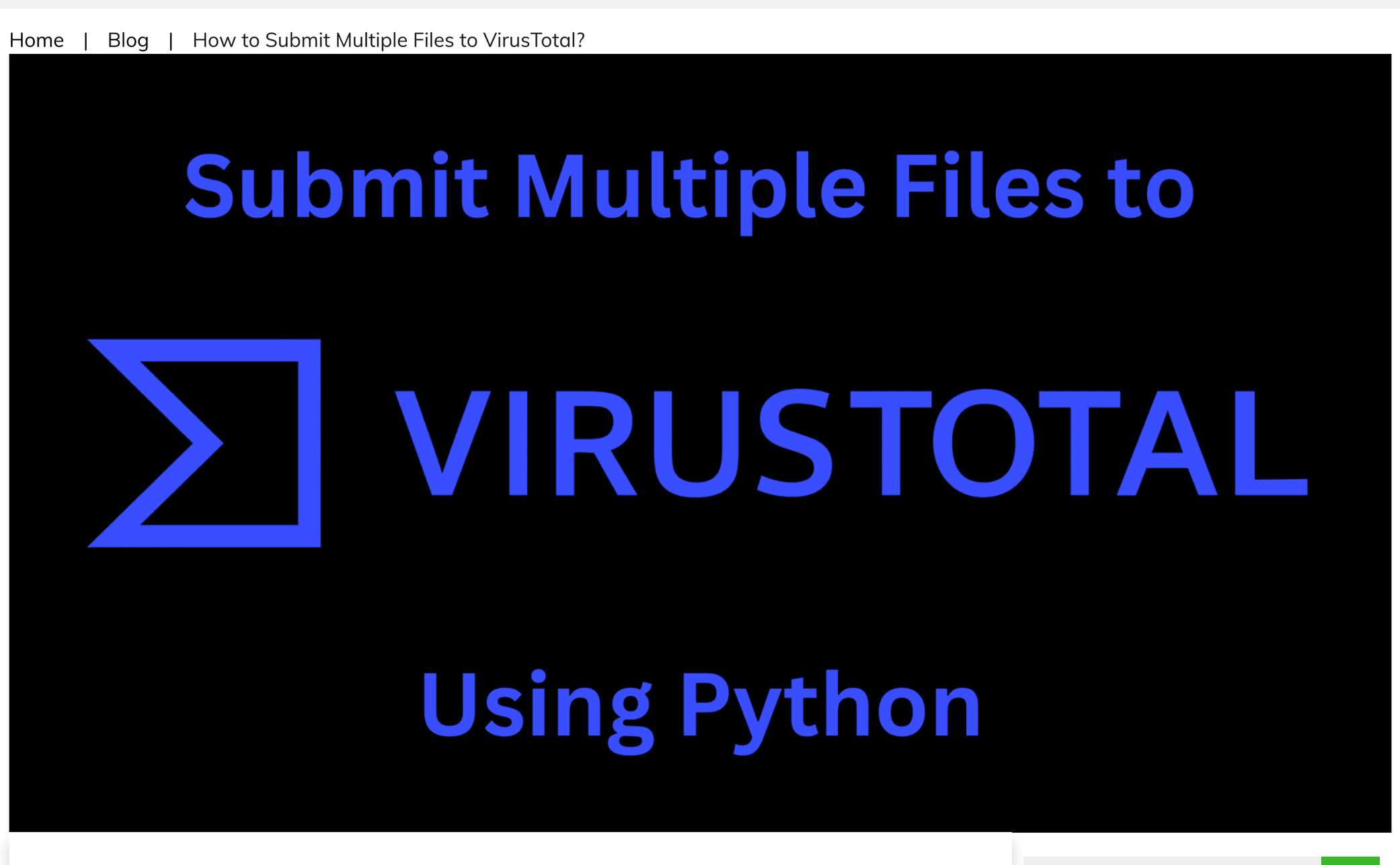


How to Submit Multiple Files to VirusTotal?

If you are ever part of security teams like a Security Operations Center (SOC) or CERT teams, you might be tasked with many threat analyses as part of your job. As a security professional, you may know the initial infection vector of malware. The days when attackers used to directly send malware files are long gone. Now, attackers have learned more sophisticated ways to deliver malware by hiding it inside legitimate files. Some attackers use fileless techniques to infect systems. Moreover, these days attackers leave no stone unturned to deliver malware. Malware could be delivered through update patch files – have you heard about supply chain attacks?

