INFORMATION SHARING AND TAX-ONOMIES

PRACTICAL CLASSIFICATION OF THREAT INDICATORS US-

CIRCL / TEAM MISP PROJECT

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

MISP PROJECT



Information Sharing and Taxonomies

15



FROM TAGGING TO FLEXIBLE TAXONOMIES

OSINT - Fancy Bear Source Code

Event ID	5703
Uuld	58724cbf-5508-4425-ab89-4f61950d210f
Org	CIRCL
Owner org	CIRCL
Contributors	
Email	alexandre.dulaunoy@circl.lu
Tags	tlp:white x osint:certainty="75" x osint:source-type="source-code-repository" x circl:osint-feed x
	ms-caro-malware:malware-platform="Python" x +
Date	2017-01-08
Threat Level	Medium
Analysis	Initial
Distribution	All communities
Info	OSINT - Fancy Bear Source Code
Published	Yes
Sightings	0 (0) 差
Activity	

- Tagging is a simple way to attach a classification to an event or an attribute.
- In the early version of MISP, tagging was local to an instance.
- Classification must be globally used to be efficient.
- After evaluating different solutions of classification, we built a new scheme using the concept of machine tags.

Information Sharing and Taxonomies

└─From Tagging to Flexible Taxonomies

24	(A),
And the	100
benefit after the	
(mail	and Association
hep.	
ben .	2010-18
Propil and	Netwo
ALC: NO	101
Desiration	N convolution
13	TRAY - beto his back line
Automa .	
Summer .	
And a	
Tag or a	ging is a simple way to attach a classification to an an attribute.

-04-15

2024-

MACHINE TAGS

Information Sharing and Taxonomies

└─Machine Tags

15

2024-04



Triple tag, or machine tag, format was introduced in 2004 to extend geotagging on images.

admiralty-scale:source-reliability="c"

namespace

- A machine tag is just a tag expressed in way that allows systems to parse and interpret it.
- Still have a human-readable version:
 - admiralty-scale:source-reliability="Fairly reliable"

predicate value

MISP TAXONOMIES

Information Sharing and Taxonomies

└─MISP Taxonomies

15

2024-04

- Taxonomies are implemented in a simple JSON format.
 Anyone can create their own taxonomy or reuse an existing one
- The taxonomies are in an independent git repository¹.
- These can be freely reused and integrated into other threat intel tools.
 Taxonomies are licensed under Creative Commons (public
- taxonomies are licensed under Creative Commons (public domain) except if the taxonomy author decided to use another license.

https://www.github.com/RISP/misp-taxonomies/

- **Taxonomies are implemented in a simple JSON format.**
- Anyone can create their own taxonomy or reuse an existing one.
- The taxonomies are in an independent git repository¹.
- These can be freely reused and integrated into other threat intel tools.
- Taxonomies are licensed under Creative Commons (public domain) except if the taxonomy author decided to use another license.

https://www.github.com/MISP/misp-taxonomies/

EXISTING TAXONOMIES

■ NATO - Admiralty Scale

- CIRCL Taxonomy Schemes of Classification in Incident Response and Detection
- eCSIRT and IntelMQ incident classification
- EUCI EU classified information marking
- Information Security Marking Metadata from DNI (Director of National Intelligence - US)
- NATO Classification Marking
- OSINT Open Source Intelligence Classification
- TLP Traffic Light Protocol
- Vocabulary for Event Recording and Incident Sharing VERIS
- And many more like ENISA, Europol, or the draft FIRST SIG Information Exchange Policy.

Information Sharing and Taxonomies

Existing Taxonomies

EXISTING TAXONOMI

NATO - Admiralty Scale

- CIRCL Taxonomy Schemes of Classification in Incident
 Response and Detection
- CSIRT and IntelMQ incident classification
- EUCI EU classified information marking
- Information Security Marking Metadata from DNI (Director of National Intelligence - US)
- NATO Classification Marking
- OSINT Open Source Intelligence Classificatio
 TLP Traffic Light Protocol
- Vocabulary for Event Recording and Incident Sharing VERIS
- And many more like ENISA, Europol, or the draft FIRST SIG Information Exchange Policy.

5

2024-04

WANT TO WRITE YOUR OWN TAXONOMY? 1/2

Information Sharing and Taxonomies

S

2024-

 \square Want to write your own taxonomy? 1/2

IANT TO WRITE YOUR OWN TAXONOMY? 1/2

Transport: "relation-relation", Transport: "relations and the second se

```
1
    "namespace": "admiralty-scale",
    "description": "The Admiralty Scale (also called the NATO System
        ) is used to rank the reliability of a source and the
        credibility of an information.",
    "version": 1,
4
    "predicates": [
        "value": "source-reliability",
        "expanded": "Source Reliability"
      },
        "value": "information-credibility",
11
        "expanded": "Information Credibility"
12
15
```

WANT TO WRITE YOUR OWN TAXONOMY? 2/2

Information Sharing and Taxonomies

ഹ

2024-

 \square Want to write your own taxonomy? 2/2

WANT TO WRITE YOUR OWN TAXONOMY? 2/2

Publishing your taxonomy is as easy as a simple git pull request on misp-taxonomies².

https://github.com/MISP/misp-taxonomies

```
1 {
2 "values": [
3 {
4 "predicate": "source-reliability",
5 "entry": [
6 {
7 "value": "a",
8 "expanded": "Completely reliable"
9 },
10 ....
```

Publishing your taxonomy is as easy as a simple git pull request on misp-taxonomies².

