

Network Working Group  
Internet-Draft  
Intended status: Informational  
Expires: September 2, 2018

A. Dulaunoy  
A. Iklody  
D. Servili  
CIRCL  
March 1, 2018

**MISP galaxy format**  
**draft-dulaunoy-misp-galaxy-format-01**

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 September 2, 2018.

Copyright Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect

to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

## Table of Contents

<a href="#">1.</a>	Introduction . . . . .	<a href="#">2</a>
<a href="#">1.1.</a>	Conventions and Terminology . . . . .	<a href="#">2</a>
<a href="#">2.</a>	Format . . . . .	<a href="#">2</a>
<a href="#">2.1.</a>	Overview . . . . .	<a href="#">3</a>
<a href="#">2.2.</a>	values . . . . .	<a href="#">3</a>
<a href="#">2.3.</a>	meta . . . . .	<a href="#">3</a>
<a href="#">3.</a>	Acknowledgements . . . . .	<a href="#">4</a>
<a href="#">4.</a>	References . . . . .	<a href="#">4</a>
<a href="#">4.1.</a>	Normative References . . . . .	<a href="#">4</a>
<a href="#">4.2.</a>	Informative References . . . . .	<a href="#">5</a>
	Authors' Addresses . . . . .	<a href="#">5</a>

## [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 source is represented as a string and MUST be present. Authors are represented as an array containing one or more author and MUST be present.

Values are represented as an array containing one or more value 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 represents 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' wherever applicable.

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



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.

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.

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.

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 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.

derivated\_from, refs, synonyms SHALL be used to give further informations. refs is represented as an containing one or ore string and SHALL be present. synonyms is represented as an containing one or ore string and SHALL be present. derivated\_from is represented as an containing one or ore string and SHALL be present.

### **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**

- [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](mailto:deborah.servili@circl.lu)