Workgroup: Network Working Group
Internet-Draft: draft-06
Published: 24 December 2023
Intended Status: Informational
Expires: 26 June 2024
Authors: A. Dulaunoy   A. Iklody
         CIRCL   CIRCL

MISP object template format

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

Copyright Notice

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 [RFC8259] 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
      "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 sim
  "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 potenti
      "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) includi
  "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

- objects/ADS - An object defining ADS - Alerting and Detection Strategy by PALANTIR. Can be used for detection engineering.
- objects/abuseipdb - AbuseIPDB checks an ip address, domain name, or subnet against a central blacklist.
- objects/ai-chat-prompt - Object describing an AI prompt such as ChatGPT.
- objects/ail-leak - An information leak as defined by the AIL Analysis Information Leak framework.
- objects/ais - Automatic Identification System (AIS) is an automatic tracking system that uses transceivers on ships.
- objects/ais-info - Automated Indicator Sharing (AIS) Information Source Markings.
- objects/android-app - Indicators related to an Android app.

*objects/android-permission - A set of android permissions - one or more permission(s) which can be linked to other objects (e.g. malware, app).

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

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

*objects/apivoid-email-verification - Apivoid email verification API result. Reference: https://www.apivoid.com/api/email-verify/.

*objects/artifact - The Artifact object permits capturing an array of bytes (8-bits), as a base64-encoded string, or linking to a file-like payload. From STIX 2.1 (6.1).

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

*objects/attack-pattern - Attack pattern describing a common attack pattern enumeration and classification.

*objects/attack-step - An object defining a singular attack-step. Especially useful for red/purple teaming, but can also be used for actual attacks.

*objects/authentication-failure-report - Authentication Failure Report.

*objects/authenticode-signerinfo - Authenticode Signer Info.

*objects/av-signature - Antivirus detection signature.

*objects/availability-impact - Availability Impact object as described in STIX 2.1 Incident object extension.

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

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

*objects/bgp-ranking - BGP Ranking object describing the ranking of an ASN for a given day, along with its position, 1 being the most malicious ASN of the day, with the highest ranking. This object is meant to have a relationship with the corresponding ASN object and represents its ranking for a specific date.

*objects/blog - Blog post like Medium or WordPress.

*objects/boleto - A common form of payment used in Brazil.

*objects/btc-transaction - An object to describe a Bitcoin transaction. Best to be used with bitcoin-wallet.

*objects/btc-wallet - An object to describe a Bitcoin wallet. Best to be used with btc-transaction object.

*objects/c2-list - List of C2-servers with common ground, e.g. extracted from a blog post or ransomware analysis.

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

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

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

*objects/cloth - Describes clothes a natural person wears.

*objects/coin-address - An address used in a cryptocurrency.

*objects/command - Command functionalities related to specific commands executed by a program, whether it is malicious or not. Command-line are attached to this object for the related commands.

*objects/command-line - Command line and options related to a specific command executed by a program, whether it is malicious or not.

*objects/concordia-mtmf-intrusion-set - Intrusion Set - Phase Description.

*objects/confidentiality-impact - Confidentiality Impact object as described in STIX 2.1 Incident object extension.

*objects/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.

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

*objects/cortex-taxonomy - Cortex object describing a Cortex Taxonomy (or mini report).

*objects/course-of-action - An object describing a specific measure taken to prevent or respond to an attack.

*objects/covid19-csse-daily-report - CSSE COVID-19 Daily report.

*objects/covid19-dxy-live-city - COVID 19 from dxy.cn - Aggregation by city.

*objects/covid19-dxy-live-province - COVID 19 from dxy.cn - Aggregation by province.

*objects/cowrie - Cowrie honeypot object template.

*objects/cpe-asset - An asset which can be defined by a CPE. This can be a generic asset. CPE is a structured naming scheme for information technology systems, software, and packages.

*objects/credential - Credential describes one or more credential(s) including password(s), api key(s) or decryption key(s).

