apiosintDS

Release 1.8.3

Jul 07, 2023

Contents

CHAPTER 1

apiosintDS

Latest stable release is **v1.8** (*Changelog*)

apiosintDS is a python client library for public *API* lookup service over *OSINT* IoCs stored at DigitalSide Threat-Intel repository. It can be defined a **service as a library** tool designed to act both as a standard Python library to be included in your own Python application and as command line tools. Query can be performed against souspicious IPs, domains and urls. Data stored has a 7 days retention.

DigitalSide Threat-Intel shares a set of **Open Source Cyber Threat Intellegence** information, monstly based on malware analysis and compromised URLs, IPs and domains. The purpose of the project is to develop and test new wayes to hunt, analyze, collect and share relevants sets of IoCs to be used by SOC/CSIRT/CERT with minimun effort.

This library has been specially designed for people and organizations don't want to import the whole DigitalSide Threat-Intel dataset and prefer to use it as on demand service.

1.1 Welcome to apiosintDS's documentation!

Documentation contents

1.1.1 Installation guide

Install python > 3.5.2

Make sure you installed on your system python > 3.5.2. Try typing `python3` on your terminal.

```
~$ python3
Python 3.6.8 (default, Oct  7 2019, 12:59:55)
[GCC 8.3.0] on linux
Type "help", "copyright", "credits" or "license" for more information.
>>>
```

Install via python3-setuptools

Make sure you installed `python3-setuptools` and `git` packages on your system. If not, install missings according your distribution.

```
~$ cd /your/path/src/
~$ git clone https://github.com/davidonzo/apiosintDS.git
~$ cd apiosintDS/
~$ python3 setup.py build
~$ sudo python3 setup.py install
```

Install via pip3

Make sure you installed `python3-pip` package on your system. If not, install it according your distribution.

```
~$ pip3 install apiosintDS
```

Windows support

The library has never been tested on Windows platform. Actually only UNIX system are supported.

1.1.2 Usage via command line (CLI)

```
~$ apiosintDS [-h] [-e [IPv4|domain|url]] [-f /path/to/file.txt]
              [-o /path/to/output.json] [-v] [-c] [-cd /path/to/cachedir]
              [-cc] [-i] [-s]
```

Command line options

-h, –help ***(bool)*** Show the help and exit.

-e, –entity ***[IPv4|domain|url|hash(['md5', 'sha1', 'sha256'])]*** Single item to search. Supported entities are IPv4/FQDN/URLs or file hashes in MD5, SHA1 or SHA256 format. It can't be used in combination with the –file option.

-f, –file ***[/path/to/file.txt]*** Path to file containing entities to search. Supported entities are IPv4/FQDN/URLs. It can't be used in combination with the –entity option.

-o, –output ***[/path/to/output.json]*** Path to output file (/path/to/output.json). If not specified the output will be redirect to the system STDOUT.

-v, –verbose ***(bool)*** Include unmatched results in report.

-c, –cache ***(bool)*** Enable cache mode. Downloaded lists will be stored and won't be downloaded for the next 4 hours.

-cd, –cachedirectory ***[/path/to/cachedir]*** The cache directory where the script check for cached lists files and where them will be stored on cache creation or update. Must be specified the same every script run unless your are using the system temp directory. Default is the temporary user directory.

-cc, –clearcache ***(bool)*** Force the script to download updated lists even if the 4 hours timeout has not yet been reached. Must be used in combination with –cache.

-i, –info ***(bool)*** Print information about the program.

-s, –schema ***(bool)*** Display the response json schema.

