Building Information Sharing Communities
Best Practices and Lessons Learned

CIRCL
Computer Incident Response Center
Luxembourg

Alexandre Dulaunoy @adulau
TLP:WHITE

MISP
Threat Sharing

Borderless Security -
September 8, 2016
The bright side of information sharing

- We build a community of 600 organizations with more than 1300 users sharing and updating daily cybersecurity indicators, financial indicators or threats in both ways.
- To achieve this we actively maintain and support MISP (an open source threat sharing platform).
- Beside the tools, practices, standard formats and classifications play an important role.
- These practices need to be shared among the communities to support efficient collaboration.

\(^1\) also called TIP, CTI platform. http://www.misp-project.org
How to be successful in building an information sharing community?

*There was never a plan. There was just a series of mistakes.*

Robert Caro, journalist.
MISP and starting from a practical use-case

- During a malware analysis workgroup in 2012, we discovered that we worked on the analysis of the same malware.
- We wanted to share information in an easy and automated way to avoid duplication of work.
- Christophe Vandeplas (then working at the CERT for the Belgian MoD) showed us his work on a platform that later became MISP.
- A first version of the MISP Platform was used by the MALWG and the increasing feedback of users helped us to build an improved platform.
- MISP is now a community-driven development.
Development based on practical user feedback

- There are many different types of users of an information sharing platform like MISP:
  - **Malware reversers** willing to share indicators of analysis with respective colleagues.
  - **Security analysts** searching, validating and using indicators in operational security.
  - **Intelligence analysts** gathering information about specific adversary groups.
  - **Law-enforcement** relying on indicators to support or bootstrap their DFIR cases.
  - **Risk analysis teams** willing to know about the new threats, likelyhood and occurences.
  - **Fraud analysts** willing to share financial indicators to detect financial frauds.
Many objectives from different user-groups

- Sharing indicators for a detection matter.
  - 'Do I have infected systems in my infrastructure or the ones I operate?'
- Sharing indicators to block.
  - 'I use these attributes to block, sinkhole or divert traffic.'
- Sharing indicators to perform intelligence.
  - 'Gathering information about campaigns and attacks. Are they related? Who is targeting me? Who are the adversaries?'
- → These objectives can be conflicting (e.g. False-positives have different impacts)
Sharing Difficulties

- Legal restriction
  - "Our legal framework doesn’t allow us to share information."
  - "Risk of information leak is too high and it’s too risky for our organization or partners."
- Practical restriction
  - "We don’t have information to share."
  - "We don’t have time to process or contribute indicators."
  - "Our model of classification doesn’t fit your model."
  - "Tools for sharing information are tied to a specific format, we use a different one."
Beyond Sharing Difficulties

The art of information sharing is to share more than your adversaries.
Quick MISP introduction

• MISP\(^2\) is an IOC and threat indicators sharing free software.
• MISP has **many functionalities** e.g. flexible sharing groups, automatic correlation, free-text import helper, event distribution and collaboration.
• MISP project recently grown into multiple sub-projects to support information sharing practices.
• CIRCL operates multiple MISP instances with a significant user base (more than 600 organizations with more than 1300 users).
• After some years of trial-and-error, we explain the background behind current and new **MISP features**.

\(^2\)https://github.com/MISP/MISP
MISP core distributed sharing functionality

- MISP’s core functionality is sharing where everyone can be a consumer and/or a contributor/producer.
- Quick benefit without the obligation to contribute.
- Low barrier access to get acquainted to the system.
Events and Attributes in MISP

- MISP attributes\(^3\) initially started with a standard set of "cyber security" indicators.
- MISP attributes are purely based on usage (what people and organizations use daily).
- Evolution of MISP attributes is based on practical usage and users (e.g. recent addition of the financial indicators in 2.4).
- In version 3.0, MISP objects and galaxy will be added to give the freedom to the community to create new and combined attributes and share them.

\(^3\)attributes can be anything that helps describe the intent of the event package from indicators, vulnerabilities or any relevant information
Helping Contributors in MISP

- Contributors can use the UI, API or using the freetext import to add events and attributes.
  - Modules existing in Viper (a binary framework for malware reverser) to populate and use MISP from the vty or via your IDA.
- Contribution can be direct by creating an event but users can propose attributes updates to the event owner.
- Users should not be forced to use a single interface to contribute.
Example: Freetext import in MISP

Freetext Import Tool

Paste a list of IOCs into the field below for automatic detection.

This is a sample text to show how indicators can be extracted. Just paste your text including indicators such as 23.100.122.175, host.microsoft.com, or b447c27a00e3a34881b0030177000cd here and the tool will automatically detect the indicators and save them as attributes - after allowing you to make some last minute changes. For more information, visit [https://www.github.com/MISP/MISP](https://www.github.com/MISP/MISP)

Submit

Cancel

Freetext Import Results

Below you can see the attributes that are to be created. Make sure that the categories and the types are correct, often several options will be offered based on an inclusive automatic resolution.

