VT HUNTING - IOC updater

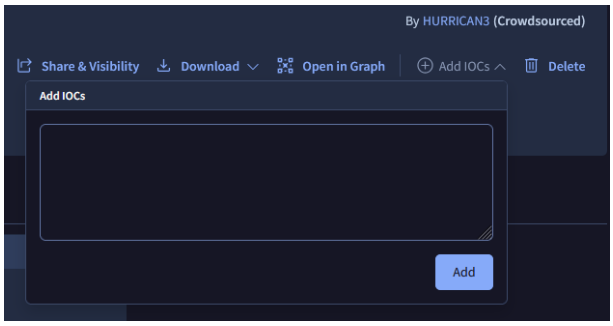
Guida all'uso - by HURRICAN3

Contents

1 Introduzione

Il tool IOC Updater nasce dall'esigenza di aggiornare collezioni (di seguito collection) di indicatori di compromissione (di seguito IoC) realizzabili sulla nota piattaforma VirusTotal.

Di base è possibile inserire manualmente gli IOC in una collection attraverso l'interfaccia web come mostrato di seguito:



Tuttavia questo può risultare scomodo in caso di liste di IoC con formati particolari o molto lunghe.

Il presente script cerca di mitigare questo problema agevolando l'inserimento di IoC in maniera manuale o da file direttamente da CLI.

2 Installazione e prerequisiti

Attualmente sono necessari 3 moduli per il corretto funzionamento dello script:

- **requests**: impiegato per l'interazione con VirusTotal attraverso API
- **datetime**: parte della standard library
- **getpass**: parte della standard library

Per installare il modulo **requests** è sufficiente lanciare il comando:

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

3 Uso dello script

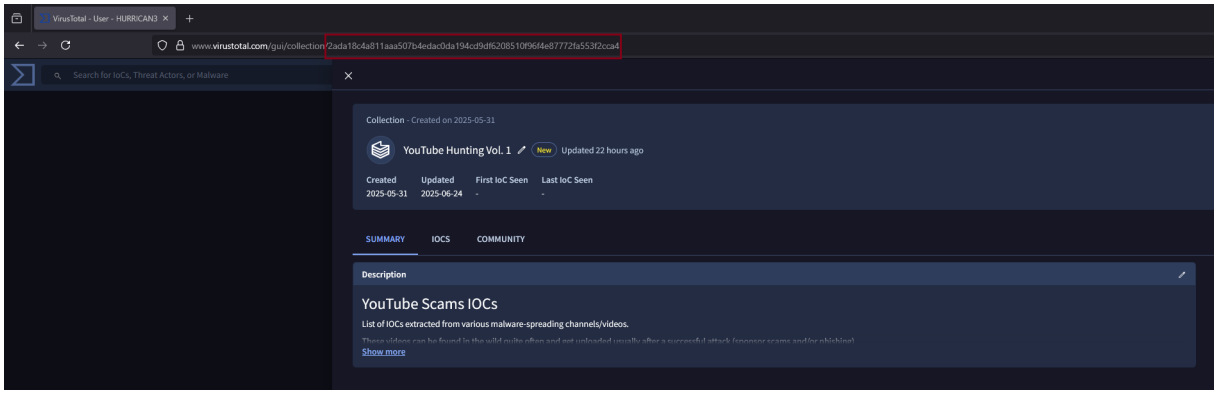
L'uso dello script si articola in 3 passi fondamentali:

- Scelta della collection
- Inserimento della chiave API
- Inserimento degli IoC

3.1 Scelta della collection

Il primo input richiesto è la collection in cui si intende inserire un IoC.

Per procedere è richiesto l'ID della collection, ottenibile dall'URL della pagina VirusTotal:

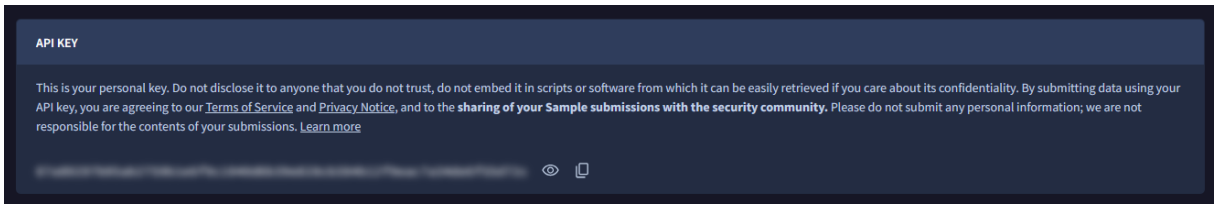


Dopo l'inserimento dell'ID e della chiave API, verrà effettuata una prima chiamata API per verificare l'effettiva esistenza della collection, stampando dettagli quali nome, descrizione e numero di elementi presenti al suo interno.

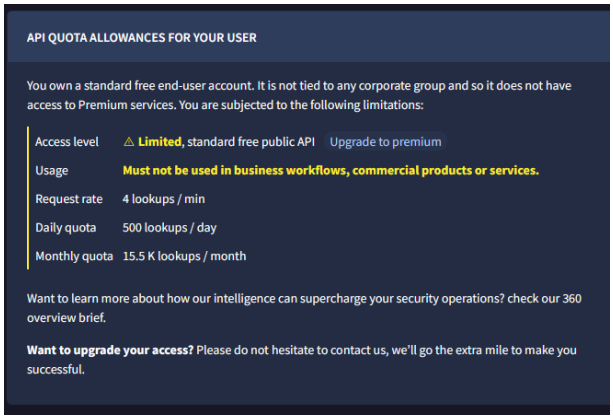
Nelle successive versioni dello script verrà valutato l'hardcoding dell'ID della collection al fine di evitare inserimenti ad ogni avvio.

3.2 Inserimento della chiave API

Il secondo input richiesto è la propria chiave API, ottenibile dal proprio profilo VirusTotal come mostrato di seguito:



È importante sottolineare come l'uso del presente strumento con API gratuite sia vietato in ambienti di produzione, prodotti commerciali e servizi:



L'uso del presente script con API gratuite è stato limitato a collezioni personali non volte ad attività lavorative.

Nelle successive versioni dello script verrà valutato l'hardcoding della chiave API al fine di evitare inserimenti ad ogni avvio.

3.3 Inserimento degli IoC

Dopo aver verificato l'esistenza della collection inserita e la correttezza della chiave API, è possbile inserire gli IoC.

Attualmente, gli IOC supportati dalle collection di VirusTotal sono di 4 tipi:

- **File** tramite MD5, SHA-1 e SHA-256
- **URLs**
- **Domini**
- **IPs**

Sono possibili due modalità d'inserimento, scrivendo la parola corretta come indicato da terminale:

- **Manuale**: inserimento di un IoC alla volta, oppure di più IoC separati da virgole
- **Da file**: è possibile fornire il path di un file testuale dove sono presenti gli IoC.

  Con questa modalità d'inserimento gli IoC possono essere presenti tutti su una riga oppure uno per riga