There are several security solutions and applications available in the market that help security professionals achieve their goals smarter. However, growing cyber threat trends show the game is not over yet, and probably won't be anytime soon. Palo Alto Networks survey data shows SOC analysts can only handle 14% of alerts generated by security tools. This clearly indicates there is still a massive gap. The resources we have today are not enough to deal with the threats. Some sort of automation is required.

Tools like VirusTotal would help security professionals identify such malicious files faster, better, and more accurately. Today, we can automate such tasks with services like VirusTotal combined with scripting languages like Python. As cybersecurity professionals, we want to help security analysts who need to validate or identify tons of malware files hidden inside legitimate files in bulk. We will show you the complete process to submit multiple files to VirusTotal using the VirusTotal API and a simple Python script. Let's explore what VirusTotal and its API offerings are and automate the file scanning process by learning how to scan multiple files with VirusTotal in this blog post.

Note: If you want to submit multiple IOCs like domains, IPs, URLs, or file hashes to VirusTotal to scan. See here.

Table of Contents

1. Upload an Archive
2. A Short Note About VirusTotal and Its API Service
   2.1. Public vs Private API
3. Prerequisites to Submit Multiple Files to VirusTotal
4. Why You Need to Submit IOCs to VirusTotal in Bulk?
5. How to Submit Multiple Files to VirusTotal?
   5.1. Step 1: Signup on VirusTotal and Acquire API Key
   5.2. Step 2: Download the vtSubmit script
   5.3. Step 3: Install Python Interpreter, PyCharm or Conda (Optional Step)
   5.4. Step 4: Run the Python script to Submit multiple files to VirusTotal
6. Conclusion
   6.1. Similar Posts:

Upload an Archive

Before we dive into the Python script that automates this process, let's explore a simple and effective solution that may work for your problem. If you have a small number of files to submit infrequently, you can package the files into a compressed archive (e.g. zip, rar) and upload the archive to VirusTotal. VirusTotal will automatically extract and scan the contents. This works through both the web interface and APIs. Once scanning is complete, you can find the results for all your files under the "RELATIONS" tab.

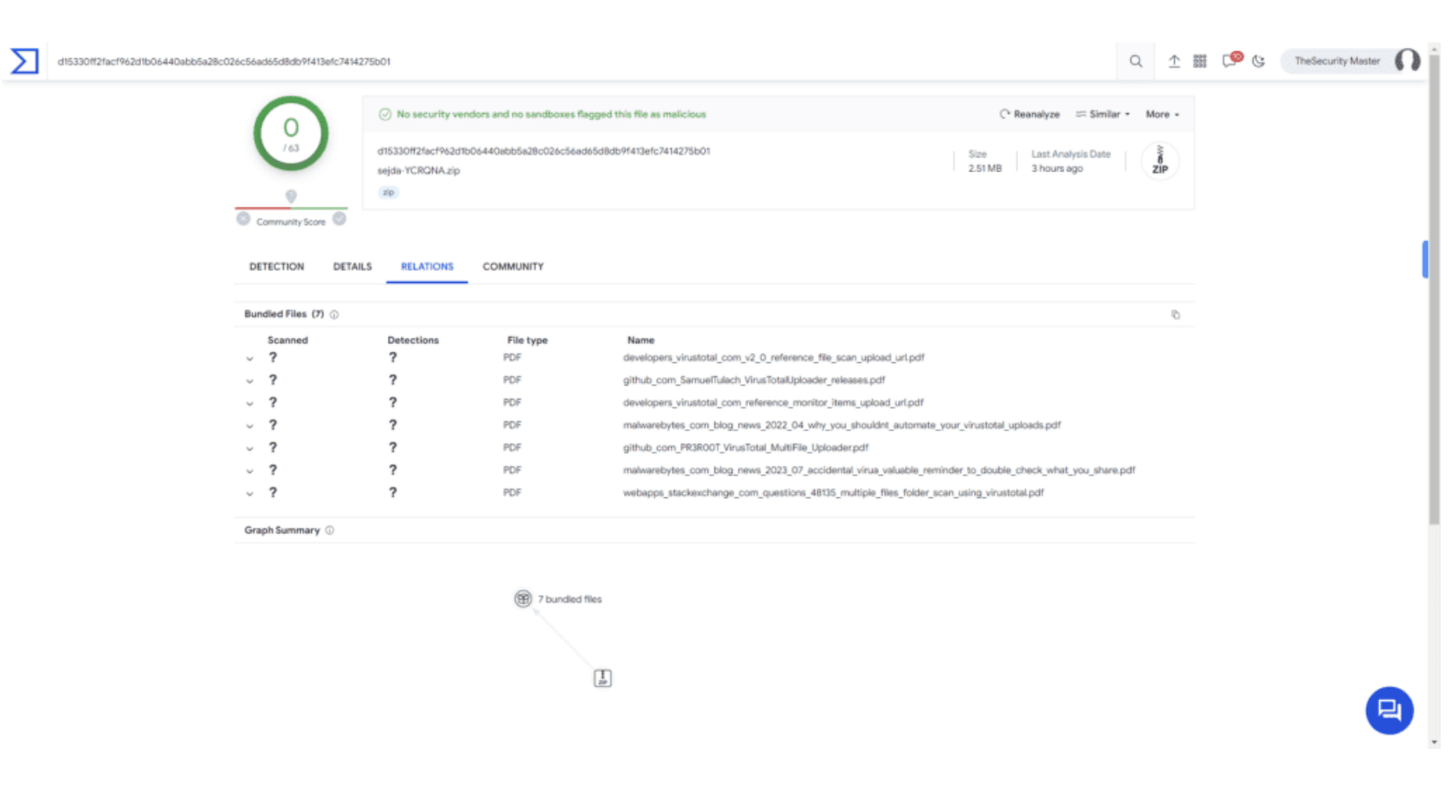
However, there are limitations – you can't upload a file larger than 32 MB in size directly into the app and you won't get a detailed independent report for each file. Wait, if you really want to upload a larger file, there is a way to do so. You need to get a special URL from VirusTotal to upload. Check out these links:

