

OSS is changing the Security information sharing landscape.
Focus on the MISP objects and other recent improvements on the platform



CIRCL

Computer Incident
Response Center
Luxembourg

Raphaël Vinot - *TLP:WHITE*

info@circl.lu

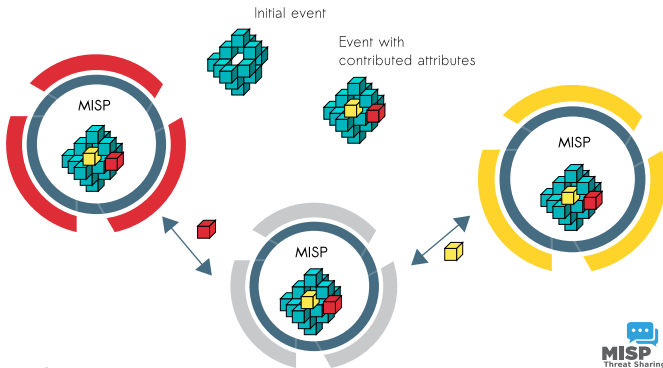
RMLL 2017

TL;DR

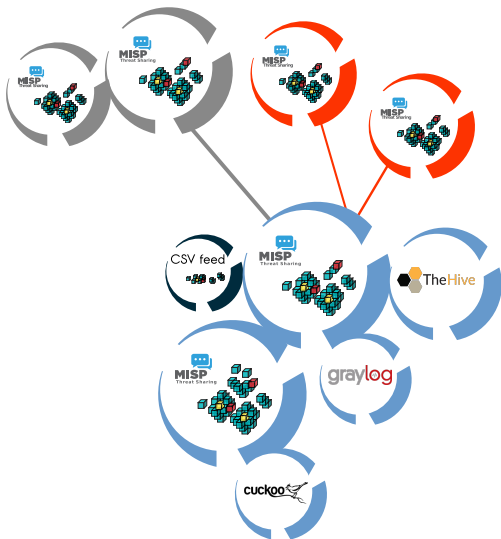
- Started in 2012 by Christophe Vandeplass (Belgian MoD)
- Supports automation and pluggable with other tools
- Help information sharing within a team and with 3rd parties
- Supports plenty of usecases (from the **malware reverser** to the **Fraud analysts**)
- MISP's development is **community-driven**

MISP core distributed sharing functionality

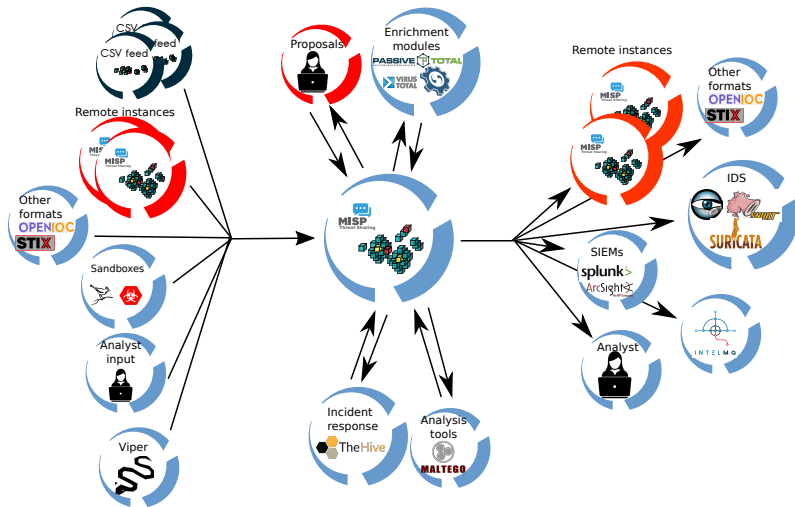
- MISP's core functionality is sharing where everyone can be a consumer and/or a contributor/producer.
- Quick benefit without the obligation to contribute.
- Low barrier access to get acquainted to the system.



A Common Integration



The MISP pipeline



Recent updates and changes

- Big improvement in the **sightings**
- Continuous expansion of the **galaxies**
- **Feeds overlap** matrix
- Now... -ish: **objects**

Question

” My IDS cannot ingest all those indicators, how do I keep the list sane?”

Sightings

- Lifetime and evolution of an indicator
- Improve the feedback loop
- 3 options:
 - Positive: currently compromised infrastructure
 - Negative: false positive
 - Expiration: date where the indicator should be considered as expired
- Mapped to an organisation
- Type of source (SIEM, honeypot, ...)

