Network Working Group
Internet-Draft
Intended status: Informational
Expires: December 25, 2019

A. Dulaunoy
A. Iklody
CIRCL

June 23, 2019

MISP object template format
draft-dulaunoy-misp-object-template-format-03

Abstract

This document describes the MISP object template format which describes a simple JSON format to represent the various templates used to construct MISP objects. A public directory of common vocabularies MISP object templates [MISP-O] is available and relies on the MISP object reference format.

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 December 25, 2019.

Table of Contents

1. Introduction

Due to the increased maturity of threat information sharing, the need arose for more complex and exhaustive data-points to be shared across the various sharing communities. MISP's information sharing in general relied on a flat structure of attributes contained within an event, where attributes served as atomic secluded data-points with some commonalities as defined by the encapsulating event. However, this flat structure restricted the use of more diverse and complex data-points described by a list of atomic values, a problem solved by the MISP object structure.

MISP objects combine a list of attributes to represent a singular object with various facets. In order to bootstrap the object creation process and to maintain uniformity among objects describing similar data-points, the MISP object template format serves as a reusable and share-able blueprint format.

MISP object templates also include a vocabulary to describe the various inter object and object to attribute relationships and are leveraged by MISP object references.

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

MISP object templates are composed of the MISP object template (MUST) structure itself and a list of MISP object template elements (SHOULD) describing the list of possible attributes belonging to the resulting object, along with their context and settings.

MISP object templates themselves consist of a name (MUST), a meta-category (MUST) and a description (SHOULD). They are identified by a uuid (MUST) and a version (MUST). For any updates or transfer of the same object reference. UUID version 4 is RECOMMENDED when assigning it to a new object reference. The list of requirements when it comes to the contained MISP object template elements is defined in the requirements field (OPTIONAL).

MISP object template elements consist of an object_relation (MUST), a type (MUST), an object_template_id (SHOULD), a ui_priority (SHOULD), a list of categories (MAY), a list of sane_default values (MAY) or a values_list (MAY).

2.1. Overview

The MISP object template format uses the JSON [RFC4627] format. Each template is represented as a JSON object with meta information including the following fields: uuid, requiredOneOf, description, version, meta-category, name.

2.1.1. Object Template

2.1.1.1. uuid

uuid represents the Universally Unique IDentifier (UUID) [RFC4122] of the object template. The uuid MUST be preserved for to keep consistency of the templates across instances. UUID version 4 is RECOMMENDED when assigning it to a new object template.

uuid is represented as a JSON string. uuid MUST be present.

2.1.1.2. requiredOneOf

requiredOneOf is represented as a JSON list and contains a list of attribute relationships of which one must be present in the object to be created based on the given template. The requiredOneOf field MAY be present.

2.1.1.3. required

required is represented as a JSON list and contains a list of attribute relationships of which all must be present in the object to be created based on the given template. The required field MAY be present.

2.1.1.4. description

description is represented as a JSON string and contains the assigned meaning given to objects created using this template. The description field MUST be present.

2.1.1.5. version

version represents a numeric incrementing version of the object template. It is used to associate the object to the correct version of the template and together with the uuid field forms an association to the correct template type and version.

version is represented as a JSON string. version MUST be present.

2.1.1.6. meta-category

meta-category represents the sub-category of objects that the given object template belongs to. meta-categories are not tied to a fixed list of options but can be created on the fly.

meta-category is represented as a JSON string. meta-category MUST be present.

2.1.1.7. name

name represents the human-readable name of the objects created using the given template, describing the intent of the object package.

name is represented as a JSON string. name MUST be present

2.1.2. attributes

attributes is represented as a JSON list and contains a list of template elements used as a template for creating the individual attributes within the object that is to be created with the object.

attributes is represented as a JSON list. attributes MUST be present.

2.1.2.1. description

description is represented as a JSON string and contains the description of the given attribute in the context of the object with the given relationship. The description field MUST be present.

2.1.2.2. ui-priority

ui-priority is represented by a numeric values in JSON string format and is meant to provide a priority for the given element in the object template visualisation. The ui-priority MAY be present.

