

mail_to_misp

Connect your mail infrastructure to MISP to create

<http://www.misp-project.org/>

Twitter: *@MISPProject*

MISP Training @ CIRCL
20181218



MISP
Threat Sharing

- You receive emails with IoC's inside
- How to create an event out of it?
- Create event manually and copy paste
- → This works once or twice
- Forwarding the email would be nice
- → mail_to_misp

- Extraction of URLs and IP addresses and port numbers
- Extraction of hostnames from URLs
- Extraction of hashes (MD5, SHA1, SHA256)
- DNS expansion
- Subject filters
- Refanging of URLs ('hxxp://...')
- ... and more

FEATURES: SUPPORT MISP FEATURES

- Add tags automatically
- Ignore 'whitelisted' domains
- Configurable list of attributes not to enable the IDS flag
- DNS expansion
- Automatically create 'external analysis' links based on filter list (e.g. VirusTotal, malwr.com)
- Automatically filter out attributes that are on a server side warning list
- Support for value sighting
- ... and more

■ Legacy

- ▶ Email → Apple Mail → Mail rule → AppleScript
→ AppleScript → mail_to_misp → PyMISP → MISP
- ▶ Email → Thunderbird → Mail rule → filterscript →
thunderbird_wrapper → mail_to_misp → PyMISP → MISP

■ Postfix and others

- ▶ Email → mail_to_misp

■ mail_to_misp

1. `git clone`
`git://github.com/MISP/mail_to_misp.git`
2. Install dependencies - See Github site

■ MTA (Postfix or alike)

1. Setup a new email address in the aliases file (e.g. `/etc/aliases`)
`misp_handler: "|/path/to/mail_to_misp.py -"`
2. Rebuild the DB
`sudo newaliases`
3. Configure `mail_to_misp_config.py`

```
misp_url = 'http://127.0.0.1/'  
misp_key = 's5jPWClud36Z8XHgsiCVI7SaL1XsMTyfEsN45tTe'  
misp_verifycert = True  
body_config_prefix = 'm2m'  
...  
...
```

■ Bonus:

https://github.com/MISP/mail_to_misp_test

```
./mail_to_misp.py -r mail_to_misp_test/simple_forward.eml
```

■ Bonus: Fake-SMTPD spamtrap

```
./fake_smtp.py
```

```
telnet 127.0.0.1 2526
  Trying 127.0.0.1...
  Connected to 127.0.0.1.
  Escape character is '^]'.
  220 misp Python SMTP 1.1
  helo misp
  250 misp
  mail from: mikel
  250 OK
  rcpt to: m2m
  250 OK
  data
  354 End data with <CR><LF>.<CR><LF>
```