Building and designing MISP

A practical information-sharing tool for cybersecurity and fraud indicators

CIRCL
Computer Incident
Response Center
Luxembourg

MISP
Threat Sharing

Alexandre Dulaunoy @adulau

TLP:WHITE

O'Reilly Security 20161111

The bright side of information sharing

- CIRCL has 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[1] 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?'
- $\rightarrow$ These objectives can be conflicting (e.g. False-positives have different impacts)

Sharing Difficulties

- Sharing difficulties are not really technical issues but often it's a matter of **social interactions** (e.g. **trust**).
- 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 (and smarter) than your adversaries.

MISP Project Overview

- The **core project**[a] (PHP/Python) supports the backend, API and UI.
- Modules (Python) to expand MISP functionalities (import, export or enrich).
- Taxonomies (JSON) to add categories and global tagging.
- Warning-lists (JSON) to help analysts to detect potential false-positives.
- Galaxy (JSON) to add threat-actors, tools or "intelligence".

[a] `http://github.com/MISP/`

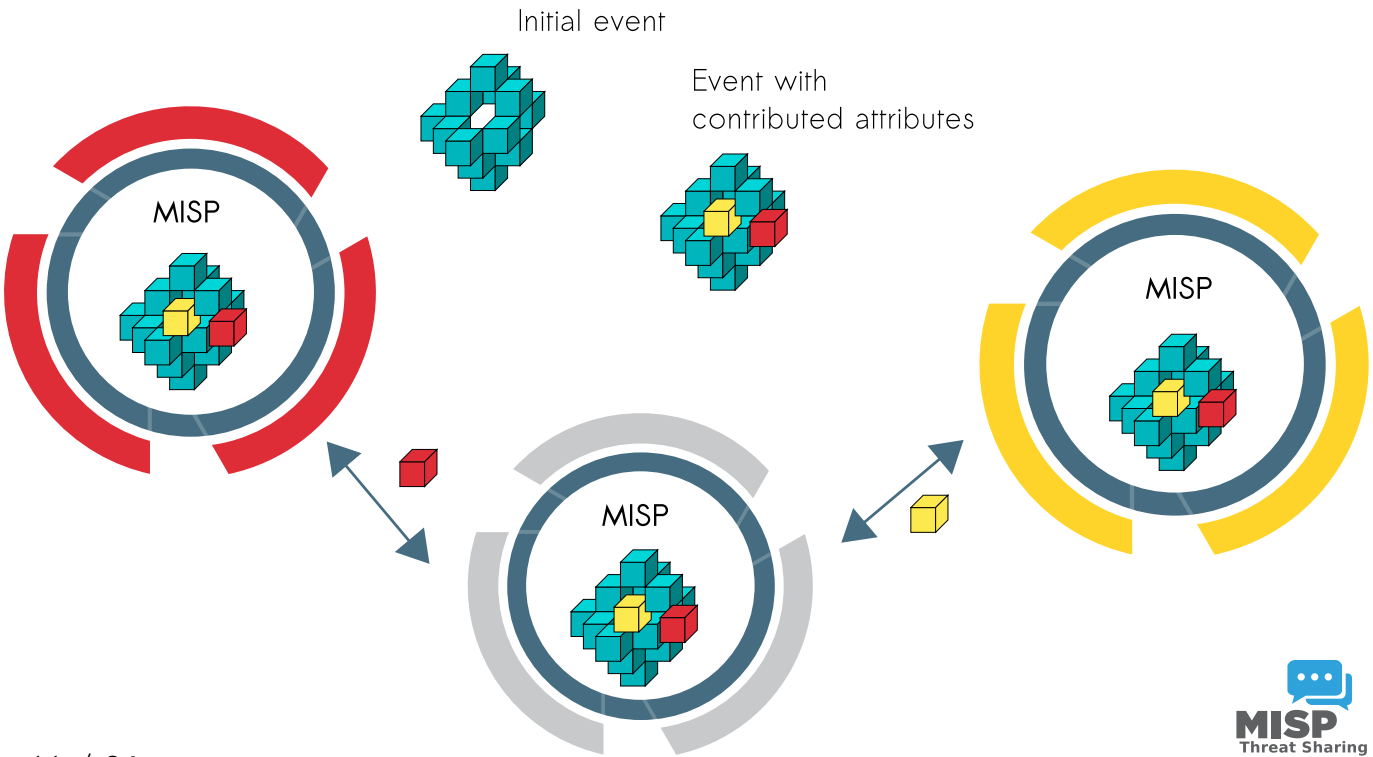
MISP features

- 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.
- Many export formats which support IDSes / IPSes (e.g. Suricata, Bro, Snort), SIEMs (eg CEF), Host scanners (e.g. OpenIOC, STIX, CSV, yara), analysis tools (e.g. Maltego), DNS policies (e.g. RPZ)
- 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

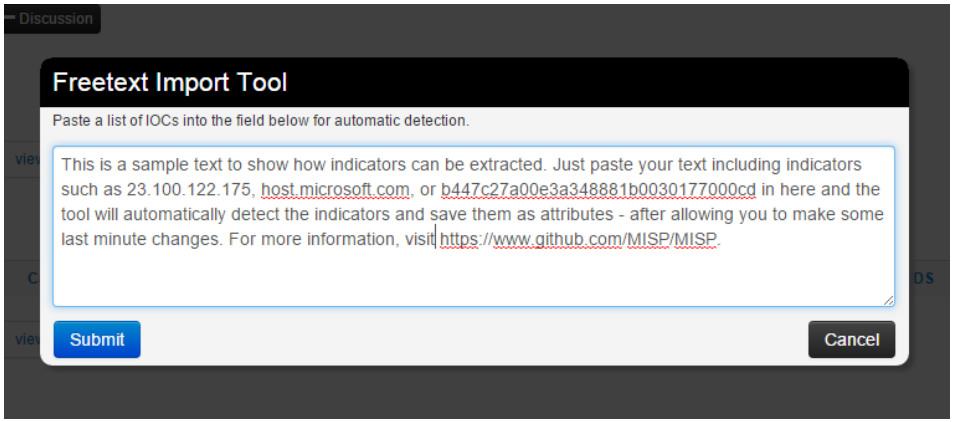
