fn_URLhaus

Introduction

This function incorporates APIs available from URLhaus (https://urlhaus.abuse.ch/) to enrich data on:

- urls
- domains
- IP Addresses
- MD5 and SHA-256 Hash
- tags (ex. Troldesh)

It also includes the capability to submit a url as distributing malware to a public searchable database.

This package include 2 functions, 2 workflows and 2 example rules.

Installation

To install in "development mode"

```
pip install -e ./fn_urlhaus/
```

or to the python libraries

```
pip install fn_urlhaus-1.0.0.tar.gz
```

To configure `app.conf` and update with your settings, run

```
resilient-circuits config [-c or -u] -l fn-urlhaus
```

To load Resilient with all the object definitions needed for use, run

```
resilient-circuits customize -l fn-urlhaus
```

After installation, the package will be loaded and executed with `resilient-circuits run`.

To uninstall:

```
pip uninstall fn-urlhaus
```

Results

The resulting data is placed in an incident note for review. Your process may parse and process the data differently. Below are sample results from different queries:

URLs

```
{
  u'larted': u'true',
  u'urlhaus_reference': u'https://urlhaus.abuse.ch/url/163113/',
  u'url_status': u'online',
  u'payloads': [
    {
      u'firstseen': u'2019-03-20',
      u'filename': None,
      u'content_type': u'elf',
      u'signature': None,
      u'virustotal': {
        u'result': u'31 / 55',
        u'link': u'https://www.virustotal.com/file/a04ac6d98ad989312783d4fe3456c53730
b212c79a426fb215708b6c6daa3de3/analysis/1553114950/',
        u'percent': u'56.36'
      },
      u'response_md5': u'9b6c3518a91d23ed77504b5416bfb5b3',
      u'response_size': u'80280',
      u'response_sha256': u'a04ac6d98ad989312783d4fe3456c53730b212c79a426fb215708b6c6
daa3de3',
      u'urlhaus_download': u'https://api.urlhaus.abuse.ch/v1/download/a04ac6d98ad9893
12783d4fe3456c53730b212c79a426fb215708b6c6daa3de3/'
    }
  ],
  u'blacklists': {
    u'surbl': u'not listed',
    u'gsb': u'not listed',
    u'spamhaus_dbl': u'not listed'
  },
  u'query_status': u'ok',
  u'reporter': u'zbetcheckin',
  u'url': u'http://46.121.26.229:33107/.i',
  u'tags': [
    u'elf',
    u'hajime'
  ],
  u'date_added': u'2019-03-20 22:22:11 UTC',
  u'host': u'46.121.26.229',
  u'takedown_time_seconds': None,
  u'id': u'163113',
  u'threat': u'malware_download'
}
```


Hashes

```
{
  u'sha256_hash': u'bde429df1f93e30af80c336d375ee9a014ea8b76266092f292a76abfcce9588d'
,
  u'firstseen': u'2019-03-20 19:26:32',
  u'lastseen': u'2019-03-21 00:04:11',
  u'urls': [
    {
      u'firstseen': u'2019-03-20',
      u'lastseen': u'2019-03-21',
      u'urlhaus_reference': u'https://urlhaus.abuse.ch/url/163046/',
      u'filename': None,
      u'url_status': u'online',
      u'url_id': u'163046',
      u'url': u'http://fretarget.cf/new.exe'
    }
  ],
  u'md5_hash': u'68ab4ce40dcb00aea21e13427547b0e3',
  u'content_type': u'exe',
  u'signature': None,
  u'query_status': u'ok',
  u'virustotal': {
    u'result': u'32 / 68',
    u'link': u'https://www.virustotal.com/file/bde429df1f93e30af80c336d375ee9a014ea8b
76266092f292a76abfcce9588d/analysis/1552756543/',
    u'percent': u'47.06'
  },
  u'file_size': u'884826',
  u'url_count': u'1',
  u'urlhaus_download': u'https://api.urlhaus.abuse.ch/v1/download/bde429df1f93e30af80
c336d375ee9a014ea8b76266092f292a76abfcce9588d/'
}
```


IP Addresses

```
{
  u'firstseen': u'2019-03-20 22:22:07 UTC',
  u'urlhaus_reference': u'https://urlhaus.abuse.ch/host/46.121.26.229/',
  u'urls': [
    {
      u'date_added': u'2019-03-20 22:22:11 UTC',
      u'larted': u'true',
      u'urlhaus_reference': u'https://urlhaus.abuse.ch/url/163113/',
      u'url_status': u'online',
      u'reporter': u'zbetcheckin',
      u'takedown_time_seconds': None,
      u'id': u'163113',
      u'threat': u'malware_download',
      u'url': u'http://46.121.26.229:33107/.i',
      u'tags': [
        u'elf',
        u'hajime'
      ]
    }
  ],
  u'blacklists': {
    u'surbl': u'not listed',
    u'spamhaus_dbl': u'unknown_return_code'
  },
  u'query_status': u'ok',
  u'host': u'46.121.26.229',
  u'url_count': u'1'
}
```


Domains

```
{
  u'firstseen': u'2019-03-20 19:26:19 UTC',
  u'urlhaus_reference': u'https://urlhaus.abuse.ch/host/fretarget.cf/',
  u'urls': [
    {
      u'date_added': u'2019-03-20 19:26:33 UTC',
      u'larted': u'true',
      u'urlhaus_reference': u'https://urlhaus.abuse.ch/url/163046/',
      u'url_status': u'online',
      u'reporter': u'Techhelplistcom',
      u'takedown_time_seconds': None,
      u'id': u'163046',
      u'threat': u'malware_download',
      u'url': u'http://fretarget.cf/new.exe',
      u'tags': None
    }
  ],
  u'blacklists': {
    u'surbl': u'listed',
    u'spamhaus_dbl': u'abused_legit_malware'
  },
  u'query_status': u'ok',
  u'host': u'fretarget.cf',
  u'url_count': u'1'
}
```


Tags

```
{
  u'firstseen': u'2018-09-20 16:56:05',
  u'lastseen': u'2019-03-21 20:04:03',
  u'urls': [
    {
      u'urlhaus_reference': u'https://urlhaus.abuse.ch/url/163698/',
      u'url_status': u'online',
      u'reporter': u'zbetcheckin',
      u'threat': u'malware_download',
      u'url_id': u'163698',
      u'dateadded': u'2019-03-21 20:02:09',
      u'url': u'http://thebackslant.com/wordpress/wp-admin/css/colors/blue/gr.mpwq'
    },
    {
      u'urlhaus_reference': u'https://urlhaus.abuse.ch/url/163687/',
      u'url_status': u'online',
      u'reporter': u'zbetcheckin',
      u'threat': u'malware_download',
      u'url_id': u'163687',
      u'dateadded': u'2019-03-21 19:43:08',
      u'url': u'http://jornalvisao.net/templates/beez3/css/gr.mpwq'
    }
  ],
  u'query_status': u'ok',
  u'url_count': u'2'
}
```


No results


```
{u'query_status': u'no_results'}
```