*objects/credit-card - A payment card like credit card, debit card or any similar cards which can be used for financial transactions.

*objects/crowdsec-ip-context - CrowdSec Threat Intelligence - IP CTI search.

*objects/crowdstrike-report - An Object Template to encode an Crowdstrike detection report.

*objects/crypto-material - Cryptographic materials such as public or/and private keys.

*objects/cryptocurrency-transaction - An object to describe a cryptocurrency transaction.

*objects/cs-beacon-config - Cobalt Strike Beacon Config.

*objects/cytomic-orion-file - Cytomic Orion File Detection.

*objects/cytomic-orion-machine - Cytomic Orion File at Machine Detection.

*objects/dark-pattern-item - An Item whose User Interface implements a dark pattern.

*objects/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 or using the type field.

*objects/device - An object to define a device.

*objects/diameter-attack - Attack as seen on the diameter signaling protocol supporting LTE networks.

*objects/diamond-event - A diamond model event object consisting of the four diamond features advesary, infrastructure, capability and victim, several meta-features and ioc attributes.

*objects/directory - Directory object describing a directory with meta-information.

*objects/dkim - DomainKeys Identified Mail - DKIM.

*objects/dns-record - A set of DNS records observed for a specific domain.

*objects/domain-crawled - A domain crawled over time.

*objects/domain-ip - A domain/hostname and IP address seen as a tuple in a specific time frame.

*objects/edr-report - An Object Template to encode an EDR detection report.

*objects/elf - Object describing a Executable and Linkable Format.

*objects/elf-section - Object describing a section of an Executable and Linkable Format.

*objects/email - Email object describing an email with meta-information.

*objects/employee - An employee and related data points.

*objects/error-message - An error message which can be related to the processing of data such as import, export scripts from the original MISP instance.

*objects/event - Event object as described in STIX 2.1 Incident object extension.

*objects/exploit - Exploit object describes a program in binary or source code form used to abuse one or more vulnerabilities.

*objects/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.

*objects/external-impact - External Impact object as described in STIX 2.1 Incident object extension.

*objects/facebook-account - Facebook account.
*objects/facebook-group - Public or private facebook group.
*objects/facebook-page - Facebook page.
*objects/facebook-post - Post on a Facebook wall.
*objects/facebook-reaction - Reaction to facebook posts.
*objects/facial-composite - An object which describes a facial composite.
*objects/fail2ban - Fail2ban event.
*objects/favicon - A favicon, also known as a shortcut icon, website icon, tab icon, URL icon, or bookmark icon, is a file containing one or more small icons, associated with a particular website or web page. The object template can include the murmur3 hash of the favicon to facilitate correlation.
*objects/file - File object describing a file with meta-information.
*objects/flowintel-cm-case - A case as defined by flowintel-cm.
*objects/flowintel-cm-task - A task as defined by flowintel-cm.
*objects/forensic-case - An object template to describe a digital forensic case.
*objects/forensic-evidence - An object template to describe a digital forensic evidence.
*objects/forged-document - Object describing a forged document.
*objects/ftm-Airplane - An airplane, helicopter or other flying vehicle.
*objects/ftm-Assessment - Assessment with meta-data.
*objects/ftm-Asset - A piece of property which can be owned and assigned a monetary value.
*objects/ftm-Associate - Non-family association between two people.
*objects/ftm-Audio - Audio with meta-data.
*objects/ftm-BankAccount - An account held at a bank and controlled by an owner. This may also be used to describe more complex arrangements like correspondent bank settlement accounts.
*objects/ftm-Call - Phone call object template including the call and all associated meta-data.
*objects/ftm-Company - A legal entity representing an association of people, whether natural, legal or a mixture of both, with a specific objective.
*objects/ftm-Contract - An contract or contract lot issued by an authority. Multiple lots may be awarded to different suppliers (see ContractAward). .
*objects/ftm-ContractAward - A contract or contract lot as awarded to a supplier.
*objects/ftm-CourtCase - Court case.
*objects/ftm-CourtCaseParty - Court Case Party.
*objects/ftm-Debt - A monetary debt between two parties.
*objects/ftm-Directorship - Directorship.
*objects/ftm-Document - Document.
*objects/ftm-Documentation - Documentation.

