EXTENDING MISP WITH PYTHON MODULES

MISP - Threat Sharing

CIRCL / Team MISP Project

HTTP://WWW.MISP-PROJECT.ORG/
TWITTER: @MISPPROJECT

FIRST.ORG/Africa CERT
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

Why we want to go more modular...
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 functionality introduced in MISP 2.4.28.

MISP import/export modules introduced in MISP 2.4.50.
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.
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 service</td>
</tr>
<tr>
<td>Recommended</td>
<td>Plugin.Enrichment_dns_enabled</td>
<td>true</td>
<td>Enable or disable the DNS module service</td>
</tr>
<tr>
<td>Recommended</td>
<td>Plugin.Enrichment_sourcecache_enabled</td>
<td>false</td>
<td>Enable or disable the sourcecache module service</td>
</tr>
<tr>
<td>Recommended</td>
<td>Plugin.Enrichment_sourcecache_archivelpath</td>
<td></td>
<td>Set this required module spec</td>
</tr>
<tr>
<td>Recommended</td>
<td>Plugin.Enrichment_passivetotal_enabled</td>
<td>true</td>
<td>Enable or disable the passive total module service</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 spec</td>
</tr>
<tr>
<td>Recommended</td>
<td>Plugin.Enrichment_passivetotal_password</td>
<td></td>
<td>Set this required module spec</td>
</tr>
</tbody>
</table>
Choose the enrichment module that you wish to use for the expansion

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

body.json

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

and the response of the dns module:

```json
1
{"results": [{"values": ["149.13.33.14"],
   "types": ["ip-src", "ip-dst"]}]}
```
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
  
  ```bash
  [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
# 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']))
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
Similar to expansion modules
Input is a file upload or a text paste
Output is a list of parsed attributes to be edited and verified by the user
Some examples
- Cuckoo JSON import
- email import
- OCR module
- Open IoC import
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
Backward compatible - an additional field to extend the format

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

Takes a standard MISP attribute as input

Returns MISP format

- Attributes
- Objects (with their references)
- Tags

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

First modules supporting this new export format

- urlhaus expansion module
- Joe Sandbox import & query module
### New Expansion & Import Modules View (MISP 2.4.110)

**Enrichment Results**

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

<table>
<thead>
<tr>
<th>Category</th>
<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>Event ID</td>
<td></td>
<td>1229</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event UUD</td>
<td></td>
<td>5cc30412-86d1-4837-9564-47ace96451a</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event Creator Org</td>
<td></td>
<td>ORGNAME</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Event Info</td>
<td></td>
<td>urhaus test</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>iResolved Attributes</td>
<td>14 (2 Objects)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

#### Name: vienntial-report

- **Reference:** 0

#### Other

- **detection-ratio:** text
  - Value: 10 / 68
  - UUID: e595bb4-4601-421a-a556-5a12d9f64be1

- **External analysis:** permanent
  - Value: https://www.virustotal.com/file/5fd89d951b98be0e94eb6f8a2f5e8c92a2/7017b66bc7f8757ef947
  - UUID: 46cd33d0-5e21-48c7-9fe7-7e2b8f6d427b

#### ID: 12700

- **Name:** file

- **References:** 1

#### Payload delivery

- **sha256:** shaf256
  - Value: dab789c0-8080-1e6d4e688b23ecb6c27a73017b66bc7f8757ef9475
  - UUID: 502ad0b0-8dcd-4904-a410-6b5e9262c5b

#### Other

- **size-in-bytes:** size-in-bytes
  - Value: 98384
  - UUID: f9e4442d-67c8-4210-8e0b-4013595a471

#### Network activity

- **url:** http://automotive/dreamteam.com/vexe
  - Value: e877610c-8e72-4051-9be6-2dc39456d5c0

- **url:** http://shoporganizagropoop.exe
  - Value: a3b4ebc9-4e40-4d00-90a9-50795d402bc

- **url:** http://poopbioe/operfranchise.com/vexe
  - Value: 377f987b-7fba-419a-e502-7468a3959b40

- **url:** http://cherrythpoopoisopoopcoopers.com/vexe
  - Value: b8044c74-4af2-4c07-72ab-4d68781411a

- **url:** http://logopsnprop.net/vexe
  - Value: 890d265b-9f2b-4760-8c41-3f82b06bcaae

- **url:** http://logopsnpop.mobu/vexe
  - Value: 84b0d75b-7472-ac08-2e2406ed8c3

- **url:** http://logopsnpop.info/vexe
  - Value: 90c2d8f6-2788-3415-8544-5a29d532947

- **url:** http://logopsnpop.biz/vexe
  - Value: 90c2d8f6-2788-3415-8544-5a29d532947
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)
We welcome new modules and pull requests.

MISP modules can be designed as standalone application.