mail_to_misp

MAIL_TO_MISP CONNECT YOUR MAIL INFRASTRUCTURE TO MISS GRCL / Taxm MISP PROJECT HTTP://WWW.MISP-PROJECT.ORG/) TWITTE:- GOULD/PROJECT.ORG/)

CA. | Trans MSP Project PP-|| WWW.MSP-PROJECT.ORG | TITURE: @MISPPROJECT Threat Sha

MAIL_TO_MISP

CONNECT YOUR MAIL INFRASTRUCTURE TO MISP TO

CIRCL / TEAM MISP PROJECT

HTTP://WWW.MISP-PROJECT.ORG/

TWITTER: @MISPPROJECT

MISP PROJECT



CONTEXT

- 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
- \blacksquare \rightarrow mail_to_misp

mail_to_misp

**Wor receive enails with lock inside

**Wo

FEATURES: EMAIL HANDLING

- 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

mail_to_misp

Statestion of Milks and IP addresses and port numbers # totatestion of Johns States (Milks and IP addresses and port numbers # totatestion of Johns States (Milks States

2022-09

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

mail_to_misp

2022-09-13

-Features: Support MISP features

JRES: SUPPORT MISP FEATURES

Add tags automatically

re 'whitelisted' domains

Configurable list of attributes not to enable the IDS flag
 DNS expansion

Automatically create 'external analysis' links based on filt
 list (e.g. Misse Total malus com)

Autorial life out attributes that are on a server

warning list

Support for value sighting

■ Support for value sighti ■ ... and more

IMPLEMENTATION

Legacy

- ► Email → Apple Mail → Mail rule → AppleScript → AppleScript → mail_to_misp → PyMISP → MISP
- ► Email \rightarrow Thunderbird \rightarrow Mail rule \rightarrow filterscript \rightarrow thunderbird_wrapper \rightarrow mail_to_misp \rightarrow PyMISP \rightarrow MISP
- Postfix and others
 - ► Email → mail_to_misp

mail_to_misp

Ingle

Ingle

**Implementation

**Trucks and in the last one - Appendix of the Trucks and the Control of the Control of

INSTALLATION

- 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'
```

mail_to_misp mail_to_misp MTA (Postfox or alike) 2022--Installation

EXERCISE: MAIL 2 MISP.PY

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>
```

mail_to_misp

Brace

Brace

Street

St

2022-09