MISP Galaxy

Team CIRCL

http://www.misp-project.org/
Twitter: @MISPProject

MISP Training @ Luxembourg December Edition 2019
20191203
MISP started out as a platform for technical indicator sharing.

The need for a way to describe threat actors, tools and other commonalities became more and more pressing.

**Taxonomies quickly became essential for classifying events.**

The weakness of the tagging approach is that it’s not very descriptive.

We needed a way to attach more complex structures to data.

Also, with the different naming conventions for the same "thing" attribution was a mess.

This is where the Galaxy concept came in.
Solution

- Pre-crafted galaxy "clusters" via GitHub project
- Attach them to an event and attribute(s)
- The main design principle was that these higher level informations are meant for human consumption
- This means flexibility - key value pairs, describe them dynamically
- Technical indicators remain strongly typed and validated, galaxies are loose key value lists
The Galaxy Object Stack

- **Galaxy**: The type of data described (Threat actor, Tool, ...)
- **Cluster**: An individual instance of the galaxy (Sofacy, Turla, ...)
- **Element**: Key value pairs describing the cluster (Country: RU, Synonym: APT28, Fancy Bear)
- **Reference**: Referenced galaxy cluster (Such as a threat actor using a specific tool)
(Some) Existing Galaxies

- **Exploit-Kit**: An enumeration of known exploitation kits used by adversaries
- **Microsoft activity group**: Adversary groups as defined by Microsoft
- **Preventive measure**: Potential preventive measures against threats
- **Ransomware**: List of known ransomwares
- **TDS**: Traffic Direction System used by adversaries
- **Threat-Actor**: Known or estimated adversary groups
- **Tool**: Tools used by adversaries (from Malware to common tools)
- **MITRE ATT&CK**: Adversarial Tactics, Techniques, and Common Knowledge (ATT&CK™)
What a cluster looks like

Galaxies

**Threat Actor**

- **Sofacy**
  - **Description**: The Sofacy Group (also known as APT28, Pawn Storm, Fancy Bear and Sednit) is a cyber espionage group believed to have ties to the Russian government. Likely operating since 2007, the group is known to target government, military, and security organizations. It has been characterized as an advanced persistent threat.

  **Synonyms**: APT 28, APT28, Pawn Storm, Fancy Bear, Sednit, TsarTeam, TG-4127, Group-4127, STRONTIUM, Grey-Cloud

**Source**: MISP Project

**Authors**: Alexandre Dulaunoy, Florian Roth, Thomas Schreck, Timo Steffens, Various

**Country**: RU

Internally simply using a taxonomy-like tag to attach them to events

Example: misp-galaxy:threat-actor="Sofacy"

**Synchronisation works out of the box** with older instances too. They will simply see the tags until they upgrade.

Currently, as mentioned we rely on the community’s contribution of galaxies
ATTACHING CLUSTERS

- Use a searchable synonym database to find what you’re after
Creating your own galaxy

- Creating galaxy clusters has to be straightforward to get the community to contribute
- Building on the prior success of the taxonomies and warninglists
- Simple JSON format in similar fashion
- Just drop the JSON in the proper directory and let MISP ingest it
- We always look forward to contributions to our galaxies repository
If you want to create a completely new galaxy instead of enriching an existing one

```json
{
    "name": "Threat Actor",
    "type": "threat-actor",
    "description": "Threat actors are characteristics of malicious actors (or adversaries) representing a cyber attack threat including presumed intent and historically observed behaviour.",
    "version": 1,
    "uuid": "698774c7-8022-42c4-917f-8d6e4f06ada3"
}
```
Clusters contain the meat of the data

Skeleton structure as follows

```json
{
    "values": [
        {
            "meta": {},
            "description": "",
            "value": "",
            "related_clusters": [{}],
        }
    ]
}
```
Cluster JSON value example

```json
{
    "meta": {
        "synonyms": [
            "APT 28", "APT28", "Pawn Storm", "Fancy Bear",
            "Sednit", "TsarTeam", "TG–4127", "Group–4127",
            "STRONTIUM", "Grey–Cloud"
        ],
        "country": "RU",
        "refs": [
            "https://en.wikipedia.org/wiki/Sofacy_Group"
        ]
    },
    "description": "The Sofacy Group (also known as APT28, Pawn Storm, Fancy Bear and Sednit) is a cyber espionage group believed to have ties to the Russian government. Likely operating since 2007, the group is known to target government, military, and security organizations. It has been characterized as an advanced persistent threat.",
    "value": "Sofacy"
}
```
Reusing existing values such as complexity, effectiveness, country, possible_issues, colour, motive, impact, refs, synonyms, derivated_from, status, date, encryption, extensions, ransomnotes, cfr-suspected-victims, cfr-suspected-state-sponsor, cfr-type-of-incident, cfr-target-category, kill_chain.

