

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)

13TH ENISA-EC3 WORKSHOP



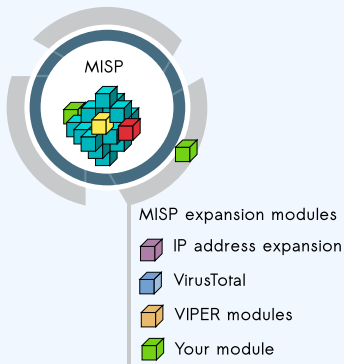
MISP
Threat Sharing

- 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 | jq .`

```
1      {
2      "type": "expansion",
3      "name": "dns",
4      "meta": {
5        "module-type": [
6          "expansion",
7          "hover"
8        ],
9      "description": "Simple DNS expansion service
10         to resolve IP address from MISP
11         attributes",
12      "author": "Alexandre Dulaunoy",
13      "version": "0.1"
14    },
15    "mispattributes": {
16      "output": [
17        "ip-src",
18        "ip-dst"
19      ],
20      "input": [
21        "hostname",
22        "domain"
23      ]
24    }
25  }
```

MISP MODULES - CONFIGURATION IN THE UI

Server settings

Overview	MISP settings (18)	GUI/RG settings (3)	Proxy settings (5)	Security settings (2)	Misc settings (1)	Plugin settings (22)	Diagnos...	Workere...
	Binary Message	Priority	Shifting			Value		
		Charset						
0.0.0.0:8080	Value not set.	Recommended						
0.0.0.0:8080	Value not set.	Recommended						
	Value not set.	Recommended						
		Recommended						
	Value not set.	Recommended						
	Value not set.	Recommended						
		Recommended						
		Recommended						
		Recommended						
		Recommended						
		Recommended						

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

Filters: All	File	Network	Financial	Proposal	Correlation
Value	Comment	Related Events	IDS	Distribution	Actions
microsoft.com			No	Inherit	
google.com		25	No	Inherit	
circl.lu			No	Inherit	

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

dns

Cancel

Org	Category	Type	Value	Comment	Related Events	IDS
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	IDS <input type="checkbox"/>	Comment	Actions
23.100.122.175	Network activity	ip-src	<input type="checkbox"/>	Imported via the freetext import.	

ip-src → ip-dst

Update all comment fields

- 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" -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', 'domain|ip'], 'output': ['ip-src', 'ip-dst']}
moduleinfo = {'version': '0.3', 'author': 'Alexandre Dulaunoy', 'description': 'Simple DNS expansion service to resolve IP address from MISP attributes',
              'module-type': ['expansion', 'hover']}
moduleconfig = {'nameserver'}

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']
    elif request.get('domain|ip'):
        toquery = request['domain|ip']
    else:
        return False
    r = dns.resolver.Resolver()
    r.timeout = 2
    r.lifetime = 2

    if request.get('config'):
        if request['config'].get('nameserver'):
            nameservers = []
            nameservers.append(request['config'].get('nameserver'))
            r.nameservers = nameservers
    else:
        r.nameservers = ['8.8.8.8']

    try:
        answer = r.resolve(toquery, 'A')
    except dns.resolver.NXDOMAIN:
        misperrors['error'] = "NXDOMAIN"
        return misperrors
    except ...

    return {'results': [{'types': mispattributes['output'], 'values': [str(answer[o])]}]}

def introspection():
    return mispattributes

def version():
    moduleinfo['config'] = moduleconfig
    return moduleinfo
```

- 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 not request.get('config'):
    return {'error': 'CIRCL Passive SSL authentication is missing.'}

if not request['config'].get('username') or not request['config'].get('password'):
    return {'error': 'CIRCL Passive SSL authentication is incomplete, please provide your username and password.'}
authentication = (request['config']['username'], request['config']['password'])

if not request.get('attribute') or not check_input_attribute(request['attribute']):
    return {'error': f'{standard_error_message}, which should contain at least a type, a value and an uuid.'}
attribute = request['attribute']

pssl_parser = PassiveSSLParser(attribute, authentication)
```

