MISP Objects

MISP Objects

Introduction

The MISP threat sharing platform is a free and open source software helping information sharing of threat intelligence including cyber security indicators, financial fraud or counter-terrorism information. The MISP project includes multiple sub-projects to support the operational requirements of analysts and improve the overall quality of information shared.

MISP objects are used in MISP (starting from version 2.4.80) system and can be used by other information sharing tool. MISP objects are in addition to MISP attributes to allow advanced combinations of attributes. The creation of these objects and their associated attributes are based on real cyber security use-cases and existing practices in information sharing. The objects are just shared like any other attributes in MISP even if the other MISP instances don't have the template of the object. The following document is generated from the machine-readable JSON describing the MISP objects.

Funding and Support

The MISP project is financially and resource supported by CIRCL Computer Incident Response Center Luxembourg .

circl.lu
Computer Incident
Response Center
LUXEMBOURG

A CEF (Connecting Europe Facility) funding under CEF-TC-2016-3 - Cyber Security has been granted from 1st September 2017 until 31th August 2019 as **Improving MISP as building blocks for next-generation information sharing**.

Co-financed by the European Union
Connecting Europe Facility

If you are interested to co-fund projects around MISP, feel free to get in touch with us.

MISP objects

ail-leak

An information leak as defined by the AIL Analysis Information Leak framework.

ail-leak is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
duplicate	text	Duplicate of the existing leaks.	−	✓
duplicate_number	counter	Number of known duplicates.	✓	−
first-seen	datetime	When the leak has been accessible or seen for the first time.	✓	−
last-seen	datetime	When the leak has been accessible or seen for the last time.	✓	−
origin	text	The link where the leak is (or was) accessible at first-seen.	−	−
original-date	datetime	When the information available in the leak was created. It's usually before the first-seen.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
raw-data	attachment	Raw data as received by the AIL sensor compressed and encoded in Base64.	✓	−
sensor	text	The AIL sensor uuid where the leak was processed and analysed.	✓	−
text	text	A description of the leak which could include the potential victim(s) or description of the leak.	✓	−

ais-info

Automated Indicator Sharing (AIS) Information Source Markings.

ais-info is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
administrative-area	text	AIS Administrative Area represented using ISO-3166-2.	−	−
country	text	AIS Country represented using ISO-3166-1_alpha-2.	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
industry	text	AIS IndustryType. ['Chemical Sector', 'Commercial Facilities Sector', 'Communications Sector', 'Critical Manufacturing Sector', 'Dams Sector', 'Defense Industrial Base Sector', 'Emergency Services Sector', 'Energy Sector', 'Financial Services Sector', 'Food and Agriculture Sector', 'Government Facilities Sector', 'Healthcare and Public Health Sector', 'Information Technology Sector', 'Nuclear Reactors, Materials, and Waste Sector', 'Transportation Systems Sector', 'Water and Wastewater Systems Sector', 'Other']	−	✓
organisation	text	AIS Organisation Name.	−	−

android-permission

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

android-permission is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
comment	comment	Comment about the set of android permission(s)	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
permission	text	Android permission ['ACCESS_CHECKIN_PROPERTIES', 'ACCESS_COARSE_LOCATION', 'ACCESS_FINE_LOCATION', 'ACCESS_LOCATION_EXTRA_COMMANDS', 'ACCESS_NETWORK_STATE', 'ACCESS_NOTIFICATION_POLICY', 'ACCESS_WIFI_STATE', 'ACCOUNT_MANAGER', 'ADD_VOICEMAIL', 'ANSWER_PHONE_CALLS', 'BATTERY_STATS', 'BIND_ACCESSIBILITY_SERVICE', 'BIND_APPWIDGET', 'BIND_AUTOFILL_SERVICE', 'BIND_CARRIER_MESSAGING_SERVICE', 'BIND_CHOOSER_TARGET_SERVICE', 'BIND_CONDITION_PROVIDER_SERVICE', 'BIND_DEVICE_ADMIN', 'BIND_DREAM_SERVICE', 'BIND_INCALL_SERVICE', 'BIND_INPUT_METHOD', 'BIND_MIDI_DEVICE_SERVICE', 'BIND_NFC_SERVI	−	✓

annotation

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

annotation is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

CE', 'BIND_NOTIFICATION_LISTENER_SERVICE', 'BIND_PRINT_SERVICE',

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
attachment	attachment	An attachment to support the annotation	−	✓
creation-date	datetime	Initial creation of the annotation	−	−
format	text	Format of the annotation ['text', 'markdown', 'asciidoctor', 'MultiMarkdown', 'GFM', 'pandoc', 'Fountain', 'CommonWork', 'kramdown-rfc2629', 'rfc7328', 'Extra']	✓	−
modification-date	datetime	Last update of the annotation	−	−
ref	link	Reference(s) to the annotation	−	✓
text	text	Raw text of the annotation	−	−

, 'BROADCAST_STICKY', 'BROADCAST_WAP_PUSH', 'CALL_PHONE', 'CALL_PRIVILEGED', 'CAMERA', 'CAPTURE_AUDIO_OUTPUT', 'CAPTURE_SECUR

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
type	text	Type of the annotation ['Annotation', 'Executive Summary', 'Introduction', 'Conclusion', 'Disclaimer', 'Keywords', 'Acknowledgement', 'Other', 'Copyright', 'Authors', 'Logo', 'Full Report']	✓	−

'CLEAR_APP_CACHE', 'CONTROL_LOCATION_UPDATES', 'DELETE_CACHE_FILES', 'DELETE_PACKAGES', 'DIAGNOSTIC', 'DISABLE_KEYGUARD', 'DUMP'

anonymisation

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

anonymisation is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
description	text	Description of the anonymisation technique or tool used	✓	−

ZE', 'GET_TASKS', 'GLOBAL_SEARCH', 'INSTALL_LOCATION_PROVIDER', 'INSTALL_PACKAGES', 'INSTALL_SHORTCUT', 'INSTANT_APP_FOREGROUND_SERVICE', 'INTERNET', 'KILL_BACKGROUND_PROCESSES', 'LOCATION_HARDWARE',

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
encryption-function	text	Encryption function or algorithm used to anonymise the attribute ['aes128', 'aes-128-cbc', 'aes-128-cfb', 'aes-128-cfb1', 'aes-128-cfb8', 'aes-128-ctr', 'aes-128-ecb', 'aes-128-ofb', 'aes192', 'aes-192-cbc', 'aes-192-cfb', 'aes-192-cfb1', 'aes-192-cfb8', 'aes-192-ctr', 'aes-192-ecb', 'aes-192-ofb', 'aes-256-cfb', 'aes-256-cfb1', 'aes-256-cfb8', 'aes-256-ctr', 'aes-256-ecb', 'aes-256-ofb', 'bf', 'bf-cbc', 'bf-cfb', 'bf-ecb', 'bf-ofb', 'blowfish', 'camellia128', 'camellia-128-cbc', 'camellia-128-cfb', 'camellia-128-cfb1', 'camellia-128-cfb8', 'camellia-128-ctr', 'camellia-128-ecb', 'camellia-128-ofb', 'camellia192', 'camellia-192-cbc', 'camellia-192-cfb', 'camellia-192-cfb1', 'camellia-192-cfb8', 'camellia-192-ctr', 'camellia-192-ecb', 'camellia-192-ofb', 'camellia256', 'camellia-256-cbc', 'camellia-256-cfb', 'camellia-256-cfb1', 'camellia-256-cfb8',	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
iv	text	Initialisation vector for the encryption function used to anonymise the attribute	✓	━
key	text	Key (such as a PSK in a keyed-hash-function) used to anonymise the attribute	✓	━
keyed-hash-function	text	Keyed-hash function used to anonymise the attribute ['hmac-sha1', 'hmac-md5', 'hmac-sha256', 'hmac-sha384', 'hmac-sha512']	✓	━
level-of-knowledge	text	Level of knowledge of the organisation who created this object ['Only the anonymised data is known', 'Deanonymised data is known']	✓	━

'SET_TIME',
'SET_TIME_ZONE',
'SET_WALLPAPER'
,
'SET_WALLPAPER
_HINTS',
'SIGNAL_PERSIST
ENT_PROCESSES',
'STATUS_BAR',
'SYSTEM_ALERT_
WINDOW',
'TRANSMIT_IR',
'UNINSTALL_SHO
RTCUT',
'UPDATE_DEVICE_
STATS',

sm4-cbc', 'sm4-
ctr', 'sm4-ecb',
'sm4-ofb']

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
method	text	Anonymisation (or pseudo-anonymisation) method(s) used ["hiding - Attribute is replaced with a constant value (typically 0) of the same size. Sometimes called 'black marker'.", 'hash - A hash function maps each attribute to a new (not necessarily unique) attribute.', 'permutation - Maps each original value to a unique new value.', "prefix-preserving - Any two values that had the same n-bit prefix before anonymisation will still have the same n-bit prefix as each other after anonymization. (Would be more accurately called 'prefix-relationship-preserving', because the actual prefix values are not preserved.) ", 'shift - Adds a fixed offset to each value/attribute.', 'enumeration - Map each original value to a new value such that	✓	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
regexp	text	Regular expression to perfom the anonymisation (reversible or not)	✓	−

sets; actual values are replaced with a fixed value from the same set. E.g., TCP port numbers 0 to 1023 are replaced with 0, and 1024 to 65535 replaced with 65535.', updated - Checksums are

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.

asn is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
asn	AS	Autonomous System Number	−	−
country	text	Country code of the main location of the autonomous system	−	−
description	text	Description of the autonomous system	−	−
export	text	The outbound routing policy of the AS in RFC 2622 – Routing Policy Specification Language (RPSL) format	−	✓
first-seen	datetime	First time the ASN was seen	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
import	text	The inbound IPv4 routing policy of the AS in RFC 2622 – Routing Policy Specification Language (RPSL) format	−	✓
last-seen	datetime	Last time the ASN was seen	✓	−
mp-export	text	This attribute performs the same function as the export attribute above. The difference is that mp-export allows both IPv4 and IPv6 address families to be specified. The export is described in RFC 4012 – Routing Policy Specification Language next generation (RPSLng), section 4.5. format	−	✓
mp-import	text	The inbound IPv4 or IPv6 routing policy of the AS in RFC 4012 – Routing Policy Specification Language next generation (RPSLng), section 4.5. format	−	✓
subnet-announced	ip-src	Subnet announced	−	✓

attack-pattern

Attack pattern describing a common attack pattern enumeration and classification.

attack-pattern is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
id	text	CAPEC ID.	✓	−
name	text	Name of the attack pattern.	−	−
prerequisites	text	Prerequisites for the attack pattern to succeed.	−	−
references	link	External references	−	✓
related-weakness	weakness	Weakness related to the attack pattern.	−	✓
solutions	text	Solutions for the attack pattern to be countered.	−	−
summary	text	Summary description of the attack pattern.	−	−

authenticode-signerinfo

Authenticode Signer Info.

authenticode-signerinfo is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
content-type	text	Content type	−	−
digest_algorithm	text	Digest algorithm	✓	−
issuer	text	Issuer of the certificate	✓	−
program-name	text	Program name	−	−
signature_algorithm	text	Signature algorithm ['SHA1_WITH_RSA_ENCRYPTION', 'SHA256_WITH_RSA_ENCRYPTION']	✓	−
text	text	Free text description of the signer info	−	−
url	url	Url	−	✓
version	text	Version of the certificate	✓	−

av-signature

Antivirus detection signature.

av-signature is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
datetime	datetime	Datetime	✓	−
signature	text	Name of detection signature	−	−
software	text	Name of antivirus software	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
text	text	Free text value to attach to the file	✓	—

bank-account

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

bank-account is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
aba-rtn	aba-rtn	ABA routing transit number	—	—
account	bank-account-nr	Account number	—	—
account-name	text	A field to freely describe the bank account details.	—	—
balance	text	The balance of the account after the suspicious transaction was processed.	✓	—
beneficiary	text	Final beneficiary of the bank account.	✓	—
beneficiary-comment	text	Comment about the final beneficiary.	✓	—
branch	text	Branch code or name	✓	—
client-number	text	Client number as seen by the bank.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
closed	datetime	When the account was closed.	✓	−
comments	text	Comments about the bank account.	✓	−
currency-code	text	Currency of the account. ['USD', 'EUR']	✓	−
date-balance	datetime	When the balance was reported.	✓	−
iban	iban	IBAN of the bank account.	−	−
institution-code	text	Institution code of the bank.	✓	−
institution-name	text	Name of the bank or financial organisation.	✓	−
non-banking-institution	boolean	A flag to define if this account belong to a non-banking organisation. If set to true, it’s a non-banking organisation.	✓	−
opened	datetime	When the account was opened.	✓	−
personal-account-type	text	Account type. ['A - Business', 'B - Personal Current', 'C - Savings', 'D - Trust Account', 'E - Trading Account', 'O - Other']	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
report-code	text	Report code of the bank account. ['CTR Cash Transaction Report', 'STR Suspicious Transaction Report', 'EFT Electronic Funds Transfer', 'IFT International Funds Transfer', 'TFR Terror Financing Report', 'BCR Border Cash Report', 'UTR Unusual Transaction Report', 'AIF Additional Information File – Can be used for example to get full disclosure of transactions of an account for a period of time without reporting it as a CTR.', 'IRI Incoming Request for Information – International', 'ORI Outgoing Request for Information – International', 'IRD Incoming Request for Information – Domestic', 'ORD Outgoing Request for Information – Domestic']	✓	▬

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
status-code	text	Account status at the time of the transaction processed. ['A - Active', 'B - Inactive', 'C - Dormant']	✓	−
swift	bic	SWIFT or BIC as defined in ISO 9362.	✓	−
text	text	A description of the bank account.	✓	−

bgp-hijack

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

bgp-hijack is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
country	text	Country code of the main location of the attacking autonomous system	−	−
description	text	BGP Hijack details	−	−
detected-asn	AS	Detected Autonomous System Number	−	−
end	datetime	Last time the Prefix hijack was seen	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
expected-asn	AS	Expected Autonomous System Number	−	−
start	datetime	First time the Prefix hijack was seen	✓	−
subnet-announced	ip-src	Subnet announced	−	✓

blog

Blog post like Medium or WordPress.

blog is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
archive	link	Archive of the original document (Internet Archive, Archive.is, etc).	−	✓
creation-date	datetime	Initial creation of the blog post.	−	−
embedded-link	url	Site linked by the blog post.	−	✓
embedded-safe-link	link	Safe site linked by the blog post.	−	✓
link	link	Original link into the blog post (Supposed harmless).	−	−
modification-date	datetime	Last update of the blog post.	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
post	text	Raw post.	−	−
removal-date	datetime	When the blog post was removed.	−	−
title	text	Title of blog post.	−	−
type	text	Type of blog post. ['Medium', 'WordPress', 'Blogger', 'Tumbler', 'LiveJournal', 'Forum', 'Other']	✓	−
url	url	Original URL location of the blog post (potentially malicious).	−	−
username	text	Username who posted the blog post.	−	−
username-quoted	text	Username who are quoted into the blog post.	−	✓
verified-username	text	Is the username account verified by the operator of the blog platform. ['Verified', 'Unverified', 'Unknown']	✓	−

btc-transaction

An object to describe a Bitcoin transaction. Best to be used with bitcoin-wallet.

btc-transaction is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
btc-address	btc	A Bitcoin transactional address	✓	−
time	datetime	Date and time of transaction	✓	−
transaction-number	text	A Bitcoin transaction number in a sequence of transactions	✓	✓
value_BTC	float	Value in BTC at date/time displayed in field 'time'	✓	−
value_EUR	float	Value in EUR with conversion rate as of date/time displayed in field 'time'	✓	−
value_USD	float	Value in USD with conversion rate as of date/time displayed in field 'time'	✓	−

btc-wallet

An object to describe a Bitcoin wallet. Best to be used with bitcoin-transactions.

btc-wallet is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
BTC_received	float	Value of received BTC	✓	−
BTC_sent	float	Value of sent BTC	✓	−
balance_BTC	float	Value in BTC at date/time displayed in field 'time'	✓	−
time	datetime	Date and time of lookup/conversion	✓	−
wallet-address	btc	A Bitcoin wallet address	−	−

cap-alert

Common Alerting Protocol Version (CAP) alert object.