Or adding your own meta fields.
"description": "Putter Panda were the subject of an extensive report by CrowdStrike, which stated: '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.'",

"meta": {
  "cfr−suspected−state−sponsor": "China",
  "cfr−suspected−victims": [
    "U.S. satellite and aerospace sector"
  ],
  "cfr−target−category": [
    "Private sector",
    "Government"
  ],
  "cfr−type−of−incident": "Espionage",
  "country": "CN",
  "refs": [
    "http://cdnO.vox−cdn.com/assets/4589853/crowdstrike−intelligence−report−putter−panda.original.pdf",
    "https://www.cfr.org/interactive/cyber−operations/putter−panda"
  ]
}
# Galaxy JSON Matrix-Like

<table>
<thead>
<tr>
<th>Propose Attribute</th>
<th>Analysis</th>
<th>Initial</th>
</tr>
</thead>
<tbody>
<tr>
<td>Setup</td>
<td>party/candidate registration (3 items)</td>
<td>Setup</td>
</tr>
<tr>
<td>DoS or overload of party/campaign registration, causing them to miss the deadline</td>
<td>Deleting or tampering with voter data</td>
<td>Hacking campaign websites (defacement, DoS)</td>
</tr>
<tr>
<td>Fabricated signatures from sponsor</td>
<td>DoS or overload of voter registration system, suppressing voters</td>
<td>Hacking candidate laptops or email accounts</td>
</tr>
<tr>
<td>Tampering with registrations</td>
<td>Identity fraud during voter registration</td>
<td>Leak of confidential information</td>
</tr>
</tbody>
</table>

Select Some Options
"description": "Universal Development and Security Guidelines as Applicable to Election Technology.",
"icon": "map",
"kill_chain_order": {
  "example-of-threats": [
    "setup | party/candidate-registration",
    "setup | electoral-rolls",
    "campaign | campaign-IT",
    "all-phases | government-IT",
    "voting | election-technology",
    "campaign/public-communication | media/press"
  ]
},
"name": "Election guidelines",
"namespace": "misp",
"type": "guidelines",
"uuid": "c1dc03b2–89b3–42a5–9d41–782ef726435a",
"version": 1


```json
1 {
2   "description": "DoS or overload of party/campaign registration, causing them to miss the deadline",
3   "meta": {
4     "date": "March 2018."
5     "kill_chain": [ "Define in which column the cluster should be placed"
6       "example-of-threats:setup | party/candidate-registration"
7     ],
8     "refs": [
10      ]
11   },
12   "uuid": "154c6186–a007–4460–a029–ea23163448fe",
13   "value": "DoS or overload of party/campaign registration, causing them to miss the deadline"
14 }
```
Cluster can be related to one or more clusters using default relationships from MISP objects and a list of tags to classify the relation.

```
"related": [
    {
      "dest-uuid": "5ce5392a-3a6c-4e07-9df3-9b6a9159ac45",
      "tags": [
        "estimative-language:likelihood:probability="likely"
      ],
      "type": "similar"
    },
    "uuid": "Oca45163-e223-4167-b1af-f088ed14a93d",
    "value": "Putter Panda"
]
```
```python
from pymispgalaxies import Clusters

c = Clusters()

list(g.keys())
#
# ["threat-actor", 'ransomware', 'exploit-kit', 'tds', 'tool', 'rat', 'mitre-attack-pattern',
# 'mitre-tool', 'microsoft-activity-group', 'mitre-course-of-action', 'mitre-malware',
# 'mitre-intrusion-set', 'preventive-measure']

print(c.get("rat"))
#
# misp-galaxy:rat="Brat"
# misp-galaxy:rat="Loki RAT"
# misp-galaxy:rat="join.me"
# misp-galaxy:rat="Setro"
# misp-galaxy:rat="drat"
# misp-galaxy:rat="Plasma RAT"
# misp-galaxy:rat="NanoCore"
# misp-galaxy:rat="DarkTrack"
# misp-galaxy:rat="Theef"
# misp-galaxy:rat="Greame"
# misp-galaxy:rat="Nuclear RAT"
# misp-galaxy:rat="DameWare Mini Remote Control"
# misp-galaxy:rat="ProRat"
# misp-galaxy:rat="death"
# misp-galaxy:rat="Dark DDoSeR"
#

print(c.get("rat").description)
#
# remote administration tool or remote access tool (RAT), also called sometimes remote
# access trojan, is a piece of software or programming that allows a remote "operator"
# to control a system as if they have physical access to that system.
```
- 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/
- We welcome any contributions to the project, be it pull requests, ideas, github issues,...