²https://github.com/MISP/misp-taxonomies

HOW ARE TAXONOMIES INTEGRATED IN MISP?

18	~	×	admiralty-scale:information-credibility="1"	admiralty-scale	4	0			C I
19	*	×	admiralty-scale:information-credibility="2"	admiralty-scale	15	1	L		g İ
20	~	×	admiralty-scale:Information-credibility="3"	admiralty-scale	12	4		0	C Î
21	*	×	admiralty-scale:information-credibility="4"	admiralty-scale	1	0			g i
22	~	×	admiratty-scale:information-credibility="5"	admiralty-scale	1	0	. l.	0	c î
23	*	×	admiralty-scale:information-credibility="6"	admiralty-scale	2	0	λ		C 🗎
12	~	×	admiralty-scale:source-reliability-"a"	admiralty-scale	0	0		0	C Î
13	*	×	admiralty-scale:source-reliability="b"	admiralty-scale	15	53			C 🗎
14	~	×	admiralty-scale:source-reliability="6"	admiralty-scale	5	2			c î
15	*	×	admiralty-scale:source-reliability="d"	admiralty-scale	1	0		\Box	C II
16	~	×	admiralty-scale:source-reliability="e"	admiralty-scale	0	0			C 🗎
17	*	×	admiralty-scale:source-reliability="1"	admiralty-scale	4	2			C İ
1203	*	×	adversary:infrastructure-action="monitoring-active"	adversary	1	0			c i
1201	*	×	adversary:Infrastructure-action="passive-only"	adversary	0	0		0	c i

- MISP administrator can just import (or even cherry pick) the namespace or predicates they want to use as tags.
- **Tags can be exported to other instances.**
- Tags are also accessible via the MISP REST API.

Information Sharing and Taxonomies

How are taxonomies integrated in MISP?



5

2024-04

FILTERING THE DISTRIBUTION OF EVENTS AMONG MISP INSTANCES

Applying rules for distribution based on tags:



Information Sharing and Taxonomies

Filtering the distribution of events among MISP instances FILTERING THE DISTRIBUTION OF EVENTS AMONG MISP INSTANCES

these lags	Analasia Kep	Rodat by	
ty setter	BB Species	000 ⁰⁰¹³⁰⁰⁻³⁰⁰⁰⁰	
	alterity and more		
food Pagements	Analise Statistics	Receive Spinsters	
CHO.	88	88	

OTHER USE CASES USING MISP TAXONOMIES

2024-04-15

Information Sharing and Taxonomies

└─Other use cases using MISP taxonomies

 Tage can be used to set events or attributes for further processing by external tools (e.g. Vinstotal auto-expansion using typer).
 Ensuring a classification manager classifies the events before release (e.g. release of information from air-gapped (classified networks).
 Enriching 105 seport with tags to fit your ND5 deployment.
 Using IntelBiograd MISP together to process events (tags

- Tags can be used to set events or attributes for further processing by external tools (e.g. VirusTotal auto-expansion using Viper).
- Ensuring a classification manager classifies the events before release (e.g. release of information from air-gapped/classified networks).
- **Enriching IDS export** with tags to fit your NIDS deployment.
- Using IntelMQ and MISP together to process events (tags limited per organization introduced in MISP 2.4.49).

FUTURE FUNCTIONALITIES RELATED TO MISP TAXONOMIES

Information Sharing and Taxonomies

Future functionalities related to MISP taxonomies

FUTURE FUNCTIONALITIES RELATED TO MISP TAXONOMIES

- Sighting support (thanks to NCSC-NL) is integrated in MISP allowing to auto expire IOC based on user detection.
 Adjusting taxonomies (adding/removing tags) based on their score or visibility via aighting.
 Simple taxonomy editors to bein pon-technical users to
- create their taxonomies. ■ Filtering mechanisms in MISP to rename or replace
- taxonomies/tags at pull and push synchronisatio More public taxonomies to be included.

- **Sighting** support (thanks to NCSC-NL) is integrated in MISP allowing to auto expire IOC based on user detection.
- Adjusting taxonomies (adding/removing tags) based on their score or visibility via sighting.
- Simple taxonomy editors to help non-technical users to create their taxonomies.
- **Filtering mechanisms** in MISP to rename or replace taxonomies/tags at pull and push synchronisation.
- More public taxonomies to be included.