cap-alert is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
addresses	text	The group listing of intended recipients of the alert message. (1) Required when <scope> is “Private”, optional when <scope> is “Public” or “Restricted”. (2) Each recipient SHALL be identified by an identifier or an address. (3) Multiple space-delimited addresses MAY be included. Addresses including whitespace MUST be enclosed in double-quotes.	✓	−
code	text	The code denoting the special handling of the alert message.	✓	−
identifier	text	The identifier of the alert message in a number or string uniquely identifying this message, assigned by the sender.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
incident	text	The group listing naming the referent incident(s) of the alert message. (1) Used to collate multiple messages referring to different aspects of the same incident. (2) If multiple incident identifiers are referenced, they SHALL be separated by whitespace. Incident names including whitespace SHALL be surrounded by double-quotes.	✓	−
msgType	text	The code denoting the nature of the alert message. ['Alert', 'Update', 'Cancel', 'Ack', 'Error']	✓	−
note	text	The text describing the purpose or significance of the alert message.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
references	text	The group listing identifying earlier message(s) referenced by the alert message. (1) The extended message identifier(s) (in the form sender,identifier,sent) of an earlier CAP message or messages referenced by this one. (2) If multiple messages are referenced, they SHALL be separated by whitespace.	✓	━
restriction	text	The text describing the rule for limiting distribution of the restricted alert message.	✓	━
scope	text	The code denoting the intended distribution of the alert message. ['Public', 'Restricted', 'Private']	✓	━

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
sender	text	The identifier of the sender of the alert message which identifies the originator of this alert. Guaranteed by assigner to be unique globally; e.g., may be based on an Internet domain name.	✓	–
sent	datetime	The time and date of the origination of the alert message.	✓	–
source	text	The text identifying the source of the alert message. The particular source of this alert; e.g., an operator or a specific device.	✓	–
status	text	The code denoting the appropriate handling of the alert message. ['Actual', 'Exercise', 'System', 'Test', 'Draft']	–	–

cap-info

Common Alerting Protocol Version (CAP) info object.

cap-info is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
audience	text	The text describing the intended audience of the alert message.	✓	−
category	text	The code denoting the category of the subject event of the alert message. ['Geo', 'Met', 'Safety', 'Security', 'Rescue', 'Fire', 'Health', 'Env', 'Transport', 'Infra', 'CBRNE', 'Other']	✓	−
certainty	text	The code denoting the certainty of the subject event of the alert message. For backward compatibility with CAP 1.0, the deprecated value of “Very Likely” SHOULD be treated as equivalent to “Likely”. ['Likely', 'Possible', 'Unlikely', 'Unknown']	✓	−
contact	text	The text describing the contact for follow-up and confirmation of the alert message.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
description	text	The text describing the subject event of the alert message.	✓	−
effective	datetime	The effective time of the information of the alert message.	✓	−
event	text	The text denoting the type of the subject event of the alert message.	✓	−
eventCode	text	A system-specific code identifying the event type of the alert message.	✓	−
expires	datetime	The expiry time of the information of the alert message.	✓	−
headline	text	The text headline of the alert message.	✓	−
instruction	text	The text describing the recommended action to be taken by recipients of the alert message.	✓	−
language	text	The code denoting the language of the info sub-element of the alert message.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
onset	datetime	The expected time of the beginning of the subject event of the alert message.	✓	−
parameter	text	A system-specific additional parameter associated with the alert message.	✓	−
responseType	text	The code denoting the type of action recommended for the target audience. ['Shelter', 'Evacuate', 'Prepare', 'Execute', 'Avoid', 'Monitor', 'Assess', 'AllClear', 'None']	✓	−
senderName	text	The text naming the originator of the alert message.	✓	−
severity	text	The code denoting the severity of the subject event of the alert message. ['Extreme', 'Severe', 'Moderate', 'Minor', 'Unknown']	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
urgency	text	The code denoting the urgency of the subject event of the alert message. ['Immediate', 'Expected', 'Future', 'Past', 'Unknown']	✓	−
web	link	The identifier of the hyperlink associating additional information with the alert message.	✓	−

cap-resource

Common Alerting Protocol Version (CAP) resource object.

cap-resource is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
derefUri	attachment	The base-64 encoded data content of the resource file.	✓	−
digest	sha1	The code representing the digital digest (“hash”) computed from the resource file (OPTIONAL).	−	−
mimeType	mime-type	The identifier of the MIME content type and sub-type describing the resource file.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
resourceDesc	text	The text describing the type and content of the resource file.	✓	−
size	text	The integer indicating the size of the resource file.	✓	−
uri	link	The identifier of the hyperlink for the resource file.	−	−

coin-address

An address used in a cryptocurrency.

coin-address is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
address	btc	Bitcoin address used as a payment destination in a cryptocurrency	−	−
address-xmr	xmr	Monero address used as a payment destination in a cryptocurrency	−	−
current-balance	float	Current balance of address	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
first-seen	datetime	First time this payment destination address has been seen	✓	−
last-seen	datetime	Last time this payment destination address has been seen	✓	−
last-updated	datetime	Last time the balances and totals have been updated	✓	−
symbol	text	The (uppercase) symbol of the cryptocurrency used. Symbol should be from https://coinmarketcap.com/all/views/all/ ['BTC', 'ETH', 'BCH', 'XRP', 'MIOTA', 'DASH', 'BTG', 'LTC', 'ADA', 'XMR', 'ETC', 'NEO', 'NEM', 'EOS', 'XLM', 'BCC', 'LSK', 'OMG', 'QTUM', 'ZEC', 'USDT', 'HSR', 'STRAT', 'WAVES', 'PPT', 'ETN']	✓	−
text	text	Free text value	✓	−
total-received	float	Total balance received	✓	−
total-sent	float	Total balance sent	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
total-transactions	text	Total transactions performed	✓	−

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.

ℹ command is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
description	text	Description of the command functionalities	−	−
location	text	Location of the command functionality ['Bundled', 'Module', 'Libraries', 'Unknown']	✓	−
trigger	text	How the commands are triggered ['Local', 'Network', 'Unknown']	✓	−

command-line

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

ℹ command-line is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
description	text	description of the command	−	−
value	text	command code	−	✓

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.

cookie is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
cookie	cookie	Full cookie	−	−
cookie-name	text	Name of the cookie (if splitted)	−	−
cookie-value	text	Value of the cookie (if splitted)	−	−
expires	datetime	Expiration date/time of the cookie	✓	−
http-only	boolean	True if send only through HTTP	✓	−
path	text	Path defined in the cookie	✓	−
secure	boolean	True if cookie is sent over TLS	✓	−
text	text	A description of the cookie.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
type	text	Type of cookie and how it’s used in this specific object. ['Session management', 'Personalization', 'Tracking', 'Exfiltration', 'Malicious Payload', 'Beaconing']	━	━

cortex

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

cortex is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
full	text	Cortex report object (full report) in JSON	✓	━
name	text	Cortex analyser/worker name	✓	━
server-name	text	Name of the cortex server	✓	━
start-date	datetime	When the Cortex analyser was started	✓	━
success	boolean	Result of the cortex job	✓	━

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
summary	text	Cortex summary object (summary) in JSON	−	−

cortex-taxonomy

Cortex object describing an Cortex Taxonomy (or mini report).

cortex-taxonomy is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
cortex_url	link	URL to the Cortex job	✓	−
level	text	Cortex Taxonomy Level ['info', 'safe', 'suspicious', 'malicious']	✓	−
namespace	text	Cortex Taxonomy Namespace	✓	−
predicate	text	Cortex Taxonomy Predicate	✓	−
value	text	Cortex Taxonomy Value	✓	−

course-of-action

An object describing a specific measure taken to prevent or respond to an attack.

course-of-action is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
cost	text	The estimated cost of applying the course of action. ['High', 'Medium', 'Low', 'None', 'Unknown']	✓	−
description	text	A description of the course of action.	✓	−
efficacy	text	The estimated efficacy of applying the course of action. ['High', 'Medium', 'Low', 'None', 'Unknown']	✓	−
impact	text	The estimated impact of applying the course of action. ['High', 'Medium', 'Low', 'None', 'Unknown']	✓	−
name	text	The name used to identify the course of action.	✓	−
objective	text	The objective of the course of action.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
stage	text	The stage of the threat management lifecycle that the course of action is applicable to. ['Remedy', 'Response', 'Further Analysis Required']	✓	−
type	text	The type of the course of action. ['Perimeter Blocking', 'Internal Blocking', 'Redirection', 'Redirection (Honey Pot)', 'Hardening', 'Patching', 'Eradication', 'Rebuilding', 'Training', 'Monitoring', 'Physical Access Restrictions', 'Logical Access Restrictions', 'Public Disclosure', 'Diplomatic Actions', 'Policy Actions', 'Other']	✓	−

covid19-csse-daily-report

CSSE COVID-19 Daily report.

ℹ covid19-csse-daily-report is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
active	counter	the number of active cases.	✓	−
confirmed	counter	the number of confirmed cases. For Hubei Province: from Feb 13 (GMT +8), we report both clinically diagnosed and lab-confirmed cases. For lab-confirmed cases only (Before Feb 17), please refer to https://github.com/CSSEGISandData/COVID-19/tree/master/who_covid_19_situation_reports.	✓	−
country-region	text	country/region name conforming to WHO (will be updated).	✓	−
county	counter	US County (US Only)	✓	−
death	counter	the number of deaths.	✓	−
fips	counter	Federal Information Processing Standard county code (US Only)	✓	−
latitude	float	Approximate latitude of the entry	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
longitude	float	Approximate longitude of the entry	✓	−
province-state	text	province name; US/Canada/Australia/ - city name, state/province name; Others - name of the event (e.g., "Diamond Princess" cruise ship); other countries - blank.	✓	−
recovered	counter	the number of recovered cases.	✓	−
update	datetime	Time of the last update that day (UTC)	✓	−

covid19-dxy-live-city

COVID 19 from dxy.cn - Aggregation by city.

ℹ covid19-dxy-live-city is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
city	text	Name of the Chinese city, in Chinese.	✓	−
current-confirmed	counter	Current number of confirmed cases	✓	−
total-confirmed	counter	Total number of confirmed cases.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
total-cured	counter	Total number of cured cases.	✓	−
total-death	counter	Total number of deaths.	✓	−
update	datetime	Approximate time of the update (~hour)	✓	−

covid19-dxy-live-province

COVID 19 from dxy.cn - Aggregation by province.

covid19-dxy-live-province is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
comment	text	Comment, in chinese	✓	−
current-confirmed	counter	Current number of confirmed cases	✓	−
province	text	Name of the Chinese province, in Chinese.	✓	−
total-confirmed	counter	Total number of confirmed cases.	✓	−
total-cured	counter	Total number of cured cases.	✓	−
total-death	counter	Total number of deaths.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
update	datetime	Approximate time of the update (~hour)	✓	−

cowrie

Cowrie honeypot object template.

cowrie is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
compCS	text	SSH compression algorithm supported in the session	✓	✓
dst_ip	ip-dst	Destination IP address of the session	✓	−
dst_port	port	Destination port of the session	✓	−
encCS	text	SSH symmetric encryption algorithm supported in the session	✓	✓
eventid	text	Eventid of the session in the cowrie honeypot	✓	−
hassh	hassh-md5	HASSH of the client SSH session following Salesforce algorithm	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
input	text	Input of the session	−	−
isError	text	isError	✓	−
keyAlgs	text	SSH public-key algorithm supported in the session	✓	✓
macCS	text	SSH MAC supported in the sesssion	✓	✓
message	text	Message of the cowrie honeypot	✓	−
password	text	Password	−	✓
protocol	text	Protocol used in the cowrie honeypot	✓	−
sensor	text	Cowrie sensor name	✓	−
session	text	Session id	−	−
src_ip	ip-src	Source IP address of the session	−	−
src_port	port	Source port of the session	✓	−
system	text	System origin in cowrie honeypot	✓	−
timestamp	datetime	When the event happened	✓	−
username	text	Username related to the password(s)	−	−

credential

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

credential is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
format	text	Format of the password(s) ['clear-text', 'hashed', 'encrypted', 'unknown']	✓	−
notification	text	Mention of any notification(s) towards the potential owner(s) of the credential(s) ['victim-notified', 'service-notified', 'none']	✓	✓
origin	text	Origin of the credential(s) ['bruteforce-scanning', 'malware-analysis', 'memory-analysis', 'network-analysis', 'leak', 'unknown']	✓	−
password	text	Password	−	✓
text	text	A description of the credential(s)	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
type	text	Type of password(s) ['password', 'api-key', 'encryption-key', 'unknown']	✓	−
username	text	Username related to the password(s)	−	−

credit-card

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

credit-card is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
bank_name	text	Name of the bank which have issued the card	−	−
card-security-code	text	Card security code (CSC, CVD, CVV, CVC and SPC) as embossed or printed on the card.	−	−
cc-number	cc-number	credit-card number as encoded on the card.	−	−
comment	comment	A description of the card.	−	−
expiration	datetime	Maximum date of validity	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
iin	text	International Issuer Number (First eight digits of the credit card number	−	−
issued	datetime	Initial date of validity or issued date.	−	−
name	text	Name of the card owner.	−	−
version	text	Version of the card.	−	−

crypto-material

Cryptographic materials such as public or/and private keys.

crypto-material is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
Gx	text	Curve Parameter - Gx in decimal	✓	−
Gy	text	Curve Parameter - Gy in decimal	✓	−
b	text	Curve Parameter - B in decimal	✓	−
curve-length	text	Length of the Curve in bits	✓	−
e	text	RSA public exponent	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
ecdsa-type	text	Curve type of the ECDSA cryptographic materials ['Anomalous', 'M-221', 'E-222', 'NIST P-224', 'Curve1174', 'Curve25519', 'BN(2,254)', 'brainpoolP256t1', 'ANSSI FRP256v1', 'NIST P-256', 'secp256k1', 'E-382', 'M-383', 'Curve383187', 'brainpoolP384t1', 'NIST P-384', 'Curve41417', 'Ed448-Goldilocks', 'M-511', 'E-521']	✓	‒
g	text	Curve Parameter - G in decimal	✓	‒
generic-symmetric-key	text	Generic symmetric key (please precise the type)	‒	‒
modulus	text	Modulus Parameter - in hexadecimal - no 0x, no :	‒	‒
n	text	Curve Parameter - N in decimal	✓	‒

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
origin	text	Origin of the cryptographic materials ['mathematical-attack', 'exhaustive-search', 'bruteforce-attack', 'malware-extraction', 'memory-interception', 'network-interception', 'leak', 'unknown']	✓	−
p	text	Prime Parameter - P in decimal	−	−
private	text	Private part of the cryptographic materials in PEM format	−	−
q	text	Prime Parameter - Q in decimal	−	−
rsa-modulus-size	text	RSA modulus size in bits	✓	−
text	text	A description of the cryptographic materials.	✓	−
type	text	Type of crytographic materials ['RSA', 'DSA', 'ECDSA', 'RC4', 'XOR', 'unknown']	✓	−
x	text	Curve Parameter - X in decimal	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
y	text	Curve Parameter - Y in decimal	✓	−

cytomic-orion-file

Cytomic Orion File Detection.

ℹ cytomic-orion-file is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
classification	text	File classification - number	−	−
classificationName	text	File classification	−	−
fileName	filename	Original filename	−	−
fileSize	size-in-bytes	Size of the file	−	−
first-seen	datetime	First seen timestamp of the file	−	−
last-seen	datetime	Last seen timestamp of the file	−	−

cytomic-orion-machine

Cytomic Orion File at Machine Detection.

