VirusTotal Scanning

VirusTotal is a website that provides a scanning service for files. This can also be done through their public API (<https://www.virustotal.com/en/documentation/public-api/>). The python script driver\_virus\_test.py is the script that will be scanning the ‘exe’ files that may be falsely flagged for malware/viruses. This script should be run in the CLI/terminal:

`python driver\_virus\_test.py <parameters>`

It accepts three (3) parameters and requires a couple libraries and files to function.

* Parameters: <Customer> <Release> <Build>

- Customer: [Customer\_Kits|Default]

- Release: xx.x (ex. 02.2, 05.4, 11.4, etc.)

- Build: xx.x. xx (ex. 11.4.16)

- Required Libraries: ConfigObj, requests

- ConfigObj: Download tarball, unzip, and execute `python setup.py install` in CLI/terminal <https://pypi.python.org/pypi/configobj/5.0.5>

- requests: Follow installation instructions <http://docs.python-requests.org/en/latest/user/install/>

* Required Files: virus\_total.cfg, postfile.py

- virus\_total.cfg: api\_key, [CustomerKit], [FileList], [AntivirusList]

api\_key: Key used to request scans (must NEVER be changed)

[CustomerKit]: Section containing list of installers scanned for the Customer Kit

[FileList]: List of drivers/installers all other OEMs need scanned (must be updated)

[AntivirusList]: List of significant antivirus software (update as needed)

- postfile.py: Handles file scan and report retrieval requests.

Output -

The runtime output of the script should be a stream (usually slow) of messages describing what is being done. Runtime errors will be displayed as a traceback followed by a generic error message and will only kill the thread in which the error occurs; each file being scanned is done so on its own thread. For each file that Virus Total suspects of being malicious, a text file containing a list of the antiviruses that detected the problem as well as the possible threat will be generated. If Virus Total does not detect anything malicious about the file in question nothing will be generated.