*objects/ftm-EconomicActivity - A foreign economic activity.
*objects/ftm-Email - Email.
*objects/ftm-Event - Event.
*objects/ftm-Family - Family relationship between two people.
*objects/ftm-Folder - Folder.
*objects/ftm-HyperText - HyperText.
*objects/ftm-Image - Image.
*objects/ftm-Land - Land.
*objects/ftm-LegalEntity - A legal entity may be a person or a company.
*objects/ftm-License - A grant of land, rights or property. A type of Contract.
*objects/ftm-Membership - Membership.
*objects/ftm-Message - Message.
*objects/ftm-Organization - Organization.
*objects/ftm-Ownership - Ownership.
*objects/ftm-Package - Package.
*objects/ftm-Page - Page.
*objects/ftm-Pages - Pages.
*objects/ftm-Passport - Passport.
*objects/ftm-Payment - A monetary payment between two parties.
*objects/ftm-Person - An individual.
*objects/ftm-PlainText - Plaintext.
*objects/ftm-PublicBody - A public body, such as a ministry, department or state company.
*objects/ftm-RealEstate - A piece of land or property.
*objects/ftm-Representation - A mediatory, intermediary, middleman, or broker acting on behalf of a legal entity.
*objects/ftm-Row - Row.
*objects/ftm-Sanction - A sanction designation.
*objects/ftm-Succession - Two entities that legally succeed each other.
*objects/ftm-Table - Table.
*objects/ftm-TaxRoll - A tax declaration of an individual.
*objects/ftm-UnknownLink - Unknown Link.
*objects/ftm-UserAccount - User Account.
*objects/ftm-Vehicle - Vehicle.
*objects/ftm-Vessel - A boat or ship.
*objects/ftm-Video - Video.
*objects/ftm-Workbook - Workbook.
*objects/game-cheat - Describes a game cheat or a cheatware.
*objects/geolocation - An object to describe a geographic location.
*objects/git-vuln-finder - Export from git-vuln-finder.
*objects/github-user - GitHub user.
*objects/gitlab-user - GitLab user. Gitlab.com user or self-hosted GitLab instance.
*objects/google-safe-browsing - Google Safe checks a URL against Google's constantly updated list of unsafe web resources.

*objects/greynoise-ip - GreyNoise IP Information.

*objects/gtp-attack - GTP attack object as attack as seen on the GTP signaling protocol supporting GPRS/LTE networks.

*objects/hashlookup - hashlookup object as described on hashlookup services from circl.lu - https://www.circl.lu/services/hashlookup.

*objects/hhhash - An object describing a HHHash object with the hash value along with the crawling parameters. For more information: https://www.foo.be/2023/07/HTTP-Headers-Hashing_HHHash.

*objects/http-request - A single HTTP request header.

*objects/identity - Identities can represent actual individuals, organizations, or groups (e.g., ACME, Inc.) as well as classes of individuals, organizations, systems or groups (e.g., the finance sector). The Identity SDO can capture basic identifying information, contact information, and the sectors that the Identity belongs to. Identity is used in STIX to represent, among other things, targets of attacks, information sources, object creators, and threat actor identities. (ref. STIX 2.1 - 4.5).

*objects/ilr-impact - Institut Luxembourgeois de Regulation - Impact.

*objects/ilr-notification-incident - Institut Luxembourgeois de Regulation - Notification d'incident.

*objects/image - Object describing an image file.

*objects/impersonation - Represent an impersonating account.

*objects/imsi-catcher - IMSI Catcher entry object based on the open source IMSI cather.