ℹ cytomic-orion-machine is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
clientCreationDateUTC	datetime	Client creation date UTC	−	−
clientId	text	Client id	−	−
clientName	target-org	Client name	−	−
creationDate	datetime	Client creation date	−	−
first-seen	datetime	First seen on machine	−	−
last-seen	datetime	Last seen on machine	−	−
lastSeenUtc	datetime	Client last seen UTC	−	−
machineMuid	text	Machine UID	−	−
machineName	target-machine	Machine name	−	−
machinePath	text	Path of observable	−	−

dark-pattern-item

An Item whose User Interface implements a dark pattern.

dark-pattern-item is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
comment	text	textual comment about the item	✔	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
gain	text	What is the implementer is gaining by deceiving the user ['registration', 'personal data', 'money', 'contacts', 'audience']	✓	−
implementer	text	Who is the vendor / holder of the item	✓	−
location	text	Location where to find the item	✓	✓
screenshot	attachment	A screencapture or a screengrab of the item at work	✓	−
time	datetime	Date and time when first-seen	✓	−
user	text	who are the user of the item	✓	−

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.

ddos is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
domain-dst	domain	Destination domain (victim)	−	−
dst-port	port	Destination port of the attack	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
first-seen	datetime	Beginning of the attack	✓	−
ip-dst	ip-dst	Destination IP (victim)	−	−
ip-src	ip-src	IP address originating the attack	−	−
last-seen	datetime	End of the attack	✓	−
protocol	text	Protocol used for the attack ['TCP', 'UDP', 'ICMP', 'IP']	−	−
src-port	port	Port originating the attack	−	−
text	text	Description of the DDoS	✓	−
total-bps	counter	Bits per second	−	−
total-pps	counter	Packets per second	−	−

device

An object to define a device.

device is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
MAC-address	mac-address	Device MAC address	−	−
OS	text	OS of the device	✓	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
alias	text	Alias of the Device	−	✓
analysis-date	datetime	Date of device analysis	−	−
attachment	attachment	An attachment	−	✓
description	text	Description of the Device	✓	−
device-type	text	Type of the device ['PC', 'Mobile', 'Laptop', 'HID', 'TV', 'IoT', 'Hardware', 'Other']	✓	−
dns-name	text	Device DNS Name	−	✓
ip-address	ip-src	Device IP address	−	✓
name	text	Name of the Device	−	−
version	text	Version of the device/ OS	✓	−

diameter-attack

Attack as seen on diameter authentication against a GSM, UMTS or LTE network.

diameter-attack is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
ApplicationId	text	Application-ID is used to identify for which Diameter application the message is applicable. Application-ID is a decimal representation.	−	−
CmdCode	text	A decimal representation of the diameter Command Code.	✓	−
Destination-Host	text	Destination-Host.	−	✓
Destination-Realm	text	Destination-Realm.	−	✓
IdrFlags	text	IDR-Flags.	✓	−
Origin-Host	text	Origin-Host.	−	✓
Origin-Realm	text	Origin-Realm.	−	✓
SessionId	text	Session-ID.	−	−
Username	text	Username (in this case, usually the IMSI).	−	✓
category	text	Category. ['Cat0', 'Cat1', 'Cat2', 'Cat3', 'CatSMS']	✓	−
first-seen	datetime	When the attack has been seen for the first time.	✓	−
text	text	A description of the attack seen.	✓	−

dns-record

A set of dns records observed for a specific domain.

dns-record is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
a-record	ip-dst	IP Address sassociated with A Records	-	✓
mx-record	domain	Domain associated with MX Record	-	✓
ns-record	domain	Domain associated with NS Records	-	✓
queried-domain	domain	Domain name	-	-
text	text	A description of the records	-	-

domain-crawled

A domain crawled over time.

domain-crawled is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
domain	domain	Domain name	-	-
text	text	A description of the tuple	✓	-
url	url	domain url	-	✓

domain-ip

A domain and IP address seen as a tuple in a specific time frame.

domain-ip is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
domain	domain	Domain name	−	✓
first-seen	datetime	First time the tuple has been seen	✓	−
ip	ip-dst	IP Address	−	✓
last-seen	datetime	Last time the tuple has been seen	✓	−
port	port	Associated TCP port with the domain	−	✓
registration-date	datetime	Registration date of domain	−	−
text	text	A description of the tuple	✓	−

elf

Object describing a Executable and Linkable Format.

elf is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
arch	text	Architecture of the ELF file ['None', 'M32', 'SPARC', 'i386', 'ARCH_68K', 'ARCH_88K', 'IAMCU', 'ARCH_860', 'MIPS', 'S370', 'MIPS_RS3_LE', 'PARISC', 'VPP500', 'SPARC32PLUS', 'ARCH_960', 'PPC', 'PPC64', 'S390', 'SPU', 'V800', 'FR20', 'RH32', 'RCE', 'ARM', 'ALPHA', 'SH', 'SPARCV9', 'TRICORE', 'ARC', 'H8_300', 'H8_300H', 'H8S', 'H8_500', 'IA_64', 'MIPS_X', 'COLDFIRE', 'ARCH_68HC12', 'MMA', 'PCP', 'NCPU', 'NDR1', 'STARCORE', 'ME16', 'ST100', 'TINYJ', 'x86_64', 'PDSP', 'PDP10', 'PDP11', 'FX66', 'ST9PLUS', 'ST7', 'ARCH_68HC16', 'ARCH_68HC11', 'ARCH_68HC08', 'ARCH_68HC05', 'SVX', 'ST19', 'VAX', 'CRIS', 'JAVELIN', 'FIREPATH', 'ZSP', 'MMIX', 'HUANY', 'PRISM', 'AVR', 'FR30', 'D10V', 'D30V', 'V850', 'M32R', 'MN10300', 'MN10200', 'PJ', 'OPENRISC',	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
entrypoint-address	text	Address of the entry point	✓	−
number-sections	counter	Number of sections	✓	−
os_abi	text	Header operating system application binary interface (ABI) ['AIX', 'ARM', 'AROS', 'C6000_ELFABI', 'C6000_LINUX', 'CLOUDABI', 'FENIXOS', 'FREEBSD', 'GNU', 'HPUX', 'HURD', 'IRIX', 'MODESTO', 'NETBSD', 'NSK', 'OPENBSD', 'OPENVMS', 'SOLARIS', 'STANDALONE', 'SYSTEMV', 'TRU64']	✓	−
text	text	Free text value to attach to the ELF	✓	−
type	text	Type of ELF ['CORE', 'DYNAMIC', 'EXECUTABLE', 'HIPROC', 'LOPROC', 'NONE', 'RELOCATABLE']	✓	−

'MANIK',
'CRAYNV2', 'RX',
'METAG',
'MCST_ELBRUS',
'ECOG16', 'CR16',
'ETPU', 'SLE9X',
'L10M', 'K10M',
'AARCH64',
'AVR32', 'STM8',
'TILE64',
'TILEPRO', 'CUDA',

elf-section

Object describing a section of an Executable and Linkable Format.

elf-section is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
entropy	float	Entropy of the whole section	✓	−
flag	text	Flag of the section ['ALLOC', 'EXCLUDE', 'EXECINSTR', 'GROUP', 'HEX_GPREL', 'INFO_LINK', 'LINK_ORDER', 'MASKOS', 'MASKPROC', 'MERGE', 'MIPS_ADDR', 'MIPS_LOCAL', 'MIPS_MERGE', 'MIPS_NAMES', 'MIPS_NODUPES', 'MIPS_NOSTRIP', 'NONE', 'OS_NONCONFORMING', 'STRINGS', 'TLS', 'WRITE', 'XCORE_SHF_CP_SECTION']	✓	✓
md5	md5	[Insecure] MD5 hash (128 bits)	−	−
name	text	Name of the section	✓	−
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	−	−
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	−	−
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	−	−
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	−	−
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	−	−
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	−	−
size-in-bytes	size-in-bytes	Size of the section, in bytes	✓	−
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	−	−
text	text	Free text value to attach to the section	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
type	text	Type of the section ['NULL', 'PROGBITS', 'SYMTAB', 'STRTAB', 'RELA', 'HASH', 'DYNAMIC', 'NOTE', 'NOBITS', 'REL', 'SHLIB', 'DYNSYM', 'INIT_ARRAY', 'FINI_ARRAY', 'PREINIT_ARRAY', 'GROUP', 'SYMTAB_SHNDX', 'LOOS', 'GNU_ATTRIBUTES', 'GNU_HASH', 'GNU_VERDEF', 'GNU_VERNEED', 'GNU_VERSYM', 'HIOS', 'LOPROC', 'ARM_EXIDX', 'ARM_PREEMPTMAP', 'HEX_ORDERED', 'X86_64_UNWIND', 'MIPS_REGINFO', 'MIPS_OPTIONS', 'MIPS_ABIFLAGS', 'HIPROC', 'LOUSER', 'HIUSER']	✓	−

email

Email object describing an email with meta-information.

ℹ email is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
attachment	email-attachment	Attachment	−	✓
cc	email-dst	Carbon copy	✓	✓
email-body	email-body	Body of the email	✓	−
eml	attachment	Full EML	✓	−
from	email-src	Sender email address	−	✓
from-display-name	email-src-display-name	Display name of the sender	−	✓
header	email-header	Full headers	✓	✓
ip-src	ip-src	Source IP address of the email sender	−	✓
message-id	email-message-id	Message ID	✓	−
mime-boundary	email-mime-boundary	MIME Boundary	✓	−
received-header-hostname	hostname	Extracted hostname from parsed headers	−	✓
received-header-ip	ip-src	Extracted IP address from parsed headers	−	✓
reply-to	email-reply-to	Email address the reply will be sent to	−	−
return-path	email-src	Message return path	−	−
screenshot	attachment	Screenshot of email	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
send-date	datetime	Date the email has been sent	✓	—
subject	email-subject	Subject	—	✓
thread-index	email-thread-index	Identifies a particular conversation thread	✓	—
to	email-dst	Destination email address	✓	✓
to-display-name	email-dst-display-name	Display name of the receiver	—	✓
user-agent	text	User Agent of the sender	✓	—
x-mailer	email-x-mailer	X-Mailer generally tells the program that was used to draft and send the original email	✓	—

employee

An employee and related data points.

employee is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
business-unit	target-org	the organizational business unit associated with the employee	✓	—
email-address	target-email	Employee Email Address	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
employee-type	text	type of employee ['Mid-Level Manager', 'Senior Manager', 'Non-Manager', 'Supervisor', 'First-Line Manager', 'Director']	✓	−
first-name	first-name	First name of Employee	✓	−
last-name	last-name	Last name Employee	✓	−
primary-asset	target-machine	Asset tag of the primary asset assigned to employee	−	−
text	text	A description of the person or identity.	✓	−
userid	target-user	EMployee user identification	✓	−

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.

exploit-poc is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
author	text	Author of the exploit - proof of concept	✓	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
description	text	Description of the exploit - proof of concept	−	−
poc	attachment	Proof of Concept or exploit (as a script, binary or described process)	✓	✓
references	link	External references	−	✓
vulnerable_configuration	text	The vulnerable configuration described in CPE format where the exploit/proof of concept is valid	−	✓

facial-composite

An object which describes a facial composite.

facial-composite is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
facial-composite	attachment	Facial composite image.	−	✓
technique	text	Construction technique of the facial composite. ['E-FIT', 'PROfit', 'Sketch', 'Photofit', 'EvoFIT', 'PortraitPad']	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
text	text	A description of the facial composite.	✓	−

fail2ban

Fail2ban event.

fail2ban is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
attack-type	text	Type of the attack	✓	−
banned-ip	ip-src	IP Address banned by fail2ban	−	−
failures	counter	Amount of failures that lead to the ban.	✓	−
logfile	attachment	Full logfile related to the attack.	✓	−
logline	text	Example log line that caused the ban.	✓	−
processing-timestamp	datetime	Timestamp of the report	✓	−
sensor	text	Identifier of the sensor	✓	−
victim	text	Identifier of the victim	✓	−

file

File object describing a file with meta-information.

file is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
attachment	attachment	A non-malicious file.	−	−
authentihash	authentihash	Authenticode executable signature hash	−	−
certificate	x509-fingerprint-sha1	Certificate value if the binary is signed with another authentication scheme than authenticode	−	−
compilation-timestamp	datetime	Compilation timestamp	−	−
entropy	float	Entropy of the whole file	✔	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
file-encoding	text	Encoding format of the file ['Adobe-Standard-Encoding', 'Adobe-Symbol-Encoding', 'Amiga-1251', 'ANSI_X3.110-1983', 'ASMO_449', 'Big5', 'Big5-HKSCS', 'BOCU-1', 'BRF', 'BS_4730', 'BS_viewdata', 'CESU-8', 'CP50220', 'CP51932', 'CSA_Z243.4-1985-1', 'CSA_Z243.4-1985-2', 'CSA_Z243.4-1985-gr', 'CSN_369103', 'DEC-MCS', 'DIN_66003', 'dk-us', 'DS_2089', 'EBCDIC-AT-DE', 'EBCDIC-AT-DE-A', 'EBCDIC-CA-FR', 'EBCDIC-DK-NO', 'EBCDIC-DK-NO-A', 'EBCDIC-ES', 'EBCDIC-ES-A', 'EBCDIC-ES-S', 'EBCDIC-FI-SE', 'EBCDIC-FI-SE-A', 'EBCDIC-FR', 'EBCDIC-IT', 'EBCDIC-PT', 'EBCDIC-UK', 'EBCDIC-US', 'ECMA-cyrillic', 'ES', 'ES2', 'EUC-KR', 'Extended_UNIX_Code_Fixed_Width_for_Japanese', 'Extended_UNIX_Code_Packed_Format_for_Japanese', 'GB18030',	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
filename	filename	Filename on disk	✓	✓
fullpath	text	Complete path of the filename including the filename	−	✓
malware-sample	malware-sample	The file itself (binary)	−	−
md5	md5	[Insecure] MD5 hash (128 bits)	−	−
mimetype	mime-type	Mime type	✓	−
path	text	Path of the filename complete or partial	✓	✓
pattern-in-file	pattern-in-file	Pattern that can be found in the file	−	✓
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	−	−
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	−	−
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	−	−
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	−	−
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	−	−

'IBM904', 'IBM905', 'IBM918', 'IBM-Symbols', 'IBM-Thai', 'IEC_P27-1',

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	−	−
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	−	−
size-in-bytes	size-in-bytes	Size of the file, in bytes	✓	−
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	−	−
state	text	State of the file ['Malicious', 'Harmless', 'Signed', 'Revoked', 'Expired', 'Trusted']	✓	✓
text	text	Free text value to attach to the file	✓	−
tlsh	tlsh	Fuzzy hash by Trend Micro: Locality Sensitive Hash	−	−

8859-1-Windows-3.0-Latin-1', 'ISO-8859-1-Windows-3.1-Latin-1', 'ISO_8859-2:1987', 'ISO-8859-2-Windows-Latin-2', 'ISO_8859-3:1988', 'ISO_8859-4:1988',

forensic-case

An object template to describe a digital forensic case.

forensic-case is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
additional-comments	text	Comments.	✓	−

'ISO_8859-7:1987', 'ISO_8859-8:1988', 'ISO_8859-8-E',

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
analysis-start-date	datetime	Date when the analysis began.	✓	—
case-name	text	Name to address the case.	—	—
case-number	text	Any unique number assigned to the case for unique identification.	—	—
name-of-the-analyst	text	Name(s) of the analyst assigned to the case.	✓	✓
references	link	External references	—	✓

'JIS_C6226-1978', 'JIS_C6226-1983', 'JIS_C6229-1984-a', 'JIS_C6229-1984-b', 'JIS_C6229-1984-b-add', 'JIS_C6229-1984-hand', 'JIS_C6229-1984-hand-add', 'JIS_C6229-1984-

forensic-evidence

An object template to describe a digital forensic-evidence.

forensic-evidence is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
acquisition-method	text	Method used for acquisition of the evidence. ['Live acquisition', 'Dead/Offline acquisition', 'Physical collection', 'Logical collection', 'File system extraction', 'Chip-off', 'Other']	✓	—

'Microsoft-Publishing', 'MNEM', 'MNEMONIC',

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
acquisition-tools	text	Tools used for acquisition of the evidence. ['dd', 'dc3dd', 'dcfldd', 'EnCase', 'FTK Imager', 'FDAS', 'TrueBack', 'Guymager', 'IXimager', 'Other']	✓	✓
additional-comments	text	Comments.	✓	–
case-number	text	A unique number assigned to the case for unique identification.	–	–
evidence-number	text	A unique number assigned to the evidence for unique identification.	–	–
name	text	Name of the evidence acquired.	–	–
references	link	External references	–	✓
type	text	Evidence type. ['Computer', 'Network', 'Mobile Device', 'Multimedia', 'Cloud', 'IoT', 'Other']	✓	✓

forged-document

Object describing a forged document.

