KEYLOGGER DETECTOR WITH VIRUSTOTAL

This Python script is designed to detect keylogger-like behavior on a Windows machine using **YARA rules, VirusTotal hash checks, and process scanning**. It also supports interval-based scanning and custom YARA rule files for extended flexibility.

Features

- Scans running processes for suspicious activity

- Heuristics based on process names and PE imports

- YARA-based rule scanning

- VirusTotal API integration for file hash checking

- Interval-based continuous monitoring

- Custom YARA rules via command-line

Requirements

Ensure Python 3.x is installed.

Install dependencies:

pip install psutil yara-python requests python-dotenv pefile argparse datetime

Directory Structure:

```
KEYLOGGER_DETECTOR_WITH_VIRUSTOTAL/
        detectiontesting.exe            # Compiled suspicious keylogger binary (for testing)
        keylogger_rules.yar             # Default YARA rules
        keylogger_detector_with_virustotal.py   # Main detection script
        test_keylogger.c                # Keylogger C source code (for simulation)
       .gitignore
        README.md
```

Simulating Keylogger Behavior:

To test this project, follow these steps:

1. Compile the Suspicious C File

Use GCC or MinGW or Visual Studio:

```
gcc test_keylogger.c -o detectiontesting.exe
```

2. Run the Keylogger Test Executable in terminal:

```
detectiontesting.exe
```

This will simulate keylogger behavior that your detector script can identify.

Running the Detection Script

Show Help Menu:

```
python keylogger_detector_with_virustotal.py -h
```

Basic Usage:

```
python keylogger_detector_with_virustotal.py
```

Run with Interval-Based Scanning (every 60 seconds):

```
python keylogger_detector_with_virustotal.py -i 60
```

Run with Custom YARA Rule File:

```
python keylogger_detector_with_virustotal.py -r keylogger_rules.yar
```

Full Example:

```
python keylogger_detector_with_virustotal.py -i 100 -r custom_rules.yar
```

VirusTotal API Key Setup:

Get your free API key from https://virustotal.com

Create a .env file in the same directory and add your key:

```
VT_API_KEY=your_virustotal_api_key_here
```