IntelMQ – Use Cases and 2.0 Highlights
57th TF-CSIRT Meeting

Sebastian Wagner <wagner@cert.at>
Whois

Sebastian Wagner
Software Development and other things
At CERT.at since 2015
Part of nic.at
12 people

GovCERT Austria
Incident Handling Automation Project

~3 IHAP meetings/year

Often co-located with TF-CSIRT

Focus on Tooling, Development & Cooperation


ihap@lists.trusted-introducer.org

→ kaplan@cert.at
The IntelMQ project

Started in 2014

- We receive “Threat intelligence” feeds for AT
  - Infected systems, vulnerable servers, hacked websites, etc
- We want to contact the infrastructure owners

For CERTs, SOCs, other security teams

Included in MeliCERTes and csirt-kit
CERT.at’s role

Contributing most development

Maintainer role
- Packaging
- Release management

Co-financed by the Connecting Europe Facility of the European Union
Requirements I

- **Data Format**
  - Sanitation: Syntactical

- **Harmonization:**
  - Add Malware Family Name (optional)
  - Classification
    - Reference Incident Classification Taxonomy

- **Scalability**
Requirements II

• Easy to use
• Easy to extend
• Flexible in the data format
  - Extensible
  - But syntactical correctness
• Handle changes in feeds
Available Bots and Feeds

- 21 collectors
- 59 parsers
- 24 experts
- 15 outputs
- 138 documented feeds
class MyBot(Bot):
    def init(self):
        # optional initialization
    def process(self):
        event = self.receive_message()
        # process event
        self.send_message()

BOT = MyBot
Write a Bot

class MyBot(Bot):
    def init(self):
        with open('foobar.txt'):
            self.database = db.readlines()
    def process(self):
        event = self.receive_message()
        if 'source.ip' in event:
            if event['source.ip'] in self.database:
                event['source.tor_node'], True
            self.send_message()
BOT = MyBot
"do-portal"

- ISP
- Eventdownload
- stats portal
- Contact Portal
- CERT

Relations:
- ISP fetches from Eventdownload
- Eventdownload views stats portal
- stats portal provides data to IntelMQ
- CERT views Contact Portal
- Contact Portal queriesCERT
- CERT queries Eventdownload
- Eventdownload updates stats portal

https://github.com/certat/do-portal/
Classification.* over time

The following graph shows the 3 classification.* fields over time:

- "classification.taxonomy",
- "classification.type",
- "classification.identifier",

Panel Title

Taxonomy All* over time (log scale)

Type over time (log scale) / All

https://github.com/certtools/stats-portal/
Intelmq-mailgen / -fody

- Sending with SMTP
- Compatible with OTRS
- Rulesets and contacts from intelmq-fody
- Webinterface for tickets, contacts, rules, event database search & stats
- Developed by BSI/Intevation

https://github.com/Intevation/intelmq-mailgen/
https://github.com/Intevation/intelmq-fody/
https://github.com/Intevation/intelmq-mailgen/
https://github.com/Intevation/intelmq-fody/
# intelmq-webinput-csv

[GitHub Link](https://github.com/certat/intelmq-webinput-csv/)

### Timezone
+00:00

### Dry Run
- [x]

### Constant Fields (fallback):

**Classification Type**
- Malware Configuration

**Taxonomy**: Malicious Code

**Feed Code**
- oneshot

**Classification Identifier**
- test

### Table

<table>
<thead>
<tr>
<th>time</th>
<th>source.ip</th>
<th>destination.ip</th>
<th>protocol</th>
<th>port</th>
</tr>
</thead>
<tbody>
<tr>
<td>2018-12-09 02:53:18</td>
<td>85.126.145.244</td>
<td></td>
<td>tcp</td>
<td>548</td>
</tr>
<tr>
<td>2018-12-09 02:53:18</td>
<td>77.119.237.121</td>
<td></td>
<td>tcp</td>
<td>548</td>
</tr>
<tr>
<td>2018-12-09 02:53:18</td>
<td>77.119.229.227</td>
<td></td>
<td>tcp</td>
<td>548</td>
</tr>
<tr>
<td>2018-12-09 02:53:21</td>
<td>178.18.164.3</td>
<td></td>
<td>tcp</td>
<td>548</td>
</tr>
<tr>
<td>2018-12-09 02:53:21</td>
<td>78.132.127.172</td>
<td></td>
<td>tcp</td>
<td>548</td>
</tr>
<tr>
<td>2018-12-09 02:53:49</td>
<td>62.40.138.97</td>
<td></td>
<td>tcp</td>
<td>548</td>
</tr>
<tr>
<td>2018-12-09 02:53:49</td>
<td>212.197.156.245</td>
<td></td>
<td>tcp</td>
<td>548</td>
</tr>
</tbody>
</table>
IntelMQ & Manager 2.0

- Generic Multithreading
  - Additional to Multiprocessing
- AMQP as message broker
- *Named queues aka paths* (1.1)
- Bot load’s statistics
- Etc.
IntelMQ Manager 2.0

- Live View
- More interactive views
- Shortcuts
- Optional physics
- Etc.
Malware Name Mapping

- Goal: different names in different feeds for the same or very similar malware (version)
- Non-goal: map names between av vendors
- existing work done by Malpedia

https://github.com/certtools/malware_name_mapping
Contribute!

Sharing is caring

Thanks to Australia CSC, BSI/Intevation, CERT-EE, CERT-LV, CSIRT-CZ, NBU (CZ), SK-CERT, SWITCH, ...