International', 'Ventura-Math', 'Ventura-US', 'videotex-suppl', 'VIQR', 'VISCII', 'windows-1250', 'windows-1251', 'windows-1252', 'windows-1253', forged-document is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

'windows-1254',
'windows-1255',

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
archive	link	Archive of the original document (Internet Archive, Archive.is, etc).	–	✓
attachment	attachment	The forged document file.	–	–
document-name	text	Title of the document.	–	–
document-text	text	Raw text of document	–	–
document-type	text	The type of document (not the file type). ['email', 'letterhead', 'speech', 'literature', 'blog', 'microblog', 'photo', 'audio', 'invoice', 'receipt', 'other']	✓	✓
first-seen	datetime	When the document has been accessible or seen for the first time.	✓	–
last-seen	datetime	When the document has been accessible or seen for the last time.	✓	–

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
link	link	Original link into the document (Supposed harmless)	—	—
objective	text	Objective of the forged document. ['Disinformation', 'Advertising', 'Parody', 'Other']	✓	✓
purpose-of-document	text	What the document is used for. ['Identification', 'Travel', 'Health', 'Legal', 'Financial', 'Government', 'Military', 'Media', 'Communication', 'Other']	✓	✓
url	url	Original URL location of the document (potentially malicious)	—	—

geolocation

An object to describe a geographic location.

geolocation is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
accuracy-radius	float	The approximate accuracy radius, in kilometers, around the latitude and longitude for the geographical entity (country, subdivision, city or postal code) associated with the related object. (based on geoip2 accuracy of maxmind)	✓	−
address	text	Address.	−	−
altitude	float	The altitude is the decimal value of the altitude in the World Geodetic System 84 (WGS84) reference.	✓	−
city	text	City.	−	−
country	text	Country.	−	−
epsg	text	EPSG Geodetic Parameter value. This is an integer value of the EPSG.	✓	−
first-seen	datetime	When the location was seen for the first time.	✓	−
last-seen	datetime	When the location was seen for the last time.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
latitude	float	The latitude is the decimal value of the latitude in the World Geodetic System 84 (WGS84) reference.	✔	—
longitude	float	The longitude is the decimal value of the longitude in the World Geodetic System 84 (WGS84) reference	✔	—
neighborhood	text	Neighborhood.	—	—
region	text	Region.	—	—
spacial-reference	text	Default spacial or projection refence for this object. ['WGS84 EPSG:4326', 'Mercator EPSG:3857']	✔	—
text	text	A generic description of the location.	✔	—
zipcode	text	Zip Code.	—	—

gtp-attack

GTP attack object as seen on a GSM, UMTS or LTE network.

gtp-attack is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
GtpImei	text	GTP IMEI (International Mobile Equipment Identity).	−	−
GtpImsi	text	GTP IMSI (International mobile subscriber identity).	−	−
GtpInterface	text	GTP interface. ['S5', 'S11', 'S10', 'S8', 'Gn', 'Gp']	✓	✓
GtpMessageType	text	GTP defines a set of messages between two associated GSNs or an SGSN and an RNC. Message type is described as a decimal value.	✓	−
GtpMsisdn	text	GTP MSISDN.	−	−
GtpServingNetwork	text	GTP Serving Network.	✓	−
GtpVersion	text	GTP version ['0', '1', '2']	✓	−
PortDest	text	Destination port.	✓	−
PortSrc	port	Source port.	✓	−
first-seen	datetime	When the attack has been seen for the first time.	✓	−
ipDest	ip-dst	IP destination address.	−	−
ipSrc	ip-src	IP source address.	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
text	text	A description of the GTP attack.	✓	−

http-request

A single HTTP request header.

http-request is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
basicauth-password	text	HTTP Basic Authentication Password	−	−
basicauth-user	text	HTTP Basic Authentication Username	−	−
content-type	other	The MIME type of the body of the request	−	−
cookie	text	An HTTP cookie previously sent by the server with Set-Cookie	−	✓
header	text	An HTTP header sent during HTTP request	−	✓
host	hostname	The domain name of the server	−	−
ip-dst	ip-dst	The IP address of the server	−	−
ip-src	ip-src	The IP address of the client	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
method	http-method	HTTP Method invoked (one of GET, POST, PUT, HEAD, DELETE, OPTIONS, CONNECT)	✔	−
proxy-password	text	HTTP Proxy Password	−	−
proxy-user	text	HTTP Proxy Username	−	−
referer	other	This is the address of the previous web page from which a link to the currently requested page was followed	−	−
text	text	HTTP Request comment	✔	−
uri	uri	Request URI	−	−
url	url	Full HTTP Request URL	−	−
user-agent	user-agent	The user agent string of the user agent	−	−

ilr-impact

Institut Luxembourgeois de Regulation - Impact.

ilr-impact is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
duree	text	Duree de l’incident en hh : mm	✓	−
nombre-utilisateurs-touches	text	Nombre d’utilisateurs touches par l’incident	✓	−
pourcentage-utilisateurs-touches	text	Pourcentage d’utilisateurs du service touches par l’incident	✓	−
service	text	Service impacte par l’incident ['Telephonie fixe', 'Acces Internet fixe', 'Telephonie mobile', 'Acces Internet mobile']	✓	✓

ilr-notification-incident

Institut Luxembourgeois de Regulation - Notification d’incident.

ilr-notification-incident is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
Nom entreprise	text	Nom de l’entreprise notifiee	✓	−
actions-corrective	text	Actions correctives a long terme	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
actions-posterieur	text	Actions posterieures de l’incident pour minimiser le risque	✓	−
autres-informations	text	Autres informations concernant la nature de l’incident notamment la liste des actifs affectes et les causes subsequentes eventuelles, declenches par la cause initiale	✓	−
cause-initiale-incident	text	Cause initiale de l’incident ['rreur humaine', "Defaut systeme 'hardware', 'software', 'procedures'", 'Attaque malveillante', 'Defaut d’une partie tierce ou externe', 'Catastrophe naturelle']	✓	−
date-incident	datetime	Date/heure de la detection de l’incident:	✓	−
date-pre-notification	text	Date de la pre-notification	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
delimitation-geographique	text	Delimitation geographique ['Nationale', 'Regionale']	✓	━
description-incident	text	Description generale de l’incident	✓	━
description-probleme-services-urgence	text	Description du probleme sur les services d’urgences impactes	✓	━
details-service	text	Details relatifs au service concerne et a l’impact de l’incident	✓	━
email-contact-incident	text	Email de la personne de contact en rapport avec l’incident	✓	━
impact-servicesw-urgence	text	Services d’urgences impactes ? ['Oui', 'Non']	✓	━
interconnections-affectees	text	Interconnections nationales et/ou internationales affectees	✓	━
nom-contact-incident	text	Nom de la personne de contact en rapport avec l’incident	✓	━

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
remarques	text	Remarque(s), notamment les experiences gagnees et les leçons tirees de l'incident	✓	−
telephone-contact-incident	text	Telephone de la personne de contact en rapport avec l'incident	✓	−
traitement-incident	text	Traitement de l'incident et actions effectuees en ordre chronologique	✓	−
zone-impactee	text	zones/communes/villes impactees	✓	✓

impersonation

Represent an impersonating account.

impersonation is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
account-name	text	Name of the impersonating account	−	−
account-url	url	url of the impersonating account	−	−
impersonated-account-name	text	Name of the impersonated account	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
impersonated-account-url	link	url of the impersonated account	−	−
objective	text	Objective of the impersonation ['Information stealing', 'Disinformation', 'Distrusting', 'Advertising', 'Parody', 'Other']	✓	✓
real-name	text	Real name of the impersonated person or entity	−	−
type	text	Type of the account ['Person', 'Association', 'Enterprise', 'Other']	✓	−
type-of-account	text	Type of the impersonated account ['Twitter', 'Facebook', 'LinkedIn', 'Reddit', 'Google+', 'Instagram', 'Forum', 'Other']	✓	−

imsi-catcher

IMSI Catcher entry object based on the open source IMSI cather.

imsi-catcher is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
brand	text	Brand associated with the IMSI registration.	✓	−
cellid	text	CellID	✓	−
country	text	Country where the IMSI is registered.	✓	−
first-seen	datetime	When the IMSI has been accessible or seen for the first time.	✓	−
imsi	text	A usually unique International Mobile Subscriber Identity (IMSI) is allocated to each mobile subscriber in the GSM/UMTS/EPS system. IMSI can also refer to International Mobile Station Identity in the ITU nomenclature.	−	−
lac	text	LAC - Location Area Code	✓	−
mcc	text	MCC - Mobile Country Code	✓	−
mnc	text	MNC - Mobile Network Code	✓	−
operator	text	Operator associated with the IMSI registration.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
seq	counter	A sequence number for the collection	✓	−
text	text	A description of the IMSI record.	✓	−
tmsi-1	text	Temporary Mobile Subscriber Identities (TMSI) to visiting mobile subscribers can be allocated.	−	−
tmsi-2	text	Temporary Mobile Subscriber Identities (TMSI) to visiting mobile subscribers can be allocated.	−	−

instant-message

Instant Message (IM) object template describing one or more IM message.

instant-message is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
app-used	text	The IM application used to send the message. ['WhatsApp', 'Google Hangouts', 'Facebook Messenger', 'Telegram', 'Signal', 'WeChat', 'BlackBerry Messenger', 'TeamSpeak', 'TorChat', 'RetroShare', 'Slack']	✓	−
archive	link	Archive of the original message (Internet Archive, Archive.is, etc).	−	✓
attachment	attachment	The message file or screen capture.	−	✓
body	text	Message body of the IM.	−	−
from-name	text	Name of the person that sent the message.	−	✓
from-number	phone-number	Phone number used to send the message.	−	✓
from-user	text	User account that sent the message.	−	✓
link	link	Original link into the message (Supposed harmless).	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
received-date	datetime	Received date of the message.	✓	−
sent-date	datetime	Initial sent date of the message.	✓	−
subject	text	Subject of the message if any.	−	−
to-name	text	Name of the person that received the message.	−	✓
to-number	phone-number	Phone number receiving the message.	−	✓
to-user	text	User account that received the message.	−	✓
url	url	Original URL location of the message (potentially malicious).	−	−

instant-message-group

Instant Message (IM) group object template describing a public or private IM group, channel or conversation.

instant-message-group is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
app-used	text	The IM application used to send the message. ['WhatsApp', 'Google Hangouts', 'Facebook Messenger', 'Telegram', 'Signal', 'WeChat', 'BlackBerry Messenger', 'TeamSpeak', 'TorChat', 'RetroShare', 'Slack']	✓	✓
archive	link	Archive of the original group (Internet Archive, Archive.is, etc).	−	✓
attachment	attachment	A screen capture or exported list of contacts, group members, etc.	−	✓
group-alias	text	Aliases of group, channel or community.	−	✓
group-name	text	The name of the group, channel or community.	−	−
link	link	Original link into the group (Supposed harmless).	−	−
person-name	text	A person who is a member of the group.	−	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
url	url	Original URL location of the group (potentially malicious).	−	−
username	text	A user account who is a member of the group.	−	✓

intelmq_event

IntelMQ Event.

intelmq_event is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
classification.identifier	text	The lowercase identifier defines the actual software or service (e.g. 'heartbleed' or 'ntp_version') or standardized malware name (e.g. 'zeus'). Note that you MAY overwrite this field during processing for your individual setup. This field is not standardized across IntelMQ setups/users.	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
classification.taxonomy	text	We recognize the need for the CSIRT teams to apply a static (incident) taxonomy to abuse data. With this goal in mind the type IOC will serve as a basis for this activity. Each value of the dynamic type mapping translates to a an element in the static taxonomy. The European CSIRT teams for example have decided to apply the eCSIRT.net incident classification. The value of the taxonomy key is thus a derivative of the dynamic type above. For more information about check [ENISA taxonomies](http://www.enisa.europa.eu/activities/cert/support/incident-management/browsable/incident-handling-process/incident-taxonomy/existing-taxonomies).	▬	▬

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
classification.type	text	The abuse type IOC is one of the most crucial pieces of information for any given abuse event. The main idea of dynamic typing is to keep our ontology flexible, since we need to evolve with the evolving threatscape of abuse data. In contrast with the static taxonomy below, the dynamic typing is used to perform business decisions in the abuse handling pipeline. Furthermore, the value data set should be kept as minimal as possible to avoid 'type explosion', which in turn dilutes the business value of the dynamic typing. In general, we normally have two types of abuse type IOC: ones referring to a compromised resource or ones referring to pieces of the criminal infrastructure, such as a command and control servers for example.	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
comment	text	Free text commentary about the abuse event inserted by an analyst.	-	-
destination.abuse_contact	text	Abuse contact for destination address. A comma separated list.	-	-
destination.account	text	An account name or email address, which has been identified to relate to the destination of an abuse event.	-	-
destination.allocated	datetime	Allocation date corresponding to BGP prefix.	-	-
destination.as_name	text	The autonomous system name to which the connection headed.	-	-
destination.asn	AS	The autonomous system number to which the connection headed.	-	-
destination.domain_suffix	text	The suffix of the domain from the public suffix list.	-	-

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
destination.fqdn	domain	A DNS name related to the host from which the connection originated. DNS allows even binary data in DNS, so we have to allow everything. A final point is stripped, string is converted to lower case characters.	−	−
destination.geolocation.cc	text	Country-Code according to ISO3166-1 alpha-2 for the destination IP.	−	−
destination.geolocation.city	text	Some geolocation services refer to city-level geolocation.	−	−
destination.geolocation.country	text	The country name derived from the ISO3166 country code (assigned to cc field).	−	−
destination.geolocation.latitude	float	Latitude coordinates derived from a geolocation service, such as MaxMind geoip db.	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
destination.geolocation.longitude	float	Longitude coordinates derived from a geolocation service, such as MaxMind geoip db.	−	−
destination.geolocation.region	text	Some geolocation services refer to region-level geolocation.	−	−
destination.geolocation.state	text	Some geolocation services refer to state-level geolocation.	−	−
destination.ip	ip-dst	The IP which is the target of the observed connections.	−	−
destination.local_hostname	hostname	Some sources report a internal hostname within a NAT related to the name configured for a compromized system	−	−
destination.local_ip	ip-dst	Some sources report a internal (NATed) IP address related a compromized system. N.B. RFC1918 IPs are OK here.	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
destination.network	ip-dst	CIDR for an autonomous system. Also known as BGP prefix. If multiple values are possible, select the most specific.	━	━
destination.port	counter	The port to which the connection headed.	━	━
destination.registry	text	The IP registry a given ip address is allocated by.	━	━
destination.reverse_dns	text	Reverse DNS name acquired through a reverse DNS query on an IP address. N.B. Record types other than PTR records may also appear in the reverse DNS tree. Furthermore, unfortunately, there is no rule prohibiting people from writing anything in a PTR record. Even JavaScript will work. A final point is stripped, string is converted to lower case characters.	━	━
destination.tor_node	boolean	If the destination IP was a known tor node.	━	━

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
destination.url	url	A URL denotes on IOC, which refers to a malicious resource, whose interpretation is defined by the abuse type. A URL with the abuse type phishing refers to a phishing resource.	−	−
destination.urlpath	text	The path portion of an HTTP or related network request.	−	−
event_description.target	text	Some sources denominate the target (organization) of a an attack.	−	−
event_description.text	text	A free-form textual description of an abuse event.	−	−
event_description.url	url	A description URL is a link to a further description of the the abuse event in question.	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
event_hash	text	Computed event hash with specific keys and values that identify a unique event. At present, the hash should default to using the SHA1 function. Please note that for an event hash to be able to match more than one event (deduplication) the receiver of an event should calculate it based on a minimal set of keys and values present in the event. Using for example the observation time in the calculation will most likely render the checksum useless for deduplication purposes.	▬	▬