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)
- 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 editend 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	ORONAME							
Event info	urhaus test							
#Resolved Attributes	14 (2 Objects)							
Category	Type	Value	UUID	Tags	IDS	Disable Correlation	Comment	Distribution
Name: virustotal-report ⌵ References: 0 ⌵ Inherit event								
Other	detection-ratio: text	10 / 66	adc3209e-4651-41a1-4558-5a10399e4be1			<input checked="" type="checkbox"/>	72b701d43a43315105d649612b2c	Inherit event
External analysis	permalink: link	https://www.virustotal.com/file/13fa09118f0be1d654e688ba23fcbcd0c21aa73017b6dbcf78570ef47552ed/analysis/1554403108/	40b3d10d-5e81-48c7-91e7-be2b898427b			<input type="checkbox"/>	72b701d43a43315105d649612b2c	Inherit event
ID: 12700 ⌵ Name: file ⌵ References: 11 ⌵ Inherit event								
Payload delivery	sha256: sha256	d3fa09118f0be1d654e688ba23fcbcd0c21aa73017b6dbcf78570ef47552ed	5026ab08-8f0c-49e4-a485-d69a9280295b			<input checked="" type="checkbox"/>	72b701d43a43315105d649612b2c	Inherit event
Other	size-in-bytes: size-in-bytes	98304	9ee64454-bef4-4210-a88a-e401599b4f71			<input checked="" type="checkbox"/>	72b701d43a43315105d649612b2c	Inherit event
Network activity	url	http://automotiveadteam.com/v.exe	e687650e-b672-405f-9be9-2dc39459e5e0			<input checked="" type="checkbox"/>	72b701d43a43315105d649612b2c	Inherit event
Network activity	url	http://shpaldogpoop.com/v.exe	a3986a11-4e60-4b55-ba40-999666402zbc			<input checked="" type="checkbox"/>	72b701d43a43315105d649612b2c	Inherit event
Network activity	url	http://pooperscoopertfranchise.com/v.exe	3778d0bd-47b6-4186-a052-746a389509e0			<input checked="" type="checkbox"/>	72b701d43a43315105d649612b2c	Inherit event
Network activity	url	http://cherryhillpooperscoopers.com/v.exe	b804db74-4a62-4cd7-abef-a4b68781411e			<input checked="" type="checkbox"/>	72b701d43a43315105d649612b2c	Inherit event
Network activity	url	http://haldogpoop.net/v.exe	09a672e8-62f9-469f-9c11-53159d22644			<input checked="" type="checkbox"/>	72b701d43a43315105d649612b2c	Inherit event
Network activity	url	http://haldogpoop.mobi/v.exe	4bae6a96-b739-47ad-94c1-d583b2b9c4ae			<input checked="" type="checkbox"/>	72b701d43a43315105d649612b2c	Inherit event
Network activity	url	http://haldogpoop.info/v.exe	0f5ad15b-47e0-4772-act8-d2240e6e8c3			<input checked="" type="checkbox"/>	72b701d43a43315105d649612b2c	Inherit event
Network activity	url	http://haldogpoop.biz/v.exe	90b29d98-d778-4415-8544-5a2cf53d847			<input checked="" type="checkbox"/>	72b701d43a43315105d649612b2c	Inherit event

- Flexibility, no need to install MISP
- User friendly interface
- Easiest way to test new modules

- Add multiple entries
- Choose different modules

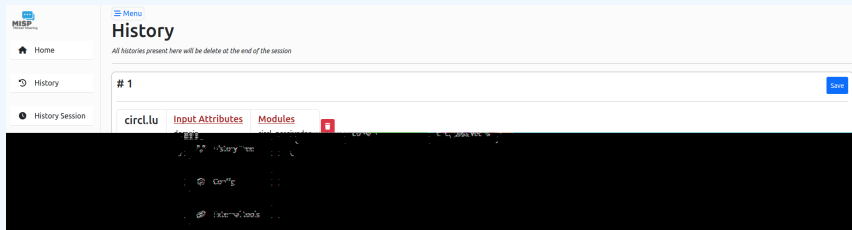
The screenshot displays the MISP Modules web interface. On the left is a navigation sidebar with the MISP logo and menu items: Home, History, History Session, History Tree, Config (highlighted in blue), and External tools. The main content area is titled 'MISP Modules' and features a search bar containing 'circl.lu'. Below the search bar are two buttons: 'Add new entry' and 'Delete entry'. Under the heading 'Input Attributes', a dropdown menu is set to 'domain'. Under the heading 'Modules', a search box contains 'circl_passivedns' with a close button. At the bottom, there is a checkbox labeled 'Configure all modules' which is currently unchecked.

