

Simple Antivirus Scanner

This application scans files and folders for malware using the VirusTotal API. It calculates the MD5 hash of files and checks them against VirusTotal to determine if they have been flagged as malware by any antivirus engines. The script can run in a default mode providing concise detection summaries, or with detailed output including comprehensive malware reports when specified.

Features

- Scans individual files or entire folders recursively.
- Uses MD5 hashing to check files against VirusTotal database.
- Optional detailed malware report via the VirusTotal API.

Installation

Prerequisites

- Python 3.x
- pip (Python package installer)

Dependencies

Install all required dependencies by running the following command in the root directory of this project:

```
pip install -r requirements.txt
```

This will install the following Python package:

- **requests** for making HTTP requests to the VirusTotal API.

Obtaining and Configuring the VirusTotal API Key

Obtaining the API Key

1. Create an Account:

- Visit [VirusTotal](#).
- Sign up for an account by providing your email address and creating a password.

2. Get the API Key:

- Once registered, log in to your VirusTotal account.
- Navigate to your profile settings.
- Find the API key section and copy your API key.

Configuring Your Application

Replace the API key placeholder in the script with your actual VirusTotal API key:

```
API_KEY = 'YOUR_VIRUSTOTAL_API_KEY_HERE'
```

Replace 'YOUR_VIRUSTOTAL_API_KEY_HERE' with the API key you obtained from VirusTotal.

Usage

To use this script, you need a valid VirusTotal API key set up as described above.

Basic Command

```
python malware_scan.py <path_to_scan>
```

This command will scan the specified file or directory and provide a summary report of any detections.

Detailed Report

```
python malware_scan.py <path_to_scan> -m
```

Use the `-m` option to get detailed information about detected malware, including the detection date and detailed results from various antivirus engines.

Script Functions

`get_file_report(resource)`

Fetches the report of a file based on its MD5 hash from the VirusTotal API.

- **Parameters:**
 - `resource`: MD5 hash of the file.
- **Returns:**
 - JSON response from the VirusTotal API or `None` if no data is available.

`scan_file(filepath, detailed)`

Calculates the MD5 hash of a file, queries the VirusTotal API, and prints the result.

- **Parameters:**
 - `filepath`: Path to the file to scan.
 - `detailed`: Boolean flag to determine whether to print detailed information.

`scan_folder(folder_path, detailed)`

Recursively scans all files in a folder.

- **Parameters:**

- `folder_path`: Path to the folder to scan.
- `detailed`: Boolean flag for detailed output.

`main()`

Parses command line arguments and initiates file or folder scanning based on the input.

Contributing

Contributions to this project are welcome. Please fork the repository and submit a pull request with your improvements.

License

Specify your license or leave this blank if you have not decided on one.