- MISP attributes[3] initially started with a standard set of "cyber security" indicators.
- MISP attributes are purely **based on usage** (what people and organizations use daily).
- Evolution of MISP attributes is based on practical usage and users (e.g. recent addition of the **financial indicators** in 2.4).
- In next release, MISP 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

Contributing data to MISP

- Offering a wide range of data creation possibilities
  - Various ways of contributing data via the MISP UI including a freetext parser and a dynamic templating system
  - Flexible APIs that ease automation
  - PyMISP Python library
  - Import tools and Python Import/Enrichment module system
  - Integration with external tools such as Viper, sandboxes such as Cuckoo, etc
- Contribution can be direct by creating an event but **users can propose attributes updates** to the event owner or simply indicate a sighting.
- **Users should not be forced to use a single interface to contribute**.

Example: Freetext import in MISP



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 inconclusive automatic resolution.

Value	Category	Type	IDS	Comment	Actions
23.100.122.175	Network activity	ip-dst	☑	Imported via the freetext import.	✖
host.microsoft.com	Network activity	hostname	☑	Imported via the freetext import.	✖
b447c27a00e3a348881b0030177000cd	Payload delivery	md5	☑	Imported via the freetext import.	✖
https://www.github.com/MISP/MISP	Network activity	url	☑	Imported via the freetext import.	✖

