Network Working Group
Internet-Draft
Intended status: Informational
Expires: February 4, 2019

A. Dulaunoy
A. Iklody
D. Servili
CIRCL

August 3, 2018

MISP galaxy format
draft-dulaunoy-misp-galaxy-format-03

Abstract

This document describes the MISP galaxy format which describes a simple JSON format to represent galaxies and clusters that can be attached to MISP events or attributes. A public directory of MISP galaxies is available and relies on the MISP galaxy format. MISP galaxies are used to add further informations on a MISP event. MISP galaxy is a public repository [MISP-G] of known malware, threats actors and various other collections of data that can be used to mark, classify or label data in threat information sharing.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on February 4, 2019.

Table of Contents

1. Introduction

Sharing threat information became a fundamental requirements on the Internet, security and intelligence community at large. Threat information can include indicators of compromise, malicious file indicators, financial fraud indicators or even detailed information about a threat actor. Some of these informations, such as malware or threat actors are common to several security events. MISP galaxy is a public repository [MISP-G] of known malware, threats actors and various other collections of data that can be used to mark, classify or label data in threat information sharing.

In the MISP galaxy context, clusters help analysts to give more informations about their cybersecurity events, indicators or threats. MISP galaxies can be used for classification, filtering, triggering actions or visualisation depending on their use in threat intelligence platforms such as MISP [MISP-P].

1.1. Conventions and Terminology

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 [RFC2119].

2. Format

A cluster is composed of a value (MUST), a description (OPTIONAL) and metadata (OPTIONAL).

Clusters are represented as a JSON [RFC4627] dictionary.

2.1. Overview

The MISP galaxy format uses the JSON [RFC4627] format. Each galaxy is represented as a JSON object with meta information including the following fields: name, uuid, description, version, type, authors, source, values.

name defines the name of the galaxy. The name is represented as a string and MUST be present. The uuid represents the Universally Unique IDentifier (UUID) [RFC4122] of the object reference. The uuid MUST be preserved. For any updates or transfer of the same object reference. UUID version 4 is RECOMMENDED when assigning it to a new object reference and MUST be present. The description is represented as a string and MUST be present. The uuid is represented as a string and MUST be present. The version is represented as a decimal and MUST be present. The type is represented as a string and MUST be present and MUST match the name of the galaxy file. The source is represented as a string and MUST be present. Authors are represented as an array containing one or more authors and MUST be present.

Values are represented as an array containing one or more values and MUST be present. Values defines all values available in the galaxy.

2.2. values

The values array contains one or more JSON objects which represent all the possible values in the galaxy. The JSON object contains four fields: value, description, uuid and meta. The value is represented as a string and MUST be present. The description is represented as a string and SHOULD be present. The meta or metadata is represented as a JSON list and SHOULD be present. The uuid represents the Universally Unique IDentifier (UUID) [RFC4122] of the value reference. The uuid SHOULD can be present and MUST be preserved.

2.3. meta

Meta contains a list of custom defined JSON key value pairs. Users SHOULD reuse commonly used keys 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 wherever applicable.

properties is used to provide clusters with additional properties. Properties are represented as an array containing one or more strings ans MAY be present.

derivated_from, refs, synonyms SHALL be used to give further informations. refs is represented as an array containing one or more strings and SHALL be present. synonyms is represented as an array containing one or more strings and SHALL be present. derivated_from is represented as an array containing one or more strings and SHALL be present.

date, status MAY be used to give time information about an cluster. date is represented as a string describing a time or period and SHALL be present. status is represented as a string describing the current status of the clusters. It MAY also describe a time or period and SHALL be present.

colour fields MAY be used at predicates or values level to set a specify colour that MAY be used by the implementation. The colour field is described as an RGB colour fill in hexadecimal representation.

complexity, effectiveness, impact, possible_issues MAY be used to give further information in preventive-measure galaxy. complexity is represented by an enumerated value from a fixed vocabulary and SHALL be present. effectiveness is represented by an enumerated value from a fixed vocabulary and SHALL be present. impact is represented by an enumerated value from a fixed vocabulary and SHALL be present. possible_issues is represented as a string and SHOULD be present.

Example use of the complexity, effectiveness, impact, possible_issues fields in the preventive-measure galaxy:


```
{
  "meta": {
    "refs": [
      "http://www.windowsnetworking.com/kbase/WindowsTips/WindowsXP/AdminTips/
Customization/DisableWindowsScriptingHostWSH.html"
    ],
    "complexity": "Low",
    "effectiveness": "Medium",
    "impact": "Medium",
    "type": [
      "GPO"
    ],
    "possible_issues": "Administrative VBS scripts on Workstations"
  },
  "value": "Disable WSH",
  "description": "Disable Windows Script Host",
  "uuid": "e6df1619-f8b3-476c-b5cf-22b4c9e9dd7f"
}
```

country, motive MAY be used to give further information in threat-actor galaxy. country is represented as a string and SHOULD be present. motive is represented as a string and SHOULD be present.

Example use of the country, motive fields in the threat-actor galaxy:

```
{
  "meta": {
    "country": "CN",
    "synonyms": [
      "APT14",
      "APT 14",
      "QAZTeam",
      "ALUMINUM"
    ],
    "refs": [
      "http://www.crowdstrike.com/blog/whois-anchor-panda/"
    ],
    "motive": "Espionage"
  },
  "value": "Anchor Panda",
  "description": "PLA Navy",
  "uuid": "c82c904f-b3b4-40a2-bf0d-008912953104"
}
```

encryption, extensions, ransomnotes MAY be used to give further information in ransomware galaxy. encryption is represented as a string and SHALL be present. extensions is represented as an array containing one or more strings and SHALL be present. ransomnotes is represented as an array containing one or more strings ans SHALL be present.

