Spy vs. Spy: VirusTotal Your Shield in the Cybersecurity Battle

VirusTotal is a vital cybersecurity service that allows users to analyze suspicious files and URLs. This service detects malware and other malicious content by leveraging multiple antivirus engines and various scanning tools. VirusTotal's analysis is based on historical data, previously detected malware, and numerous other resources, including hashing, IPs, domains, hostnames, threat feeds, and reputation databases such as AbuseIPDB.

When you submit a file or URL to VirusTotal, it is scanned using numerous antivirus engines and tools. For instance, if you search for a URL, VirusTotal will provide detailed reports on whether any security vendors have flagged the site as "malicious," "suspicious," "spam," or any other designation. Additionally, the report includes extensive details related to the URL, which may be helpful for further investigation and understanding the threat landscape.

It is important to remember that uploading a URL, file, hash, or IP address to VirusTotal for analysis will make it publicly accessible. This transparency can be a double-edged sword. While it aids the cybersecurity community in identifying and combating threats, it may also tip off adversaries that their activities have been detected. For example, if an attacker has used a specific file to target only a few individuals or organizations, uploading that file to VirusTotal could alert the attacker, leading them to change or modify their attack methods. An attacker can verify if their URL or file has been uploaded to VirusTotal much like any regular user. They would search using their malicious URL or the hash of their malicious file. Finding a match indicates that the URL or file has been uploaded and analyzed. VirusTotal provides a “Last Analysis Date” which shows how recently it was examined, detailing whether it was analyzed 'a moment ago' or “# minutes ago”. If their URL or file does not appear in VirusTotal's results, it suggests that it has not yet been uploaded or publicly scanned, or it may have been submitted via private scanning.

If you want to scan a file or URL without making it public, consider using VirusTotal's premium service for private scanning. This ensures that the information remains confidential and does not alert potential adversaries. VirusTotal is an invaluable tool in the cybersecurity arsenal, providing detailed analyses of suspicious files and URLs using multiple scanning engines and reputation databases. However, users must be mindful of the implications of uploading sensitive information, as it could potentially alert adversaries.

If the adversary is already detected and you want to share their tactics, techniques, and procedures (TTPs), go ahead and report the file or URL. However, if you have not yet determined the exact threat, it might be wise to keep the information private for the time being. This will allow you to identify the threat and understand their complete strategy before taking further action. By understanding how to use VirusTotal effectively, individuals and organizations can better protect themselves against malicious threats.