Submit

ip-dst → ip-src Change all

Update all comment fields Change all

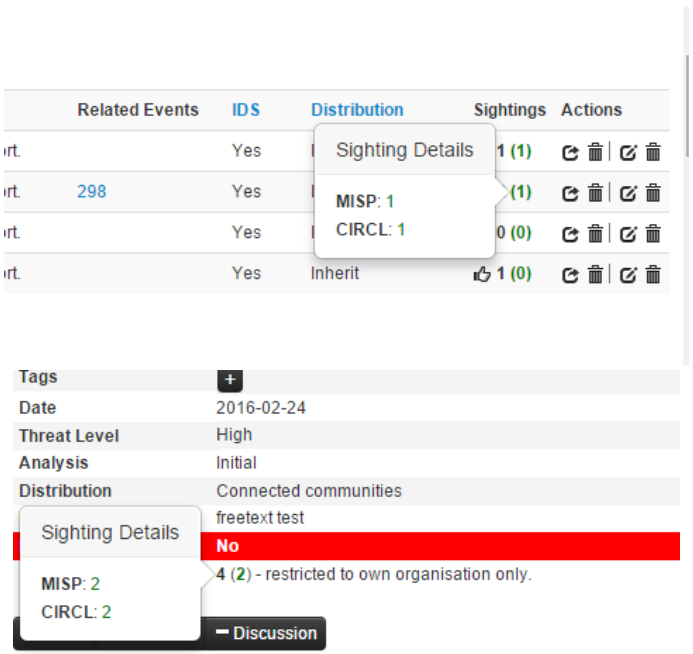
Filters: All File Network Financial Proposal Correlation

Date	Org	Category	Type	Value	Comment	Related Events	IDS	Distribution	Actions
2016-02-24		Network activity	hostname	host.microsoft.com	Imported via the freetext import.		Yes	Inherit	
2016-02-24		Network activity	ip-dst	23.100.122.175	Imported via the freetext import.	298	Yes	Inherit	
2016-02-24		Network activity	url	https://www.github.com/MISP/MISP	Imported via the freetext import.		Yes	Inherit	
2016-02-24		Payload delivery	md5	b447c27a00e3a348881b0030177000cd	Imported via the freetext import.		Yes	Inherit	

Supporting Sharing in MISP

- Delegate event 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 for the 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 across MISP instances.
  - **Sharing groups** can be done at **event level or attribute level** (e.g. financial indicators shared to a financial sharing group and cyber security indicators to CSIRT community).

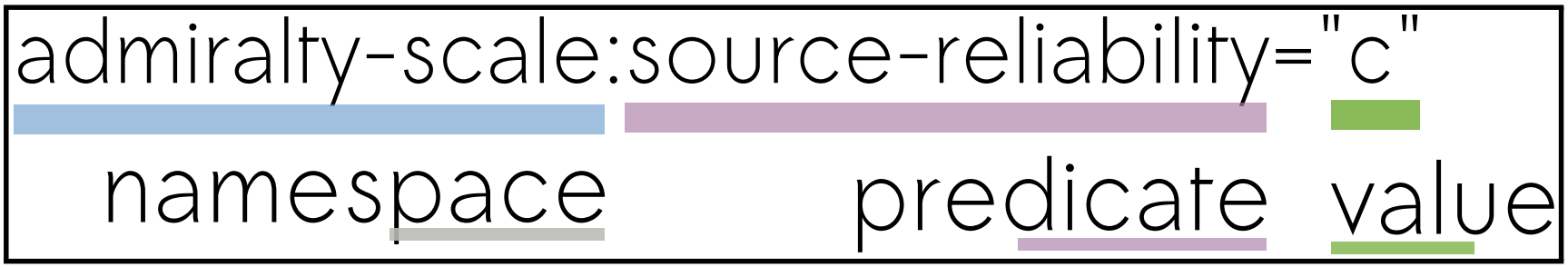
Sightings support



- 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 user's sighting.

Machine Tags

- Triple tag (or machine tag) was introduced in 2004 to extend geotagging on images.



- A machine tag is just a tag expressed in way that allows systems to parse and interpret it.
- Still have a human-readable version:
  - admiralty-scale:Source Reliability="Fairly reliable"

MISP taxonomy statistics and overview

Statistics

Usage data | Organisations | Tags | Attribute histogram

A treemap of the currently used event tags. Click on any of the taxonomies to hide it and click it again to show it.

34+ taxonomies available

- NATO - **Admiralty Scale**
- CIRCL Taxonomy - **Schemes of Classification in Incident Response and Detection**
- eCSIRT and IntelMQ incident classification
- EUCI **EU classified information marking**
- NATO Classification Marking
- OSINT **Open Source Intelligence - Classification**
- TLP - **Traffic Light Protocol**
- Vocabulary for Event Recording and Incident Sharing - **VERIS**
- and many more like **ENISA**, **Europol**, or the FIRST SIG Information Exchange Policy.