Example use of the encryption, extensions, ransomnotes fields in the ransomware galaxy:

```
{
  "meta": {
    "refs": [
      "https://www.bleepingcomputer.com/news/security/revenge-ransomware-a-
cryptomix-variant-being-distributed-by-rig-exploit-kit/",
      "https://id-ransomware.blogspot.co.il/2017/03/revenge-ransomware.html"
    ],
    "ransomnotes": [
      "https://2.bp.blogspot.com/-KkPVDxjy8tk/WM7LtYHmuAI/AAAAAAAAEUw/kDJghaq-
j1AZuqjzqk2Fkxpp4yr9Yeb5wCLcB/s1600/revenge-note-2.jpg",
      "===ENGLISH=== All of your files were encrypted using REVENGE Ransomware.
The action required to restore the files. Your files are not lost, they can be
returned to their normal state by decoding them. The only way to do this is to
get the software and your personal decryption key. Using any other software
that claims to be able to recover your files will result in corrupted or
destroyed files. You can purchase the software and the decryption key by
sending us an email with your ID. And we send instructions for payment. After
payment, you receive the software to return all files. For proof, we can
decrypt one file for free. Attach it to an e-mail.",
      "# !!!HELP_FILE!!! #.txt"
    ],
    "encryption": "AES-256 + RSA-1024",
    "extensions": [
      ".REVENGE"
    ],
    "date": "March 2017"
  },
  "description": "This is most likely to affect English speaking users, since
the note is written in English. English is understood worldwide, thus anyone
can be harmed. The hacker spread the virus using email spam, fake updates, and
harmful attachments. All your files are compromised including music, MS Office,
Open Office, pictures, videos, shared online files etc.. CryptoMix / CryptFile2
Variant",
  "value": "Revenge Ransomware",
  "uuid": "987d36d5-6ba8-484d-9e0b-7324cc886b0e"
}
```


source-uuid, target-uuid SHALL be used to describe relationships. source-uuid and target-uuid represent the Universally Unique IDentifier (UUID) [RFC4122] of the value reference. source-uuid and target-uuid MUST be preserved.

Example use of the source-uuid, target-uuid fields in the mitre-enterprise-attack-relationship galaxy:


```
      {
        "meta": {
          "source-uuid": "222fbd21-fc4f-4b7e-9f85-0e6e3a76c33f",
```

```
          "target-uuid": "2f1a9fd0-3b7c-4d77-a358-78db13adbe78"
        },
        "uuid": "cfc7da70-d7c5-4508-8f50-1c3107269633",
        "value": "menuPass (G0045) uses EvilGrab (S0152)"
      }
```

cfr-suspected-victims, cfr-suspected-state-sponsor, cfr-type-of-incident and cfr-target-category MAY be used to report information gathered from CFR's (Council on Foreign Relations) [CFR] Cyber Operations Tracker. cfr-suspected-victims is represented as an array containing one or more strings and SHALL be present. cfr-suspected-state-sponsor is represented as a string and SHALL be present. cfr-type-of-incident is represented as a string and SHALL be present. cfr-target-category is represented as an array containing one or more strings ans SHALL be present.

Example use of the cfr-suspected-victims, cfr-suspected-state-sponsor, cfr-type-of-incident, cfr-target-category fields in the threat-actor galaxy:

```
{
  "meta": {
    "country": "CN",
    "refs": [
      "https://www.fireeye.com/blog/threat-research/2015/12/
the_eps_awakens.html",
      "https://www.cfr.org/interactive/cyber-operations/apt-16"
    ],
    "cfr-suspected-victims": [
      "Japan",
      "Taiwan"
    ],
    "cfr-suspected-state-sponsor": "China",
    "cfr-type-of-incident": "Espionage",
    "cfr-target-category": [
      "Private sector"
    ]
  },
  "value": "APT 16",
  "uuid": "1f73e14f-b882-4032-a565-26dc653b0daf"
},
```

3. Acknowledgements

The authors wish to thank all the MISP community who are supporting the creation of open standards in threat intelligence sharing.

4. References

4.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/info/rfc2119>.

[RFC4122] Leach, P., Mealling, M., and R. Salz, "A Universally Unique IDentifier (UUID) URN Namespace", RFC 4122, DOI 10.17487/RFC4122, July 2005, <https://www.rfc-editor.org/info/rfc4122>.

[RFC4627] Crockford, D., "The application/json Media Type for JavaScript Object Notation (JSON)", RFC 4627, DOI 10.17487/RFC4627, July 2006, <https://www.rfc-editor.org/info/rfc4627>.

4.2. Informative References

[CFR] CFR, "Cyber Operations Tracker - Council on Foreign Relations", 2018, <https://www.cfr.org/interactive/cyber-operations>.

[MISP-G] MISP, "MISP Galaxy -", <https://github.com/MISP/misp-galaxy>.

[MISP-P] MISP, "MISP Project - Malware Information Sharing Platform and Threat Sharing", <https://github.com/MISP>.

Authors' Addresses

Alexandre Dulaunoy
Computer Incident Response Center Luxembourg
16, bd d'Avranches
Luxembourg L-1611
Luxembourg

Phone: +352 247 88444
Email: alexandre.dulaunoy@circl.lu

Andras Iklody
Computer Incident Response Center Luxembourg
16, bd d'Avranches
Luxembourg L-1611
Luxembourg

Phone: +352 247 88444
Email: andras.iklody@circl.lu

Deborah Servili
Computer Incident Response Center Luxembourg
16, bd d'Avranches
Luxembourg L-1611
Luxembourg

Phone: +352 247 88444
Email: deborah.servili@circl.lu