Sightings

- Contextual activity based on tags and galaxies

<code>circi:incident-classification="malware"</code>	<code>circi</code>	361	0		<input type="checkbox"/>
<code>circi:incident-classification="phishing"</code>	<code>circi</code>	56	0		<input type="checkbox"/>
<code>circi:incident-classification="scam"</code>	<code>circi</code>	13	0		<input type="checkbox"/>

- Automation based on PCAP:

```
usage: pcapreader.py [-h] -r READ [-f FILTER] [-s SOURCE] [-t TYPE] [-v] [-d]
```

optional arguments:

```
-r READ, --read READ  pcap/dumpcap file that should be read by tshark
-f FILTER, --filter FILTER
                        Prefix that should be skipped (substring)
-s SOURCE, --source SOURCE
                        Describe the source of the pcap
-t TYPE, --type TYPE  Specify the type of sightings: 0=Default,1=False
                        positive
```

- <https://github.com/MISP/misp-sighting-tools>

Question

” How can I keep track of all the cyber names made up by the cyber vendors for cyber communication purposes?”

” ... and create my own names?”

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 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 (or soon attribute)
- 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)

Existing clusters

- **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)

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

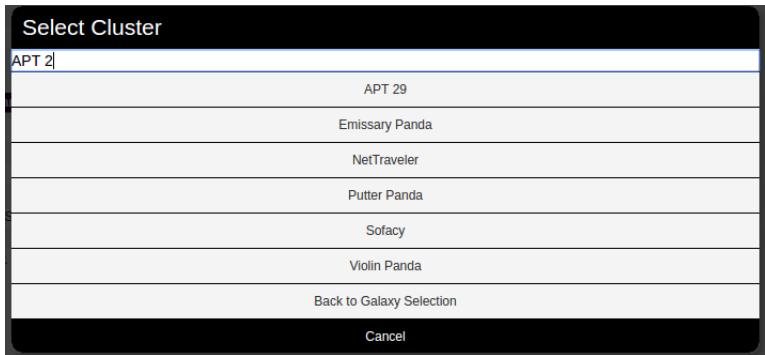
Add new cluster

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



The image shows a 'Select Cluster' dialog box with a search input field containing 'APT 2'. Below the input field is a list of search results, each on a separate line. The results are: APT 29, Emissary Panda, NetTraveler, Putter Panda, Sofacy, Violin Panda, and Back to Galaxy Selection. At the bottom of the dialog box is a 'Cancel' button.

Search Input	Results
APT 2	APT 29
	Emissary Panda
	NetTraveler
	Putter Panda
	Sofacy
	Violin Panda
	Back to Galaxy Selection
	Cancel

Cluster JSON value example

```
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 }
```

Question

”\$CYBER_VENDOR has new
cyber feed for USD 100.000,
should I get it?”

”They said it will make me sleep better at night. I like sleeping.”

Feed integration

- Objective: Get all the feeds in one single place
- Profit of the functionalities of MISP (correlation with other events)
- Automatic updates
- Add your own
- Problem: Lots of duplicates

