

Vulnerability management

Vulnerability management is the process of identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them. This, implemented alongside with other security tactics, is vital for organizations to prioritize possible threats and minimize their "attack surface."

HOW CAN VIRUSTOTAL HELP YOU?

Virustotal provides you with a unique visibility on how vulnerabilities are being actively exploited by attackers and what kind of malware and actors are behind them, as well as how quickly these malicious campaigns are spreading.

For instance, you can see which CVEs are being exploited by attackers in the wild at this moment or during the last few weeks, what kind of malware they are distributing, and what actors are behind.

This is essential information to do a proper risk assessment depending on your profile as a potential victim for attackers, so you can properly prioritize any relevant vulnerabilities that need to be addressed.

Use Cases

GET THE LIST OF CVEs BEING ACTIVELY EXPLOITED BY ATTACKERS

With a simple search on VirusTotal, you have access to different types of new files, even those that have not yet been classified as malware by antivirus engines.

How to do it?

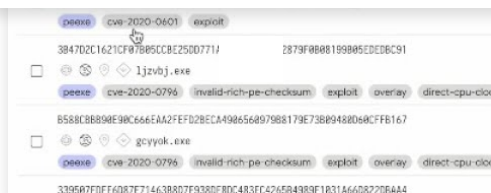
1. Go to VirusTotal Search: <https://www.virustotal.com/gui/home/search>
2. Create your query. For instance, the following query corresponds to the example in the video:

```
engines:ransom tag:exploit fs:date+ tag:cve-2020*
```

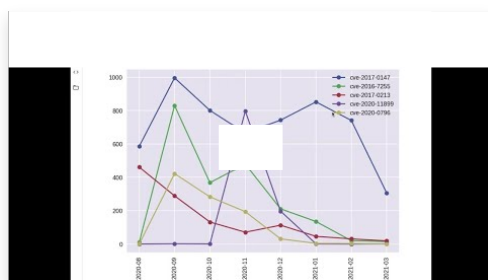
We look for Malware classified as Ransom ([engines:ransom](#)), tagged as an exploit ([tag:exploit](#)) and as CVE 2020 ([tag:cve-2020*](#)), specifying the date from which it has been seen for the first time ([fs:"date"](#)).

This search can be more precise by adding more search conditions and modifiers. For more information on VirusTotal modifiers [click here](#).

[Click here](#) for seeing the result of the previous query.


[Contact us](#)


Pro tip: You can use our API to check what vulnerabilities are being exploited the most by ransomware!



FIND HOW A SPECIFIC VULNERABILITY IS BEING EXPLOITED

You can search for a specific vulnerability and see the new malicious files that are exploiting it. This will help you understand how and who is abusing these security flaws and properly prioritize your vulnerability patching, anticipating to attackers and minimizing your exposure.

How to do it?

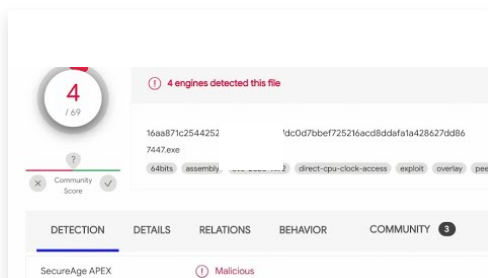
- Go to VirusTotal Search: <https://www.virustotal.com/gui/home/search>
- Create your query. For instance, the following query corresponds to the example in the video:

entity:file tag:CVE-2020-1472

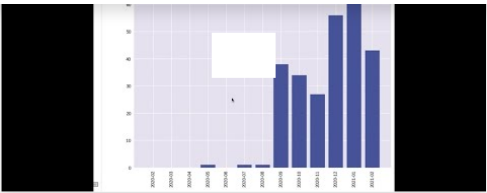
In this query, we look for files tagged us CVE-2020-1472.

The search can be as specific as we would like, specifying dates, file sizes, the behavior of the malware, signatures and much more. If you want more information about VirusTotal Search modifiers click [here](#).

[Click here](#) for seeing the result of the previous query.



Pro tip: Check how popular is a vulnerability in the wild using our API!



Please reach out to us if we can help you with anything else.

Contact us

- VirusTotal**
- [Contact us](#)
- How It Works
- Terms of Service
- Privacy Policy
- Blog
- Community**
- [Join Community](#)
- Vote and Comment
- Contributors
- Top Users
- Latest Comments
- Tools**
- API Scripts
- YARA
- Desktop Apps
- Browser Extensions
- Mobile App
- Premium Services**
- Intelligence
- Hunting
- Graph
- API v3 | v2
- Monitor
- Documentation**
- Intelligence
- Hunting
- Graph
- API v3 | v2
- [Use Cases](#)