Scanner.py

User Documentation

By Robert Blanchett

Introduction

Scanner.py is a Command-line tool that polls the VirusTotal.com API, reporting on the URLs, Filehashes (SHA1-256 and md5), Fully Qualified Domain Names the user supplies

The tool returns a small number (three) of datum: the number of reports in various categories (Malicious, Harmless, etc) by dozens of Anti-Virus engines that are maintained by Virus Total.

A Virus Total API key is Required for the service to accept requests.

You can obtain one for free (subjust to rate and usage limitations) at

To see the a complete report of the information on offer, sample the Virus Total Web interface at VT Web Interface

Virus Total offer a Premium API with access to more information

Current Limitations

Currently the tool only reports on URLs submitted to Virus Total.

Future Releases will allow querying of filehashes and FQDN (Fully Qualified Domain Names)

Installation

1. Download and Copy scanner.py into a directory in your Computer, preferably one in your PATH.
   at Holmesglen this is "%USERPROFILE%\AppData\Local\Microsoft\WindowsApps".

on Linux ~/.local/bin is recommended.

2. on Linux, issue "chmod u+x scanner.py" to allow the script to be executable
3. on either windows or linux, issue "pip install vt-py validators"

This will install the needed modules from PyPI, the Python Package Index.

4. Having obtained your VirusTotal API key, edit scanner.py and place your API key in the line beginning:
   VTAPIKEY, replacing the dummy key on that line in the publically distributed file.
5. You're Ready to go!

First Run

Before doing anything else run "scanner.py init"

This will initialise the configuration file called ".scanrc"

Querying VirusTotal

1. Prepare one or more plaintext files containing the URLs you wish to scan.

   they MUST contain one and **only** one item per line (currently only URLs)

   eg:

   `http://www.news.com.au`

   `https://badsite.ru/malware.vbs`

   `http://hellosailor.xxx/`

A Sample Run

```
C:\Users\User\Documents>scanner.py scan test1.txt

Internet available. Continuing.

processing supplied files.
test1.txt

please wait. VirusTotal limits requests to 4/minute.
and so does this script!

5 items to be validated before scanning.

['8.8.8.8', 'google.com', 'C:\\Windows\\System32\\cmd.exe', 'https://annzon-tkshlf-co-jp.mvoxhsd.buzz/', 'X5O!P%@AP[4\\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*']

Previous Runs 8

Submitting Url:  https://annzon-tkshlf-co-jp.mvoxhsd.buzz/

Scanner run 9 Report Saturday, 07 Aug 19:00
The number of virus products and how the URL was reported by them.
Results from The VirusTotal.com Public API

URL: https://annzon-tkshlf-co-jp.mvoxhsd.buzz/
harmless    : 67
malicious   : 10
suspicious  : 2
undetected  : 10
timeout     : 0

C:\Users\User\Documents>
```