2.1.2.3. misp-attribute

misp-attribute is represented by a JSON string or a JSON object with a list of values. The value(s) are taken from the pool of types defined by the MISP core format's Attribute Object's type list. type can contain a JSON object with a list of suggested value alternatives encapsulated in a list within a sane_default key or a list of enforced value alternatives encapsulated in a list_values key.

The misp-attribute field MUST be present.

2.1.2.4. disable_correlation

disable_correlation is represented by a JSON boolean. The disable_correlation field flags the attribute(s) created by the given object template element to be marked as non correlating.

The misp-attribute field MAY be present.

2.1.2.5. categories

categories is represented by a JSON list containing one or several valid options from the list of verbs valid for the category field in the Attribute object within the MISP core format.

The categories field MAY be present.

2.1.2.6. multiple

multiple is represented by a JSON boolean value. It marks the MISP object template element as a multiple input field, allowing for several attributes to be created by the element within the same object.

The multiple field MAY be present.

2.1.2.7. sane_default

sane_default is represented by a JSON list containing one or several recommended/sane values for an attribute. sane_default is mutually exclusive with values_list.

The sane_default field MAY be present.

2.1.2.8. values_list

values_list is represented by a JSON List containing one or several of fixed values for an attribute. values_list is mutually exclusive with sane_default.

The value_list field MAY be present.

2.1.3. Sample Object Template object

The MISP object template directory is publicly available [MISP-O] in a git repository and contains more than 60 object templates. As illustration, two sample objects templates are included.

2.1.3.1. credit-card object template

```
{
  "requiredOneOf": [
    "cc-number"
  ],
  "attributes": {
    "version": {
      "description": "Version of the card.",
      "ui-priority": 0,
      "misp-attribute": "text"
    },
    "comment": {
      "description": "A description of the card.",
      "ui-priority": 0,
      "misp-attribute": "comment"
    },
    "card-security-code": {
      "description": "Card security code (CSC, CVD, CVV, CVC and SPC) as
embossed or printed on the card.",
      "ui-priority": 0,
      "misp-attribute": "text"
    },
    "name": {
      "description": "Name of the card owner.",
      "ui-priority": 0,
      "misp-attribute": "text"
    },
    "issued": {
      "description": "Initial date of validity or issued date.",
      "ui-priority": 0,
      "misp-attribute": "datetime"
    },
    "expiration": {
      "description": "Maximum date of validity",
      "ui-priority": 0,
      "misp-attribute": "datetime"
    },
    "cc-number": {
      "description": "credit-card number as encoded on the card.",
      "ui-priority": 0,
      "misp-attribute": "cc-number"
    }
  },
  "version": 2,
  "description": "A payment card like credit card, debit card or any similar
cards which can be used for financial transactions.",
  "meta-category": "financial",
  "uuid": "2b9c57aa-daba-4330-a738-56f18743b0c7",
  "name": "credit-card"
```

```
}
```

2.1.3.2. credential object template

```
{
  "requiredOneOf": [
    "password"
  ],
  "attributes": {
    "text": {
      "description": "A description of the credential(s)",
      "disable_correlation": true,
      "ui-priority": 1,
      "misp-attribute": "text"
    },
    "username": {
      "description": "Username related to the password(s)",
      "ui-priority": 1,
      "misp-attribute": "text"
    },
    "password": {
      "description": "Password",
      "multiple": true,
      "ui-priority": 1,
      "misp-attribute": "text"
    },
    "type": {
      "description": "Type of password(s)",
      "ui-priority": 1,
      "misp-attribute": "text",
      "values_list": [
        "password",
        "api-key",
        "encryption-key",
        "unknown"
      ]
    },
    "origin": {
      "description": "Origin of the credential(s)",
      "ui-priority": 1,
      "misp-attribute": "text",
      "sane_default": [
        "bruteforce-scanning",
        "malware-analysis",
        "memory-analysis",
        "network-analysis",
        "leak",
        "unknown"
      ]
    },
```

```
    "format": {
      "description": "Format of the password(s)",
      "ui-priority": 1,
      "misp-attribute": "text",
      "values_list": [
        "clear-text",
        "hashed",
        "encrypted",
        "unknown"
      ]
    },
    "notification": {
      "description": "Mention of any notification(s) towards the potential
owner(s) of the credential(s)",
      "ui-priority": 1,
      "misp-attribute": "text",
      "multiple": true,
      "values_list": [
        "victim-notified",
        "service-notified",
        "none"
      ]
    }
  },
  "version": 2,
  "description": "Credential describes one or more credential(s) including
password(s), api key(s) or decryption key(s).",
  "meta-category": "misc",
  "uuid": "a27e98c9-9b0e-414c-8076-d201e039ca09",
  "name": "credential"
}
```