Multiple tabs for visualization in different formats

The screenshot displays a web interface for a security tool. On the left is a sidebar with navigation options: Home, History, History Session, History Tree, Config, and External tools. The main area shows a query for 'circl.lu' with the input attribute 'domain' and the module 'circl_passivedns'. The interface includes a top navigation bar with 'New query', 'Query', and a refresh icon. A status bar indicates the query stopped at 2024-07-08 13:34 with 1 success and 0 errors. Below the query details are tabs for 'Visual', 'Json', and 'Markdown'. The 'Visual' tab is active, showing a table of results. On the right, there are buttons for 'circl.lu', 'Errors', and 'circl.lu'. The table below contains the following data:

IP	Host	ASN	Country	City	Region	Postal	Time
192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1	192.168.1.1
192.168.1.2	192.168.1.2	192.168.1.2	192.168.1.2	192.168.1.2	192.168.1.2	192.168.1.2	192.168.1.2
192.168.1.3	192.168.1.3	192.168.1.3	192.168.1.3	192.168.1.3	192.168.1.3	192.168.1.3	192.168.1.3
192.168.1.4	192.168.1.4	192.168.1.4	192.168.1.4	192.168.1.4	192.168.1.4	192.168.1.4	192.168.1.4
192.168.1.5	192.168.1.5	192.168.1.5	192.168.1.5	192.168.1.5	192.168.1.5	192.168.1.5	192.168.1.5
192.168.1.6	192.168.1.6	192.168.1.6	192.168.1.6	192.168.1.6	192.168.1.6	192.168.1.6	192.168.1.6
192.168.1.7	192.168.1.7	192.168.1.7	192.168.1.7	192.168.1.7	192.168.1.7	192.168.1.7	192.168.1.7
192.168.1.8	192.168.1.8	192.168.1.8	192.168.1.8	192.168.1.8	192.168.1.8	192.168.1.8	192.168.1.8
192.168.1.9	192.168.1.9	192.168.1.9	192.168.1.9	192.168.1.9	192.168.1.9	192.168.1.9	192.168.1.9
192.168.1.10	192.168.1.10	192.168.1.10	192.168.1.10	192.168.1.10	192.168.1.10	192.168.1.10	192.168.1.10

■ Save your researches and pivot from them



The screenshot displays the MISP (Metasploit Incident Response System) web interface. On the left is a navigation sidebar with 'Home', 'History', and 'History Session' options. The main content area is titled 'History' and includes a warning: 'All histories present here will be delete at the end of the session'. A single history entry, labeled '# 1', is shown with a 'Save' button. Below the entry are three tabs: 'circl.lu', 'Input Attributes', and 'Modules'. The 'Input Attributes' tab is active, showing a list of attributes with columns for 'Name', 'Type', and 'Value'. The 'Modules' tab is also visible, showing a list of modules with columns for 'Name', 'Type', and 'Value'. The interface is clean and professional, with a light blue and white color scheme.

■ Export results to other tools. (Still in dev)

The screenshot displays the NISP web interface. On the left is a sidebar with navigation options: Home, History, History Session, History Tree, Config, and External tools. The main content area is titled 'External tools' and includes a search bar. A list of tools is shown, with 'flowintel' selected. A modal window is open for editing 'flowintel', showing its name and URL: 'http://localhost:7006/analyzer/recieve_result'. The modal has 'Save' and 'Delete' buttons. A '[Go Back Tool]' link is visible in the bottom right corner of the interface.

Menu
External tools +

Search tools

flowintel

flowintel

Name:
flowintel

Url:
http://localhost:7006/analyzer/recieve_result

Save Delete

[\[Go Back Tool\]](#)

- 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.