What's next?
MISP - Malware Information Sharing Platform & Threat Sharing

CIRCL
Computer Incident
Response Center
Luxembourg

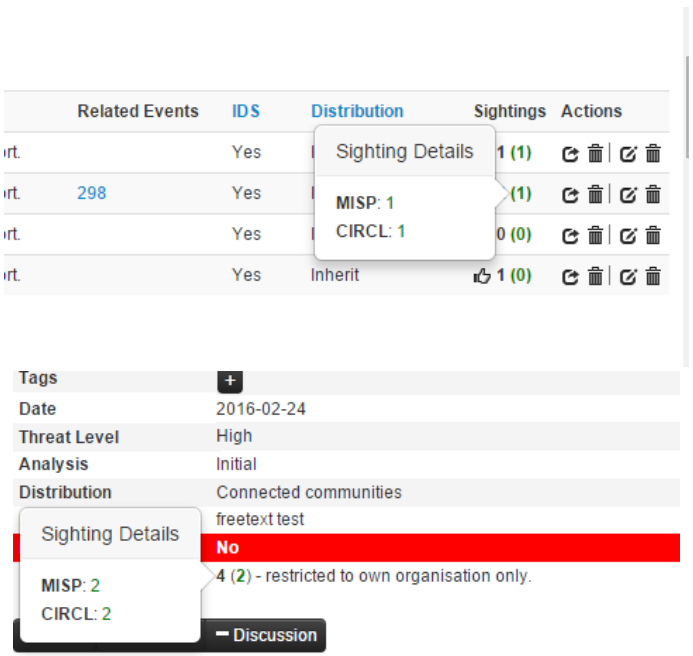
Alexandre Dulaunoy -
Andras Iklody - *TLP:WHITE*

March 22, 2016

What's cooking?

MISP next features and work in progress

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, TAXII and UI.
- Project sponsored by NCSC-NL.
- To be released in 2.5.

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.

```
{
 "synonyms": [
   "PLA Unit 61486",
   "APT 2",
   "Group 36",
   "APT-2",
   "MSUpdater",
   "4HCrew",
   "SULPHUR"
 ],
 "country": "CN",
 "refs": [
   "http://cdn0.vox-cdn.com/assets/4589853/
    crowdstrike-intelligence-report-putter-
       panda.original.pdf"
 ],
 "description": "The CrowdStrike
    Intelligence team has been
 tracking this particular unit since 2012,
 under the codename PUTTER PANDA, and has
    documented activity
 dating back to 2007. The report identifies
 Chen Ping, aka cpyy, and the primary
    location of Unit 61486. ",
 "group": "Putter Panda"
}
```

MISP galaxy - elements of threat actors tools

- An element list of tools used by various threat actors.
- The key-values can be freely combined.

```
            {
              "value": "MSUpdater"
            },
            {
              "value": "Poison Ivy",
              "description": "Poison Ivy is a RAT which
                  was freely available and first
                  released in 2005.",
              "refs": ["https://www.fireeye.com/content/
                  dam/fireeye-www/global/en/current-
                  threats/pdfs/rpt-poison-ivy.pdf"]
            },
            {
              "value": "Torn RAT"
            },
            {
              "value": "ZeGhost"
            },
            {
              "value": "Elise Backdoor",
              "synonyms": ["Elise"]
            }
```

MISP galaxy - A cluster is composed of various elements

```
{
"name" : "threat actor",
"description": "threat actor cluster",
"version": 1,
"elementOneOf": ["adversary-groups", "threat-actor-intended-effect-vocabulary", "planning-and-operational-support-vocabulary", "threat-actor-motivation-vocabulary", "threat-actor-type-vocabulary", "threat-actor-sophistication-vocabulary", "certainty-level", "threat-actor-tools"]
}
```

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.
- MISP is evolving into a modular tool for information sharing and "CTI".
- Contributions and ideas originate from the community of users.

Q&A

- `https://github.com/MISP/MISP`
- `https://github.com/MISP/` for misp-modules, misp-objects, misp-taxonomies and misp-galaxy.
- 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