See Also How To Fix CVE-2021-30883, A Memory Corruption Issue In iOS 15.0.1 And Below?

https://developers.virustotal.com/reference/monitor-items-upload-url

https://developers.virustotal.com/v2.0/reference/file-scan-upload-url

Well, you can upload up to 200 MB. Go ahead if these limitations don't bother you. If they do, follow this article to learn how to do this using a Python script.



A Short Note About VirusTotal and Its API Service

VirusTotal is a free online service that analyzes files and URLs, enabling the identification of viruses, worms, trojans, and other kinds of malicious content using antivirus engines and website scanners. It also enables the generation and sharing of threat intelligence with its vast URL and file analysis database.

VirusTotal offers both public and private APIs that allow users to programmatically interact with their services. The public API has some limitations, like only allowing 500 requests per day and 4 requests per minute. The private API, on the other hand, provides more flexibility and advanced capabilities like allowing users to choose their own request rate and quota, download submitted samples, get more detailed analysis reports, etc.

If you are an individual security researcher who wants to scan multiple URLs, domains, IPs, and file hashes with VirusTotal infrequently, then the public API services are enough to have. If you are working for a corporate company that needs to do far more than just scan URLs, domains, IPs, and file hashes, then you should get the private API services.

Public vs Private API

Here is a quick comparison of VirusTotal's public and private APIs:

Feature	Public API	Private API
Request rate limit	500 requests/day, 4 requests/min	Flexible based on service tier
File download	No	Yes
Additional metadata	No	Yes e.g. first submission date, prevalence etc.
File behaviors	No	Yes
Advanced hunting APIs	No	Yes e.g. YARA based hunting
SLA	No	Yes

Prerequisites to Submit Multiple Files to VirusTotal

To submit multiple files to VirusTotal using a Python script, you will need:

- **VirusTotal API Key**: Sign up for a free VirusTotal Community account to get an API key. This will provide access to scan files through the public API.
- **Python Interpreter**: Install Python 3.6 or higher on your system if not already available. This is required to run the script.
- **Optional Python IDE**: Using an IDE like PyCharm, Visual Studio or Anaconda can help run Python scripts easily. But it's optional.
- **vtSubmit Python Script**: A small code written in Python language that takes VirusTotal API and directory path as an input. The script uses the API key to submit files in the directory to the VirusTotal API Endpoint through POST requests. And store the result in a CSV file. You can download the script from our GitHub repo.

Once you have these prerequisites ready, you can start the bulk file submission process to VirusTotal.

Why You Need to Submit IOCs to VirusTotal in Bulk?

The main purpose of this program is to automate the file submission process to get files scanned across multiple antivirus engines. This speeds up malware analysis and threat detection processes.

Security advisories or threat intelligence teams often share lists of files with an organization's security team. The goal is to analyze the files and block them on proxies, endpoints, firewalls, SIEMs, and other security solutions. This curbs the spread of malware infections on corporate networks.