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
extra	text	All anecdotal information, which cannot be parsed into the data harmonization elements. E.g. os.name, os.version, etc. **Note**: this is only intended for mapping any fields which can not map naturally into the data harmonization. It is not intended for extending the data harmonization with your own fields.	−	−
feed.accuracy	float	A float between 0 and 100 that represents how accurate the data in the feed is	−	−
feed.code	text	Code name for the feed, e.g. DFGS, HSDAG etc.	−	−
feed.documentation	text	A URL or hint where to find the documentation of this feed.	−	−
feed.name	text	Name for the feed, usually found in collector bot configuration.	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
feed.provider	text	Name for the provider of the feed, usually found in collector bot configuration.	−	−
feed.url	url	The URL of a given abuse feed, where applicable	−	−
malware.hash.md5	md5	A string depicting an MD5 checksum for a file, be it a malware sample for example.	−	−
malware.hash.sha1	sha1	A string depicting a SHA1 checksum for a file, be it a malware sample for example.	−	−
malware.hash.sha256	sha256	A string depicting a SHA256 checksum for a file, be it a malware sample for example.	−	−
malware.name	text	The malware name in lower case.	−	−
malware.version	text	A version string for an identified artifact generation, e.g. a crime-ware kit.	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
misp.attribute_uuid	text	MISP - Malware Information Sharing Platform & Threat Sharing UUID of an attribute.	-	-
misp.event_uuid	text	MISP - Malware Information Sharing Platform & Threat Sharing UUID.	-	-
output	text	Event data converted into foreign format, intended to be exported by output plugin.	-	-
protocol.application	text	e.g. vnc, ssh, sip, irc, http or smtp.	-	-
protocol.transport	text	e.g. tcp, udp, icmp.	-	-
raw	text	The original line of the event from encoded in base64.	-	-
rtir_id	counter	Request Tracker Incident Response ticket id.	-	-

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
screenshot_url	url	Some source may report URLs related to a an image generated of a resource without any metadata. Or an URL pointing to resource, which has been rendered into a webshot, e.g. a PNG image and the relevant metadata related to its retrieval/generation.	−	−
source.abuse_contact	text	Abuse contact for source address. A comma separated list.	−	−
source.account	text	An account name or email address, which has been identified to relate to the source of an abuse event.	−	−
source.allocated	datetime	Allocation date corresponding to BGP prefix.	−	−
source.as_name	text	The autonomous system name from which the connection originated.	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
source.asn	AS	The autonomous system number from which originated the connection.	-	-
source.domain_suffix	text	The suffix of the domain from the public suffix list.	-	-
source.fqdn	domain	A DNS name related to the host from which the connection originated. DNS allows even binary data in DNS, so we have to allow everything. A final point is stripped, string is converted to lower case characters.	-	-
source.geolocation.cc	text	Country-Code according to ISO3166-1 alpha-2 for the source IP.	-	-
source.geolocation.city	text	Some geolocation services refer to city-level geolocation.	-	-
source.geolocation.country	text	The country name derived from the ISO3166 country code (assigned to cc field).	-	-

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
source.geolocation.cymru_cc	text	The country code denoted for the ip by the Team Cymru asn to ip mapping service.	−	−
source.geolocation.geoip_cc	text	MaxMind Country Code (ISO3166-1 alpha-2).	−	−
source.geolocation.latitude	float	Latitude coordinates derived from a geolocation service, such as MaxMind geoip db.	−	−
source.geolocation.longitude	float	Longitude coordinates derived from a geolocation service, such as MaxMind geoip db.	−	−
source.geolocation.region	text	Some geolocation services refer to region-level geolocation.	−	−
source.geolocation.state	text	Some geolocation services refer to state-level geolocation.	−	−
source.ip	ip-src	The ip observed to initiate the connection	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
source.local_hostname	hostname	Some sources report a internal hostname within a NAT related to the name configured for a compromised system	−	−
source.local_ip	ip-src	Some sources report a internal (NATed) IP address related a compromised system. N.B. RFC1918 IPs are OK here.	−	−
source.network	ip-src	CIDR for an autonomous system. Also known as BGP prefix. If multiple values are possible, select the most specific.	−	−
source.port	counter	The port from which the connection originated.	−	−
source.registry	text	The IP registry a given ip address is allocated by.	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
source.reverse_dns	text	Reverse DNS name acquired through a reverse DNS query on an IP address. N.B. Record types other than PTR records may also appear in the reverse DNS tree. Furthermore, unfortunately, there is no rule prohibiting people from writing anything in a PTR record. Even JavaScript will work. A final point is stripped, string is converted to lower case characters.	━	━
source.tor_node	boolean	If the source IP was a known tor node.	━	━
source.url	url	A URL denotes an IOC, which refers to a malicious resource, whose interpretation is defined by the abuse type. A URL with the abuse type phishing refers to a phishing resource.	━	━
source.urlpath	text	The path portion of an HTTP or related network request.	━	━

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
status	text	Status of the malicious resource (phishing, dropzone, etc), e.g. online, offline.	−	−
time.observation	datetime	The time the collector of the local instance processed (observed) the event.	−	−
time.source	datetime	The time of occurence of the event as reported the feed (source).	−	−
tlp	text	Traffic Light Protocol level of the event.	−	−

intelmq_report

IntelMQ Report.

intelmq_report is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
extra	text	All anecdotal information of the report, which cannot be parsed into the data harmonization elements. E.g. subject of mails, etc. This is data is not automatically propagated to the events.	−	−
feed.accuracy	float	A float between 0 and 100 that represents how accurate the data in the feed is	−	−
feed.code	text	Code name for the feed, e.g. DFGS, HSDAG etc.	−	−
feed.documentation	text	A URL or hint where to find the documentation of this feed.	−	−
feed.name	text	Name for the feed, usually found in collector bot configuration.	−	−
feed.provider	text	Name for the provider of the feed, usually found in collector bot configuration.	−	−
feed.url	url	The URL of a given abuse feed, where applicable	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
raw	text	The original raw and unparsed data encoded in base64.	▬	▬
rtir_id	counter	Request Tracker Incident Response ticket id.	▬	▬
time.observation	datetime	The time the collector of the local instance processed (observed) the event.	▬	▬

internal-reference

Internal reference.

internal-reference is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
comment	comment	Comment associated to the identifier.	▬	▬
identifier	text	Identifier of the reference. Should be unique in your system.	▬	▬
link	link	Link associated to the identifier.	▬	▬
type	text	Type of internal reference.	▬	▬

interpol-notice

An object which describes a Interpol notice.

interpol-notice is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
alias	text	Alias name or known as.	−	✓
charges	text	Charges published as provided by requesting entity	✓	✓
colour-of-eyes	text	Description of a person's colour of eyes.	✓	−
colour-of-hair	text	Description of a person's colour of hair.	✓	−
date-of-birth	date-of-birth	Date of birth of a natural person (in YYYY-MM-DD format).	−	−
date-of-disappearance	text	Date of disappearance of a missing person.	−	−
distinguishing-marks-and-characteristics	text	Distinguishing marks and characteristics of a person.	✓	−
father-s-family-name-&-forename	text	Father's family name & forename.	−	−
forename	first-name	First name of a natural person.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
height	text	Height of a person.	✓	−
language-spoken	text	Languages spoken by a person.	✓	✓
mother-s-family-name-&-forename	text	Mother’s family name & forename.	−	−
nationality	nationality	The nationality of a natural person.	✓	✓
notice-color	text	The color/type of the notice ['Red', 'Yellow', 'Blue', 'Black', 'Green', 'Orange', 'Purple']	−	−
place-of-birth	place-of-birth	Place of birth of a natural person.	✓	−
place-of-disappearance	text	Place of birth of a natural person.	−	−
portrait	attachment	Portrait of the person.	−	✓
present-family-name	last-name	Last name of a natural person.	−	−
sex	gender	The gender of a natural person. ['Male', 'Female', 'Other', 'Prefer not to say']	✓	−
weight	text	weight of a person.	✓	−

iot-device

An IoT device.

iot-device is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
architecture	text	architecture of the IoT device ['ARC', 'ARM', 'M68000', 'MicroBlaze', 'MIPS', 'NSD32', 'Nios II', 'PowerPC', 'RISC-V', 'Sandbox', 'SH', 'x86', 'Xtensa']	—	—
boot-log	attachment	Boot log of the IoT device	—	✓
fcc-id	text	FCC-ID of the IoT device	—	✓
jtag-interface	text	JTAG interface of the IoT device ['Yes', 'No', 'Unknown', 'Disabled']	✓	—
model	text	Model of the IoT device	—	✓
picture-device	attachment	Picture of the IoT device	—	✓
picture-pcb	attachment	Picture of the IoT device PCB	—	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
platform	text	Platform of of the IoT device ['mach-aspeed', 'mach-at91', 'mach-bcm283x', 'mach-bcmstb', 'mach-cortina', 'mach-davinci', 'mach-exynos', 'mach-highbank', 'mach-imx', 'mach-integrator', 'mach-k3', 'mach-keystone', 'mach-kirkwood', 'mach-mediatek', 'mach-meson', 'mach-mvebu', 'mach-omap2', 'mach-orion5x', 'mach-owl', 'mach-qemu', 'mach-rmobile', 'mach-rockchip', 'mach-s5pc1xx', 'mach-snapdragon', 'mach-socfpga', 'mach-sti', 'mach-stm32', 'mach-stm32mp', 'mach-sunxi', 'mach-tegra', 'mach-u8500', 'mach-uniphier', 'mach-versal', 'mach-versatile', 'mach-zynq', 'mach-zynqmp', 'mach-zynqmp-r5', 'mcf5227x', 'mcf523x', 'mcf52x2', 'mcf530x', 'mcf532x', 'mcf5445x', 'mcf547x_8x', 'mach-ath79', 'mach-bmips',	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
reference	link	Reference of the IoT device	━	✔
serial-interface	text	Serial interface of the IoT device ['Yes', 'No', 'Unknown', 'Disabled']	✔	━
spi-interface	text	SPI interface of the IoT device ['Yes', 'No', 'Unknown', 'Disabled']	✔	━
vendor	text	Vendor of the IoT device	━	━

iot-firmware

A firmware for an IoT device.

iot-firmware is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
binwalk-entropy-graph	attachment	Entropy graph of the firmware	✔	━
binwalk-output	attachment	Binwalk output of the firmware image	━	━
boot-log	attachment	Boot log of the IoT device for this firmware	━	✔
filename	text	Filename of the firmware	━	━

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
firmware	attachment	Firmware of the IoT device	−	✓
format	text	Format of the firmware ['raw', 'Intel hex', 'Motorola S-Record', 'Unknown']	−	−
md5	md5	[Insecure] MD5 hash (128 bits)	−	−
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	−	−
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	−	−
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	−	−
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	−	−
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	−	−
size-in-bytes	size-in-bytes	Size of the file, in bytes	✓	−
version	text	Version of the firmware	−	✓

ip-api-address

IP Address information. Useful if you are pulling your ip information from ip-api.com.

ip-api-address is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
ISP	text	ISP.	✓	—
asn	AS	Autonomous System Number	✓	—
city	text	City.	✓	—
country	text	Country name	✓	—
country code	text	Country code	✓	—
first-seen	datetime	First time the ASN was seen	✓	—
ip-src	ip-src	Source IP address of the network connection.	—	—
last-seen	datetime	Last time the ASN was seen	✓	—
latitude	float	The latitude is the decimal value of the latitude in the World Geodetic System 84 (WGS84) reference.	✓	—
longitude	float	The longitude is the decimal value of the longitude in the World Geodetic System 84 (WGS84) reference	✓	—
organization	text	organization	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
region	text	Region. example: California.	✓	−
region code	text	Region code. example: CA	✓	−
state	text	State.	✓	−
zipcode	text	Zip Code.	✓	−

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.

ip-port is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
domain	domain	Domain	−	✓
dst-port	port	Destination port	✓	✓
first-seen	datetime	First time the tuple has been seen	✓	−
hostname	hostname	Hostname	−	✓
ip	ip-dst	IP Address	−	✓
ip-dst	ip-dst	destination IP address	−	✓
ip-src	ip-src	source IP address	−	✓
last-seen	datetime	Last time the tuple has been seen	✓	−
src-port	port	Source port	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
text	text	Description of the tuple	✓	−

irc

An IRC object to describe an IRC server and the associated channels.

ℹ irc is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
channel	text	IRC channel associated to the IRC server	−	✓
dst-port	port	Destination port to reach the IRC server	✓	✓
first-seen	datetime	First time the IRC server with the associated channels has been seen	✓	−
hostname	hostname	Hostname of the IRC server	−	✓
ip	ip-dst	IP address of the IRC server	−	✓
last-seen	datetime	Last time the IRC server with the associated channels has been seen	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
nickname	text	IRC nickname used to connect to the associated IRC server and channels	−	✓
text	text	Description of the IRC server	✓	−

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.

ℹ ja3 is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
description	text	Type of detected software ie software, malware	−	−
first-seen	datetime	First seen of the SSL/TLS handshake	✓	−
ip-dst	ip-dst	Destination IP address	−	−
ip-src	ip-src	Source IP Address	−	−
ja3-fingerprint-md5	ja3-fingerprint-md5	Hash identifying source	−	−
last-seen	datetime	Last seen of the SSL/TLS handshake	✓	−

leaked-document

Object describing a leaked document.

leaked-document is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
archive	link	Archive of the original document (Internet Archive, Archive.is, etc).	–	✓
attachment	attachment	The leaked document file.	–	–
document-name	text	Title of the document.	–	–
document-text	text	Raw text of document	–	–
document-type	text	The type of document (not the file type). ['email', 'letterhead', 'speech', 'literature', 'photo', 'audio', 'invoice', 'receipt', 'other']	✓	✓
first-seen	datetime	When the document has been accessible or seen for the first time.	✓	–
last-seen	datetime	When the document has been accessible or seen for the last time.	✓	–

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
link	link	Original link into the document (Supposed harmless)	−	−
objective	text	Reason for leaking the document. ['Disinformation', 'Influence', 'Whistleblowing', 'Extortion', 'Other']	✓	✓
origin	text	Original source of leaked document.	−	−
purpose-of-document	text	What the document is used for. ['Identification', 'Travel', 'Health', 'Legal', 'Financial', 'Government', 'Military', 'Media', 'Communication', 'Other']	✓	✓
url	url	Original URL location of the document (potentially malicious)	−	−

legal-entity

An object to describe a legal entity.

legal-entity is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
business	text	Business area of the entity.	−	−
commercial-name	text	Commercial name of the entity.	−	−
legal-form	text	Legal form of the entity.	−	−
logo	attachment	Logo of the entity.	−	−
name	text	Name of the entity.	−	−
phone-number	phone-number	Phone number of the entity.	−	−
registration-number	text	Registration number of the entity in the relevant authority.	−	−
text	text	A description of the entity.	✓	−
website	link	Website of the entity.	−	−

lnk

LNK object describing a Windows LNK binary file (aka Windows shortcut).

lnk is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
birth-droid-file-identifier	text	Birth droid volume identifier (UUIDv1 where MAC can be extracted)	−	−
birth-droid-volume-identifier	text	Droid volume identifier	−	−
droid-file-identifier	text	Droid file identifier (UUIDv1 where MAC can be extracted)	−	−
droid-volume-identifier	text	Droid volume identifier	−	−
entropy	float	Entropy of the whole file	✓	−
filename	filename	Filename on disk	✓	✓
fullpath	text	Complete path of the LNK filename including the filename	−	✓
lnk-access-time	datetime	Access time of the LNK	✓	−
lnk-command-line-arguments	text	LNK command line arguments	✓	−
lnk-creation-time	datetime	Creation time of the LNK	✓	−
lnk-description	text	LNK description	✓	−
lnk-drive-serial-number	text	Drive serial number	−	−
lnk-drive-type	text	Drive type	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
lnk-file-attribute-flags	text	File attribute flags	✓	−
lnk-file-size	size-in-bytes	Size of the target file, in bytes	✓	−
lnk-hot-key-value	text	Hot Key value	✓	−
lnk-icon-index	text	Icon index	✓	−
lnk-local-path	text	Local path	✓	−
lnk-modification-time	datetime	Modification time of the LNK	✓	−
lnk-relative-path	text	Relative path	✓	−
lnk-show-window-value	text	Show Window value	✓	−
lnk-volume-label	text	Volume label	✓	−
lnk-working-directory	text	LNK working path	✓	−
machine-identifier	text	Machine identifier	−	−
malware-sample	malware-sample	The LNK file itself (binary)	−	−
md5	md5	[Insecure] MD5 hash (128 bits)	−	−
path	text	Path of the LNK filename complete or partial	✓	✓
pattern-in-file	pattern-in-file	Pattern that can be found in the file	−	✓
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	−	−
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	−	−
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	−	−
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	−	−
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	−	−
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	−	−
size-in-bytes	size-in-bytes	Size of the LNK file, in bytes	✓	−
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	−	−
state	text	State of the LNK file ['Malicious', 'Harmless', 'Trusted']	✓	✓
text	text	Free text value to attach to the file	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
tlsh	tlsh	Fuzzy hash by Trend Micro: Locality Sensitive Hash	−	−

macho

Object describing a file in Mach-O format.

