MISP Training: Galaxies

CIRCL
Computer Incident
Response Center
Luxembourg

MISP
Threat Sharing

Team CIRCL

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

Univ. Lorraine
20181124

MISP Galaxies

- 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 aproach 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

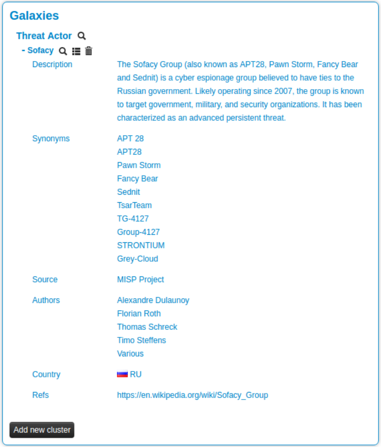
The galaxy object stack

- **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^{TM})

What a cluster looks like



Galaxies

Threat Actor

- Sofacy

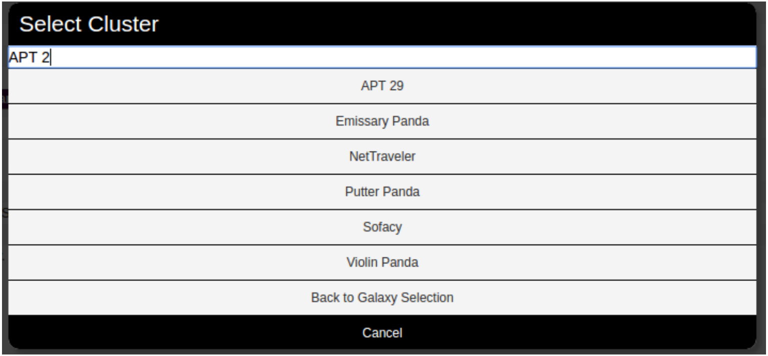
Description	The Sofacy Group (also known as APT28, Pawn Storm, Fancy Bear and Sednit) is a cyber espionage group believed to have ties to the Russian government. Likely operating since 2007, the group is known to target government, military, and security organizations. It has been characterized as an 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
Refs	https://en.wikipedia.org/wiki/Sofacy_Group

Attaching clusters to events

- 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



Select Cluster

APT 2

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

Galaxy JSON

- If you want to create a completely new galaxy instead of enriching an existing one

```
{
    "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"
}
```

Cluster JSON

- Clusters contain the meat of the data
- Skeleton structure as follows

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

Cluster JSON value example

```
    {
      "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"
    },
```

meta best practices

- Reusing existing values such as **properties, 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**.
- Or adding your own meta fields.

meta best practices - a sample

```
{
    "description": "Putter Panda were the subject of an extensive report by CrowdStrike, which stated: 'The CrowdStrike Intelligence team has been tracking this particular unit since2012, 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://cdn0.vox-cdn.com/assets/4589853/crowdstrike-intelligence-report-putter-panda.original.pdf",
```

Expressing relation between clusters

- 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": "0ca45163-e223-4167-b1af-f088ed14a93d",
  "value": "Putter Panda"
```

PyMISPGalaxies

```
from pymispgalaxies import Clusters
c = Clusters()
list(g.keys())
# ['threat-actor', 'ransomware', 'exploit-kit', 'tds', 'tool', 'rat', 'mitre-attack-patter
#  '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.
```

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/`
- We welcome any contributions to the project, be it pull requests, ideas, github issues,...