Example usage and response for one listed item

```
$ apiosintDS -e 198.12.97.68
{
   "ip": {
        "items": [
            {
                "item": "198.12.97.68",
                "response": true,
                "response_text": "Item found in latestips.txt list",
                "related_urls": [
                    {
                        "url": "http://198.12.97.68/bins/sora.arm",
                        "hashes": {
                            "md5": "b330c76dd7cdea845897615ebdc6fab6",
                            "sha1": "d674d3fbaed43e4276b1f6d7beaf4f7adb9e78c0",
                            "sha256":
↪"85295a1e9b2e176e9a734b8a4ed61cd24b05cd33b1ddefb148fd2149f324e81a"
                        }
                    },
                    {
                        "url": "http://198.12.97.68/bins/sora.arm5",
                        "hashes": {
                            "md5": "06549632f0a7c9cc5e8f2e19792c8d1b",
                            "sha1": "b16b9af9b3260c98f8dcf4f2aae33e3e01603f89",
                            "sha256":
↪"2698619d84fd2caca5b965adb1b5ab048137c8559a5e424a054c2294bb935a31"
                        }
                    },
                    {
                        "url": "http://198.12.97.68/bins/sora.arm6",
                        "hashes": {
                            "md5": "78ed5dd94f31d5d04a6262b36f560d50",
                            "sha1": "28b1dc5f31e6b9d5ee3a633812528df4caa75742",
                            "sha256":
↪"c447c79ef27e30e104739835ebdb35fb8c4f31634fd1d47fae40b77d05201123"
                        }
                    },
                   [...CUT...]
                    {
                        "url": "http://198.12.97.68/bins/sora.sh4",
                        "hashes": {
                            "md5": "647ccaac0bf7f52a70dfde452e1c1ee6",
                            "sha1": "e37eee00f5e0b6417ef5925ab1fe2dac73158add",
                            "sha256":
↪"45d2e4420a37220d4184901dce18d9dac0afa83e3c2e948ac09ebb4635048993"
                        }
                    },
                    {
                        "url": "http://198.12.97.68/bins/sora.spc",
                        "hashes": {
                            "md5": "2b0b7590e13451f4622d89a4c8142a78",
                            "sha1": "fe322e0850c610e362ab1d770b5358d5450f5079",
                            "sha256":
↪"117fa981a81b6194506edd5e41fa9351550ce91f2e49ba2d8678cf14cd73eafa"
                        }
                    },
```

(continues on next page)

(continued from previous page)

```
                    {
                        "url": "http://198.12.97.68/bins/sora.x86",
                        "hashes": {
                            "md5": "6d20e81e3caf2c3e973394481dd9b4fb",
                            "sha1": "75e05ebb935aef4b323d58a40a6d5de3539951ae",
                            "sha256":
↪"e08c6ed33e2ac106b277d781848b69759f2687e905bd7db490e4d2c481a81471"
                        }
                    }
                ]
            }
        ],
        "statistics": {
            "itemFound": 1,
            "itemSubmitted": 1
        },
        "list": {
            "file": "latestips.txt",
            "date": "2019-10-22 12:21:59+02:00",
            "url": "https://raw.githubusercontent.com/davidonzo/Threat-Intel/master/
↪lists/latestips.txt"
        }
    }
```

Example usage and response submitting a file

Example file ioc.txt.

```
~$ cat ioc.txt
104.217.254.20
helloyoungmanqq.com
http://hellomydearqq.com/80.exe
0a2d170abbf5031566377b01431e3b82d342630a
```

Response.

```
~$ apiosintDS -f ioc.txt
{
    "url": {
        "items": [
            {
                "item": "http://hellomydearqq.com/80.exe",
                "response": true,
                "response_text": "Item found in latesturls.txt list",
                "hashes": {
                    "md5": "d41d8cd98f00b204e9800998ecf8427e",
                    "sha1": "da39a3ee5e6b4b0d3255bfef95601890afd80709",
                    "sha256":
↪"e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"
                },
                "related_urls": [
                    {
                        "url": "http://hellomydearqq.com/69.exe",
                        "hashes": {
                            "md5": "d41d8cd98f00b204e9800998ecf8427e",
```

(continues on next page)

(continued from previous page)


```
                            "sha1": "da39a3ee5e6b4b0d3255bfef95601890afd80709",
                            "sha256":
↪"e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"
                        }
                    }
                ]
            }
        ],
        "statistics": {
            "itemFound": 1,
            "itemSubmitted": 1
        },
        "list": {
            "file": "latesturls.txt",
            "date": "2019-10-22 12:21:59+02:00",
            "url": "https://raw.githubusercontent.com/davidonzo/Threat-Intel/master/
↪lists/latesturls.txt"
        }
    },
    "ip": {
        "items": [],
        "statistics": {
            "itemFound": 0,
            "itemSubmitted": 1
        },
        "list": {
            "file": "latestips.txt",
            "date": "2019-10-22 12:21:59+02:00",
            "url": "https://raw.githubusercontent.com/davidonzo/Threat-Intel/master/
↪lists/latestips.txt"
        }
    },
    "domain": {
        "items": [
            {
                "item": "helloyoungmanqq.com",
                "response": true,
                "response_text": "Item found in latestdomains.txt list",
                "related_urls": [
                    {
                        "url": "http://helloyoungmanqq.com/25.exe",
                        "hashes": {
                            "md5": "d41d8cd98f00b204e9800998ecf8427e",
                            "sha1": "da39a3ee5e6b4b0d3255bfef95601890afd80709",
                            "sha256":
↪"e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"
                        }
                    },
                   [...CUT...]
                    {
                        "url": "http://helloyoungmanqq.com/93.exe",
                        "hashes": {
                            "md5": "d41d8cd98f00b204e9800998ecf8427e",
                            "sha1": "da39a3ee5e6b4b0d3255bfef95601890afd80709",
                            "sha256":
↪"e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"
                        }
```