*objects/incident - Incident object template as described in STIX 2.1 Incident object and its core extension.

*objects/infrastructure - The Infrastructure object represents a type of TTP and describes any systems, software services and any associated physical or virtual resources intended to support some purpose (e.g., C2 servers used as part of an attack, device or server that are part of defense, database servers targeted by an attack, etc.). While elements of an attack can be represented by other objects, the Infrastructure object represents a named group of related data that constitutes the infrastructure. STIX 2.1 - 4.8.

*objects/instant-message - Instant Message (IM) object template describing one or more IM message.

*objects/instant-message-group - Instant Message (IM) group object template describing a public or private IM group, channel or conversation.

*objects/integrity-impact - Integrity Impact object as described in STIX 2.1 Incident object extension.

*objects/intel471-vulnerability-intelligence - Intel 471 vulnerability intelligence object.

*objects/intelmq_event - IntelMQ Event.

*objects/intelmq_report - IntelMQ Report.

*objects/internal-reference - Internal reference.
*objects/interpol-notice - An object which describes a Interpol notice.
*objects/intrusion-set - A object template describing an Intrusion Set as defined in STIX 2.1. An Intrusion Set is a grouped set of adversarial behaviors and resources with common properties that is believed to be orchestrated by a single organization. An Intrusion Set may capture multiple Campaigns or other activities that are all tied together by shared attributes indicating a commonly known or unknown Threat Actor. New activity can be attributed to an Intrusion Set even if the Threat Actors behind the attack are not known. Threat Actors can move from supporting one Intrusion Set to supporting another, or they may support multiple Intrusion Sets. Where a Campaign is a set of attacks over a period of time against a specific set of targets to achieve some objective, an Intrusion Set is the entire attack package and may be used over a very long period of time in multiple Campaigns to achieve potentially multiple purposes. While sometimes an Intrusion Set is not active, or changes focus, it is usually difficult to know if it has truly disappeared or ended. Analysts may have varying level of fidelity on attributing an Intrusion Set back to Threat Actors and may be able to only attribute it back to a nation state or perhaps back to an organization within that nation state.
*objects/iot-device - An IoT device.
*objects/iot-firmware - A firmware for an IoT device.
*objects/ip-api-address - IP Address information. Useful if you are pulling your ip information from ip-api.com.
*objects/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.
*objects/irc - An IRC object to describe an IRC server and the associated channels.
*objects/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.
*objects/ja3s - JA3S is JA3 for the Server side of the SSL/TLS communication and fingerprints how servers respond to particular clients. JA3S fingerprints are composed of Server Hello packet; SSL Version, Cipher, SSLExtensions. https://github.com/salesforce/ja3.
*objects/jarm - Jarm object to describe an TLS/SSL implementation used for malicious or legitimate use-case.
*objects/keybase-account - Information related to a keybase account, from API Users Object.
*objects/language-content - The Language Content object represents text content for objects represented in languages other than that

of the original object. Language content may be a translation of the original object by a third-party, a first-source translation by the original publisher, or additional official language content provided at the time of creation. STIX 2.1 ref 7.1.

*objects/leaked-document - Object describing a leaked document.

*objects/legal-entity - An object to describe a legal entity.

*objects/lnk - LNK object describing a Windows LNK binary file (aka Windows shortcut).

*objects/macho - Object describing a file in Mach-O format.

*objects/macho-section - Object describing a section of a file in Mach-O format.

*objects/mactime-timeline-analysis - Mactime template, used in forensic investigations to describe the timeline of a file activity.

*objects/malware - Malware is a type of TTP that represents malicious code.

*objects/malware-analysis - Malware Analysis captures the metadata and results of a particular static or dynamic analysis performed on a malware instance or family.

*objects/malware-config - Malware configuration recovered or extracted from a malicious binary.

*objects/meme-image - Object describing a meme (image).

