

MISP GALAXY

CIRCL / TEAM MISP PROJECT

HTTP://WWW.MISP-PROJECT.ORG/

TWITTER: @MISPPROJECT

CIISI-IE DUBLIN 2024



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

MISP Galaxy

.

-MISP Galaxies

GALAXIES

m MISP started out as a platform for technical indicator sl

commonalities became more and more pressing

 The weakness of the tagging aproach is that it's not very descriptive

We needed a way to attach more complex structures to dat
 Also, with the different naming conventions for the same

 Also, with the different naming conventions for the "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

MISP Galaxy -Solution

■ Technical indicators remain strongly typed and validate

■ Pre-crafted galaxy "clusters" via GitHub project

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)

MISP Galaxy

└─The galaxy object stack

ALAXY 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)

 m 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™)

MISP Galaxy

–(some) Existing galaxies

- m Microsoft activity group: Adversary groups as defined by

WHAT A CLUSTER LOOKS LIKE

Galaxies Threat Actor Q - Sofacy Q III iii 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. APT 28 APT28 Pawn Storm Fancy Bear Sednit TsarTeam TG-4127 Group-4127 STRONTIUM Grey-Cloud Alexandre Dulaunoy Florian Roth Thomas Schreck Timo Steffens Country Refs https://en.wikipedia.org/wiki/Sofacy_Group Add new cluster

MISP Galaxy

—What a cluster looks like

The state of the s

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

MISP Galaxy

-Attaching clusters to events

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

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

Synchronisation works out of the box with older in

too. They will simply see the tags until they upgrad

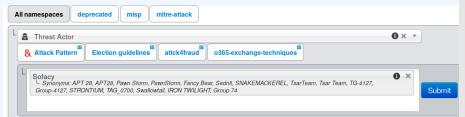
Currently, as mentioned we rely on the community

ATTACHING CLUSTERS

MISP Galaxy

Attaching clusters

■ Use a searchable synonym database to find what you're after



B Use a searchable synonym database to find what you're after the search of the search

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

MISP Galaxy

-Creating your own galaxy

G 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

 We always look forward to contributions to our galaxie 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"
```

MISP Galaxy

If you want to create a completely new palacy lentered of mindows an estimate on the create and completely new palacy lentered of mindows an estimate on the create and completely new palacy lentered of mindows and estimate on the create and completely new palacy lentered of the completely new palacy lentered on the comp

CLUSTER JSON

- Clusters contain the meat of the data
- Clusters contain the meat of the dat

MISP Galaxy

**Cluster JSON

Cluster JSON

**Cluster JSON

CLUSTER ISON 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"
```

11 19

MISP Galaxy

Cluster JSON value example

Tomach | Tomach | Tomach Boom's "Famou Boom'

), "description": "The Sofacy Group (also known as APT36 Paws Storm, Fancy Bear and Sedmil) is a cyber explosing group believed to have ties to the Russian government. Likely operating since 2007, the group is known to Larget government, military and security organizations. It has been Characterized as an advanced permittent threat."

META BEST PRACTICES

- 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.

MISP Galaxy

2024-07-08

meta best practices

MEIA DEST FRACTICES

 Reusing existing values such as complexity, effectivenes 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,

Crr-target-category, ioit_chain.

META BEST PRACTICES - A SAMPLE

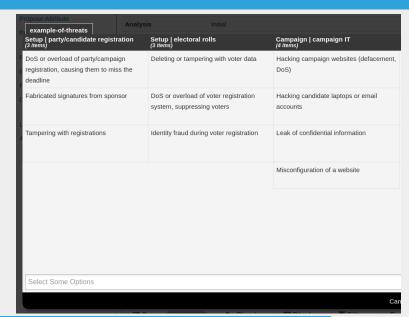
1	· {
2	"description": "Putter Panda were the subject of an
	extensive report by CrowdStrike, which stated: 'The
	CrowdStrike Intelligence team has been tracking this
	particular unit since2012, under the codename PUTTER
	PANDA, and has documented activity dating back to 2007.
	The report identifies Chen Ping, aka cpyy, and the
	primary location of Unit 61486.'",
3	"meta": {
4	"cfr-suspected-state-sponsor": "China",
5	"cfr-suspected-victims": [
6	"U.S. satellite and aerospace sector"
7	1,
8	"cfr-target-category": [
9	"Private sector",
10	"Government"
11	1,
12	"cfr-type-of-incident": "Espionage",
13	"country": "CN",
14	"refs": [
15	"http://cdno.vox-cdn.com/assets/4589853/crowdstrike-
	intelligence-report-putter-panda.original.pdf",
16	"https://www.cfr.org/interactive/cyber-operations/putte
	-panda"

meta best practices - a sample

MISP Galaxy

excription": "Putter Panda were the subject of an

GALAXY JSON MATRIX-LIKE



19

MISP Galaxy

└─Galaxy JSON matrix-like



GALAXY JSON MATRIX-LIKE

```
"description": "Universal Development and Security Guidelines as
           Applicable to Election Technology.",
     "icon": "map",
     "kill_chain_order": {
                                      \\Tab in the matrix
          "example-of-threats": [
                                      \\Column in the matrix
          "setup | party/candidate-registration",
          "setup | electoral-rolls",
          "campaign | campaign-IT",
          "all-phases | governement-IT",
          "voting | election-technology",
         "campaign/public-communication | media/press"
12
13
     "name": "Election guidelines",
     "namespace": "misp",
     "type": "guidelines",
     "uuid": "c1dco3b2-89b3-42a5-9d41-782ef726435a",
     "version": 1
19
```

MISP Galaxy

2024-07-08

-Galaxy JSON matrix-like

GALLANY SOUR MATERIAL TO THE STATE OF THE ST

CLUSTER ISON MATRIX-LIKE

```
"description": "DoS or overload of party/campaign
             registration, causing them to miss the deadline",
         "meta": {
           "date": "March 2018.",
            "kill_chain": [ \\Define in which column the cluster should be placed
              "example-of-threats:setup | party/candidate-registration"
           "refs": [
             "https://www.ria.ee/sites/default/files/content-editors/
                  kuberturve/cyber_security_of_election_technology.pdf
         "uuid": "154c6186-a007-4460-a029-ea23163448fe",
         "value": "DoS or overload of party/campaign registration,
             causing them to miss the deadline"
14
```

MISP Galaxy

2024-07-08

-Cluster JSON matrix-like

Secretaria This is worted at partylements are considered to the control of th

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.

MISP Galaxy

-Expressing relation between clusters

Cluster can be related to one or more clusters using default relationships from MSP objects and a list of tags to classify the relation.

Transfer [**Transfer** [

PYMISPGALAXIES

```
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-aalaxy:rat="Loki RAT"
# misp-galaxy:rat="join.me"
# misp-galaxy:rat="Setro"
# misp-aalaxy:rat="drat"
# misp-galaxy:rat="Plasma RAT"
# misp-galaxy:rat="NanoCore"
# misp-aalaxy:rat="DarkTrack"
# misp-aalaxv: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-aalaxv: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.
```

MISP Galaxy

PyMISPGalaxies

POTENTIAL AND SERVICE AND SERV

OpenPGP fingerprint: 3812 DCC2 82FA 2931 2F58 709A 09E2 CD49 44E6 CBCD # https://github.com/MISP/-

We welcome any contributions to the project, be it pull

- 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,...

19 / 19