

EXTENDING MISP WITH PYTHON MODULES

MISP - THREAT SHARING

CIRCL / TEAM MISP PROJECT

[HTTP://WWW.MISP-PROJECT.ORG/](http://www.misp-project.org/)

TWITTER: [@MISPPROJECT](https://twitter.com/MISPPROJECT)

NSPA



MISP
Threat Sharing

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

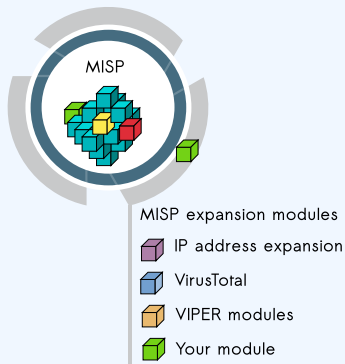
- Needs a deep understanding of MISP internals

- 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**

MISP MODULES - EXTENDING MISP WITH PYTHON SCRIPTS



- 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 &'`

- `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`

```
1  {
2  "type": "expansion",
3  "name": "dns",
4  "meta": {
5      "module-type": [
6          "expansion",
7          "hover"
8      ],
9      "description": "Simple DNS expansion service
        to resolve IP address from MISP
        attributes",
10     "author": "Alexandre Dulaunoy",
11     "version": "0.1"
12 },
13 "mispattributes": {
14     "output": [
15         "ip-src",
16         "ip-dst"
17     ],
18     "input": [
19         "hostname",
20         "domain"
21     ]
22 }
```

MISP MODULES - CONFIGURATION IN THE UI

Server settings

Overview MISP settings (18) GnuPG settings (3) Proxy settings (5) Security settings (2) Misc settings (1) Plugin settings (22) Diagnostics Workers

Enrichment

| Priority | Setting | Value | Description |
|-------------|---|-----------------------------|---|
| Critical | Plugin.Enrichment_services_enable | true | Enable/disable the enrichment services |
| Recommended | Plugin.Enrichment_services_url | http://127.0.0.1 | The url used to access the enrichment services |
| Recommended | Plugin.Enrichment_services_port | 6666 | The port used to access the enrichment services |
| Recommended | Plugin.Enrichment_cve_enabled | false | Enable or disable the cve module |
| Recommended | Plugin.Enrichment_dns_enabled | true | Enable or disable the dns module |
| Recommended | Plugin.Enrichment_sourcecache_enabled | false | Enable or disable the sourcecache module |
| Recommended | Plugin.Enrichment_sourcecache_archivepath | | Set this required module parameter |
| Recommended | Plugin.Enrichment_passivetotal_enabled | true | Enable or disable the passivetotal module |
| Recommended | Plugin.Enrichment_passivetotal_username | alexandre.dulaunoy@circl.lu | Set this required module parameter |
| Recommended | Plugin.Enrichment_passivetotal_password | | Set this required module parameter |

MISP MODULES - HOW IT'S INTEGRATED IN THE UI?

Filters: **All** File Network Financial Proposal Correlation

| Value | Comment | Related Events | ID \$ | Distribution | Actions |
|---------------|---------|----------------|-------|--------------|---------|
| microsoft.com | | No | No | Inherit | |
| google.com | | 25 | No | Inherit | |
| circl.lu | | No | No | Inherit | |

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

dns

Cancel

next view

Filters: **All** File Network Financial Proposal Correlation

| Org | Category | Type | Value | Comment | Related Events | ID \$ |
|-----|------------------|--------|---------------|---------|----------------|-------|
| 3 | Network activity | domain | microsoft.com | | No | |
| 3 | Network activity | domain | google.com | | 25 | No |
| 3 | Network activity | domain | circl.lu | | No | |

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 | Category | Type | ID \$ | Comment | Actions |
|----------------|------------------|--------|--------------------------|-----------------------------------|---------|
| 23.100.122.175 | Network activity | ip-src | <input type="checkbox"/> | Imported via the freetext import. | |

Submit

ip-src → ip-dst **Change all**

Update all comment fields **Change all**

- 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

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

- and the response of the dns module:

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

CREATING YOUR MODULE - DNS MODULE

```
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[o])]]}]
    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)

```
# 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):
        mispererrors['error'] = 'CIRCL Passive SSL authentication is missing'
        return mispererrors

x = pypssl.PySSL(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

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

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.

