VirusTotal

Virustotal is one of the more prominent online services, which offers a way to upload any suspicious files and analyze them.

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

And, with 55 antivirus engines and 70 detection engines. This tool is also available in application format for mobile phones, both Android and iOS, through the Mac executable.

Advantages:

- Since its tools grant the value of VirusTotal, there is no better way to guarantee good performance and avoid false positives than through extensions and powerups.
- For example, VirusTotal Graph is an additional tool that generates a graphic with a central node, consisting of the file, and the nodes to which it is linked. Sites where we find related information.
- The mission is to create a path to track the origin of that file or, at least, know if it is connected to suspicious online files.

How does it work?

VirusTotal offer different ways to submit files to the platform, be that via the web-interface, browser extensions or their very own API. The interesting thing here is that, through the use of the API, we can automate the submissions to VirusTotal and integrate the service in a SOC, when a suspicious or potentially malicious file is encountered.

VirusTotal uses a large variety of antivirus scanners and URL/domain blacklisting services.

VirusTotal has a public API, that is, an open programming interface to implement new features. The users who contribute the most get promotion through a reputation system, depending on the usefulness of their contributions. It publishes the rules of labelling and voting on its website.

Conclusion:

VirusTotal is very interesting, powerful and easy to use tool, which offers great benefits, but depending on your situation, must not always be the first option. Currently we are interested in learning more about complex obfuscation techniques used by adversaries and VirusTotal is an easy tool to use to test these techniques.