See Also How To Fix Critical Remote Code Execution Vulnerabilities In PHP Everywhere WordPress Plugin

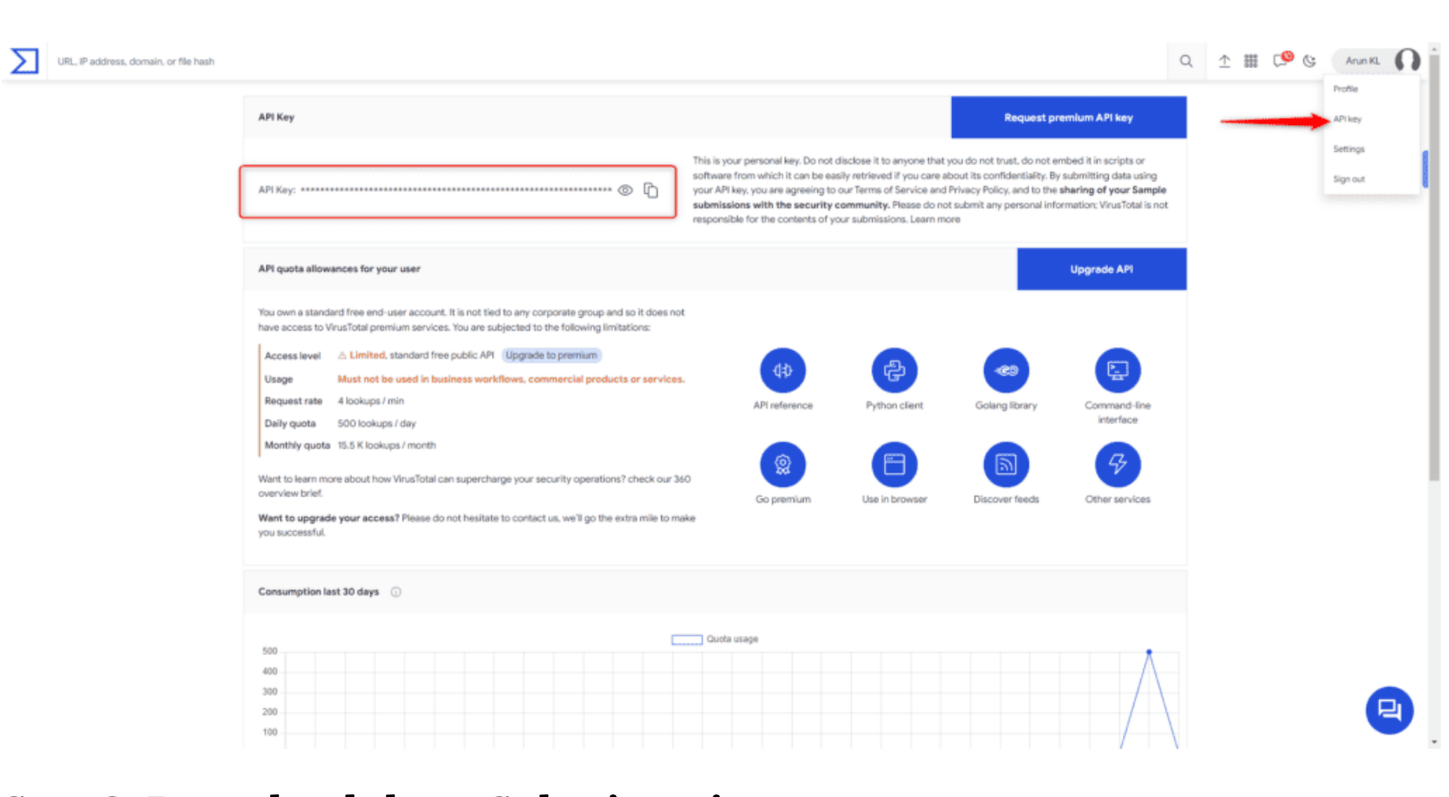
It is well known that no security product provides 100% protection against evolving threats. These scripts also help security teams determine which files were flagged as malicious by the vendors of their products. If not blacklisted already, they can block them in their security products. They can also submit unidentified file fingerprints (hash values) to vendors to block globally.

How to Submit Multiple Files to VirusTotal?