| | | | | | | | | |
|---|--------------------------------------|---|--------------------------------------|-------------------------------------|-----|-------------------------------------|-----------------------------|-----------------|
| Event ID | 1229 | | | | | | | |
| Event UUID | 5cc3042c-8bb4-4837-9564-47aca964451a | | | | | | | |
| Event creator org | ORNAME | | | | | | | |
| Event info | urhaus test | | | | | | | |
| #Resolved Attributes | 14 (2 Objects) | | | | | | | |
| Category | Type | Value | UUID | Tags | ID5 | Disable Correlation | Comment | Distribution |
| Name: virustotal-report ⓘ References: 0 | | | | | | | | Inherit event ⓘ |
| Other | detection-ratio: text | 10 / 66 | adc328ae-4651-41a1-4558-5a10399e4be1 | | | <input checked="" type="checkbox"/> | f2b701d43a43315105d649612b2 | Inherit event ⓘ |
| External analysis | permalink: link | https://www.virustotal.com/file/13fad9911b80be1d64e688ba23fcbcd8c21aa73017b6dbcf78570ef47552ed/analysis/1554403108/ | 40b3d10d-5e81-48c7-91e7-be2b898427b | | | <input type="checkbox"/> | f2b701d43a43315105d649612b2 | Inherit event ⓘ |
| ID: 12700 Name: file ⓘ References: 11 ⓘ | | | | | | | | Inherit event ⓘ |
| Payload delivery | sha256: sha256 | d3fad9911b80be1d64e688ba23fcbcd8c21aa73017b6dbcf78570ef47552ed | 5026ab08-8f08-40e4-a485-b69e92d0295b | <input checked="" type="checkbox"/> | | <input type="checkbox"/> | f2b701d43a43315105d649612b2 | Inherit event ⓘ |
| Other | size-in-bytes: size-in-bytes | 98304 | 9ee14454-f6f1-4210-a88a-e401599b4f71 | <input type="checkbox"/> | | <input checked="" type="checkbox"/> | f2b701d43a43315105d649612b2 | Inherit event ⓘ |
| Network activity | url | http://automotivedreamteam.com/v.exe | e697650e-b672-405f-9be9-2dc39459a5e0 | <input checked="" type="checkbox"/> | | <input type="checkbox"/> | f2b701d43a43315105d649612b2 | Inherit event ⓘ |
| Network activity | url | http://shoppalldogscoop.com/v.exe | a3986a11-4ee0-4b55-ba40-999666402cbc | <input checked="" type="checkbox"/> | | <input type="checkbox"/> | f2b701d43a43315105d649612b2 | Inherit event ⓘ |
| Network activity | url | http://pooperscoopfranchise.com/v.exe | 3778d0bd-77b6-4186-a052-746a3890b9e0 | <input checked="" type="checkbox"/> | | <input type="checkbox"/> | f2b701d43a43315105d649612b2 | Inherit event ⓘ |
| Network activity | url | http://cherryhillpooperscoopers.com/v.exe | b804db74-4a62-4cd7-abef-a4b68781411e | <input checked="" type="checkbox"/> | | <input type="checkbox"/> | f2b701d43a43315105d649612b2 | Inherit event ⓘ |
| Network activity | url | http://alldogscoop.net/v.exe | 09b672b8-62f9-469f-9c11-5315b226644 | <input checked="" type="checkbox"/> | | <input type="checkbox"/> | f2b701d43a43315105d649612b2 | Inherit event ⓘ |
| Network activity | url | http://alldogscoop.mobi/v.exe | 4bae6a06-b739-47ad-04c1-d583b2b9c4ae | <input checked="" type="checkbox"/> | | <input type="checkbox"/> | f2b701d43a43315105d649612b2 | Inherit event ⓘ |
| Network activity | url | http://alldogscoop.info/v.exe | 0f5ad15b-47ed-4772-act8-d2240a6e08c3 | <input checked="" type="checkbox"/> | | <input type="checkbox"/> | f2b701d43a43315105d649612b2 | Inherit event ⓘ |
| Network activity | url | http://alldogscoop.biz/v.exe | 90c29d88-d778-4415-8544-5a2fc53d4f7 | <input checked="" type="checkbox"/> | | <input type="checkbox"/> | f2b701d43a43315105d649612b2 | Inherit event ⓘ |

- 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.