<table>
<thead>
<tr>
<th>Value</th>
<th>Category</th>
<th>Type</th>
<th>IDS</th>
<th>Comment</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>23.100.122.175</td>
<td>Network activity</td>
<td>ip-dst</td>
<td>Yes</td>
<td>Imported via the freetext import.</td>
<td>✗</td>
</tr>
<tr>
<td>host.microsoft.com</td>
<td>Network activity</td>
<td>hostname</td>
<td>Yes</td>
<td>Imported via the freetext import.</td>
<td>✗</td>
</tr>
<tr>
<td>b447c27a00e3a34881b0030177000cd</td>
<td>Payload delivery</td>
<td>md5</td>
<td>Yes</td>
<td>Imported via the freetext import.</td>
<td>✗</td>
</tr>
<tr>
<td><a href="https://www.github.com/MISP/MISP">https://www.github.com/MISP/MISP</a></td>
<td>Network activity</td>
<td>url</td>
<td>Yes</td>
<td>Imported via the freetext import.</td>
<td>✗</td>
</tr>
</tbody>
</table>

Submit

ip-dst → ip-src

Change all

Update all comment fields

Change all

<table>
<thead>
<tr>
<th>Date</th>
<th>Org</th>
<th>Category</th>
<th>Type</th>
<th>Value</th>
<th>Related Events</th>
<th>IDS</th>
<th>Distribution</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-02-24</td>
<td></td>
<td>Network activity</td>
<td>hostname</td>
<td>host.microsoft.com</td>
<td>Imported via the freetext import.</td>
<td>Yes</td>
<td>Inherit</td>
<td>✗</td>
</tr>
<tr>
<td>2016-02-24</td>
<td></td>
<td>Network activity</td>
<td>ip-dst</td>
<td>23.100.122.175</td>
<td>Imported via the freetext import.</td>
<td>Yes</td>
<td>Inherit</td>
<td>✗</td>
</tr>
<tr>
<td>2016-02-24</td>
<td></td>
<td>Network activity</td>
<td>url</td>
<td><a href="https://www.github.com/MISP/MISP">https://www.github.com/MISP/MISP</a></td>
<td>Imported via the freetext import.</td>
<td>Yes</td>
<td>Inherit</td>
<td>✗</td>
</tr>
<tr>
<td>2016-02-24</td>
<td></td>
<td>Payload delivery</td>
<td>md5</td>
<td>b447c27a00e3a34881b0030177000cd</td>
<td>Imported via the freetext import.</td>
<td>Yes</td>
<td>Inherit</td>
<td>✗</td>
</tr>
</tbody>
</table>
Supporting Sharing in MISP

• Delegate events publication to another organization (introduced in MISP 2.4.18).
  ○ The other organization can take over the ownership of an event and provide pseudo-anonymity to initial organization.
• Sharing groups allow custom sharing (introduced in MISP 2.4) per event or even at attribute level.
  ○ Sharing communities can be used locally or even cross MISP instances.
  ○ Sharing groups can be done at event level or attributes level (e.g. financial indicators shared to a financial sharing groups and cyber security indicators to CSIRT community).
Sightings support

- Sightings allow users to notify the community about the activities related to an indicator.
- Refresh time-to-live of an indicator.
- Sightings can be performed via API, and UI including import of STIX sighting documents.
- Many research opportunities in scoring indicators based on users sighting.
False-positive is a recurring challenge in information sharing.

In MISP 2.4.39, we introduced the misp-warninglists[^4] to help analysts in their day-to-day job.

Predefined lists of well-known indicators which are often false-positives like RFC1918 networks, public DNS resolver are included by default.

[^4]: https://github.com/MISP/misp-warninglists
Bootstrapping MISP with indicators

- We integrate default CIRCL OSINT feeds (TLP: WHITE selected from our communities) in MISP to allow users to ease their bootstrapping.
- The format of the OSINT is based on standard JSON MISP pulled from a remote TLS/HTTP server.
- Additional content providers (public, paid, private) can provide their own MISP feed.
- Allowing users to test their MISP installations and synchronization with a real dataset.
- Opening contribution to other threat intel feed but also allowing the analysis of overlapping data\(^5\).

\(^5\) A recurring challenge in information sharing
Conclusion

- **Information sharing practices come from usage** and by example (e.g. learning by imitation from the shared information).
- MISP is just a tool. What matters is your sharing practices. The tool should be as transparent as possible to support your internal practises.
- Enable users to customize threat intelligence platform to meet their community's use-cases or mimic the sharing practices of the adversaries.
Q&A

- info@circl.lu (if you want to join the CIRCL MISP sharing community)
- OpenPGP fingerprint: 3B12 DCC2 82FA 2931 2F5B 709A 09E2 CD49 44E6 CBCD
- https://www.circl.lu/services/misp-malware-information-sharing-platform/