Four years of practical information sharing
MISP - Malware Information Sharing Platform & Threat Sharing

CIRCL
Computer Incident
Response Center
Luxembourg

Alexandre Dulaunoy -
TLP:WHITE

April 18, 2016
ADACOR workshop

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.

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, likelihood 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

- 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."

Quick MISP introduction

- MISP[1] 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.
- CIRCL operates multiple MISP instances with a significant user base (around 320 organizations with 800 users).
- After some years of trial-and-error, we explain the background behind current and new **MISP features**.

---

[1]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.
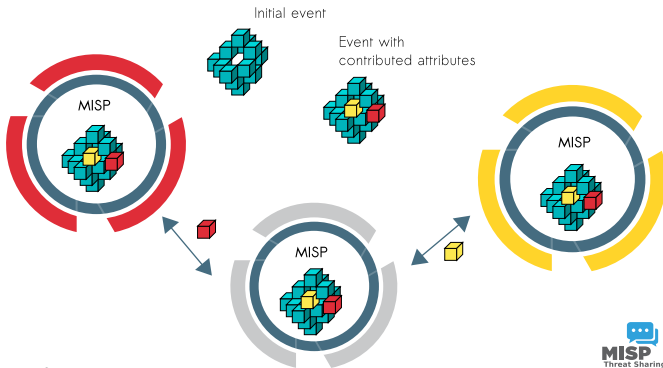
Events and Attributes in MISP

- MISP attributes[2] 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 will be added to give the freedom to the **community to create new and combined attributes** and share them.

---

[2]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

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).

From Tagging to Flexible Taxonomies

OSINT - Cyberthreats BlackEnergy2

Event ID	2910
Uuid	568e7167-4e00-4654-b5f8-4b23950d210f
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	alexandre.dulaunoy@circl.lu
Tags	tlp:white X Type:OSINT X +
Date	2016-01-07
Threat Level	Medium

- Tagging is a simple way to attach a classification to an event.
- In the early version of MISP, tagging was local to an instance.
- After evaluating different solutions of classification, we build a new scheme using the concept of machine tags.

Machine Tags

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

admiralty-scale:source-reliability="c"

    namespace   predicate value

- 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 Taxonomies

- Taxonomies are implemented in a simple JSON format.
- Anyone can create their own taxonomy or reuse an existing one.
- The taxonomies are in an independent git repository[3].
- These can be freely reused and integrated in other threat intel tools.

---

[3]https://www.github.com/MISP/misp-taxonomies/

Existing Taxonomies

- NATO - **Admiralty Scale**
- CIRCL Taxonomy - **Schemes of Classification in Incident Response and Detection**
- eCSIRT and IntelMQ incident classification
- EUCI **EU classified information marking**
- Information Security Marking Metadata from DNI (Director of National Intelligence - US)
- NATO Classification Marking
- OSINT **Open Source Intelligence** - **Classification**
- TLP - **Traffic Light Protocol**
- Vocabulary for Event Recording and Incident Sharing - **VERIS**

Want to write your own taxonomy? 1/2

```
1  {
2    "namespace": "admiralty-scale",
3    "description": "The Admiralty Scale (also called the NATO
         System) is used to rank the reliability of a source and
         the credibility of an information.",
4    "version": 1,
5    "predicates": [
6       {
7         "value": "source-reliability",
8         "expanded": "Source Reliability"
9       },
10      {
11        "value": "information-credibility",
12        "expanded": "Information Credibility"
13      }
14    ],
15  ....
```

```
 1  {
 2    "values": [
 3      {
 4        "predicate": "source-reliability",
 5        "entry": [
 6          {
 7            "value": "a",
 8            "expanded": "Completely reliable"
 9          },
10  ....
```

- Publishing your taxonomy is as easy as a simple git pull request on misp-taxonomies[4].

---

[4]https://github.com/MISP/misp-taxonomies

How are taxonomies integrated in MISP?

10	✖	TO:HIDE		2	☑ 🗑
9	✖	TODO		8	☑ 🗑
11	✖	TODO:VT-ENRICHMENT		9	☑ 🗑
1	✔	Type:OSINT		932	☑ 🗑
18	✔	admiralty-scale:information-credibility="1"	admiralty-scale	0	☑ 🗑
19	✔	admiralty-scale:information-credibility="2"	admiralty-scale	1	☑ 🗑
20	✔	admiralty-scale:information-credibility="3"	admiralty-scale	3	☑ 🗑
21	✔	admiralty-scale:information-credibility="4"	admiralty-scale	0	☑ 🗑
22	✔	admiralty-scale:information-credibility="5"	admiralty-scale	1	☑ 🗑
23	✔	admiralty-scale:information-credibility="6"	admiralty-scale	2	☑ 🗑

- MISP administrator can just import (or even cherry pick) the namespace or predicates they want to use as tag.

- Tags can be exported to other instances.

- Tags are also accessible via the MISP REST API.

