Feeding Your Bees

Imap2TheHive
TheHive in 30”

“Security Incident Response for the Masses”

https://thehive-project.org/
Email’ll Never Die!

I Don't Always Check my Email

But When I Do, I Miss Something Really Important.
Email’ll Never Die!

- OSSEC
- Splunk
- VTI
- Many many many home made hunting scripts
imap4thehive.py

xavier@barney:/usr/local/bin$ ./imap4thehive.py -h
usage: imap4thehive.py [-h] [-v] [-c CONFIG]

Process an IMAP folder to create TheHive alerts/cased.

optional arguments:
  -h, --help            show this help message and exit
  -v, --verbose         verbose output
  -c CONFIG, --config CONFIG
                          configuration file (default: /etc/imap4thehive.conf)

xavier@barney:/usr/local/bin$
imap4thehive.conf

```
xavier@barney: /usr/local/bin$ cat imap2thehive.conf
[imap]
  host: [REDACTED]
  port: 993
  user: [REDACTED]
  password: [REDACTED]
  folder: incoming
  expunge: false

[thehive]
  url: http://127.0.0.1:9000
  user: automation
  password: [REDACTED]
  observables: true
  whitelists: /usr/local/bin/imap2thehive.whitelists

[alert]
  tlp: 2
  tags: email
  keywords: \S*\(\|\(\|TVMISIOSSEC\)\|\)*

[case]
  tlp: 2
  tags: email
  tasks: Investigation,Communication,Tracking
  template: Default
  #files: application/pdf
xavier@barney: /usr/local/bin$
```
Features

• Uses TheHive4Py
• Creates Cases/Alerts
• Creates Tasks or use a pre-defined profile
• Adds tags
• Extracts IOC’s and creates observables
• Supports IOC’s whitelist
• Predefined TLP level
• Adds attachment based on MIME types
What’s Next?

- Extracts custom fields via regex
  (ex: internal assets, user names, ...)

- ???
https://blog.rootshell.be/2018/02/05/feeding-thehive-emails/
https://github.com/xme/dockers/tree/master/imap2thehive