MISP Galaxy

CIRCL / Team MISP Project

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

13th ENISA-EC3 Workshop

MISP
Threat Sharing

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

- **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™)

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

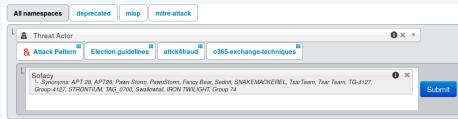`Add new cluster`

- 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 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

```
1 {
2     "name" : "Threat Actor",
3     "type" : "threat-actor",
4     "description": "Threat actors are characteristics of malicious
           actors (or adversaries) representing a cyber attack threat
           including presumed intent and historically observed
           behaviour.",
5     "version": 1,
6     "uuid": "698774c7-8022-42c4-917f-8d6e4f06ada3"
7 }
```

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

```json
1  {
2    "values": [
3      {
4        "meta": {},
5        "description": "",
6        "value": "",
7        "related_clusters": [{}],
8      }
9    ]
10 }
```

```
 1      {
 2        "meta": {
 3          "synonyms": [
 4              "APT 28", "APT28", "Pawn Storm", "Fancy Bear",
 5              "Sednit", "TsarTeam", "TG-4127", "Group-4127",
 6              "STRONTIUM", "Grey-Cloud"
 7          ],
 8          "country": "RU",
 9          "refs": [
10            "https://en.wikipedia.org/wiki/Sofacy_Group"
11          ]
12        },
13        "description": "The Sofacy Group (also known as APT28,
14            Pawn Storm, Fancy Bear and Sednit) is a cyber
15            espionage group believed to have ties to the
16            Russian government. Likely operating since 2007,
17            the group is known to target government, military,
18            and security organizations. It has been
19            characterized as an advanced persistent threat.",
20        "value": "Sofacy"
21      },
```

- 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.

```
1   {
2        "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.'",
3        "meta": {
4          "cfr-suspected-state-sponsor": "China",
5          "cfr-suspected-victims": [
6            "U.S. satellite and aerospace sector"
7          ],
8          "cfr-target-category": [
9            "Private sector",
10           "Government"
11         ],
12         "cfr-type-of-incident": "Espionage",
13         "country": "CN",
14         "refs": [
15           "http://cdn0.vox-cdn.com/assets/4589853/crowdstrike-
                 intelligence-report-putter-panda.original.pdf",
16           "https://www.cfr.org/interactive/cyber-operations/putter
                 -panda"
```

Galaxy JSON matrix-like

Propose Attribute

example-of-threats		Analysis	Initial

Setup | party/candidate registration *(3 items)*	Setup | electoral rolls *(3 items)*	Campaign | campaign IT *(4 items)*
DoS or overload of party/campaign registration, causing them to miss the deadline	Deleting or tampering with voter data	Hacking campaign websites (defacement, DoS)
Fabricated signatures from sponsor	DoS or overload of voter registration system, suppressing voters	Hacking candidate laptops or email accounts
Tampering with registrations	Identity fraud during voter registration	Leak of confidential information
		Misconfiguration of a website

Select Some Options

Can

```
 1          {
 2     "description": "Universal Development and Security Guidelines as
                Applicable to Election Technology.",
 3     "icon": "map",
 4     "kill_chain_order": {                    \\Tab in the matrix
 5         "example-of-threats": [              \\Column in the matrix
 6         "setup | party/candidate-registration",
 7         "setup | electoral-rolls",
 8         "campaign | campaign-IT",
 9         "all-phases | governement-IT",
10         "voting | election-technology",
11         "campaign/public-communication | media/press"
12         ]
13     },
14     "name": "Election guidelines",
15     "namespace": "misp",
16     "type": "guidelines",
17     "uuid": "c1dc03b2-89b3-42a5-9d41-782ef726435a",
18     "version": 1
19 }
```

CLUSTER JSON MATRIX-LIKE

```
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": [
9             "https://www.ria.ee/sites/default/files/content-editors/
                 kuberturve/cyber_security_of_election_technology.pdf
                 "
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 }
```

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.

```
 1          "related": [
 2          {
 3            "dest-uuid": "5ce5392a-3a6c-4e07-9df3-9b6a9159ac45",
 4            "tags": [
 5              "estimative-language:likelihood-probability=\"likely
                  \""
 6            ],
 7            "type": "similar"
 8          }
 9        ],
10        "uuid": "0ca45163-e223-4167-b1af-f088ed14a93d",
11        "value": "Putter Panda"
```

PyMISPGalaxies

```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.
```

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,...