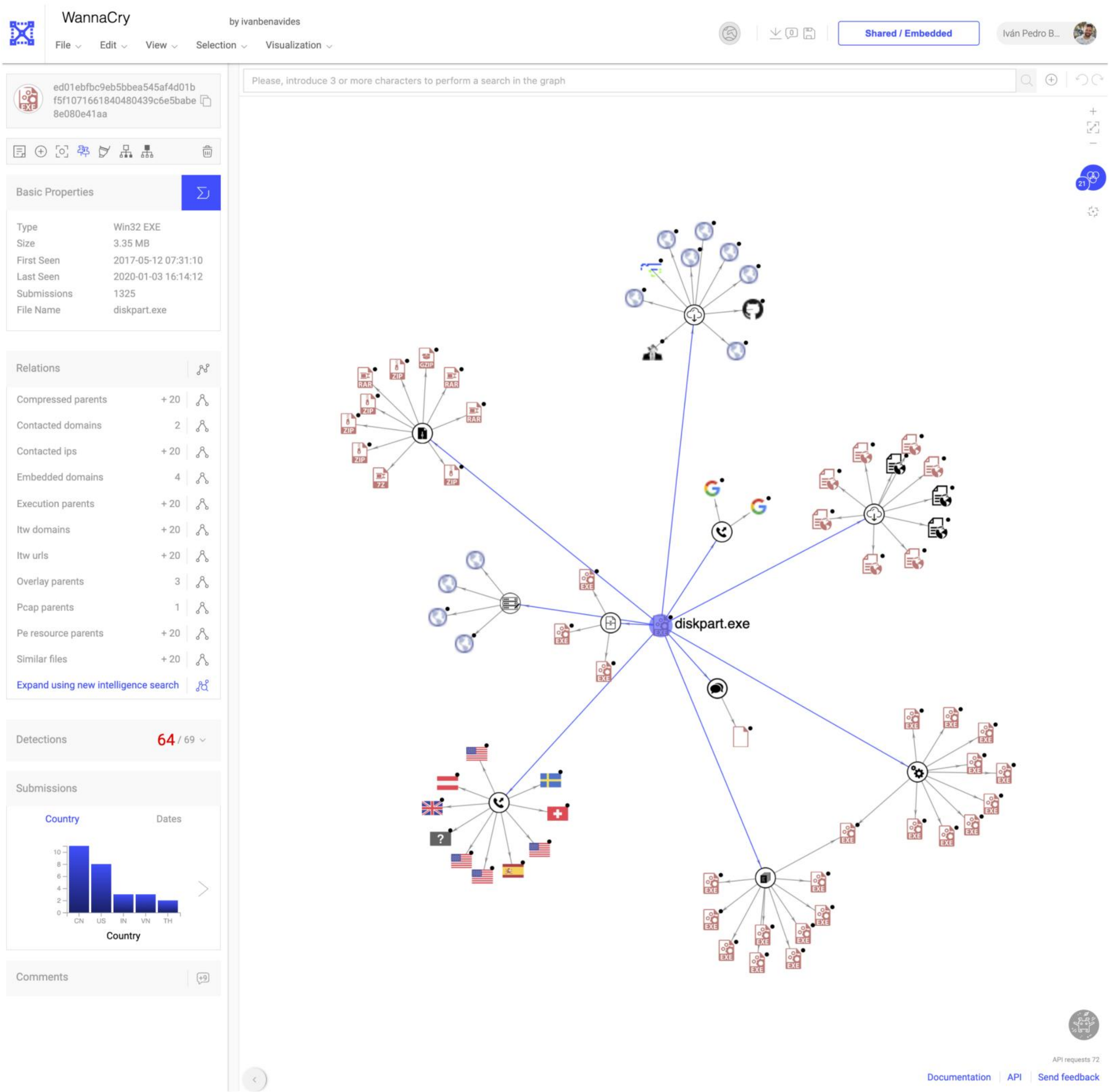
How>https://support.virustotal.com/hc/en-us/articles/360001293377-Retrohunt

Both Livehunt and Retrohunt can be automated using the VirusTotal API v3.

VirusTotal Graph

VirusTotal Graph is a visualization tool built on top of VirusTotal data set. It understands the relationship between files, URLs, domains, IP addresses and other items encountered in an ongoing investigation. With it, you can pivot intelligently over any of the malware artifacts in your graph and synthesize your findings into a threat map that you can share with your colleagues.

https://support.virustotal.com/hc/en-us/articles/360004679937-VirusTotal-Graph-overview



ed01ebfbc9eb5bbea545af4d01bf5f1071661840480439c6e5babe8e080e41aa

Basic Properties

Type	Win32 EXE
Size	3.35 MB
First Seen	2017-05-12 07:31:10
Last Seen	2020-01-03 16:14:12
Submissions	1325
File Name	diskpart.exe

Relations

Compressed parents	+ 20
Contacted domains	2
Contacted ips	+ 20
Embedded domains	4
Execution parents	+ 20
Itw domains	+ 20
Itw urls	+ 20
Overlay parents	3
Pcap parents	1
Pe resource parents	+ 20
Similar files	+ 20

Expand using new intelligence search

Detections 64 / 69

Submissions

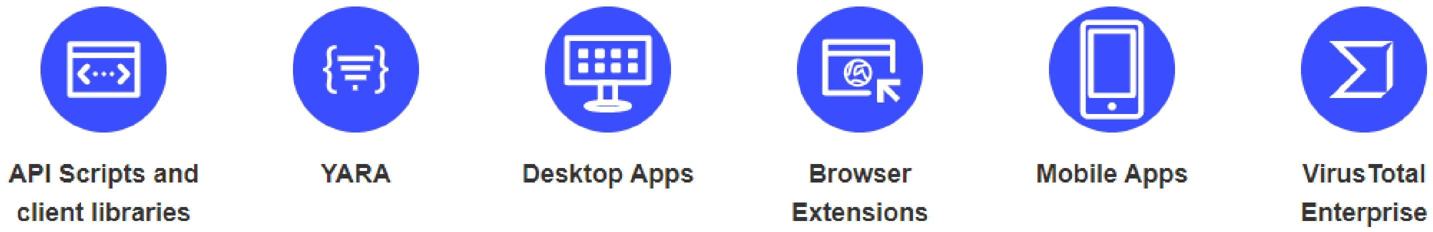
Country Dates

Comments

Tools

Over time, VirusTotal has added various tools to help users scan files and URLs more efficiently.

https://support.virustotal.com/hc/en-us/categories/360000162898-Tools



Myths about virus total: https://www.virusbulletin.com/virusbulletin/2018/01/vb2017-paper-virustotal-tips-tricks-and-myths/

How hackers use virus total: https://www.wired.com/2014/09/how-hackers-use-virustotal/