

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

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

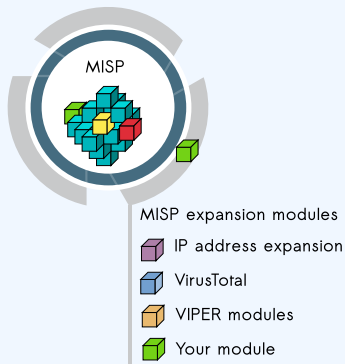
- Needs a deep understanding of MISP internals

- 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 | jq .`

```
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	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

next view

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

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 ☐	Comment	Actions
23.100.122.175	Network activity	ip-src	☐	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
mispperrors = {'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:
        mispperrors['error'] = "NXDOMAIN"
        return mispperrors
    except ...

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

def introspection():
    return misppattributes

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

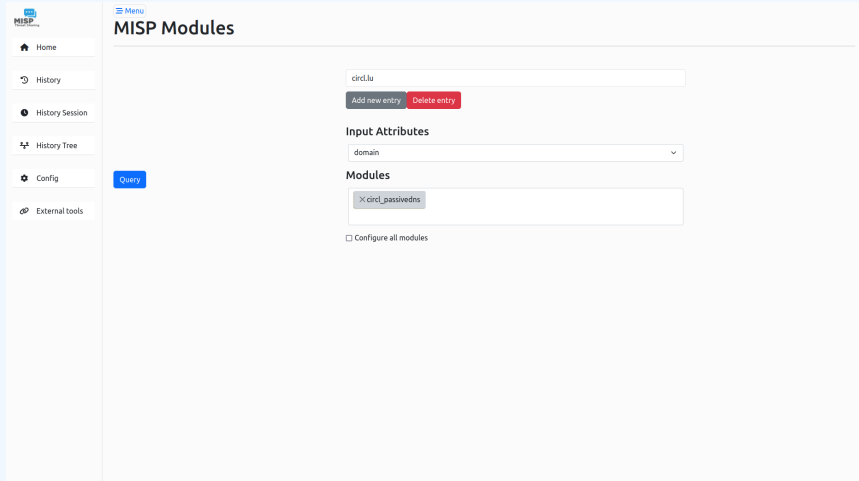
Below you can see the attributes and objects that are to be created from the results of the enrichment module.

Event ID	1229							
Event UUID	5cc3042c-8bb4-4837-9564-47aca964451a							
Event creator org	ORGNAM							
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			☒	f2b701d43a43315105d649612b2	Inherit event ⓘ
External analysis	permalink: link	https://www.virustotal.com/file/13fad9911b80be1d64e688ba23fcbcd8c21aa73017b6dbcf78570ef47552ed/analysis/1554403108/	40b3d10d-5e81-48c7-91e7-be2b898427b			☐	f2b701d43a43315105d649612b2	Inherit event ⓘ
ID: 12700 Name: file ⓘ References: 11 ⓘ								Inherit event ⓘ
Payload delivery	sha256: sha256	d3fad9911b80be1d64e688ba23fcbcd8c21aa73017b6dbcf78570ef47552ed	5026ab08-0f08-40e4-a485-b69e92d0295b	☒		☐	f2b701d43a43315105d649612b2	Inherit event ⓘ
Other	size-in-bytes: size-in-bytes	98304	9ee14454-b6f1-4210-a88a-e401599b4f71	☐		☒	f2b701d43a43315105d649612b2	Inherit event ⓘ
Network activity	url	http://automotivedreamteam.com/v.exe	e697650e-b672-405f-9be9-2dc39459a5e0	☒		☐	f2b701d43a43315105d649612b2	Inherit event ⓘ
Network activity	url	http://shop.palldogspoop.com/v.exe	a3986a11-4ee0-4b5-ba40-999666402cbc	☒		☐	f2b701d43a43315105d649612b2	Inherit event ⓘ
Network activity	url	http://pooperscoopfranchise.com/v.exe	3778d0bd-77b6-4186-a052-746a389509e0	☒		☐	f2b701d43a43315105d649612b2	Inherit event ⓘ
Network activity	url	http://cherryhillpooperscoopers.com/v.exe	b804db74-4a62-4cd7-abef-a4b68781411e	☒		☐	f2b701d43a43315105d649612b2	Inherit event ⓘ
Network activity	url	http://kiddogspoop.net/v.exe	09b672b8-62f9-469f-9c1f-53159d226444	☒		☐	f2b701d43a43315105d649612b2	Inherit event ⓘ
Network activity	url	http://kiddogspoop.mobi/v.exe	4bae6a06-b739-47ad-94c1-d583b2b9c4ae	☒		☐	f2b701d43a43315105d649612b2	Inherit event ⓘ
Network activity	url	http://kiddogspoop.info/v.exe	0f5ad15b-47ed-4772-act8-d2240a6e08c3	☒		☐	f2b701d43a43315105d649612b2	Inherit event ⓘ
Network activity	url	http://kiddogspoop.biz/v.exe	90b29d88-d778-4415-8544-5a2fc53d4f7	☒		☐	f2b701d43a43315105d649612b2	Inherit event ⓘ

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

WEB INTERFACE - QUERY

- Add multiple entries
- Choose different modules



The screenshot shows the MISP Web Interface Query page. On the left is a sidebar with navigation links: Home, History, History Session, History Tree, Config, and External tools. The main content area is titled "MISP Modules" and contains a search bar with the text "cird.lu". Below the search bar are two buttons: "Add new entry" and "Delete entry". Under the "Input Attributes" section, there is a dropdown menu showing "domain". In the "Modules" section, a box contains the text "X cird_passivedns". At the bottom, there is a checkbox labeled "Configure all modules".