*objects/microblog - Microblog post like a Twitter tweet or a post on a Facebook wall.

*objects/monetary-impact - Monetary Impact object as described in STIX 2.1 Incident object extension.

*objects/mutex - Object to describe mutual exclusion locks (mutex) as seen in memory or computer program.

*objects/narrative - Object describing a narrative.

*objects/netflow - Netflow object describes an network object based on the Netflowv5/v9 minimal definition.

*objects/network-connection - A local or remote network connection.

*objects/network-profile - Elements that can be used to profile, pivot or identify a network infrastructure, including domains, ip and urls.

*objects/network-socket - Network socket object describes a local or remote network connections based on the socket data structure.

*objects/news-agency - News agencies compile news and disseminate news in bulk.

*objects/news-media - News media are forms of mass media delivering news to the general public.

*objects/open-data-security - An object describing an open dataset available and described under the open data security model. ref. https://github.com/CIRCL/open-data-security.

*objects/organization - An object which describes an organization.

*objects/original-imported-file - Object describing the original file used to import data in MISP.

*objects/paloalto-threat-event - Palo Alto Threat Log Event.

*objects/parler-account - Parler account.

*objects/parler-comment - Parler comment.

*objects/parler-post - Parler post (parley).

*objects/passive-dns - Passive DNS records as expressed in draft-dulaunoy-dnsop-passive-dns-cof-07. See https://tools.ietf.org/id/draft-dulaunoy-dnsop-passive-dns-cof-07.html.

*objects/passive-dns-dnsdbflex - DNSDBFLEX object. This object is used at farsight security. Roughly based on Passive DNS records as expressed in draft-dulaunoy-dnsop-passive-dns-cof-07. See https://tools.ietf.org/id/draft-dulaunoy-dnsop-passive-dns-cof-07.html.

*objects/passive-ssh - Passive-ssh object as described on passive-ssh services from circl.lu - https://github.com/D4-project/passive-ssh.

*objects/paste - Paste or similar post from a website allowing to share privately or publicly posts.

*objects/pcap-metadata - Network packet capture metadata.

*objects/pe - Object describing a Portable Executable.

*objects/pe-section - Object describing a section of a Portable Executable.

*objects/Deception PersNOna - Fake persona with tasks.

*objects/person - An object which describes a person or an identity.

*objects/personification - An object which describes a person or an identity.

*objects/pgp-meta - Metadata extracted from a PGP keyblock, message or signature.

*objects/phishing - Phishing template to describe a phishing website and its analysis.

*objects/phishing-kit - Object to describe a phishing-kit.

*objects/phone - A phone or mobile phone object which describe a phone.

*objects/physical-impact - Physical Impact object as described in STIX 2.1 Incident object extension.

*objects/postal-address - A postal address.

*objects/probabilistic-data-structure - Probabilistic data structure object describe a space-efficient data structure such as Bloom filter or similar structure.

*objects/process - Object describing a system process.

*objects/publication - An object to describe a book, journal, or academic publication.

*objects/python-etvx-event-log - Event log object template to share information of the activities conducted on a system. .

*objects/query - An object describing a query, along with its format.

*objects/r2graphity - Indicators extracted from files using radare2 and graphml.

*objects/ransom-negotiation - An object to describe ransom negotiations, as seen in ransomware incidents.

*objects/ransomware-group-post - Ransomware group post as monitored by ransomlook.io.

*objects/reddit-account - Reddit account.

*objects/reddit-comment - A Reddit post comment.

*objects/reddit-post - A Reddit post.

*objects/reddit-subreddit - Public or private subreddit.

*objects/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.

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

*objects/registry-key-value - Registry key value object describing a Windows registry key value, with its data, data type and name values. To be used when a registry key has multiple values.

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

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

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

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

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

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

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

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

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

*objects/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.

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

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

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

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

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

*objects/report - Report object to describe a report along with its metadata.