The procedure is simple and straightforward. You just need to set up your Python environment with the VirusTotal API key. Follow these steps to leverage VirusTotal APIs for scanning multiple files automatically:

Step 1: Signup on VirusTotal and Acquire API Key

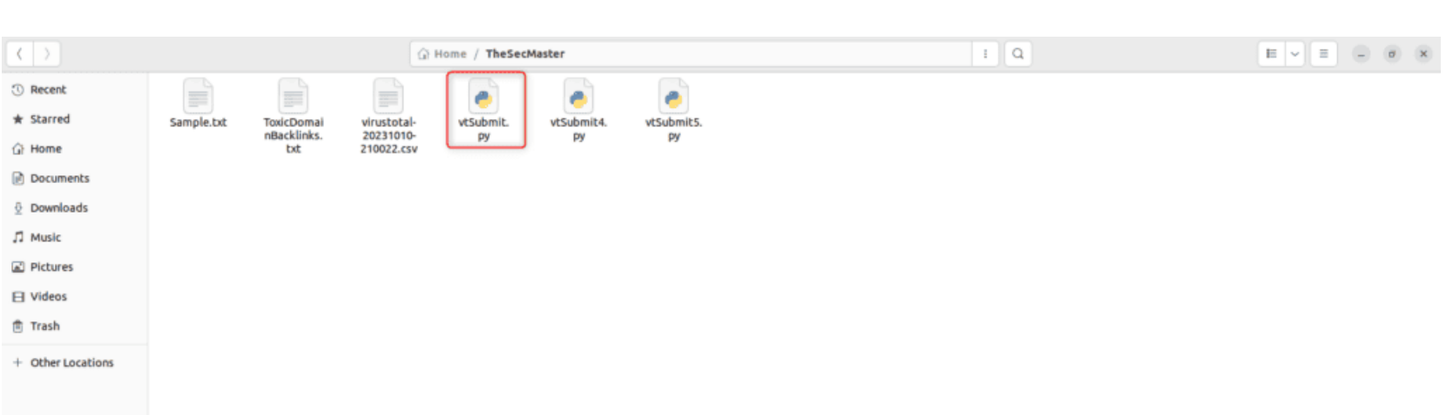
- Go to VirusTotal.com and create a free account.
- Navigate to your Profile and note down the API key provided. This will be used for authentication.



Step 2: Download the vtSubmit script

Download the Python script from here and place it on your machine. We copied it to the **/home/arunkl/TheSecMaster** Directory on our machine.

Download the Script from Git.



Step 3: Install Python Interpreter, PyCharm or Conda (Optional Step)

If you are on Windows, you should need to download and install the Python interpreter.

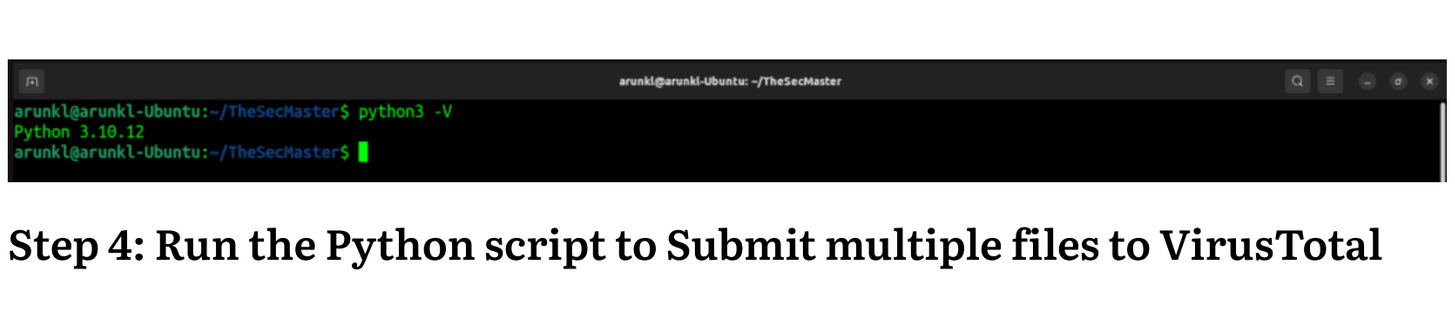
- Download the latest Python 3.x from python.org and install it.
- Add Python to a PATH environment variable.

How to Install Python:

1. Install Python on Windows:https://thesecmaster.com/step-by-step-procedure-to-install-python-on-windows/
2. Install Python on Linux:https://thesecmaster.com/3-ways-to-install-pycharm-on-linux-mint-and-ubuntu/

To ensure Python interpreter is working on your machine, run this command: python -V

Since, we are on a Linux machine, Python is preinstalled on our machine.

