

Feeding Your Bees

Imap2TheHive



TheHive in 30”

“Security Incident Response for the Masses”

The screenshot displays the TheHive web interface. At the top, the browser address bar shows 'https://'. The navigation bar includes 'TheHive' logo, a '+ New Case' button, and status indicators for 'My tasks 19', 'Waiting tasks 65', and 'Alerts 53'. A search bar is present with the text 'Case, user, URL, hash, IP, domain ...'. The user profile 'Xavier Mertens' is visible in the top right.

The main content area shows the details for 'Case # 512 - Compromized Wordpress site'. It includes a 'Show live stream' button, the creator 'Xavier Mertens', and the creation date 'Sat, Jun 9th, 2018 7:39 +02:00'. Action buttons for 'Close', 'Flag', 'Merge', and 'Share (0)' are provided.

Below the case header, there are tabs for 'Details', 'Tasks 1', 'Observables 7', and 'Investigate'. The 'Investigate' tab is active, showing a 'Basic Information' section with the following details:

Title	Investigate
Owner	Xavier Mertens
Date	Sat, Jun 9th, 2018 10:35 +02:00
Status	InProgress
Description	Not specified

The 'Task logs' section is currently empty, displaying 'No records'. It includes an 'Add new task log' button, a 'Sort by: Newest first' dropdown, and a '10 per page' selector.

At the bottom of the interface, the footer contains 'TheHive Project 2016-2017, AGPL-V3' on the left and 'Version: 3.0.9' with icons for help and chat on the right.

<https://thehive-project.org/>

Email'll Never Die!



Email'll Never Die!

- OSSEC
- Splunk
- VTI
- Many many many home made hunting scripts

imap4thehive.py

```
xavier@barney: /usr/local/bin
xavier@barney:/usr/local/bin$ ./imap2thehive.py -h
usage: imap2thehive.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/imap2thehive.conf)
xavier@barney:/usr/local/bin$
```

imap4thehive.conf

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

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

[alert]
tlp: 2
tags: email
keywords: \S*(ALERT|VTMIS|OSSEC)\S*

[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>



@xme | xavier@rootshell.be