Information Sharing and Taxonomies

└─ PyTaxonomies

15

2024-04-

Python module to handle the taxonomics
 offline and other mode (fields the taxonomics from
 Gittub)
 Simple saxext to make tagging say
 Totally independent from MISP
 No external dependencies in offline mode
 Pythony only
 Can be used to create & dump a new taxonomy

- **Python module** to handle the taxonomies
- Offline and online mode (fetch the newest taxonomies from GitHub)
- Simple **search** to make tagging easy
- Totally independent from MISP
- No external dependencies in offline mode
- Python3 only
- Can be used to create & dump a new taxonomy

PyTaxonomies

from pytaxonomies import Taxonomies taxonomies = Taxonomies() taxonomies, version # => '20160725' taxonomies.description # => 'Manifest file of MISP taxonomies available.' list(taxonomies.keys()) # => ['tlp', 'eu-critical-sectors', 'de-vs', 'osint', 'circl', 'veris', 'ecsirt', 'dhs—ciip—sectors', 'fr—classif', 'misp', 'admiralty—scale', ...] taxonomies.get('enisa').description # 'The present threat taxonomy is an initial version that has been developed on # the basis of available ENISA material. This material has been used as an ENISA-internal # structuring aid for information collection and threat consolidation purposes. # It emerged in the time period 2012-2015.' print(taxonomies.get('circl')) # circl:incident-classification="vulnerability" # circl:incident-classification="malware" # circl:incident-classification="fastflux" # circl:incident-classification ="system-compromise" # circl:incident-classification="sql-injection" # print(taxonomies.get('circl').machinetags_expanded()) # circl:incident-classification ="Phishing" # circl:incident-classification="Malware" # circl:incident-classification ="XSS" # circl:incident-classification="Copyright issue" # circl:incident-classification ="Spam" # circl:incident-classification="SQL Injection"

Information Sharing and Taxonomies

└─ PyTaxonomies

5

THE DILEMMA OF FALSE-POSITIVES

Information Sharing and Taxonomies

5

2024-04-

└─The dilemma of false-positives

- False-positives are a common issue in threat intelligence sharing.
- It's often a contextual issue:
- Faise-positives might be different per community of users sharing information.
- Organizations might have their own view on false-positives.
 Based on the success of the MISP taxonomy model, we built
- misp-warninglists.

- False-positives are a **common issue** in threat intelligence sharing.
- It's often a contextual issue:
 - False-positives might be different per community of users sharing information.
 - Organizations might have their **own view** on false-positives.
- Based on the success of the MISP taxonomy model, we built misp-warninglists.

MISP warning lists

- misp-warninglists are lists of well-known indicators that can be associated to potential false positives, errors, or mistakes.
- Simple JSON files

```
1
     "name": "List of known public DNS resolvers",
 2
     "version": 2,
     "description": "Event contains one or more public DNS resolvers
         as attribute with an IDS flag set",
     "matching_attributes": [
 5
      "ip-src",
       "ip-dst"
     ],
     "list": [
9
      "8.8.8.8",
10
11
      "8.8.4.4",...]
12 }
```

Information Sharing and Taxonomies

15

2024-04

└─MISP warning lists

1 ["mame": "List of known public DMS resolvers", 3 "Version": 4 "description": "Event contains one or more public DMS reso a attribute with an IDS flag set", 5 "matching_artibutes":[at o
6 "19-44" 7 19-44" 9 Tister [9 "18.8.4.4",] 9 2	

MISP warning lists

- The warning lists are integrated in MISP to display an info/warning box at the event and attribute level.
- Enforceable via the API where all attributes that have a hit on a warninglist will be excluded.
- This can be enabled at MISP instance level.
- Default warning lists can be enabled or disabled like known public resolver, multicast IP addresses, hashes for empty values, rfc1918, TLDs or known Google domains.
- The warning lists can be expanded or added in JSON locally or via pull requests.
- Warning lists can be also used for critical or core infrastructure warning, personally identifiable information...

Information Sharing and Taxonomies

└─MISP warning lists

5

2024-04-

MISP WARNING L

- The warning lists are integrated in MSP to display an info/warning box at the event and attribute level.
 Enforceable via the API where all attributes that have a hit on a warninglist will be excluded.
 This can be enabled at MSP instance level.
 Default warning lists can be enabled or disabled like know public resolver, multicate IP addresses, hashes for emoty
- values, rfc1918, TLDs or known Google domains. The warning lists can be expanded or added in JSON locally
- or via pull requests.
- Warning lists can be also used for critical or core infrastructure warning, personally identifiable information.



https://github.com/MISP/MISP

- https://github.com/MISP/misp-taxonomies
- https://github.com/MISP/PyTaxonomies
- https://github.com/MISP/misp-warninglists
- info@circl.lu (if you want to join one of the MISP community operated by CIRCL)
- PGP key fingerprint: CA57 2205 CO02 4E06 BA70 BE89 EAAD CFFC 22BD 4CD5

Information Sharing and Taxonomies

-0&A

5

2024-04-

Inters://jithub.com/NIS9/NIS9
 Inters://jithub.com/NIS9/NIS9
 Inters://jithub.com/NIS9/NIS9-Internation
 Inters://jithub.com/NIS9-Internation
 Inte