MISP taxonomy in use

LOCKY Ransomware via .doc/.docm/.xls/.zip(.js) files (c...

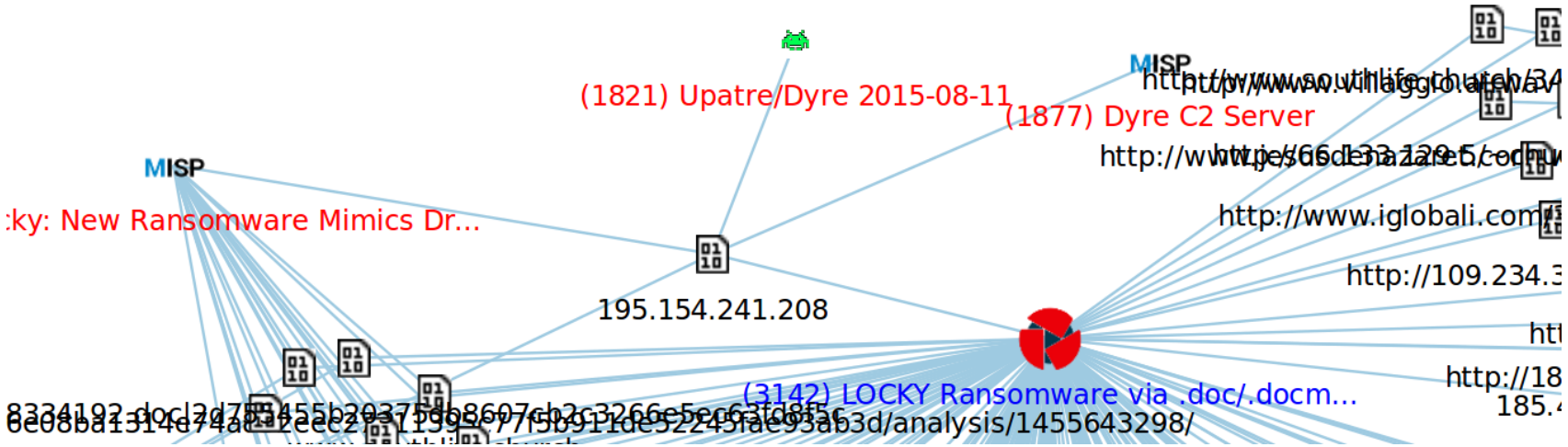
Event ID	3142
Uuid	56c2ff95-bd44-4677-8de9-3dec950d210f
Org	CIRCL
Owner org	CIRCL
Contributors	CERT
Email	sascha.rommelfangen@circl.lu
Tags	circl:incident-classification="malware" x tlp:white x ecsirt:malicious-code="ransomware" x veris:action:malware:variety="Ransomware" x ms-caro-malware:malware-type="Ransom" x enisa:nefarious-activity-abuse="ransomware" x +
Date	2016-02-16
Threat Level	Medium
Analysis	Completed
Distribution	All communities
Info	LOCKY Ransomware via .doc/.docm/.xls/.zip(.js) files (constantly updated)
Published	Yes
Sightings	0 (0)

- **Classification must be globally used to be efficient**.
- Tagging can be combined following the needs of the organizations.

Where Information Sharing Helped

- Suspicious executables which require shared analysis or evaluation (**pre-investigation** stage).
- Tracking financial malware including related cash out bank accounts (mixed events (IoC and financial indicators) with different sharing groups).
- Fake invoicing fraud bank details shared to discover the same mule acquisition network.
- Finding stable infrastructure of adversaries (malware targeting financial sector) by **sharing regularly**.

Practical Example: Benefit of 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 practices.
- Enable users to customize threat intelligence platform to meet their community's use-cases or **mimic the sharing practices of the adversaries**.
- With adequate automation, **information overflow can become an advantage** (e.g. automated take-down request).

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://github.com/MISP/` - `http://www.misp-project.org/`
- Join us in Zurich the 6th December for a training and/or the 7th December for building the next features in MISP.