Filtering the distribution of events among MISP instances

- Applying rules for distribution based on tags:

Other use cases using MISP taxonomies

- Tags can be used to set events for further processing by external tools (e.g. VirusTotal auto-expansion using Viper).
- Ensuring a classification manager classifies the events before release (e.g. release of information from air-gapped/classified networks).
- Enriching IDS export with tags to fit your NIDS deployment.
- Operational CSIRT activities on take-down and abuse handling can use their own taxonomy tags.

Future functionalities related to MISP taxonomies

- Sighting support (thanks to NCSC-NL) will be integrated in MISP allowing to auto expire IOC based on user detection.
- Adjusting taxonomies (adding/removing tags) based on their score or visibility via sighting.
- Simple taxonomy editors to help non-technical users to create their taxonomies.
- Taxonomies at attributes level.
- More public taxonomies to be included (Europol taxonomy will be included very soon).

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.
- Project sponsored by NCSC-NL.
- Many research opportunities in scoring indicators based on users sighting.

MISP modules - extending MISP with Python scripts

MISP expansion modules

- IP address expansion
- VirusTotal
- VIPER modules
- Your module
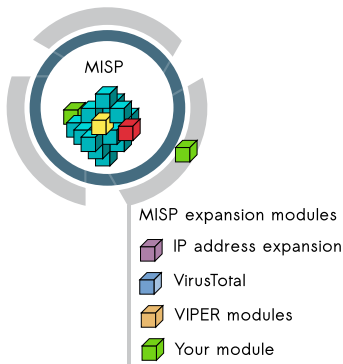
- Extending MISP with expansion modules with zero customization in MISP.
- A simple ReST API between the modules and MISP allowing auto-discovery of new modules with their features.
- Benefit from existing Python modules in Viper or any other tools.
- Current modules include: Passive Total, Passive SSL/DNS (CIRCL), CVE expansion…

MISP modules - How it's integrated in the UI?
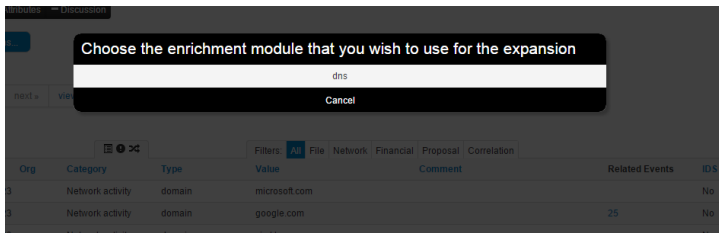
Bootstrapping MISP with indicators

- 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 can provide their own MISP feed. (https://botvrij.eu/)
- 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

What's cooking?

MISP next features and work in progress

MISP objects

- Objective: create a semi-dynamic data model.
- Using existing MISP attributes to build new objects.
- **Share the object designs within partners automatically along with the events shared** (e.g. allowing to share events with yet unknown objects).
- Have a community-driven set of default objects.
- Early work already accessible, it's also open source.

MISP galaxy

- MISP galaxy is a simple method to express a large object called cluster that can be attached to MISP events or attributes.
- A cluster can be composed of one or more elements. Elements are expressed as key-values.
- Existing clusters and elements like threat actors, adversary groups, attacker tools, campaigns are available.
- There are default elements available in MISP galaxy but those can be overwritten, replaced or updated as you wish.

MISP galaxy - elements of threat actors

- An element list of threat actors included by default.

```
 1                {
 2                  "synonyms" : [
 3                    "PLA Unit 61486",
 4                    "APT 2",
 5                    "Group 36",
 6                    "APT-2",
 7                    "MSUpdater",
 8                    "4HCrew",
 9                    "SULPHUR"
10                  ],
11                  "country" : "CN",
12                  "refs" : [
13                    "http://cdn0.vox-cdn.com/assets/4589853/
14                      crowdstrike-intelligence-report-putter-panda.
                          original.pdf"
15                  ],
16                  "description" : "The CrowdStrike Intelligence
                      team has been
17                 tracking this particular unit since 2012,
18                 under the codename PUTTER PANDA, and has
                      documented activity
19                 dating back to 2007. The report identifies
20                 Chen Ping, aka cpyy, and the primary location of
                      Unit 61486. ",
21                  "group" : "Putter Panda"
22                }
```

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 you.
- Enable users to customize MISP to meet their community's use-cases.
- **Contributions and ideas originate from the community of users**.
- Ongoing research ideas on the operational MISP platforms like "gamification of information sharing" or "sharing of privacy-aware datastructure".

Q&A

- `https://github.com/MISP/MISP`
- `https://github.com/MISP/` for misp-modules, misp-objects and misp-taxonomies
- info@circl.lu (if you want to join one of the MISP community operated by CIRCL)
- PGP key fingerprint: CA57 2205 C002 4E06 BA70 BE89 EAAD CFFC 22BD 4CD5