



PulseDive Lookup v0.1b Documentation

OVERVIEW

PulseDive (pulsedive.com / @pulsedive) is a free Cyber Threat Intelligence platform that:

- Aggregates IOCs from its' community members and OSINT feeds
- Enriches IOCs by performing WHOIS requests and active DNS resolutions
- Probes IOCs by sending HTTP GET requests to collect additional valuable data like HTTP headers, SSL certificate information, and redirects

PulseDive offers great web-based interface for Cyber Threat Intel and IT Security analysts. PulseDive also offers APIs that can be used for integrations with SIEM tools and etc.

PulseDive-Lookup.ps1 is a PowerShell script that leverages PulseDive API for bulk IPs/Domains lookups.

HOW IT WORKS

1. Save list of IPs/Domains in the Input.csv file. Square brackets around dots are optional.

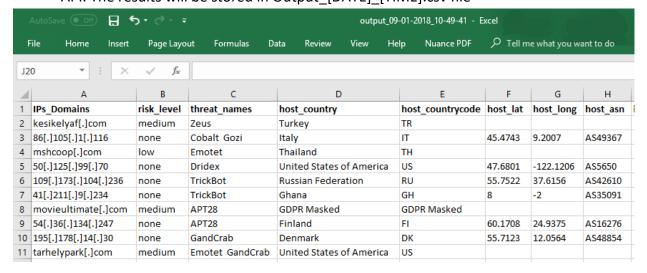
4	А
1	Input
2	kesikelyaf.com
3	86.105.1.116
4	mshcoop[.]com
5	50[.]125[.]99[.]70
6	109[.]173[.]104[.]236
7	41[.]211[.]9[.]234
8	movieultimate[.]com
9	54[.]36[.]134[.]247
10	195[.]178[.]14[.]30
11	tarhelypark[.]com

2. Execute "PulseDive-Lookup.ps1" PowerShell script

```
PS C:\PulseDive-PS> & "C:\PulseDive-PS\PulseDive-Lookup.ps1"
Importing IPs/Domains for look up from: C:\PulseDive-PS\input.csv
#1 Looking up: kesikelyaf.com
#2 Looking up: 86.105.1.116
#3 Looking up: mshcoop.com
#4 Looking up: 50.125.99.70
#5 Looking up: 109.173.104.236
#6 Looking up: 41.211.9.234
#7 Looking up: movieultimate.com
#8 Looking up: 54.36.134.247
#9 Looking up: 195.178.14.30
#10 Looking up: tarhelypark.com
C:\PulseDive-PS\output_09-01-2018_10-49-41.csv
PS C:\PulseDive-PS\
```



3. Script will grab all IOCs from Input.csv one-by-on and will look them up using PulseDive API. The results will be stored in Output [DATE] [TIME].csv file



4. Done!

CONFIGURATIONS

2. Update variable \$home_dir to define location where Input and Output .csv files will be located

#Change home_dir value to define home directory for input and output .csv files \$home dir = "C:\PulseDive-PS\"

PulseDive's Free Tier API has 30 request per min & 500 request per hour limitations





Default values of variables \$delay_between_calls & \$hr_pause_after throttle down speed of lookups to stay within the free limits of PulseDive API. Update those variables accordingly for paid plans.

```
#Throtle-Down Configuration
#2 second delay between API calls to stay under <30 Calls/Min for Free PulseDive API plan
$delay_between_calls = 0
#1 hour pause after 500 calls/hour for Free PulseDive API plan
$hr_pause_after = 500
#Throtle-Down Configuration can be updated accordingly for paid plans</pre>
```

4. If you'll get errors related to "Invoke-WebRequest", run the following commands:

```
#PS C:\> $AllProtocols = [System.Net.SecurityProtocolType]'Ssl3,Tls,Tls11,Tls12'

#PS C:\> [System.Net.ServicePointManager]::SecurityProtocol = $AllProtocols

#PS C:\> (Invoke-WebRequest -Uri "https://idp.safenames.com/").StatusCode
```

Point Of Contact

Evgueni Erchov

Kivu Consulting, Inc | Cyber Investigations

E: EErchov@KivuConsulting.com

T: @EErchov