2.1.4. Object Relationships

2.1.4.1. name

name represents the human-readable relationship type which can be used when creating MISP object relations.

name is represented as a JSON string. name MUST be present.

2.1.4.2. description

description is represented as a JSON string and contains the description of the object relationship type. The description field MUST be present.

2.1.4.3. format

format is represented by a JSON list containing a list of formats that the relationship type is valid for and can be mapped to. The format field MUST be present.

3. Directory

The MISP object template directory is publicly available [MISP-O] in a git repository. The repository contains an objects directory, which contains a directory per object type, containing a file named definition.json which contains the definition of the object template in the above described format.

A relationships directory is also included, containing a definition.json file which contains a list of MISP object relation definitions. There are more than 125 existing templates object documented in [MISP-O-DOC].

3.1. Existing and public MISP object templates

- tsk-chats - An Object Template to gather information from evidential or interesting exchange of messages identified during a digital forensic investigation.
- tsk-web-bookmark - An Object Template to add evidential bookmarks identified during a digital forensic investigation.
- tsk-web-cookie - An TSK-Autopsy Object Template to represent cookies identified during a forensic investigation.
- tsk-web-downloads - An Object Template to add web-downloads.
- tsk-web-history - An Object Template to share web history information.
- tsk-web-search-query - An Object Template to share web search query information.
- ail-leak - An information leak as defined by the AIL Analysis Information Leak framework.
- ais-info - Automated Indicator Sharing (AIS) Information Source Markings.
- android-permission - A set of android permissions - one or more permission(s) which can be linked to other objects (e.g. malware, app).

- annotation - An annotation object allowing analysts to add annotations, comments, executive summary to a MISP event, objects or attributes.

- anonymisation - Anonymisation object describing an anonymisation technique used to encode MISP attribute values. Reference: <https://www.caida.org/tools/taxonomy/anonymization.xml>.

- asn - Autonomous system object describing an autonomous system which can include one or more network operators management an entity (e.g. ISP) along with their routing policy, routing prefixes or alike.

- authenticode-signerinfo - Authenticode Signer Info.

- av-signature - Antivirus detection signature.

- bank-account - An object describing bank account information based on account description from goAML 4.0.

- bgp-hijack - Object encapsulating BGP Hijack description as specified, for example, by bgpstream.com.

- cap-alert - Common Alerting Protocol Version (CAP) alert object.

- cap-info - Common Alerting Protocol Version (CAP) info object.

- cap-resource - Common Alerting Protocol Version (CAP) resource object.

- coin-address - An address used in a cryptocurrency.

- cookie - An HTTP cookie (web cookie, browser cookie) is a small piece of data that a server sends to the user's web browser. The browser may store it and send it back with the next request to the same server. Typically, it's used to tell if two requests came from the same browser -- keeping a user logged-in, for example. It remembers stateful information for the stateless HTTP protocol. (as defined by the Mozilla foundation.

- cortex - Cortex object describing a complete cortex analysis. Observables would be attribute with a relationship from this object.

- cortex-taxonomy - Cortex object describing an Cortex Taxonomy (or mini report).

