Extending MISP with Python modules

MISP - Threat Sharing

Team CIRCL

http://www.misp-project.org/
Twitter: @MISPPProject

ESDC 20200303
Why we want to go more modular...

Ways to extend MISP before modules

- APIs (PyMISP, MISP API)
  - Works really well
  - No integration with the UI

- Change the core code
  - Have to change the core of MISP, diverge from upstream
  - Needs a deep understanding of MISP internals
  - Let’s not beat around the bush: Everyone hates PHP
Goals for the Module System

- Have a way to extend MISP without altering the core
- Get started quickly without a need to study the internals
- Make the modules as light weight as possible
  - Module developers should only have to worry about the data transformation
  - Modules should have a simple and clean skeleton
- In a friendlier language - Python
Extending MISP with expansion modules with zero customization in MISP.

A simple ReST API between the modules and MISP allowing auto-discovery of new modules with their features.

Benefit from existing Python modules in Viper or any other tools.

- MISP modules functionnality introduced in MISP 2.4.28.
- MISP import/export modules introduced in MISP 2.4.50.
MISP modules - installation

- MISP modules can be run on the same system or on a remote server.
- Python 3 is required to run MISP modules.
  - `sudo apt-get install python3-dev python3-pip libpq5`
  - `cd /usr/local/src/`
  - `sudo git clone https://github.com/MISP/misp-modules.git`
  - `cd misp-modules`
  - `sudo pip3 install -I -r REQUIREMENTS`
  - `sudo pip3 install -I .`
  - `sudo vi /etc/rc.local, add this line: ‘sudo -u www-data misp-modules -s &’`
MISP modules - Simple REST API mechanism

- http://127.0.0.1:6666/modules - introspection interface to get all modules available
  - returns a JSON with a description of each module
- http://127.0.0.1:6666/query - interface to query a specific module
  - to send a JSON to query the module

- MISP autodiscovers the available modules and the MISP site administrator can enable modules as they wish.

- If a configuration is required for a module, MISP adds automatically the option in the server settings.
Finding available MISP modules

```
curl -s http://127.0.0.1:6666/modules
```

```json
{
    "type": "expansion",
    "name": "dns",
    "meta": {
        "module-type": [
            "expansion",
            "hover"
        ],
        "description": "Simple DNS expansion service to resolve IP address from MISP attributes",
        "author": "Alexandre Dulaunoy",
        "version": "0.1"
    },
    "mispattributes": {
        "output": [
            "ip-src",
            "ip-dst"
        ],
        "input": [
            "hostname",
            "domain"
        ]
    }
}
```
### Server settings

<table>
<thead>
<tr>
<th>Priority</th>
<th>Setting</th>
<th>Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Critical</td>
<td>Plugin.Enrichment_services_enable</td>
<td>true</td>
<td>Enable/disable the enrichment service</td>
</tr>
<tr>
<td>Recommended</td>
<td>Plugin.Enrichment_services_url</td>
<td><a href="http://127.0.0.1">http://127.0.0.1</a></td>
<td>The url used to access the service</td>
</tr>
<tr>
<td>Recommended</td>
<td>Plugin.Enrichment_services_port</td>
<td>6666</td>
<td>The port used to access the service</td>
</tr>
<tr>
<td>Recommended</td>
<td>Plugin.Enrichment_cve_enabled</td>
<td>false</td>
<td>Enable or disable the cve module</td>
</tr>
<tr>
<td>Recommended</td>
<td>Plugin.Enrichment_dns_enabled</td>
<td>true</td>
<td>Enable or disable the dns module</td>
</tr>
<tr>
<td>Recommended</td>
<td>Plugin.Enrichment_sourcecache_enabled</td>
<td>false</td>
<td>Enable or disable the source cache module</td>
</tr>
<tr>
<td>Recommended</td>
<td>Plugin.Enrichment_sourcecache_archivepath</td>
<td></td>
<td>Set this required module sp</td>
</tr>
<tr>
<td>Recommended</td>
<td>Plugin.Enrichment_passivetotal_enabled</td>
<td>true</td>
<td>Enable or disable the passive total</td>
</tr>
<tr>
<td>Recommended</td>
<td>Plugin.Enrichment_passivetotal_username</td>
<td><a href="mailto:alexandre.dulaunoy@circl.lu">alexandre.dulaunoy@circl.lu</a></td>
<td>Set this required module sp</td>
</tr>
<tr>
<td>Recommended</td>
<td>Plugin.Enrichment_passivetotal_password</td>
<td></td>
<td>Set this required module sp</td>
</tr>
</tbody>
</table>
MISP MODULES - HOW IT’S INTEGRATED IN THE UI?