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

*objects/risk-assessment-report - Risk assessment report object which includes the assessment report from a risk assessment platform such as MONARC.

*objects/rogue-dns - Rogue DNS as defined by CERT.br.

*objects/rtir - RTIR - Request Tracker for Incident Response.

*objects/sandbox-report - Sandbox report.

*objects/sb-signature - Sandbox detection signature.

*objects/scan-result - Scan result object to add meta-data and the output of the scan result by itself.

*objects/scheduled-event - Event object template describing a gathering of individuals in meatspace.

*objects/scheduled-task - Windows scheduled task description.

*objects/scrippsco2-c13-daily - Daily average C13 concentrations (ppm) derived from flask air samples.

*objects/scrippsco2-c13-monthly - Monthly average C13 concentrations (ppm) derived from flask air samples.

*objects/scrippsco2-co2-daily - Daily average CO2 concentrations (ppm) derived from flask air samples.

*objects/scrippsco2-co2-monthly - Monthly average CO2 concentrations (ppm) derived from flask air samples.

*objects/scrippsco2-o18-daily - Daily average O18 concentrations (ppm) derived from flask air samples.

*objects/scrippsco2-o18-monthly - Monthly average O18 concentrations (ppm) derived from flask air samples.

*objects/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.

*objects/security-playbook - The security-playbook object provides meta-information and allows managing, storing, and sharing cybersecurity playbooks and orchestration workflows.

*objects/shadowserver-malware-url-report - This report identifies URLs that were observed in exploitation attempts in the last 24 hours. They are assumed to contain a malware payload or serve as C2 controllers. If a payload was successfully downloaded in the last 24 hours, it’s SHA256 hash will also be published. The data is primarily sourced from honeypots (in which case they will often be IoT related), but other sources are possible. As always, you only receive information on IPs found on your network/constituency or in the case of a National CSIRT, your country. Ref: https://www.shadowserver.org/what-we-do/network-reporting/malware-url-report/.

*objects/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.

*objects/shodan-report - Shodan Report for a given IP.

*objects/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.

*objects/shortened-link - Shortened link and its redirect target.

*objects/sigma - An object describing a Sigma rule (or a Sigma rule name).

*objects/sigmf-archive - An object representing an archive containing one or multiple recordings in the Signal Metadata Format Specification (SigMF).

*objects/sigmf-expanded-recording - An object representing a single IQ/RF sample in the Signal Metadata Format Specification (SigMF).

*objects/sigmf-recording - An object representing a single IQ/RF sample in the Signal Metadata Format Specification (SigMF).

*objects/social-media-group - Social media group object template describing a public or private group or channel.

*objects/software - The Software object represents high-level properties associated with software, including software products. STIX 2.1 - 6.14.

*objects/spearphishing-attachment - Spearphishing Attachment.

*objects/spearphishing-link - Spearphishing Link.

*objects/splunk - Splunk / Splunk ES object.

*objects/ss7-attack - SS7 object of an attack as seen on the SS7 signaling protocol supporting GSM/GPRS/UMTS networks.

*objects/ssh-authorized-keys - An object to store ssh authorized keys file.

*objects/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.

*objects/stock - Object to describe stock market.

*objects/submarine - Submarine description.

*objects/suricata - An object describing one or more Suricata rule(s) along with version and contextual information.

*objects/target-system - Description about an targeted system, this could potentially be a compromissed internal system.