macho is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
entrypoint-address	text	Address of the entry point	✓	−
name	text	Binary's name	−	−
number-sections	counter	Number of sections	✓	−
text	text	Free text value to attach to the Mach-O file	✓	−
type	text	Type of Mach-O ['BUNDLE', 'CORE', 'DSYM', 'DYLIB', 'DYLIB_STUB', 'DYLINKER', 'EXECUTE', 'FVMLIB', 'KEXT_BUNDLE', 'OBJECT', 'PRELOAD']	−	−

macho-section

Object describing a section of a file in Mach-O format.

macho-section is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
entropy	float	Entropy of the whole section	✓	−
md5	md5	[Insecure] MD5 hash (128 bits)	−	−
name	text	Name of the section	✓	−
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	−	−
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	−	−
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	−	−
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	−	−
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	−	−
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	−	−
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	−	−
size-in-bytes	size-in-bytes	Size of the section, in bytes	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	–	–
text	text	Free text value to attach to the section	✓	–

mactime-timeline-analysis

Mactime template, used in forensic investigations to describe the timeline of a file activity.

mactime-timeline-analysis is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
activityType	text	Determines the type of activity conducted on the file at a given time ['Accessed', 'Created', 'Changed', 'Modified', 'Other']	✓	–
datetime	datetime	Date and time when the operation was conducted on the file	✓	–
file	attachment	Mactime output file	✓	–
file-path	text	Location of the file on the disc	–	–

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
filePermissions	text	Describes permissions assigned the file	✓	−
file_size	text	Determines the file size in bytes	✓	−

malware-config

Malware configuration recovered or extracted from a malicious binary.

malware-config is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
config	text	Raw (decrypted, decoded) text of the malware configuration.	−	−
encrypted	text	Encrypted or encoded text of the malware configuration in base64.	−	−
first-seen	datetime	When the malware configuration has been seen for the first time.	✓	−
format	text	Original format of the malware configuration. ['JSON', 'yaml', 'INI', 'other']	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
last-seen	datetime	When the malware configuration has been seen for the last time.	✓	−
password	text	Password or encryption key used to encrypt the malware configuration.	−	−

meme-image

Object describing a meme (image).

ℹ meme-image is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
5Ds-of-propaganda	text	5 D's of propaganda are tactics of rebuttal used to defend against criticism and adversarial narratives. ['dismiss', 'distort', 'distract', 'dismay', 'divide']	✓	✓
a/b-test	boolean	A flag to define if this meme is part of an a/b test. If set to true, it is part of an a/b test set.	✓	−
archive	link	Archive of the original document (Internet Archive, Archive.is, etc).	−	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
attachment	attachment	The image file.	−	−
crosspost	link	Safe site where the meme has been posted.	−	✓
crosspost-unsafe	url	Unsafe site where the meme has been posted.	−	✓
document-text	text	Raw text of meme	−	−
first-seen	datetime	When the meme has been accessible or seen for the first time.	✓	−
last-seen	datetime	When the meme has been accessible or seen for the last time.	✓	−
link	link	Original link into the meme (Supposed harmless)	−	−
meme-reference	link	A link to know-your-meme or similar reference material.	−	−
objective	text	Objective of the meme. ['Disinformation', 'Advertising', 'Parody', 'Other']	✓	✓
url	url	Original URL location of the meme (potentially malicious)	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
username	text	Username who posted the meme.	—	—

microblog

Microblog post like a Twitter tweet or a post on a Facebook wall.

microblog is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
archive	link	Archive of the original document (Internet Archive, Archive.is, etc).	—	✓
attachment	attachment	The microblog post file or screen capture.	—	✓
creation-date	datetime	Initial creation of the microblog post	—	—
display-name	text	Display name of the account who posted the microblog.	—	—
embedded-link	url	Link into the microblog post	—	✓
embedded-safe-link	link	Safe link into the microblog post	—	✓
hashtag	text	Hashtag embedded in the microblog post	—	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
in-reply-to-display-name	text	The user display name of the microblog this post replies to.	−	✓
in-reply-to-status-id	text	The microblog ID of the microblog this post replies to.	−	✓
in-reply-to-user-id	text	The user ID of the microblog this post replies to.	−	✓
language	text	The language of the post.	−	✓
link	link	Original link to the microblog post (supposed harmless).	−	✓
modification-date	datetime	Last update of the microblog post	−	−
post	text	Raw text of the post.	−	−
removal-date	datetime	When the microblog post was removed.	−	−
state	text	State of the microblog post ['Informative', 'Malicious', 'Misinformation', 'Disinformation', 'Unknown']	✓	−
title	text	Title of the post.	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
twitter-id	twitter-id	The microblog post id.	−	✓
type	text	Type of the microblog post ['Twitter', 'Facebook', 'LinkedIn', 'Reddit', 'Google+', 'Instagram', 'Forum', 'Other']	✓	−
url	url	Original URL of the microblog post (potentially malicious).	−	✓
username	text	Username who posted the microblog post (without the @ prefix)	−	−
username-quoted	text	Username who are quoted in the microblog post.	−	✓
verified-username	text	Is the username account verified by the operator of the microblog platform ['Verified', 'Unverified', 'Unknown']	✓	−

mutex

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

mutex is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
description	text	Description	-	-
name	text	name of the mutex	-	-
operating-system	text	Operating system where the mutex has been seen ['Windows', 'Unix']	-	-

narrative

Object describing a narrative.

narrative is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
5Ds-of-propaganda	text	5 D's of propaganda are tactics of rebuttal used to defend against criticism and adversarial narratives. ['dismiss', 'distort', 'distract', 'dismay', 'divide']	✔	✔
archive	link	Archive of the original narrative source (Internet Archive, Archive.is, etc).	✔	✔
attachment	attachment	Documents related to the narrative.	-	-

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
external-references	link	Link to external references.	✓	−
link	link	Original link to the narrative source (Supposed harmless)	−	−
narrative-disproof	text	Disproof or evidence against the narrative.	✓	−
narrative-summary	text	A summary of the narrative.	−	−
objective	text	Objective of the narrative. ['Disinformation', 'Advertising', 'Parody', 'Other']	✓	✓
url	url	Original link to the narrative source (Supposed malicious)	−	−

netflow

Netflow object describes an network object based on the Netflowv5/v9 minimal definition.

netflow is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
byte-count	counter	Bytes counted in this flow	✓	−
community-id	community-id	Community id of the represented flow	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
direction	text	Direction of this flow ['Ingress', 'Egress']	✓	–
dst-as	AS	Destination AS number for this flow	–	–
dst-port	port	Destination port of the netflow	–	–
first-packet-seen	datetime	First packet seen in this flow	✓	–
flow-count	counter	Flows counted in this flow	✓	–
icmp-type	text	ICMP type of the flow (if the traffic is ICMP)	✓	–
ip-dst	ip-dst	IP address destination of the netflow	–	–
ip-protocol-number	size-in-bytes	IP protocol number of this flow	✓	–
ip-src	ip-src	IP address source of the netflow	–	–
ip_version	counter	IP version of this flow	✓	–
last-packet-seen	datetime	Last packet seen in this flow	✓	–
packet-count	counter	Packets counted in this flow	✓	–

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
protocol	text	Protocol used for this flow ['TCP', 'UDP', 'ICMP', 'IP']	✓	—
src-as	AS	Source AS number for this flow	—	—
src-port	port	Source port of the netflow	—	—
tcp-flags	text	TCP flags of the flow	✓	—

network-connection

A local or remote network connection.

network-connection is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
community-id	community-id	Flow description as a community ID hash value	—	—
dst-port	port	Destination port of the nework connection.	—	—
first-packet-seen	datetime	Datetime of the first packet seen.	✓	—
hostname-dst	hostname	Destination hostname of the network connection.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
hostname-src	hostname	Source hostname of the network connection.	−	−
ip-dst	ip-dst	Destination IP address of the nework connection.	−	−
ip-src	ip-src	Source IP address of the nework connection.	−	−
layer3-protocol	text	Layer 3 protocol of the network connection. ['IP', 'ICMP', 'ARP']	✓	−
layer4-protocol	text	Layer 4 protocol of the network connection. ['TCP', 'UDP']	✓	−
layer7-protocol	text	Layer 7 protocol of the network connection. ['HTTP', 'HTTPS', 'FTP']	✓	−
src-port	port	Source port of the nework connection.	−	−

network-socket

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

network-socket is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
address-family	text	Address family who specifies the address family type (AF_*) of the socket connection. ['AF_UNSPEC', 'AF_LOCAL', 'AF_UNIX', 'AF_FILE', 'AF_INET', 'AF_AX25', 'AF_IPX', 'AF_APPLETALK', 'AF_NETROM', 'AF_BRIDGE', 'AF_ATMPVC', 'AF_X25', 'AF_INET6', 'AF_ROSE', 'AF_DECnet', 'AF_NETBEUI', 'AF_SECURITY', 'AF_KEY', 'AF_NETLINK', 'AF_ROUTE', 'AF_PACKET', 'AF_ASH', 'AF_ECONET', 'AF_ATMSVC', 'AF_RDS', 'AF_SNA', 'AF_IRDA', 'AF_PPPOX', 'AF_WANPIPE', 'AF_LLC', 'AF_IB', 'AF_MPLS', 'AF_CAN', 'AF_TIPC', 'AF_BLUETOOTH', 'AF_IUCV', 'AF_RXRPC', 'AF_ISDN', 'AF_PHONET', 'AF_IEEE802154', 'AF_CAIF', 'AF_ALG', 'AF_NFC', 'AF_VSOCK', 'AF_KCM',	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
domain-family	text	Domain family who specifies the communication domain (PF_*) of the socket connection. ['PF_UNSPEC', 'PF_LOCAL', 'PF_UNIX', 'PF_FILE', 'PF_INET', 'PF_AX25', 'PF_IPX', 'PF_APPLETALK', 'PF_NETROM', 'PF_BRIDGE', 'PF_ATMPVC', 'PF_X25', 'PF_INET6', 'PF_ROSE', 'PF_DECnet', 'PF_NETBEUI', 'PF_SECURITY', 'PF_KEY', 'PF_NETLINK', 'PF_ROUTE', 'PF_PACKET', 'PF_ASH', 'PF_ECONET', 'PF_ATMSVC', 'PF_RDS', 'PF_SNA', 'PF_IRDA', 'PF_PPPOX', 'PF_WANPIPE', 'PF_LLC', 'PF_IB', 'PF_MPLS', 'PF_CAN', 'PF_TIPC', 'PF_BLUETOOTH', 'PF_IUCV', 'PF_RXRPC', 'PF_ISDN', 'PF_PHONET', 'PF_IEEE802154', 'PF_CAIF', 'PF_ALG', 'PF_NFC', 'PF_VSOCK',	-	-

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
dst-port	port	Destination port of the network socket connection.	−	−
filename	filename	Socket using filename	−	−
hostname-dst	hostname	Destination hostname of the network socket connection.	−	−
hostname-src	hostname	Source (local) hostname of the network socket connection.	−	−
ip-dst	ip-dst	Destination IP address of the network socket connection.	−	−
ip-src	ip-src	Source (local) IP address of the network socket connection.	−	−
option	text	Option on the socket connection.	−	✓
protocol	text	Protocol used by the network socket. ['TCP', 'UDP', 'ICMP', 'IP']	−	−
src-port	port	Source (local) port of the network socket connection.	−	−
state	text	State of the socket connection. ['blocking', 'listening']	−	✓

news-agency

News agencies compile news and disseminate news in bulk.

news-agency is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
address	text	Postal address of the news agency.	−	✓
alias	text	Alias of the news agency.	✓	✓
archive	link	Archive of the original document (Internet Archive, Archive.is, etc).	−	✓
attachment	attachment	The news file, screen capture, audio, etc.	−	✓
e-mail	email-src	Email address of the organization.	−	✓
fax-number	phone-number	Fax number of the news agency.	−	✓
link	link	Original link to the news agency (Supposed harmless).	−	✓
name	text	Name of the news agency.	✓	−
phone-number	phone-number	Phone number of the news agency.	−	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
url	url	Original URL location of the news agency (potentially malicious).	−	✓

news-media

News media are forms of mass media delivering news to the general public.

news-media is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
address	text	Postal address of the news source.	−	✓
alias	text	Alias of the news source.	✓	✓
archive	link	Archive of the news (Internet Archive, Archive.is, etc).	−	✓
attachment	attachment	The news file, screen capture, audio, etc.	−	✓
content	text	Raw content of the news.	−	−
e-mail	email-src	Email address of the news source.	−	✓
embedded-link	url	Site linked by the blog post.	−	✓
embedded-safe-link	link	Safe site linked by the blog post.	−	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
fax-number	phone-number	Fax number of the news source.	−	✓
link	link	Original link to news (Supposed harmless).	−	✓
phone-number	phone-number	Phone number of the news source.	−	✓
source	text	Name of the news source.	✓	−
sub-type	text	Format of the news post (business daily, local news, metasite, etc). ['Business Daily', 'Local News', 'State News', 'National News', 'Metasite', 'Political Commentary', 'Clipper', 'Pressure Group', 'Staging', 'Trade Site', 'Other']	✓	−
title	text	Title of the post.	−	−
transcription	text	Transcribed audio/visual content.	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
type	text	Type of news media (newspaper, TV, podcast, etc). ['Newspaper', 'Newspaper (Online)', 'Magazine', 'Magazine (Online)', 'TV', 'Tube', 'Radio', 'Radio (Online)', 'Podcast', 'Alternative Media', 'Other']	✓	✓
url	url	Original URL location of news (potentially malicious).	−	✓
username	text	Username who posted the blog post.	−	−

organization

An object which describes an organization.

organization is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
VAT	text	VAT or TAX-ID of the organization	−	✓
address	text	Postal address of the organization.	−	✓
alias	text	Alias of the organization	−	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
date-of-inception	date-of-birth	Date of inception of the organization	−	−
description	text	Description of the organization	−	−
e-mail	email-src	Email address of the organization.	−	✓
fax-number	phone-number	Fax number of the organization.	−	✓
name	text	Name of the organization	−	−
phone-number	phone-number	Phone number of the organization.	−	✓
role	text	The role of the organization. ['Suspect', 'Victim', 'Defendent', 'Accused', 'Culprit', 'Accomplice', 'Target']	✓	✓
type-of-organization	text	Type of the organization	−	−

original-imported-file

Object describing the original file used to import data in MISP.

original-imported-file is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
format	text	Format of data imported. ['STIX 1.0', 'STIX 1.1', 'STIX 1.2', 'STIX 2.0', 'OpenIOC']	✓	−
imported-sample	attachment	The original imported file itself (binary).	✓	−
uri	uri	URI related to the imported file.	−	−

passive-dns

Passive DNS records as expressed in draft-dulaunoy-dnsop-passive-dns-cof-01.

passive-dns is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
bailiwick	text	Best estimate of the apex of the zone where this data is authoritative	✓	−
count	counter	How many authoritative DNS answers were received at the Passive DNS Server’s collectors with exactly the given set of values as answers.	✓	−
origin	text	Origin of the Passive DNS response	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
rdata	text	Resource records of the queried resource	−	−
rrname	text	Resource Record name of the queried resource.	−	−
rrtype	text	Resource Record type as seen by the passive DNS. ['A', 'AAAA', 'CNAME', 'PTR', 'SOA', 'TXT', 'DNAME', 'NS', 'SRV', 'RP', 'NAPTR', 'HINFO', 'A6']	✓	−
sensor_id	text	Sensor information where the record was seen	✓	−
text	text	Description of the passive DNS record.	✓	−
time_first	datetime	First time that the unique tuple (rrname, rrtype, rdata) has been seen by the passive DNS	✓	−
time_last	datetime	Last time that the unique tuple (rrname, rrtype, rdata) record has been seen by the passive DNS	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
zone_time_first	datetime	First time that the unique tuple (rrname, rrtype, rdata) record has been seen via master file import	✓	—
zone_time_last	datetime	Last time that the unique tuple (rrname, rrtype, rdata) record has been seen via master file import.	✓	—

paste

Paste or similar post from a website allowing to share privately or publicly posts.

