Kivu Consulting, Inc.
44 Montgomery Street
Suite 700
San Francisco, CA 94104
415.524.7320
kivuconsulting.com

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.

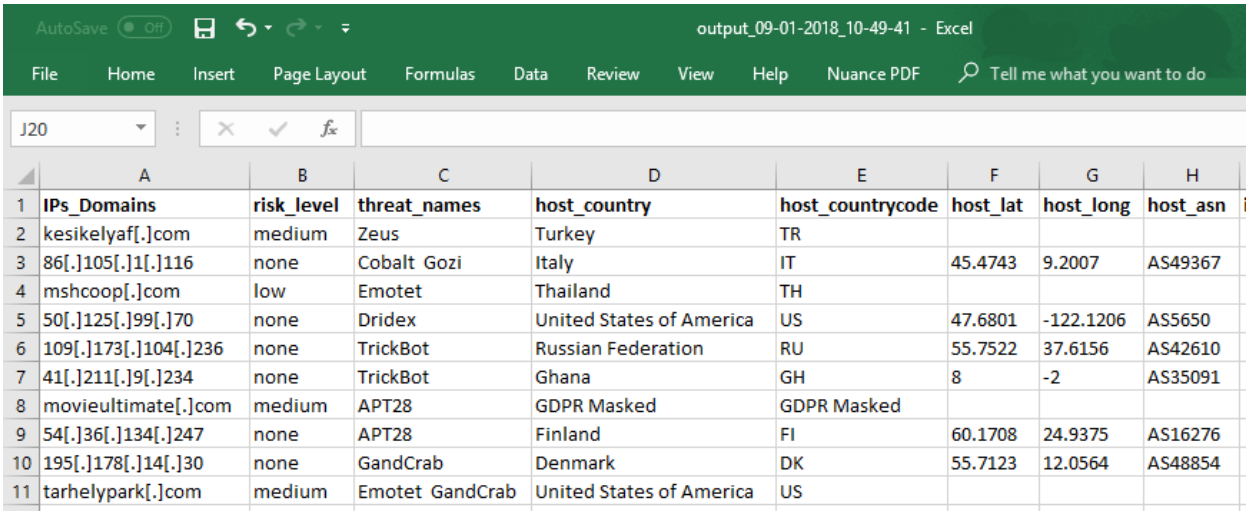
	A
1	Input
2	kesikelyaf.com
3	86.105.1.116
4	mshcoop[.]com
5	50[.]125[.]99[.]70
6	109[.]173[.]104[.]236
7	41[.]211[.]9[.]234
8	movieultimate[.]com
9	54[.]36[.]134[.]247
10	195[.]178[.]14[.]30
11	tarhelypark[.]com

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>
```

Kivu Consulting, Inc.
44 Montgomery Street
Suite 700
San Francisco, CA 94104
415.524.7320
kivuconsulting.com

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



	A	B	C	D	E	F	G	H
1	**IPs_Domains**	**risk_level**	**threat_names**	**host_country**	**host_countrycode**	**host_lat**	**host_long**	**host_asn**
2	kesikelyaf[.]com	medium	Zeus	Turkey	TR			
3	86[.]105[.]1[.]116	none	Cobalt Gozi	Italy	IT	45.4743	9.2007	AS49367
4	mshcoop[.]com	low	Emotet	Thailand	TH			
5	50[.]125[.]99[.]70	none	Dridex	United States of America	US	47.6801	-122.1206	AS5650
6	109[.]173[.]104[.]236	none	TrickBot	Russian Federation	RU	55.7522	37.6156	AS42610
7	41[.]211[.]9[.]234	none	TrickBot	Ghana	GH	8	-2	AS35091
8	movieultimate[.]com	medium	APT28	GDPR Masked	GDPR Masked			
9	54[.]36[.]134[.]247	none	APT28	Finland	FI	60.1708	24.9375	AS16276
10	195[.]178[.]14[.]30	none	GandCrab	Denmark	DK	55.7123	12.0564	AS48854
11	tarhelypark[.]com	medium	Emotet GandCrab	United States of America	US			

4. Done!

CONFIGURATIONS

1. Register for a free account on PulseDive.com and get API key associated with your profile. Update $pulsedive_api_key variable in PulseDive-Lookup.ps1 with your key

```
#Register for a free account & get API key associated with your account
$pulsedive_api_key = "12121212121212121212121212121212121212121212121212121212121212121"
```

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\"
```

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

Kivu Consulting, Inc.
44 Montgomery Street
Suite 700
San Francisco, CA 94104
415.524.7320
kivuconsulting.com

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
```

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