Choose the enrichment module that you wish to use for the expansion:

```
dns
```

Enrichment Results:

Below you can see the attributes that are to be created. Make sure that the categories and the types are correct, often several options will be offered based on an inconclusive automatic resolution.

```
Value: 23.100.122.175
Category: Network activity
Type: ip-src
IDS: [Imported via the freetext import]
Comment: [Update all comment fields]
Actions: [Change all]
```
MISP MODULES - MAIN TYPES OF MODULES

- Expansion modules - enrich data that is in MISP
  - Hover type - showing the expanded values directly on the attributes
  - Expansion type - showing and adding the expanded values via a proposal form
- Import modules - import new data into MISP
- Export modules - export existing data from MISP
**Querying a Module**

- curl -s http://127.0.0.1:6666/query -H "Content-Type: application/json" –data @body.json -X POST

body.json

```json
1
{ "module": "dns", "hostname": "www.circl.lu" }
```

- and the response of the dns module:

```json
1
2
{ "results": [{ "values": ["149.13.33.14"], "types": ["ip-src", "ip-dst"] }]
```

10
Creating your module - DNS module

```python
import json
import dns.resolver
misperrors = {'error': 'Error'}
mispattributes = {'input': ['hostname', 'domain'], 'output': ['ip-src', 'ip-dst']}
moduleinfo = {'version': '0.1', 'author': 'Alexandre_Dulaunoy',
              'description': 'Simple DNS expansion service to resolve IP address from MISP attributes', 'module-type': ['expansion', 'hover']}
def handler(q=False):
    if q is False:
        return False
    request = json.loads(q)
    if request.get('hostname'):
        toquery = request['hostname']
    elif request.get('domain'):
        toquery = request['domain']
    else:
        return False
    r = dns.resolver.Resolver()
    r.timeout = 2
    r.lifetime = 2
    r.nameservers = ['8.8.8.8']
    try:
        answer = r.query(toquery, 'A')
    except dns.resolver.NXDOMAIN:
        misperrors['error'] = 'NXDOMAIN'
        return misperrors
    except dns.exception.Timeout:
        misperrors['error'] = 'Timeout'
        return misperrors
    except:
        misperrors['error'] = 'DNS_resolving_error'
        return misperrors
    r = [{'results': [{'types': mispattributes['output'], 'values': [str(answer[0])]}]}]
    return r

def introspection():
    return mispattributes

def version():
    return moduleinfo
```
Testing your module

- Copy your module dns.py in modules/expansion/
- Restart the server misp-modules.py

```
[adulau:~/git/misp-modules/bin]$ python3 misp-modules.py
2016-03-20 19:25:43,748  -  misp-modules  -  INFO  -  MISP modules passivetotal imported
2016-03-20 19:25:43,787  -  misp-modules  -  INFO  -  MISP modules sourcecache imported
2016-03-20 19:25:43,789  -  misp-modules  -  INFO  -  MISP modules cve imported
2016-03-20 19:25:43,790  -  misp-modules  -  INFO  -  MISP modules dns imported
2016-03-20 19:25:43,797  -  misp-modules  -  INFO  -  MISP modules server started on TCP port 6666
```

- Check if your module is present in the introspection
- `curl -s http://127.0.0.1:6666/modules`
- If yes, test it directly with MISP or via curl
Code samples (Configuration)

```python
# Configuration at the top
moduleconfig = ['username', 'password']

# Code block in the handler
if request.get('config'):
    if request['config'].get('username') is None or request['config'].get('password') is None:
        miserrors['error'] = 'CIRCL_Passive_SSL_authentication_is_missing'
        return miserrors

x = pypssl.PyPSSL(basic_auth=(request['config']['username'], request['config']['password']))
```

Passive SSL authentication is missing
Default expansion module set

- asn history
- CIRCL Passive DNS
- CIRCL Passive SSL
- Country code lookup
- CVE information expansion
- DNS resolver
- DomainTools
- eupi (checking url in phishing database)
- IntelMQ (experimental)
- ipasn
- PassiveTotal - http://blog.passivetotal.org/misp-sharing-done-differently
- sourcecache
- Virustotal
- Whois
Import modules

Similar to expansion modules
Input is a file upload or a text paste
Output is a list of parsed attributes to be editend and verified by the user

Some examples
  - Cuckoo JSON import
  - email import
  - OCR module
  - Open IoC import
Export modules

- Not the preferred way to export data from MISP
- Input is currently only a single event
- Output is a file in the export format served back to the user
- Will be moved / merged with MISP built-in export modules
  - Allows export of event / attribute collections
New expansion & import modules format

- Backward compatible - an additional field to extend the format

  ```
  misp_attributes = {
    'input': [...],
    'output': [...],
    'format': 'misp_standard'
  }
  ```

- Takes a standard MISP attribute as input

- Returns MISP format
  - Attributes
  - Objects (with their references)
  - Tags

  ```
  results = {
    'Attribute': [...],
    'Object': [...],
    'Tag': [...]
  }
  ```

- First modules supporting this new export format
  - urlhaus expansion module
  - Joe Sandbox import & query module
# Enrichment Results

Below you can see the attributes and objects that are to be created from the results of the enrichment modules.