paste is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
first-seen	datetime	When the paste has been accessible or seen for the first time.	✓	—
last-seen	datetime	When the paste has been accessible or seen for the last time.	✓	—
link	link	Link to the original source of the source or post (when used legitimately for OSINT source or alike).	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
origin	text	Original source of the paste or post. ['pastebin.com', 'pastebin.com_pro', 'pastie.org', 'slexy.org', 'gist.github.com', 'codepad.org', 'safebin.net', 'hastebin.com', 'ghostbin.com', 'paste.ee', '0bin.net']	✓	−
paste	text	Raw text of the paste or post	−	−
title	text	Title of the paste or post.	−	−
url	url	Link to the original source of the paste or post (when used maliciously).	−	−
username	text	User who posted the post.	−	−

pcap-metadata

Network packet capture metadata.

pcap-metadata is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
capture-interface	text	Interface name where the packet capture was running.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
capture-length	text	Capture length set on the captured interface.	✓	−
first-packet-seen	datetime	When the first packet has been seen.	✓	−
last-packet-seen	datetime	When the last packet has been seen.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
protocol	text	Capture protocol (linktype name). ['PER_PACKET', 'UNKNOWN', 'ETHERNET', 'TOKEN_RING', 'SLIP', 'PPP', 'FDDI', 'FDDI_BITSWAPPED', 'RAW_IP', 'ARCNET', 'ARCNET_LINUX', 'ATM_RFC1483', 'LINUX_ATM_CLIP', 'LAPB', 'ATM_PDUS', 'ATM_PDUS_UNTRUNCATED', 'NULL', 'ASCEND', 'ISDN', 'IP_OVER_FC', 'PPP_WITH_PHDR', 'IEEE_802_11', 'IEEE_802_11_PRISM', 'IEEE_802_11_WITH_RADIO', 'IEEE_802_11_RADIOTAP', 'IEEE_802_11_AVS', 'SLL', 'FRELAY', 'FRELAY_WITH_PHDR', 'CHDLC', 'CISCO_IOS', 'LOCALTALK', 'OLD_PFLOG', 'HHDLC', 'DOCSIS', 'COSINE', 'WFLEET_HDLC', 'SDLC', 'TZSP', 'ENC', 'PFLOG', 'CHDLC_WITH_PHDR', 'BLUETOOTH_H4', 'MTP2', 'MTP3', 'IRDA', 'USER0', 'USER1', 'USER2', 'USER3', 'USER4', 'USER5', 'USER6',	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
text	text	A description of the packet capture.	✓	−

'USER13',
'USER14',
'USER15',
'SYMANTEC',
'APPLE_IP_OVER_IEEE1394',
'BACNET_MS_TP',
'NETTL_RAW_ICMP'

pe

Object describing a Portable Executable.

pe is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
company-name	text	CompanyName in the resources	✓	−
compilation-timestamp	datetime	Compilation timestamp defined in the PE header	−	−
entrypoint-address	text	Address of the entry point	✓	−
entrypoint-section-at-position	text	Name of the section and position of the section in the PE	✓	−
file-description	text	FileDescription in the resources	✓	−
file-version	text	FileVersion in the resources	✓	−
impfuzzy	impfuzzy	Fuzzy Hash (ssdeep) calculated from the import table	−	−

'JUNIPER_VP',
'USB_FREEBSD',
'IEEE802_16_MAC_CPS',
'NETTL_RAW_TEL

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
imphash	imphash	Hash (md5) calculated from the import table	−	−
internal-filename	filename	InternalFilename in the resources	✓	−
lang-id	text	Lang ID in the resources	✓	−
legal-copyright	text	LegalCopyright in the resources	✓	−
number-sections	counter	Number of sections	✓	−
original-filename	filename	OriginalFilename in the resources	✓	−
pehash	pehash	Hash of the structural information about a sample. See https://www.usenix.org/legacy/event/leet09/tech/full_papers/wicherski/wicherski_html/	−	−
product-name	text	ProductName in the resources	✓	−
product-version	text	ProductVersion in the resources	✓	−
text	text	Free text value to attach to the PE	✓	−
type	text	Type of PE ['exe', 'dll', 'driver', 'unknown']	✓	−

OP', 'MPEG_2_TS', 'PPP_ETHER', 'NFC_LLCP', 'NFLOG', 'V5_EF',

pe-section

Object describing a section of a Portable Executable.

pe-section is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
characteristic	text	Characteristic of the section ['read', 'write', 'executable']	–	–
entropy	float	Entropy of the whole section	✓	–
md5	md5	[Insecure] MD5 hash (128 bits)	–	–
name	text	Name of the section ['.rsrc', '.reloc', '.rdata', '.data', '.text']	✓	–
offset	hex	Section's offset	✓	–
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	–	–
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	–	–
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	–	–
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	–	–

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	−	−
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	−	−
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	−	−
size-in-bytes	size-in-bytes	Size of the section, in bytes	✓	−
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	−	−
text	text	Free text value to attach to the section	✓	−
virtual_address	hex	Section’s virtual address	✓	−
virtual_size	size-in-bytes	Section’s virtual size	✓	−

TIME', 'LOGCAT_LONG', 'PKTAP', 'EPON', 'IPMI_TRACE', 'LOOP', 'JSON', 'NSTRACE_3_5', 'ISO14443', 'GFP_T', 'GFP_F', 'IP_OVER_IB_PCAP

person

An object which describes a person or an identity.

person is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
address	text	Postal address of the person.	−	✓

'NORDIC_BLE', 'NETMON_NET_NETEVENT',

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
alias	text	Alias name or known as.	−	✓
birth-certificate-number	text	Birth Certificate Number	−	−
date-of-birth	date-of-birth	Date of birth of a natural person (in YYYY-MM-DD format).	−	−
dni	text	Spanish National ID	−	✓
e-mail	email-src	Email address of the person.	−	✓
fax-number	phone-number	Fax number of the person.	−	✓
first-name	first-name	First name of a natural person.	✓	−
gender	gender	The gender of a natural person. ['Male', 'Female', 'Other', 'Prefer not to say', 'Unknown']	✓	−
identity-card-number	identity-card-number	The identity card number of a natural person.	−	−
last-name	last-name	Last name of a natural person.	−	−
middle-name	middle-name	Middle name of a natural person.	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
mothers-name	text	Mother name, father, second name or other names following country’s regulation.	−	−
nationality	nationality	The nationality of a natural person.	✓	✓
nic-hdl	text	NIC Handle (Network Information Centre handle) of the person.	−	✓
nie	text	Foreign National ID (Spain)	−	✓
nif	text	Tax ID Number (Spain)	−	✓
ofac-identification-number	text	ofac-identification Number	−	−
passport-country	passport-country	The country in which the passport was issued.	✓	−
passport-expiration	passport-expiration	The expiration date of a passport.	✓	−
passport-number	passport-number	The passport number of a natural person.	−	−
phone-number	phone-number	Phone number of the person.	−	✓
place-of-birth	place-of-birth	Place of birth of a natural person.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
portrait	attachment	Portrait of the person.	−	✓
redress-number	redress-number	The Redress Control Number is the record identifier for people who apply for redress through the DHS Travel Redress Inquiry Program (DHS TRIP). DHS TRIP is for travelers who have been repeatedly identified for additional screening and who want to file an inquiry to have erroneous information corrected in DHS systems.	−	−
role	text	The role of a person. ['Suspect', 'Victim', 'Defendent', 'Accused', 'Culprit', 'Accomplice', 'Witness', 'Target']	✓	✓
social-security-number	text	Social security number.	−	−
text	text	A description of the person or identity.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
title	text	Title of the natural person such as Dr. or equivalent.	✓	−

pgp-meta

Metadata extracted from a PGP keyblock, message or signature.

pgp-meta is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
key-id	text	Key ID in hexadecimal	−	✓
user-id-email	text	User ID packet, email address of the key holder (UTF-8 text)	−	✓
user-id-name	text	User ID packet, name of the key holder	−	✓

phishing

Phishing template to describe a phishing website and its analysis.

phishing is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
hostname	hostname	host of the phishing website	−	✓
internal reference	text	Internal reference such as ticket ID	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
online	text	If the phishing is online and operational, by default is yes ['Yes', 'No']	✓	–
phishtank-detail-url	link	Phishtank detail URL to the reported phishing	–	–
phishtank-id	text	Phishtank ID of the reported phishing	–	–
screenshot	attachment	Screenshot of phishing site	✓	✓
submission-time	datetime	When the phishing was submitted and/or reported	–	–
takedown-request	datetime	When the phishing was requested to be taken down	✓	–
takedown-request-to	text	Destination email address for take-down request	✓	✓
takedown-time	datetime	When the phishing was taken down	✓	–
target	text	Targeted organisation by the phishing	–	✓
url	url	Original URL of the phishing website	–	–

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
url-redirect	url	Redirect URL of the phishing website	−	✓
verification-time	datetime	When the phishing was verified	✓	−
verified	text	The phishing has been verified by the team handling the phishing ['No', 'Yes']	✓	−

phishing-kit

Object to describe a phishing-kit.

phishing-kit is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
date-found	datetime	Date when the phishing kit was found	✓	✓
email-type	text	Type of the Email	✓	−
internal reference	text	Internal reference such as ticket ID	−	−
kit-mailer	text	Mailer Kit Used	✓	✓
kit-name	text	Name of the Phishing Kit	−	−
kit-url	url	URL of Phishing Kit	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
online	text	If the phishing kit is online and operational, by default is yes ['Yes', 'No']	✓	–
phishing-domain	url	Domain used for Phishing	–	✓
reference-link	link	Link where the Phishing Kit was observed	–	✓
target	text	What was targeted using this phishing kit	–	✓
threat-actor	text	Identified threat actor	–	✓
threat-actor-email	email-src	Email of the Threat Actor	–	✓

phone

A phone or mobile phone object which describe a phone.

phone is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
brand	text	Brand of the phone.	✓	–
first-seen	datetime	When the phone has been accessible or seen for the first time.	✓	–

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
gummei	text	Globally Unique MME Identifier (GUMMEI) is composed from MCC, MNC and MME Identifier (MMEI).	━	━
guti	text	Globally Unique Temporary UE Identity (GUTI) is a temporary identification to not reveal the phone (user equipment in 3GPP jargon) composed of GUMMEI and the M-TMSI.	━	━
imei	text	International Mobile Equipment Identity (IMEI) is a number, usually unique, to identify 3GPP and iDEN mobile phones, as well as some satellite phones.	━	━

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
imsi	text	A usually unique International Mobile Subscriber Identity (IMSI) is allocated to each mobile subscriber in the GSM/UMTS/EPS system. IMSI can also refer to International Mobile Station Identity in the ITU nomenclature.	−	−
last-seen	datetime	When the phone has been accessible or seen for the last time.	✓	−
model	text	Model of the phone.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
msisdn	text	MSISDN (pronounced as /'em es ai es di en/ or misden) is a number uniquely identifying a subscription in a GSM or a UMTS mobile network. Simply put, it is the mapping of the telephone number to the SIM card in a mobile/cellular phone. This abbreviation has a several interpretations, the most common one being Mobile Station International Subscriber Directory Number.	−	−
serial-number	text	Serial Number.	−	−
text	text	A description of the phone.	✓	−
tmsi	text	Temporary Mobile Subscriber Identities (TMSI) to visiting mobile subscribers can be allocated.	−	−

process

Object describing a system process.

process is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
args	text	Arguments of the process	✓	−
child-pid	text	Process ID of the child(ren) process	✓	✓
command-line	text	Command line of the process	−	−
creation-time	datetime	Local date/time at which the process was created	✓	−
current-directory	text	Current working directory of the process	✓	−
guid	text	The globally unique identifier of the assigned by the vendor product	−	−
hidden	boolean	Specifies whether the process is hidden	✓	−
image	filename	Path of process image	−	−
integrity-level	text	Integrity level of the process ['system', 'high', 'medium', 'low', 'untrusted']	✓	−
name	text	Name of the process	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
parent-command-line	text	Command line of the parent process	−	−
parent-guid	text	The globally unique idenifier of the parent process assigned by the vendor product	−	−
parent-image	filename	Path of parent process image	−	−
parent-pid	text	Process ID of the parent process	✓	−
parent-process-name	text	Process name of the parent	−	−
parent-process-path	text	Parent process path of the parent	−	−
pgid	text	Identifier of the group of processes the process belong to	✓	−
pid	text	Process ID of the process	✓	−
port	port	Port(s) owned by the process	✓	✓
start-time	datetime	Local date/time at which the process was started	✓	−
user	text	User context of the process	✓	−

python-etvx-event-log

Event log object template to share information of the activities conducted on a system. .

python-etvx-event-log is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
Computer	text	Computer name on which the event occurred	✓	−
Correlation-ID	text	Unique activity identity which relates the event to a process.	−	−
Event-data	text	Event data description.	✓	−
Keywords	text	Tags used for the event for the purpose of filtering or searching. ['Network', 'Security', 'Resource not found', 'other']	−	−
Operational-code	text	The opcode (numeric value or name) associated with the activity carried out by the event.	✓	−
Processor-ID	text	ID of the processor that processed the event.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
Relative-Correlation-ID	text	Related activity ID which identity similar activities which occurred as a part of the event.	✓	−
Session-ID	text	Terminal server session ID.	✓	−
Thread-ID	text	Thread id that generated the event.	✓	−
User	text	Name or the User ID the event is associated with.	✓	−
comment	text	Additional comments.	✓	−
event-channel	text	Channel through which the event occurred ['Application', 'System', 'Security', 'Setup', 'other']	✓	−
event-date-time	datetime	Date and time when the event was logged.	✓	−
event-id	text	A unique number which identifies the event.	✓	−
event-type	text	Event-type assigned to the event ['Admin', 'Operational', 'Audit', 'Analytic', 'Debug', 'other']	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
kernel-time	datetime	Execution time of the kernel mode instruction.	✓	−
level	text	Determines the event severity. ['Information', 'Warning', 'Error', 'Critical', 'Success Audit', 'Failure Audit']	−	−
log	text	Log file where the event was recorded.	✓	−
name	text	Name of the event.	✓	−
source	text	The source of the event log - application/software that logged the event.	−	−
task-category	text	Activity by the event publisher	✓	−
user-time	datetime	Date and time when the user instruction was executed.	✓	−

r2graphity

Indicators extracted from files using radare2 and graphml.

