MISP Workbench - Because you know better

MISP - Malware Information Sharing Platform & Threat Sharing

Marion Marschalek - Raphaël Vinot - *TLP:WHITE*

CIRCL
Computer Incident Response Center Luxembourg

July 6, 2016

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)

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.
- 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 400 organizations with more than 1000 users).

[1] https://github.com/MISP/MISP

Missing functionalities

- Impossible to **merge events** (campaign, attacker, tool, victim, ...)
- Impossible to **compare campaigns** composed of multiple events
- **Hard to expand** in a timely manner (PHP, apache, MySQL, ...)
- Limited extraction of PE indicators & correlation
- No simple way to limit an investigation on a **subset of events**
- Impossible to do **very fast lookups** or to use the dataset in an **untrusted environment**

MISP Galaxy

- List of known keywords:
  - Adversary groups (with synonyms)
  - Threat actors tools (with synonyms)
- Used to automatically group related events

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": "Elise Backdoor",
  "synonyms": ["Elise"]
}
```

PE indicators

- Original filename
- Compilation timestamp
- Import hashes
- Number of sections
- Entry points
- Soon: API calls
- Soon: Entropy of the sections
- Soon: Fuzzy hashing on the import table

SSDeep Clustering

- Compute SSDeep hashes on big datasets
- Group samples by similarity
- Allow to pick groups with a certain level of similarities
- Especially interesting on targeted and/or unpaked samples

MISP Hashstore

- Allow very **fast lookups** against big dataset.
- Only store hashed versions of the attributes.
- Can be used on untrusted or compromised systems (comparable to **bloom filter**).
- Hashstore can be used for forensic analysis (e.g. compare baseline
- Beta version available[2].

[2] `https://github.com/MISP/misp-workbench/tree/master/hashstore`

MISP Workbench

- Objective: bundle all the functionalities in one single tool
- Easily **enrich MISP dataset** with other fields (specially PE indicators)
- Simple connectors with other tools and datasets
- **Group events** using galaxies (adversaries and tools)
- **Full text indexing** and lookups for other keywords
- Display the amount of unique MISP events matching a PE attribute
- Single user **lightweitht interface**
- Stantalone and offline

Implementation

- Full python 3
- Redis backend
- Whoosh full text indexer
- Pefile for the PE processing, radare2 will be used soon
- Flask + bootstrap web interface

Setup

- Export MySQL to Redis
  - Full snapshot for workbench
  - Partial snapshot for hashstore
- Doesn't respect MISP ACL
- Redis database can be moved to an other system
- Run full text indexing
- Import the PE indicators
- Run ssdeep correlation

Demo time!

Q&A

- `https://github.com/MISP/misp-workbench`
- `https://github.com/MISP/misp-galaxy`
- `https://github.com/MISP/data-processing`
- `https://github.com/CIRCL/ssdc`
- We welcome new functionalities and pull requests.

hack.lu 2016