VT HUNTING - IOC updater

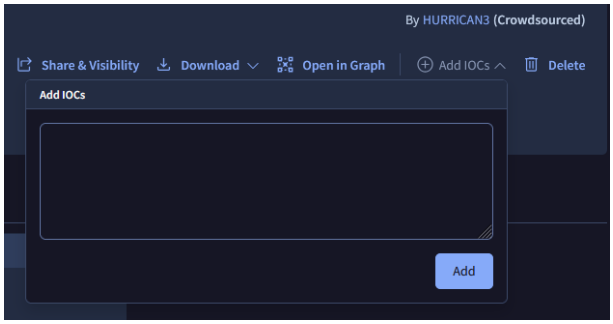
User guide - by HURRICAN3

Contents

1 Introduction

The IOC Updater tool stems from the need to update collections (hereinafter referred to as collections) of indicators of compromise (hereinafter referred to as IOCs) that can be created on the well-known VirusTotal platform.

Basically, IOCs can be manually inserted into a collection via the web interface as shown below:



However, this may be inconvenient in the case of long IOC lists with particular formats.

This script attempts to mitigate this problem by facilitating the insertion of IOCs manually or from files directly from the CLI.

2 Installation and prerequisites

Three modules are currently required for the script to run properly:

- **requests**: used for interaction with VirusTotal via API
- **datetime**: part of standard library
- **getpass**: part of standard library

To install the **requests** module, simply run the command:

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

3 Script usage

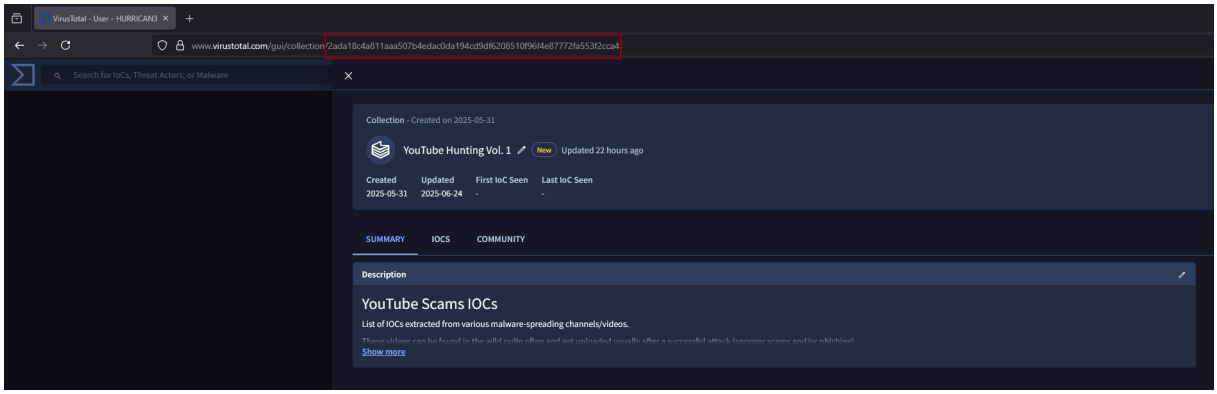
The use of the script consists of 3 basic steps:

- Choice of collection
- API key insertion
- IoC insertion

3.1 Choice of collection

The first input required is the collection in which you intend to insert an IOC.

To proceed, the collection ID is required, which can be obtained from the URL of the collection's VirusTotal page:

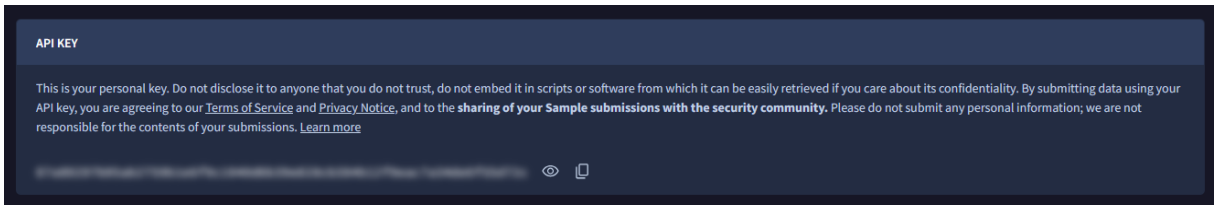


After the ID and API key have been entered, a first API call will be made to verify the actual existence of the collection, printing details such as name, description and number of items in the collection.

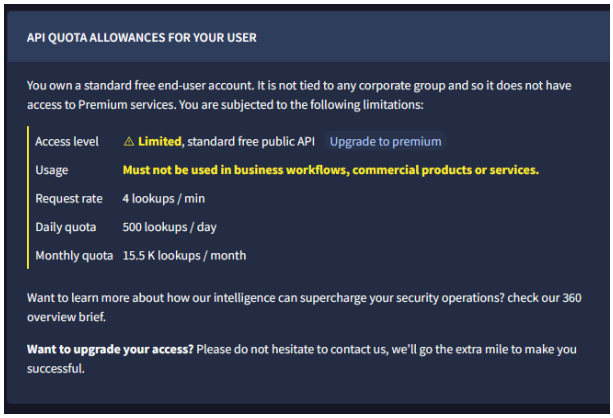
Subsequent versions of the script will evaluate the possibility of hardcoding the collection ID in order to avoid repeated inputs at start-up.

3.2 API key insertion

The second input required is the API key, which you can obtain from your VirusTotal profile as shown below:



It is important to emphasise that the use of this tool with free APIs is forbidden in production environments, commercial products and services:



During the creation of the script only public APIs and personal collections have been tested.

In subsequent versions of the script will evaluate the possibility of hardcoding the API key in order to avoid repeated inputs at start-up.

3.3 IOC insertion

After verifying the existence of the collection entered and the correctness of the API key, it is possible to enter the IOCs.

Currently, the IOCs supported by VirusTotal collections are of four types:

- **Files** with MD5, SHA-1 and SHA-256
- **URLs**
- **Domains**
- **IPs**

Two input modes are possible, typing the correct word as indicated by the terminal:

- **Manual**: insertion of one IOC at a time, or several IoCs separated by commas
- **From file**: you can provide the path to a text file where the IOCs are located.

  In this mode, IOCs can be present all on one line separated by commas or one per line