- course-of-action - An object describing a specific measure taken to prevent or respond to an attack.
- cowrie - Cowrie honeypot object template.
- credential - Credential describes one or more credential(s) including password(s), api key(s) or decryption key(s).
- credit-card - A payment card like credit card, debit card or any similar cards which can be used for financial transactions.
- ddos - DDoS object describes a current DDoS activity from a specific or/and to a specific target. Type of DDoS can be attached to the object as a taxonomy.
- device - An object to define a device.
- diameter-attack - Attack as seen on diameter authentication against a GSM, UMTS or LTE network.
- domain-ip - A domain and IP address seen as a tuple in a specific time frame.
- elf - Object describing a Executable and Linkable Format.
- elf-section - Object describing a section of an Executable and Linkable Format.
- email - Email object describing an email with meta-information.
- exploit-poc - Exploit-poc object describing a proof of concept or exploit of a vulnerability. This object has often a relationship with a vulnerability object.
- facial-composite - An object which describes a facial composite.
- fail2ban - Fail2ban event.
- file - File object describing a file with meta-information.
- forensic-case - An object template to describe a digital forensic case.
- forensic-evidence - An object template to describe a digital forensic evidence.
- geolocation - An object to describe a geographic location.

- gtp-attack - GTP attack object as seen on a GSM, UMTS or LTE network.
- http-request - A single HTTP request header.
- ilr-impact - Institut Luxembourgeois de Regulation - Impact.
- ilr-notification-incident - Institut Luxembourgeois de Regulation - Notification d'incident.
- internal-reference - Internal reference.
- interpol-notice - An object which describes a Interpol notice.
- ip-api-address - IP Address information. Useful if you are pulling your ip information from ip-api.com.
- ip-port - An IP address (or domain or hostname) and a port seen as a tuple (or as a triple) in a specific time frame.
- irc - An IRC object to describe an IRC server and the associated channels.
- ja3 - JA3 is a new technique for creating SSL client fingerprints that are easy to produce and can be easily shared for threat intelligence. Fingerprints are composed of Client Hello packet; SSL Version, Accepted Ciphers, List of Extensions, Elliptic Curves, and Elliptic Curve Formats. <https://github.com/salesforce/ja3>.
- legal-entity - An object to describe a legal entity.
- lnk - LNK object describing a Windows LNK binary file (aka Windows shortcut).
- macho - Object describing a file in Mach-O format.
- macho-section - Object describing a section of a file in Mach-O format.
- mactime-timeline-analysis - Mactime template, used in forensic investigations to describe the timeline of a file activity.
- malware-config - Malware configuration recovered or extracted from a malicious binary.
- microblog - Microblog post like a Twitter tweet or a post on a Facebook wall.

- mutex - Object to describe mutual exclusion locks (mutex) as seen in memory or computer program.
- netflow - Netflow object describes an network object based on the Netflowv5/v9 minimal definition.
- network-connection - A local or remote network connection.
- network-socket - Network socket object describes a local or remote network connections based on the socket data structure.
- misc - An object which describes an organization.
- original-imported-file - Object describing the original file used to import data in MISP.
- passive-dns - Passive DNS records as expressed in draft-dulaunoy-dnsop-passive-dns-cof-01.
- paste - Paste or similar post from a website allowing to share privately or publicly posts.
- pcap-metadata - Network packet capture metadata.
- pe - Object describing a Portable Executable.
- pe-section - Object describing a section of a Portable Executable.
- person - An object which describes a person or an identity.
- phishing - Phishing template to describe a phishing website and its analysis.
- phishing-kit - Object to describe a phishing-kit.
- phone - A phone or mobile phone object which describe a phone.
- process - Object describing a system process.
- python-etvx-event-log - Event log object template to share information of the activities conducted on a system. .
- r2graphity - Indicators extracted from files using radare2 and graphml.
- regexp - An object describing a regular expression (regex or regexp). The object can be linked via a relationship to other

attributes or objects to describe how it can be represented as a regular expression.

- registry-key - Registry key object describing a Windows registry key with value and last-modified timestamp.

- regripper-NTUser - Regripper Object template designed to present user specific configuration details extracted from the NTUSER.dat hive.

- regripper-sam-hive-single-user - Regripper Object template designed to present user profile details extracted from the SAM hive.

- regripper-sam-hive-user-group - Regripper Object template designed to present group profile details extracted from the SAM hive.

- regripper-software-hive-BHO - Regripper Object template designed to gather information of the browser helper objects installed on the system.

- regripper-software-hive-appInit-DLLS - Regripper Object template designed to gather information of the DLL files installed on the system.