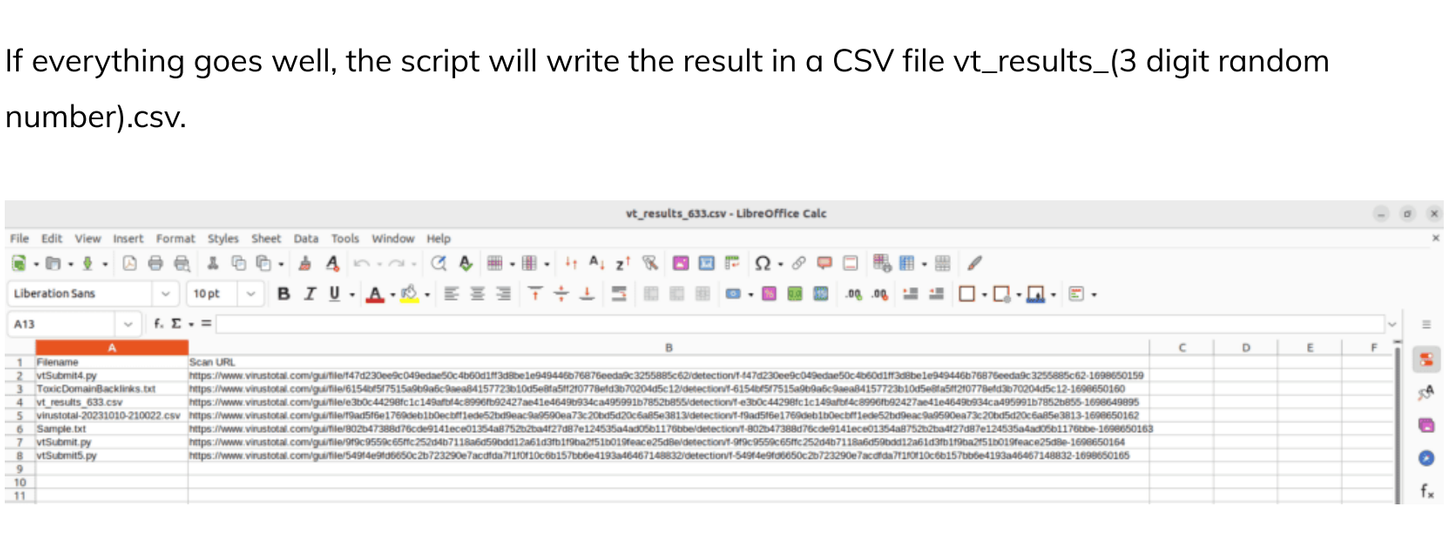


Step 4: Run the Python script to Submit multiple files to VirusTotal

Now, all set to run the script. As soon as you run the script, it prompts to enter API key and directory path in that files to be uploaded are saved. Be ready with the API key and a directory with all the files to submit.

To run the script: **python3 vtSubmit.py**

If everything goes well, the script will write the result in a CSV file vt_results_(3 digit random number).csv.



Conclusion

Analyzing tons of files is repetitive, monotonous, time-consuming, and cumbersome. We can automate this task by submitting multiple files to VirusTotal using these scripts.

The main advantages of using this program are:

1. It's faster than humans.
2. It's error-free.
3. No human intervention is required.
4. Fully automated.

Attackers' ultimate goal is to deliver and execute malware on victim machines by any means. Conversely, security professionals' ultimate goal is to protect their organizations from such malware hidden inside legitimate files. Combining VirusTotal API services with scripts allows us to reap the advantages to the greatest extent.

Using the VirusTotal public APIs and this Python script, security teams can easily submit hundreds of files for antivirus scanning automatically. This quickly analyzes potential malware samples and suspicious files at scale, accelerating threat detection and response. Automation empowers understaffed security teams to focus their time on higher value tasks while still systematically reviewing a massive volume of files.

We hope this article helped in understanding how to submit multiple files to VirusTotal to get the files scanned with more than 70 antivirus engines. Thanks for reading this post. Please share this post and help secure the digital world. Visit our website, thesecmaster.com, and our social media page on Facebook, LinkedIn, Twitter, Telegram, Tumblr, Medium, and Instagram and subscribe to receive updates like this.

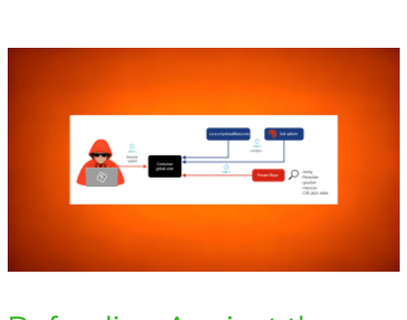
- Exploring VirisTotal: Online Malware Scanning Tool for Security Analysts (SOC Analyst)
- How to Scan Bulk IOCs with VirusTotal?
- MSBuild Fileless Malware Campaign
- How to Check Certificate, CSR, and Private Key with OpenSSL?
- Create CSR On Windows Server

See Also How To Fix Digital Signature Spoofing Vulnerabilities In LibreOffice- CVE-2021-25633, CVE-2021-25634, CVE-2021-25635?