Feed overlap matrix

Feed overlap analysis matrix

	1	2	4	5	7	8	10	11	12	15	16	18	19	20	21	24	27	28	29	30	31	32	33	34	36	37	38	39	40	41	42	43	44	45				
1 CIRCL OSGINT Feed	-	1%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	1%	1%	0%	0%	1%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%			
2 The Botvrij.eu Data	47%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%			
4 Zeus compromised URL blacklist	0%	0%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%			
5 blockrules of rules.emergingthreats.net	0%	0%	0%	-	0%	0%	0%	0%	0%	1%	12%	0%	0%	0%	0%	0%	0%	0%	26%	0%	0%	0%	0%	0%	0%	0%	1%	2%	21%	0%	24%	0%	0%	0%	0%			
7 malwaredomainlist	2%	0%	0%	0%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	1%	2%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%			
8 Tor exit nodes	17%	0%	0%	0%	0%	-	0%	0%	0%	1%	7%	0%	0%	0%	0%	0%	0%	0%	46%	0%	0%	0%	0%	0%	0%	0%	0%	0%	1%	0%	26%	0%	0%	0%	0%			
10 cyberotime-tracker.net - all	0%	0%	0%	0%	0%	0%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	1%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%			
11 Phishtank online valid phishing	0%	0%	0%	0%	0%	0%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	3%	0%	0%	0%	1%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%			
12 IISdynamic dns providers	0%	0%	0%	0%	0%	0%	0%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%			
15 longtail.it.marist.edu	4%	0%	0%	10%	0%	6%	0%	0%	0%	-	37%	0%	0%	0%	0%	0%	0%	0%	70%	0%	0%	0%	0%	0%	0%	0%	0%	6%	7%	79%	0%	69%	0%	0%	0%			
16 longtail.it.marist.edu 7 days	1%	0%	0%	8%	0%	3%	0%	0%	0%	3%	-	0%	0%	0%	0%	0%	0%	0%	70%	0%	0%	0%	0%	0%	0%	0%	2%	2%	33%	0%	68%	0%	0%	0%				
18 diamondfox_panels	44%	0%	0%	0%	0%	0%	0%	0%	0%	0%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%			
19 Mirai-only-dec2016	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	-	0%	9%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	1%	1%	0%	0%	0%	0%	0%	0%				
20 Mirai-only-jan2017	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	12%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	1%	1%	0%	0%	0%	0%	0%	0%				
21 CIRCL - honeypot	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	1%	0%	0%	0%	0%	0%				
24 booterblacklist.com Latest	0%	0%	0%	0%	0%	0%	1%	0%	0%	0%	0%	0%	0%	0%	0%	-	0%	0%	0%	0%	0%	8%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%			
27 poc3gropers	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	-	1%	0%	0%	0%	0%	0%	0%	0%	0%	0%	1%	0%	0%	0%	0%	0%	0%				
28 Inthreat test	0%	0%	0%	0%	0%	0%	1%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	4%	0%	0%	1%	0%	0%	0%	0%	1%	2%	0%	5%	0%	0%	0%	0%				
29 Ransomware Tracker CSV Feed	9%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	46%	-	0%	24%	0%	1%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%			
30 Feodo IP Blocklist	11%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	2%	0%	-	0%	0%	0%	99%	99% of the data of Feodo IP Blocklist is contained in firehol_level1 (911 matching)													
31 hosts-file.net - hphost - malwarebytes	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%				
32 hosts-file.net - hphost - malwarebytes - EMD classification ONLY	1%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	4%	0%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%				
33 OpenPhish url list	0%	0%	0%	0%	0%	0%	11%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	76%	0%	0%	0%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%			
34 firehol_level1	3%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	4%	14%	0%	0%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%				
36 ramrnt C&Cs	29%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	0%	35%	24%	0%	0%	0%	82%	-	0%	0%	0%	0%	0%	0%	0%	0%	0%				

Question

”STIX has objects, how do I represent it in MISP without creating tons of events?”

”Yes, I know, STIX is awful, but my boss wants me to use it”

MISP objects

- Objective: create a semi-dynamic data model.
- Using existing MISP attributes to build new objects.
- **Share the object designs within partners automatically along with the events shared** (e.g. allowing to share events with yet unknown objects).
- Have a community-driven set of default objects¹.

¹<https://github.com/misp/misp-objects>

Use case

- File: hashes, filename, size,
- PE: original filename, timestamp, number of sections, ...
- PE Section: entropy, hashes, ...
- ... And all other kind of objects: ELF, PDF, Office documents, VBA Macro, Embedded JavaScript, ...
- Your own object with the indicators you wish


```
{
  "name": "file",
  "uuid": "688c46fb-5edb-40a3-8273-1af7923e2215",
  "meta-category": "file",
  "description": "File object describing a file with meta-information",
  "version": 1,
  "attributes": {
    "sha256": {
      "misp-attribute": "sha256",
      "misp-usage-frequency": 1
    },
    "entropy": {
      "misp-attribute": "float",
      "misp-usage-frequency": 1,
      "disable_correlation": true
    },
    "size-in-bytes": {
      "misp-attribute": "size-in-bytes",
      "misp-usage-frequency": 0,
      "disable_correlation": true
    },
    "authentihash": {
      "misp-attribute": "authentihash",
      "misp-usage-frequency": 0
    },
    "ssdeep": {
      "misp-attribute": "ssdeep",
      "misp-usage-frequency": 0
    },
    "sha224": {
      "misp-attribute": "sha224",
      "misp-usage-frequency": 0
    },
    "sha384": {
      "misp-attribute": "sha384",
      "misp-usage-frequency": 0
    }
  }
}
```

r2graphity: Messing with binaries

- Research project of Marion Marschalek (@pinkflawd) and me
- Reversing binaries is painful and repetitive
- Families of malwares have similar patterns/features
- Automating extractions with radare2
- Push everything into graphs