- regripper-software-hive-application-paths - Regripper Object template designed to gather information of the application paths.

- regripper-software-hive-applications-installed - Regripper Object template designed to gather information of the applications installed on the system.

- regripper-software-hive-command-shell - Regripper Object template designed to gather information of the shell commands executed on the system.

- regripper-software-hive-windows-general-info - Regripper Object template designed to gather general windows information extracted from the software-hive.

- regripper-software-hive-software-run - Regripper Object template designed to gather information of the applications set to run on the system.

- regripper-software-hive-userprofile-winlogon - Regripper Object template designed to gather user profile information when the user logs onto the system, gathered from the software hive.

- regripper-system-hive-firewall-configuration - Regripper Object template designed to present firewall configuration information extracted from the system-hive.

- regripper-system-hive-general-configuration - Regripper Object template designed to present general system properties extracted from the system-hive.

- regripper-system-hive-network-information. - Regripper object template designed to gather network information from the system-hive.

- regripper-system-hive-services-drivers - Regripper Object template designed to gather information regarding the services/drivers from the system-hive.

- report - Metadata used to generate an executive level report.

- research-scanner - Information related to known scanning activity (e.g. from research projects).

- rogue-dns - Rogue DNS as defined by CERT.br.

- rtir - RTIR - Request Tracker for Incident Response.

- sandbox-report - Sandbox report.

- sb-signature - Sandbox detection signature.

- script - Object describing a computer program written to be run in a special run-time environment. The script or shell script can be used for malicious activities but also as support tools for threat analysts.

- shell-commands - Object describing a series of shell commands executed. This object can be linked with malicious files in order to describe a specific execution of shell commands.

- short-message-service - Short Message Service (SMS) object template describing one or more SMS message. Restriction of the initial format 3GPP 23.038 GSM character set doesn't apply.

- shortened-link - Shortened link and its redirect target.

- splunk - Splunk / Splunk ES object.

- ss7-attack - SS7 object of an attack seen on a GSM, UMTS or LTE network via SS7 logging.

- ssh-authorized-keys - An object to store ssh authorized keys file.
- stix2-pattern - An object describing a STIX pattern. The object can be linked via a relationship to other attributes or objects to describe how it can be represented as a STIX pattern.
- suricata - An object describing one or more Suricata rule(s) along with version and contextual information.
- target-system - Description about an targeted system, this could potentially be a compromissed internal system.
- threatgrid-report - ThreatGrid report.
- timecode - Timecode object to describe a start of video sequence (e.g. CCTV evidence) and the end of the video sequence.
- timesketch-timeline - A timesketch timeline object based on mandatory field in timesketch to describe a log entry.
- timesketch_message - A timesketch message entry.
- timestamp - A generic timestamp object to represent time including first time and last time seen. Relationship will then define the kind of time relationship.
- tor-hiddenservice - Tor hidden service (onion service) object.
- tor-node - Tor node (which protects your privacy on the internet by hiding the connection between users Internet address and the services used by the users) description which are part of the Tor network at a time.
- tracking-id - Analytics and tracking ID such as used in Google Analytics or other analytic platform.
- transaction - An object to describe a financial transaction.
- url - url object describes an url along with its normalized field (like extracted using faup parsing library) and its metadata.
- vehicle - Vehicle object template to describe a vehicle information and registration.
- victim - Victim object describes the target of an attack or abuse.
- virustotal-report - VirusTotal report.

- vulnerability - Vulnerability object describing a common vulnerability enumeration which can describe published, unpublished, under review or embargo vulnerability for software, equipments or hardware.

- whois - Whois records information for a domain name or an IP address.

- x509 - x509 object describing a X.509 certificate.

- yabin - yabin.py generates Yara rules from function prologs, for matching and hunting binaries. ref: <https://github.com/AlienVault-OTX/yabin>.

- yara - An object describing a YARA rule along with its version.

4. Acknowledgements

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

5. References

5.1. 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>.

5.2. Informative References

[MISP-O] MISP, "MISP Objects - shared and common object templates", <https://github.com/MISP/misp-objects>.

[MISP-O-DOC] "MISP objects directory", 2018, <https://www.misp-project.org/objects.html>.

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