(continues on next page)

(continued from previous page)


```
                    },
                    {
                        "url": "http://helloyoungmanqq.com/93.jpg",
                        "hashes": {
                            "md5": "d41d8cd98f00b204e9800998ecf8427e",
                            "sha1": "da39a3ee5e6b4b0d3255bfef95601890afd80709",
                            "sha256":
↪"e3b0c44298fc1c149afbf4c8996fb92427ae41e4649b934ca495991b7852b855"
                        }
                    }
                ]
            }
        ],
        "statistics": {
            "itemFound": 1,
            "itemSubmitted": 1
        },
        "list": {
            "file": "latestdomains.txt",
            "date": "2019-10-22 12:21:59+02:00",
            "url": "https://raw.githubusercontent.com/davidonzo/Threat-Intel/master/
↪lists/latestdomains.txt"
        }
    },
    "hash": {
        "items": [
            {
                "item": "9bd12a7cae1de183192bbb2d55fcd3b81fdc51d8",
                "response": true,
                "response_text": "Item found in latesthashs.txt list",
                "hashes": {
                    "md5": "09a1a8ac5e3c7875089713570937a7d7",
                    "sha1": "9bd12a7cae1de183192bbb2d55fcd3b81fdc51d8",
                    "sha256":
↪"7fc543adcebae77a2d11726151082a5b8cce3114443f15d3ae52613126304c5d"
                },
                "related_urls": [
                    "http://www.biobharati.com/wp-content/y3a/",
                    "http://lemongrasshostel.net/sdlkitj8kfd/j2y/"
                ]
            }
        ],
        "statistics": {
            "itemFound": 1,
            "itemSubmitted": 1
        },
        "list": {
            "file": "latesthashs.txt",
            "date": "2019-10-22 12:22:00+02:00",
            "url": "https://raw.githubusercontent.com/davidonzo/Threat-Intel/master/
↪lists/latesthashes.txt"
        }
    }
}
```

1.1.3 Using as Python library

Below a few examples of how to use **apiosintDS** in your code.

```
#!/usr/bin/env python3
from apiosintDS import apiosintDS

try:
        OSINTCHECK = apiosintDS.request(
                                        entities=['192.168.1.54',

↪'0a2d170abbf5031566377b01431e3b82d3426301',
                                                  'somehost.ext',
                                                  'http://www.example.com/malicious.
↪exe'],
                                        cache=True,
                                        cachedirectory="/tmp",
                                        verbose=True)
        print(OSINTCHECK) # print dict results
except:
        print("Some error") # some error
```

Module contents

apiosintDS.**request**(*entities=list*, *cache=False*, *cachedirectory=None*, *clearcache=False*, *verbose=False*, **args*, ***kwargs*)

Uniq method to query the service. Return a `dict` that can be validated against the json schema returned by the `apiosintDS.schema()` method.

Parameters

entities ***(list)*** List of entities mixed between IPv4, domains and urls.

cache ***(bool, default=False)*** Enable cache mode. Downloaded lists will be stored and won't be downloaded for the next 4 hours.

cachedirectory ***(str)*** The cache directory where the script check for cached lists files and where them will be stored on cache creation or update. Must be specified the same every script run unless your are using the system temp directory. Contrary the CLI usage, there's not a default value).

clearcache ***(bool, default=False)*** Force the script to download updated lists even if the 4 hours timeout has not yet been reached. Must be used in combination with *cache* and *cachedirectory*.

verbose ***(bool, default=False)*** Include unmatched results in returned dict.

apiosintDS.**schema**()

Return an object containing the `json` schema.

1.1.4 Changelog

1.8.2 (2019-10-25)

- Bug fix for cache management of latesthashes.txt list

1.8 (2019-10-22)

- Added MD5/SHA1/SHA256 strings as entity to search
- Added lookup to hash files for hash entities
- Added support su hash lookup for related urls detected
- Minor bug fixes
- New schema json for response

1.7 (2019-10-20)

- Added support to be used as standard python library
- Added docs
- Minor bug fixes

1.6 (2019-10-13)

- Not a real new release. Just added support to pip.

1.6 (2019-10-13)

- First release for python library version usable as CLI tool.
- Added Cache support
- Multiple IoCs submission via text file
- Output management
- New schema response

1.0 (2019-10-07)

- Released version 1.0 published on DigitalSide Threat-Intel repository.

1.1.5 License