MISP Modules

cird.lu

Add new entry Delete entry

Input Attributes

domain

Modules

X cird_passivedns

☐ Configure all modules

WEB INTERFACE - RESULTS

■ Multiple tabs for visualization in different formats

The screenshot displays the NSISP web interface for a DNS query. On the left is a sidebar with navigation links: Home, History, History Session, History Tree, Config, and External tools. The main content area is titled 'circ1.lu' and shows the 'Input Attribute: domain' and 'Modules: circ1_passivedns'. A progress bar indicates 100% completion, with a status message 'Stopped 11 Success, 0 Errors, 1 Total.' and a timestamp of '2024-07-08 13:34'. Below the progress bar are tabs for 'Visual', 'Json', and 'Markdown'. The 'Visual' tab is active, showing a tree view of the query results. The tree structure includes 'circ1.lu' (with an 'External tools' link) and 'circ1_passivedns' (with an upward arrow). Under 'circ1_passivedns', there are several sections: 'passive-dns' (with a circular icon), 'rrtype' (Type: text, Value: SOA, with a 'query' link), 'rrname' (Type: text, Value: ns1.eurodns.com hostmaster.eurodns.com 2023091306 43200 7200 1209600 86400, with a 'query' link), 'rdata' (Type: text, Value: circ1.lu, with a 'query' link), 'count' (Type: counter, Value: 260), 'origin' (Type: text, Value: https://www.circ1.lu/pdns/, with a 'query' link), and 'time_first'. On the right side of the main content area, there are three buttons: 'circ1.lu', 'Errors' (highlighted in blue), and 'circ1.lu'. At the bottom right, there is a '[Go Back Top]' link.

NSISP

Home

History

History Session

History Tree

Config

External tools

Menu

circ1.lu

Input Attribute: domain

Modules: circ1_passivedns

2024-07-08 13:34

100%

Stopped 11 Success, 0 Errors, 1 Total.

External tools

Visual Json Markdown

circ1.lu

External tools

circ1_passivedns

passive-dns

rrtype

Type: text

Value: SOA query

rrname

Type: text

Value: ns1.eurodns.com hostmaster.eurodns.com 2023091306 43200 7200 1209600 86400 query

rdata

Type: text

Value: circ1.lu query

count

Type: counter

Value: 260

origin

Type: text

Value: https://www.circ1.lu/pdns/ query

time_first

circ1.lu

Errors

circ1.lu

[Go Back Top]

■ Save your researches and pivot from them

The screenshot displays the MISP (Metasploit Information System) History interface. On the left is a sidebar with navigation links: Home, History, History Session, History Tree, Config, and External tools. The main content area is titled 'History' and includes a warning: 'All histories present here will be delete at the end of the session'. It shows a single history entry labeled '# 1'. This entry is a table with three columns: 'circl.lu' (containing 'domain'), 'Input Attributes' (containing 'domain'), and 'Modules' (containing 'circl_passivedns'). A red square icon is visible to the right of the table. A blue 'Save' button is located in the top right corner of the entry's container.

circl.lu	Input Attributes	Modules
domain	domain	circl_passivedns

WEB INTERFACE - EXTERNAL TOOLS (DEV)

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

The screenshot displays the 'External tools' section of the NISP Web Interface. On the left is a sidebar with navigation links: Home, History, History Session, History Tree, Config, and External tools. The main area is titled 'External tools' with a search bar and a list of tools. One tool, 'flowintel', is selected and its details are shown in a modal window.

External tools

Search tools

☒ flowintel

flowintel

Name: flowintel

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

[Save](#) [Delete](#)

[Go Back Top](#)

- 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.