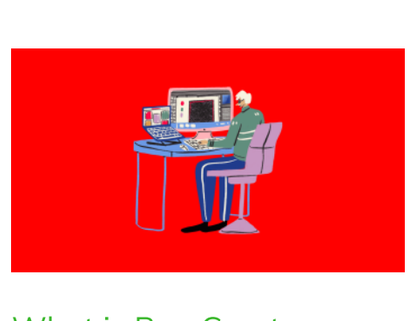
Similar Posts:

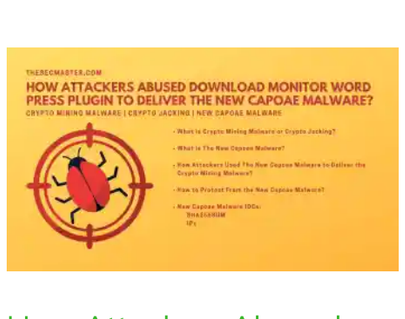

A New Security Evasion Technique- MalDoc in PDF


How MosaicLoader Malware Evade Security Detection?


Defending Against the Deceptive LABRAT Campaign

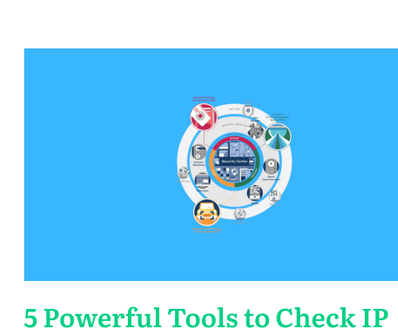

How to Protect Your WordPress Website From Redirect Malware Campaign


What is PureCrypter Malware? How Does PureCrypter Malware Work?


How Attackers Abused Download Monitor Word Press Plugin To Deliver The New Capoae Malware?

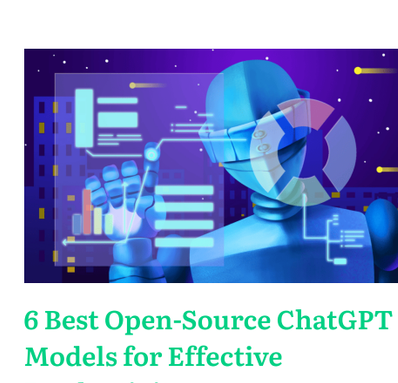
Read More:


Apple Boosts iMessage Security with Contact Key Verification


5 Powerful Tools to Check IP and URL Reputation


How to Fix CVE-2023-20238- An Authentication Bypass Vulnerability in Cisco BroadWorks?


How to Fix CVE-2023-0286- A Type Confusion Vulnerability in OpenSSL?


6 Best Open-Source ChatGPT Models for Effective Productivity

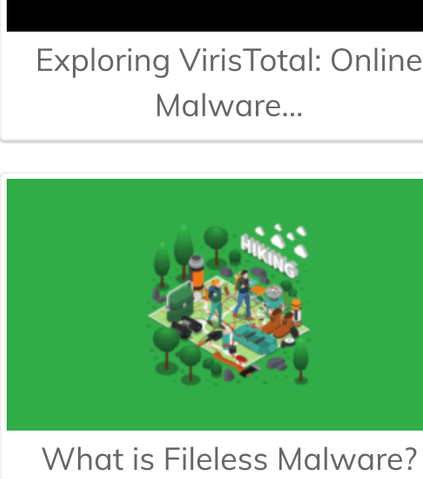

Three Security Vulnerabilities In The Audio Decoders Affects Millions Of Android Devices

Keep Exploring

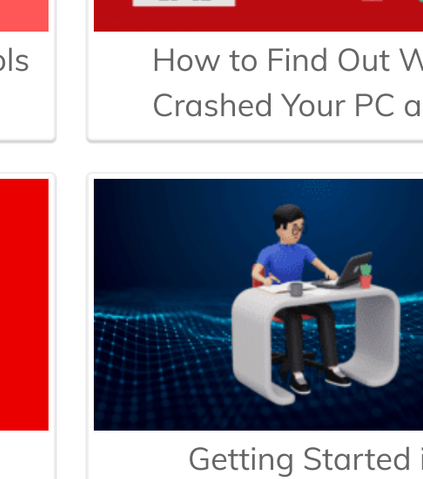

Exploring VirisTotal: Online Malware...


100 Malware Analysis Tools To Identify Malware


How to Find Out What Crashed Your PC and...