Similarity Visualization: Animalfarm Binaries

Shamelessly stolen
from Marion's slides
@ RECON 2017



```
3 funcDict = {
4     'DRIVERCOMM': ['DeviceIoControl'],
5     'CREATESTARTSERVICE': ['OpenSCManager', 'CreateService', 'OpenService', 'StartService'],
6     'CREATETHREAD': ['CreateThread'],
7     'PROCESSITER': ['CreateToolhelp32Snapshot', 'Process32First', 'Process32Next'],
8     'APILOADING': ['LoadLibrary', 'GetProcAddress'],
9     'WRITEFILE': ['CreateFile', 'WriteFile'],
10    'READFILE': ['CreateFile', 'ReadFile'],
11    'WINHOOK': ['SetWindowsHookEx'],
12    'DRIVESITER': ['GetLogicalDriveStrings', 'GetDriveType'],
13    'FILEITER': ['FindFirstFile', 'FindNextFile', 'FindClose'],
14    'REGSETVAL': ['RegOpenKey', 'RegSetValue'],
15    'REGQUERY': ['RegOpenKey', 'RegQueryValue'],
16    'DUMPRSRC': ['FindResource', 'LoadResource', 'CreateFile', 'WriteFile'],
17    'LOADRSRC': ['FindResource', 'LoadResource', 'LockResource'],
18    'WSASEND': ['WSAStartup', 'gethostbyname', 'send'],
19    'RECV': ['recv', 'send'],
20    'RETROINJECTION': ['GetCurrentProcess', 'CreatePipe', 'DuplicateHandle'],
21    'WINEXEC': ['WinExec'],
22    'SHELLEXEC': ['ShellExecute'],
23    'CREATEPROC': ['CreateProcess'],
24    'WINDOW': ['CreateWindow', 'RegisterClass', 'DispatchMessage'],
25    'EXITSYSTEM': ['ExitWindows'],
26    'TEMPFILEWRITE': ['GetTempFileName', 'CreateFile', 'WriteFile'],
27    'REMTREAD': ['CreateThread', 'WriteProcessMemory', 'ReadProcessMemory', 'ResumeThread'],
28    'FPRINT': ['fopen', 'fprintf', 'fclose'],
29    'UPDATERESOURCE': ['BeginUpdateResource', 'UpdateResource', 'EndUpdateResource'],
30    'SCREENSHOT': ['CreateCompatibleDC', 'GetDeviceCaps', 'CreateCompatibleBitmap', 'BitBlt'],
31    'CRYPT': ['CryptAcquireContext', 'CryptGenKey', 'CryptEncrypt']
32 }
```

“Behavior” Gadgets

Shamelessly stolen
from Marion's slides
@ RECON 2017

```

{
  "name": "r2graphity",
  "uuid": "b6abe0e0-52ea-4424-ba42-761c2e027b76",
  "meta-category": "file",
  "description": "Indicators extracted from files using radare2 and graphml",
  "version": 1,
  "attributes": {
    "total-functions": {
      "misp-attribute": "counter",
      "misp-usage-frequency": 0,
      "disable_correlation": true,
      "description": "Total amount of functions in the file."
    },
    "gml": {
      "misp-attribute": "attachment",
      "misp-usage-frequency": 0,
      "disable_correlation": true,
      "description": "Graph export in G>raph Modelling Language format"
    },
    "r2-commit-version": {
      "misp-attribute": "text",
      "misp-usage-frequency": 0,
      "disable_correlation": true,
      "description": "Radare2 commit ID used to generate this object"
    },
    "create-thread": {
      "misp-attribute": "counter",
      "misp-usage-frequency": 0,
      "disable_correlation": true,
      "description": "Amount of calls to CreateThread"
    },
    "shortest-path-to-create-thread": {
      "misp-attribute": "counter",
      "misp-usage-frequency": 0,
      "disable_correlation": true,
      "description": "Shortest path to the first time the binary calls CreateThread"
    }
  }
}

```

References

- Marion's talk @ RECON17 - https://github.com/pinkflawd/r2graphity/blob/master/GraphDracula_Recon17.pdf
- MISP project - <https://github.com/MISP/MISP>
- MISP Organisation - <https://github.com/MISP>
- MISP Chatroom - <https://gitter.im/MISP/MISP>
- MISP website - <http://www.misp.software>