*objects/task - Task object as described in STIX 2.1 Incident object extension.
*objects/tattoo - Describes tattoos on a natural person's body.
*objects/telegram-account - Information related to a telegram account.
*objects/telegram-bot - Information related to a telegram bot.
*objects/temporal-event - A temporal event consists of some temporal and spacial boundaries. Spacial boundaries can be physical, virtual or hybrid.
*objects/thaicert-group-cards - Adversary group cards inspired by ThaiCERT.
*objects/threatgrid-report - ThreatGrid report.
*objects/timecode - Timecode object to describe a start of video sequence (e.g. CCTV evidence) and the end of the video sequence.
*objects/timesketch-timeline - A timesketch timeline object based on mandatory field in timesketch to describe a log entry.
*objects/timesketch_message - A timesketch message entry.
*objects/timestamp - A generic timestamp object to represent time including first time and last time seen. Relationship will then define the kind of time relationship.
*objects/tor-hiddenservice - Tor hidden service (onion service) object.
*objects/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.
*objects/traceability-impact - Traceability Impact object as described in STIX 2.1 Incident object extension.
*objects/tracking-id - Analytics and tracking ID such as used in Google Analytics or other analytic platform.
*objects/transaction - An object to describe a financial transaction.
*objects/translation - Used to keep a text and its translation.
*objects/transport-ticket - A transport ticket.
*objects/trustar_report - TruStar Report.
*objects/tsk-chats - An Object Template to gather information from evidential or interesting exchange of messages identified during a digital forensic investigation.
*objects/tsk-web-bookmark - An Object Template to add evidential bookmarks identified during a digital forensic investigation.
*objects/tsk-web-cookie - An TSK-Autopsy Object Template to represent cookies identified during a forensic investigation.
*objects/tsk-web-downloads - An Object Template to add web-downloads.
*objects/tsk-web-history - An Object Template to share web history information.
*objects/tsk-web-search-query - An Object Template to share web search query information.
*objects/twitter-account - Twitter account.

- *objects/twitter-list - Twitter list.
- *objects/twitter-post - Twitter post (tweet).
- *objects/typosquatting-finder - Typosquatting info.
- *objects/typosquatting-finder-result - Typosquatting result.
- *objects/url - url object describes an url along with its normalized field (like extracted using faup parsing library) and its metadata.
- *objects/user-account - User-account object, defining aspects of user identification, authentication, privileges and other relevant data points.
- *objects/vehicle - Vehicle object template to describe a vehicle information and registration.
- *objects/victim - Victim object describes the target of an attack or abuse.
- *objects/virustotal-graph - VirusTotal graph.
- *objects/virustotal-report - VirusTotal report.
- *objects/virustotal-submission - VirusTotal Submission.
- *objects/vulnerability - Vulnerability object describing a common vulnerability enumeration which can describe published, unpublished, under review or embargo vulnerability for software, equipments or hardware.
- *objects/weakness - Weakness object describing a common weakness enumeration which can describe usable, incomplete, draft or deprecated weakness for software, equipment of hardware.
- *objects/whois - Whois records information for a domain name or an IP address.
- *objects/windows-service - Windows service and detailed about a service running a Windows operating system.
- *objects/x-header - X header generic object for SMTP, HTTP or any other protocols using X headers.
- *objects/x509 - x509 object describing a X.509 certificate.
- *objects/yabin - yabin.py generates Yara rules from function prologs, for matching and hunting binaries. ref: https://github.com/AlienVault-OTX/yabin.
- *objects/yara - An object describing a YARA rule (or a YARA rule name) along with its version.
- *objects/youtube-channel - A YouTube channel.
- *objects/youtube-comment - A YouTube video comment.
- *objects/youtube-playlist - A YouTube playlist.
- *objects/youtube-video - A YouTube video.

4. Acknowledgements

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

5. 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>.

[RFC8259] Bray, T., Ed., "The JavaScript Object Notation (JSON) Data Interchange Format", STD 90, RFC 8259, DOI 10.17487/RFC8259, December 2017, <https://www.rfc-editor.org/info/rfc8259>.

6. Informative References

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

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

Authors' Addresses

Alexandre Dulaunoy
Computer Incident Response Center Luxembourg
122, rue Adolphe Fischer
L-L-1521 Luxembourg
Luxembourg

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

Andras Iklody
Computer Incident Response Center Luxembourg
122, rue Adolphe Fischer
L-L-1521 Luxembourg
Luxembourg

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