What is Fileless Malware? How to Protect...


The Ultimate Guide to Cybersecurity: How...


Getting Started in Cybersecurity Careers:...

About the author

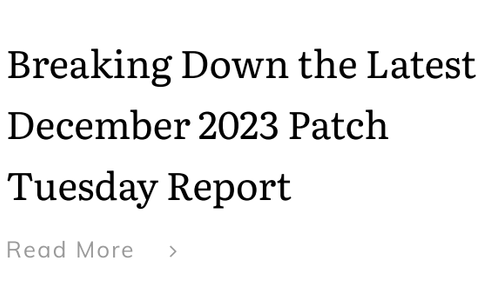
Arun KL

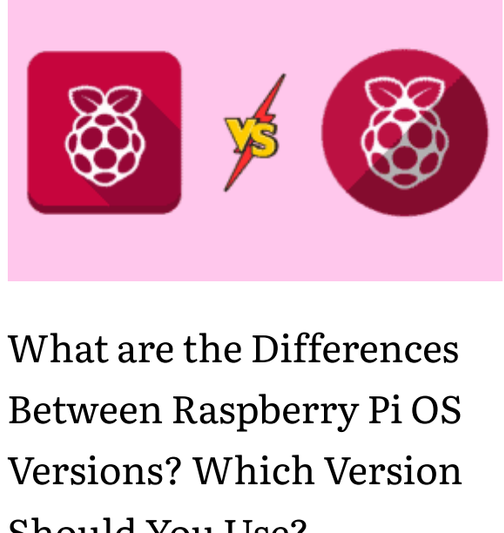
Arun KL is a cybersecurity professional with 15+ years of experience spanning IT infrastructure, cloud security, vulnerability management, Penetration Testing, security operations, and incident response. He is adept at designing and implementing robust security solutions to safeguard systems and data. Arun holds multiple industry certifications including CCNA, CCNA Security, RHCE, CEH, and AWS Security.

To know more about him, you can visit his profile on LinkedIn.

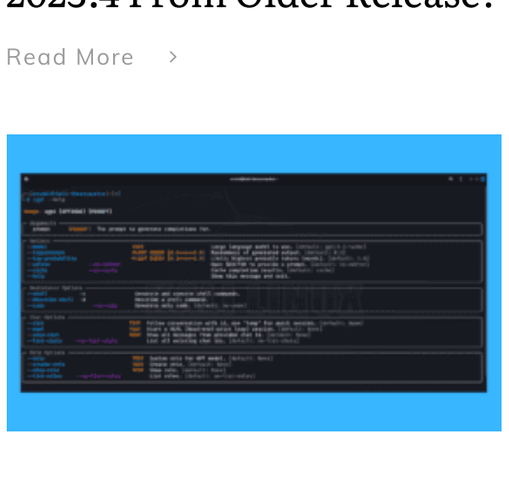
Type here...

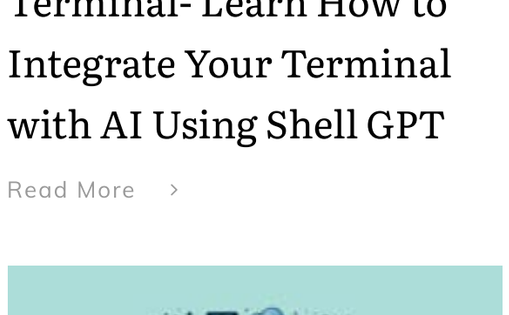
Recent Posts

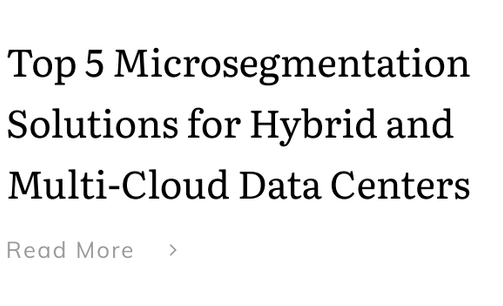

Breaking Down the Latest December 2023 Patch Tuesday Report
Read More


What are the Differences Between Raspberry Pi OS Versions? Which Version Should You Use?
Read More


What Is New in Kali Linux 2023.4? And, How to Upgrade Kali Linux to 2023.4 From Older Release?
Read More


Bring AI on Your Terminal- Learn How to Integrate Your Terminal with AI Using Shell GPT
Read More


Top 5 Microsegmentation Solutions for Hybrid and Multi-Cloud Data Centers
Read More


How to Choose the Right Microsegmentation Solution for Your Business?
Read More

Follow us