<table>
<thead>
<tr>
<th>Event ID</th>
<th>1229</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event UUD</td>
<td>5cc3042c-8b6d-4b37-956d-47ace96451a</td>
</tr>
<tr>
<td>Event creator org</td>
<td>ORGNAME</td>
</tr>
<tr>
<td>Event Info</td>
<td>urhaus test</td>
</tr>
<tr>
<td>iResolved Attributes</td>
<td>14 (2 Objects)</td>
</tr>
</tbody>
</table>

## Category

<table>
<thead>
<tr>
<th>Type</th>
<th>Value</th>
<th>UUID</th>
<th>Tags</th>
<th>Disable Correlation</th>
<th>Comment</th>
<th>Distribution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>venustabs-report</td>
<td>abc32be-4601-42a1-a556-5a1b9f8e0be1</td>
<td></td>
<td></td>
<td></td>
<td>Inherit event</td>
</tr>
<tr>
<td>Reference</td>
<td>6</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Other</td>
<td>detection-ratio: text</td>
<td>d37b65311b80be1e654eb88ba237ecbcddc7a730176d2c7f857e8f4752zed</td>
<td></td>
<td></td>
<td></td>
<td>Inherit event</td>
</tr>
<tr>
<td>External analysis</td>
<td>permalink: link</td>
<td><a href="https://www.virustotal.com/file/e38dad911b80be1e654eb88ba237ecbcddc7a730176d2c7f857e8f4752zed">https://www.virustotal.com/file/e38dad911b80be1e654eb88ba237ecbcddc7a730176d2c7f857e8f4752zed</a></td>
<td></td>
<td></td>
<td></td>
<td>Inherit event</td>
</tr>
<tr>
<td></td>
<td></td>
<td>e6b7050c-8b72-405f-9be2-39d5a005c0</td>
<td></td>
<td></td>
<td></td>
<td>Inherit event</td>
</tr>
</tbody>
</table>

## Payload delivery

| Name       | sha256                                                               | 5c0f5e0b-1c8d-4904-a485-b05f92c02b50 |      |                     |         | Inherit event |
| Reference  | 1                                                                   |                            |      |                     |         |              |
| Other      | size-in-bytes: size-in-bytes                                         | 989304                    |      |                     |         | Inherit event |

## Network activity

| Name       | url                                                                  | e6b7050c-8b72-405f-9be2-39d5a005c0 |      |                     |         | Inherit event |
| Reference  | a                                                                    |                            |      |                     |         |              |
| Other      | network activity                                                     | a3951ba1-4e6b-4d90-9996-6402b0c   |      |                     |         | Inherit event |
| External analysis | network activity                                                      | 377839df-479b-495e-9c5d-985959599859 |      |                     |         | Inherit event |
|            |                                                                       | b8d4b74-4a5d-4c67-a7e4-a48b8783411a |      |                     |         | Inherit event |
|            |                                                                       | 0f90730f-8b2b-46f9-9c13-313502296d4 |      |                     |         | Inherit event |
|            |                                                                       | 44ab3cb6-73b-47a0-94c1-d3830b8b0c4ae |      |                     |         | Inherit event |
|            |                                                                       | 05a5151b-47e3-4772-ac08-d22406e6ed6c3 |      |                     |         | Inherit event |
|            |                                                                       | 9e02398d-d778-4415-85a4-5a2f536f747 |      |                     |         | Inherit event |

## Other

| Name       | url                                                                  | e6b7050c-8b72-405f-9be2-39d5a005c0 |      |                     |         | Inherit event |
| Reference  | a                                                                    |                            |      |                     |         |              |
| Other      | network activity                                                     | a3951ba1-4e6b-4d90-9996-6402b0c   |      |                     |         | Inherit event |
| External analysis | network activity                                                      | 377839df-479b-495e-9c5d-985959599859 |      |                     |         | Inherit event |
|            |                                                                       | b8d4b74-4a5d-4c67-a7e4-a48b8783411a |      |                     |         | Inherit event |
|            |                                                                       | 0f90730f-8b2b-46f9-9c13-313502296d4 |      |                     |         | Inherit event |
|            |                                                                       | 44ab3cb6-73b-47a0-94c1-d3830b8b0c4ae |      |                     |         | Inherit event |
|            |                                                                       | 05a5151b-47e3-4772-ac08-d22406e6ed6c3 |      |                     |         | Inherit event |
|            |                                                                       | 9e02398d-d778-4415-85a4-5a2f536f747 |      |                     |         | Inherit event |
Future of the modules system

- Enrichment on full events
- Move the modules to background processes with a messaging system
- Have a way to skip the results preview
  - Preview can be very heavy
  - Difficulty is dealing with uncertain results (without the user having final say)
https://github.com/MISP/misp-modules
https://github.com/MISP/
We welcome new modules and pull requests.
MISP modules can be designed as standalone application.