PyMISP - Using and expanding the Python API

MISP - Malware Information Sharing Platform & Threat Sharing

CIRCL
Computer Incident
Response Center
Luxembourg

Raphaël Vinot - *TLP:WHITE*

March 24, 2016

PyMISP - Basics

- Installation:
  - pip install pymisp
- Get your auth key from:
  - https://misppriv.circl.lu/events/automation
- Fetch the repository to get the examples:
  - git clone https://github.com/MISP/PyMISP.git

PyMISP - Examples

- Usage:
  - Create examples/keys.py with the following content

```
misp_url = "https://mispppriv.circl.lu"
misp_key = "<API_KEY>"
misp_verifycert = True
```

- PyMISP needs to be installed

PyMISP - Examples

- All the examples have help if you do script.py -h
- copy_list.py: Copy files from one MISp instance to an other
- searchall.py: Search in the whole database for a value
- last.py: Returns all the most recent events (on a timeframe)
- get.py: Return a specific event
- tags.py: Returns all the tags activted on the platform
- get_network_activity.py: Returns network indicators
- create_events.py: Create an event
- up.py: Update an event
- upload.py: Upload a malware sample
- yara.py: Get Yara rules
- suricata.py: Get Suricata events

PyMISP - Feed generator

- Uses PyMISP
- Used to generate the OSINT feed
- Export events as json based on tags
- Automatically update the dumps

PyMISP - Usage

- Basic example

```
from pymisp import PyMISP
api = PyMISP(url, apikey, verifycert=True, 'json', debug=False)
response = api.<function>
if response['error']:
    <something went wrong>
else:
    <do somethifng with the output>
```

PyMISP - Capabilities

- Events: get, add, update, publish and delete
- Events, more: change Threat level, add tag
- Add file attributes: hashes, registry key, patterns, pipe, mutex
- Add network attributes: IP dest/src, hostname, domain, url, UA, ...
- Add Email attrubutes: source, destination, subject, attachment, ...
- Upload/download samples
- Proposals: add, edit, accept, discard
- Full text search and search by attributes
- Tags: get and create
- Get API and platform version
- And more, look at the api file

Q&A

- `https://github.com/MISP/PyMISP`
- `https://github.com/MISP/`
- We welcome new functionalities and pull requests.