ℹ r2graphity is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
callback-average	counter	Average size of a callback	✓	−
callback-largest	counter	Largest callback	✓	−
callbacks	counter	Amount of callbacks (functions started as thread)	✓	−
create-thread	counter	Amount of calls to CreateThread	✓	−
dangling-strings	counter	Amount of dangling strings (string with a code cross reference, that is not within a function. Radare2 failed to detect that function.)	✓	−
get-proc-address	counter	Amount of calls to GetProcAddress	✓	−
gml	attachment	Graph export in G>raph Modelling Language format	✓	−
local-references	counter	Amount of API calls inside a code section	✓	−
memory-allocations	counter	Amount of memory allocations	✓	−
miss-api	counter	Amount of API call reference that does not resolve to a function offset	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
not-referenced-strings	counter	Amount of not referenced strings	✓	−
r2-commit-version	text	Radare2 commit ID used to generate this object	✓	−
ratio-api	float	Ratio: amount of API calls per kilobyte of code section	✓	−
ratio-functions	float	Ratio: amount of functions per kilobyte of code section	✓	−
ratio-string	float	Ratio: amount of referenced strings per kilobyte of code section	✓	−
referenced-strings	counter	Amount of referenced strings	✓	−
refsglobalvar	counter	Amount of API calls outside of code section (glob var, dynamic API)	✓	−
shortest-path-to-create-thread	counter	Shortest path to the first time the binary calls CreateThread	✓	−
text	text	Description of the r2graphity object	✓	−
total-api	counter	Total amount of API calls	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
total-functions	counter	Total amount of functions in the file.	✓	−
unknown-references	counter	Amount of API calls not ending in a function (Radare2 bug, probalby)	✓	−

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.

regexp is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
comment	comment	A description of the regular expression.	−	−
regexp	text	regexp	−	−
regexp-type	text	Type of the regular expression syntax. ['PCRE', 'PCRE2', 'POSIX BRE', 'POSIX ERE']	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
type	text	Specify which type corresponds to this regex. ['hostname', 'domain', 'email-src', 'email-dst', 'email-subject', 'url', 'user-agent', 'regkey', 'cookie', 'uri', 'filename', 'windows-service-name', 'windows-scheduled-task']	✓	—

registry-key

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

registry-key is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
data	text	Data stored in the registry key	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
data-type	text	Registry value type ['REG_NONE', 'REG_SZ', 'REG_EXPAND_SZ', 'REG_BINARY', 'REG_DWORD', 'REG_DWORD_LITTLE_ENDIAN', 'REG_DWORD_BIG_ENDIAN', 'REG_LINK', 'REG_MULTI_SZ', 'REG_RESOURCE_LIST', 'REG_FULL_RESOURCE_DESCRIPTOR', 'REG_RESOURCE_REQUIREMENTS_LIST', 'REG_QWORD', 'REG_QWORD_LITTLE_ENDIAN']	✓	−
hive	text	Hive used to store the registry key (file on disk)	✓	−
key	regkey	Full key path	−	−
last-modified	datetime	Last time the registry key has been modified	−	−
name	text	Name of the registry key	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
root-keys	text	Root key of the Windows registry (extracted from the key) ['HKCC', 'HKCR', 'HKCU', 'HKDD', 'HKEY_CLASSES_ROOT', 'HKEY_CURRENT_CONFIG', 'HKEY_CURRENT_USER', 'HKEY_DYN_DATA', 'HKEY_LOCAL_MACHINE', 'HKEY_PERFORMANCE_DATA', 'HKEY_USERS', 'HKLM', 'HKPD', 'HKU']	✓	−

regripper-NTUser

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

regripper-NTUser is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
applications-installed	text	List of applications installed.	−	✓
applications-run	text	List of applications set to run on the system.	−	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
comments	text	Additional information related to the user profile	✓	-
external-devices	text	List of external devices connected to the system by the user.	-	✓
key	text	Registry key where the information is retrieved from.	-	-
key-last-write-time	datetime	Date and time when the key was last updated.	✓	-
logon-user-name	text	Name assigned to the user profile.	-	-
mount-points	text	Details of the mount points created on the system.	✓	✓
network-connected-to	text	List of networks the user connected the system to.	-	✓
nukeOnDelete	boolean	Determines if the Recycle bin option has been disabled.	✓	-
recent-files-accessed	text	List of recent files accessed by the user.	-	✓
recent-folders-accessed	text	List of recent folders accessed by the user.	-	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
typed-urls	text	Urls typed by the user in internet explorer	−	✓
user-init	text	Applications or processes set to run when the user logs onto the windows system.	−	✓

regripper-sam-hive-single-user

Regripper Object template designed to present user profile details extracted from the SAM hive.

regripper-sam-hive-single-user is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
comments	text	Full name assigned to the user profile.	✓	−
full-user-name	text	Full name assigned to the user profile.	−	−
key	text	Registry key where the information is retrieved from.	−	−
key-last-write-time	datetime	Date and time when the key was last updated.	✓	−
last-login-time	datetime	Date and time when the user last logged onto the system.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
login-count	counter	Number of times the user logged-in onto the system.	✓	−
pwd-fail-date	datetime	Date and time when a password last failed for this user profile.	✓	−
pwd-reset-time	datetime	Date and time when the password was last reset.	✓	−
user-name	text	User name assigned to the user profile.	−	−

regripper-sam-hive-user-group

Regripper Object template designed to present group profile details extracted from the SAM hive.

regripper-sam-hive-user-group is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
full-name	text	Full name assigned to the profile.	−	−
group-comment	text	Any group comment added.	✓	−
group-name	text	Name assigned to the profile.	−	−
group-users	text	Users belonging to the group	−	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
key	text	Registry key where the information is retrieved from.	−	−
key-last-write-time	datetime	Date and time when the key was last updated.	✓	−
last-write-date-time	datetime	Date and time when the group key was updated.	✓	−

regripper-software-hive-BHO

Regripper Object template designed to gather information of the browser helper objects installed on the system.

regripper-software-hive-BHO is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
BHO-key-last-write-time	datetime	Date and time when the BHO key was last updated.	✓	−
BHO-name	text	Name of the browser helper object.	−	−
class	text	Class to which the BHO belongs to.	✓	−
comments	text	Additional comments.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
key	text	Software hive key where the information is retrieved from.	—	—
last-write-time	datetime	Date and time when the key was last updated.	✓	—
module	text	DLL module the BHO belongs to.	✓	—
references	link	References to the BHO.	—	✓

regripper-software-hive-appInit-DLLS

Regripper Object template designed to gather information of the DLL files installed on the system.

regripper-software-hive-appInit-DLLS is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
DLL-last-write-time	datetime	Date and time when the DLL file was last updated.	✓	—
DLL-name	text	Name of the DLL file.	—	—
DLL-path	text	Path where the DLL file is stored.	—	—
comments	text	Additional comments.	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
key	text	Software hive key where the information is retrieved from.	–	–
last-write-time	datetime	Date and time when the key was last updated.	✓	–
references	link	References to the DLL file.	–	✓

regripper-software-hive-application-paths

Regripper Object template designed to gather information of the application paths.

regripper-software-hive-application-paths is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
comments	text	Additional comments.	✓	–
executable-file-name	text	Name of the executable file.	–	✓
key	text	Software hive key where the information is retrieved from.	–	–
last-write-time	datetime	Date and time when the key was last updated.	✓	–
path	text	Path of the executable file.	–	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
references	link	References to the application installed.	−	✓

regripper-software-hive-applications-installed

Regripper Object template designed to gather information of the applications installed on the system.

regripper-software-hive-applications-installed is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
app-last-write-time	datetime	Date and time when the application key was last updated.	✓	−
app-name	text	Name of the application.	−	−
comments	text	Additional comments.	✓	−
key	text	Software hive key where the information is retrieved from.	−	−
key-path	text	Path of the key.	−	−
last-write-time	datetime	Date and time when the key was last updated.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
references	link	References to the application installed.	−	✓
version	text	Version of the application.	−	−

regripper-software-hive-command-shell

Regripper Object template designed to gather information of the shell commands executed on the system.

ℹ regripper-software-hive-command-shell is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
command	text	Command executed.	−	−
comments	text	Additional comments.	✓	−
key	text	Software hive key where the information is retrieved from.	−	−
last-write-time	datetime	Date and time when the key was last updated.	✓	−
shell	text	Type of shell used to execute the command. ['exe', 'cmd', 'bat', 'hta', 'pif', 'Other']	✓	−
shell-path	text	Path of the shell.	−	−

regripper-software-hive-software-run

Regripper Object template designed to gather information of the applications set to run on the system.

regripper-software-hive-software-run is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
application-name	text	Name of the application run.	—	✓
application-path	text	Path where the application is installed.	—	✓
comments	text	Additional comments.	✓	—
key	text	Software hive key where the information is retrieved from. ['Run', 'RunOnce', 'Runservices', 'Terminal', 'Other']	✓	—
key-path	text	Path of the key.	✓	—
last-write-time	datetime	Date and time when the key was last updated.	✓	—
references	link	References to the applications.	—	✓

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-software-hive-userprofile-winlogon is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
AutoAdminLogon	boolean	Flag value to determine if autologon is enabled for a user without entering the password.	✓	–
AutoRestartShell	boolean	Value of the flag set to auto restart the shell if it crashes or shuts down automatically.	✓	–
CachedLogonCount	counter	Number of times the user has logged into the system.	✓	–
Comments	text	Additional comments.	✓	–
DefaultUserName	text	user-name of the default user.	✓	–
DisableCAD	boolean	Flag to determine if user login is enabled by pressing Ctrl+ALT+Delete.	✓	–
Legal-notice-caption	text	Message title set to display when the user logs-in.	✓	✓
Legal-notice-text	text	Message set to display when the user logs-in.	✓	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
PasswordExpiryWarining	counter	Number of times the password expiry warning appeared.	✓	−
PowerdownAfterShutDown	boolean	Flag value- if the system is set to power down after it is shutdown.	✓	−
PreCreateKnownFolders	text	create known folders key	✓	−
ReportBootOk	boolean	Flag to check if the reboot was successful.	✓	−
SID	text	Security identifier assigned to the user profile.	✓	−
Shell	text	Shell set to run when the user logs onto the system.	✓	✓
ShutdownFlags	counter	Number of times shutdown is initiated from a process when the user is logged-in.	✓	−
ShutdownWithoutLogon	boolean	Value of the flag set to enable shutdown without requiring a user to login.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
UserInit	text	Applications and files set to run when the user logs onto the system (User logon activity).	−	✓
WinStationsDisabled	boolean	Flag value set to enable/disable logons to the system.	✓	−
user-profile-key-last-write-time	datetime	Date and time when the key was last updated.	✓	−
user-profile-key-path	text	key where the user-profile information is retrieved from.	✓	−
user-profile-last-write-time	datetime	Date and time when the user profile was last updated.	✓	−
user-profile-path	text	Path of the user profile on the system	✓	−
winlogon-key-last-write-time	datetime	Date and time when the winlogon key was last updated.	✓	−
winlogon-key-path	text	winlogon key referred in order to retrieve default user information	✓	−

regripper-software-hive-windows-general-info

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

regripper-software-hive-windows-general-info is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
BuildGUID	text	Build ID.	—	—
BuildLab	text	Windows BuildLab string.	—	—
BuildLabEx	text	Windows BuildLabEx string.	—	—
CSDVersion	text	Version of the service pack installed.	—	—
CurrentBuild	text	Build number of the windows OS.	—	—
CurrentBuildType	text	Current build type of the OS.	—	—
CurrentVersion	text	Current version of windows	✔	—
EditionID	text	Windows edition.	—	—
InstallDate	datetime	Date when windows was installed.	✔	—
InstallationType	text	Type of windows installation.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
PathName	text	Path to the root directory.	✓	−
ProductID	text	ID of the product version.	−	−
ProductName	text	Name of the windows version.	−	−
RegisteredOrganization	text	Name of the registered organization.	−	−
RegisteredOwner	text	Name of the registered owner.	−	−
SoftwareType	text	Software type of windows. ['System', 'Application', 'other']	✓	−
SystemRoot	text	Root directory.	✓	−
comment	comment	Additional comments.	✓	−
last-write-time	datetime	Date and time when the key was last updated.	✓	−
win-cv-path	text	key where the windows information is retrieved from	−	−

regripper-system-hive-firewall-configuration

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

regripper-system-hive-firewall-configuration is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
comment	text	Additional comments.	✓	−
disable-notification	boolean	Boolean flag to determine if firewall notifications are enabled.	✓	−
enbled-firewall	boolean	Boolean flag to determine if the firewall is enabled.	✓	−
last-write-time	datetime	Date and time when the firewall profile policy was last updated.	✓	−
profile	text	Firewall Profile type ['Domain Profile', 'Standard Profile', 'Network Profile', 'Public Profile', 'Private Profile', 'other']	✓	−

regripper-system-hive-general-configuration

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

regripper-system-hive-general-configuration is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
comment	text	Additional comments.	✓	−
computer-name	text	name of the computer under analysis	−	−
fDenyTSConnections:	boolean	Specifies whether remote connections are enabled or disabled on the system.	✓	−
last-write-time	datetime	Date and time when the key was last updated.	✓	−
shutdown-time	datetime	Date and time when the system was shutdown.	✓	−
timezone-bias	text	Offset in minutes from UTC. Offset added to the local time to get a UTC value.	✓	−
timezone-daylight-bias	text	value in minutes to be added to the value of timezone-bias to generate the bias used during daylight time.	✓	−
timezone-daylight-date	datetime	Daylight date - daylight saving months	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
timezone-daylight-name	text	Timezone name used during daylight saving months.	✓	−
timezone-last-write-time	datetime	Date and time when the timezone key was last updated.	✓	−
timezone-standard-bias	text	value in minutes to be added to the value of timezone-bias to generate the bias used during standard time.	✓	−
timezone-standard-date	datetime	Standard date - non daylight saving months	✓	−
timezone-standard-name	text	Timezone standard name used during non-daylight saving months.	✓	−

regripper-system-hive-network-information

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

regripper-system-hive-network-information is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
DHCP-IP-address	ip-dst	DHCP service - IP address	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
DHCP-domain	text	Name of the DHCP domain service	–	–
DHCP-name-server	ip-dst	DHCP Name server - IP address.	–	–
DHCP-server	ip-dst	DHCP server - IP address.	–	–
DHCP-subnet-mask	ip-dst	DHCP subnet mask - IP address.	–	–
TCPIP-key	text	TCPIP key	–	–
TCPIP-key-last-write-time	datetime	Datetime when the key was last updated.	✓	–
additional-comments	text	Comments.	✓	–
interface-GUID	text	GUID value assigned to the interface.	✓	–
interface-IPcheckingEnabled	boolean	–	✓	–
interface-MediaSubType	text	–	✓	–
interface-PnpInstanceID	text	Plug and Play instance ID assigned to the interface.	✓	–
interface-last-write-time	datetime	Last date and time when the interface key was updated.	✓	–
interface-name	text	Name of the interface.	–	–

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
network-key	text	Registry key assigned to the network	−	−
network-key-last-write-time	datetime	Date and time when the network key was last updated.	✓	−
network-key-path	text	Path of the key where the information is retrieved from.	✓	−

regripper-system-hive-services-drivers

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

regripper-system-hive-services-drivers is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
comment	text	Additional comments.	✓	−
display	text	Display name/information of the service or the driver.	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
group	text	Group to which the system/driver belong to. ['Base', 'Boot Bus Extender', 'Boot File System', 'Cryptography', 'Extended base', 'Event Log', 'Filter', 'FSFilter Bottom', 'FSFilter Infrastructure', 'File System', 'FSFilter Virtualization', 'Keyboard Port', 'Network', 'NDIS', 'Parallel arbitrator', 'Pointer Port', 'PnP Filter', 'ProfSvc_Group', 'PNP_TDI', 'SCSI Miniport', 'SCSI CDROM Class', 'System Bus Extender', 'Video Save', 'other']	✓	−
image-path	text	Path of the service/drive	−	−
last-write-time	datetime	Date and time when the key was last updated.	✓	−
name	text	name of the key	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
start	text	When the service/driver starts or executes. ['Boot start', 'System start', 'Auto start', 'Manual', 'Disabled']	✓	−
type	text	Service/driver type. ['Kernel driver', 'File system driver', 'Own process', 'Share process', 'Interactive', 'Other']	✓	−

report

Metadata used to generate an executive level report.

report is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
case-number	text	Case number	−	−
report-file(s)	attachment	Attachment(s) that is related to the report	−	✓
summary	text	Free text summary of the report	−	✓

research-scanner

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

research-scanner is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
asn	AS	Autonomous System Number related to project	✓	−
contact_email	email-dst	Project contact information	✓	✓
contact_phone	phone-number	Phone number related to project	✓	✓
domain	domain	Domain related to project	−	✓
project	text	Description of scanning project	✓	−
project_url	link	URL related to project	✓	✓
scanning_ip	ip-src	IP address used by project	−	✓
scheduled_end	datetime	Scheduled end of scanning activity	✓	✓
scheduled_start	datetime	Scheduled start of scanning activity	✓	✓

rogue-dns

Rogue DNS as defined by CERT.br.

rogue-dns is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
hijacked-domain	hostname	Domain/hostname hijacked by the the rogue DNS	−	−
phishing-ip	ip-dst	Resource records returns by the rogue DNS	−	−
rogue-dns	ip-dst	IP address of the rogue DNS	−	−
status	text	How many authoritative DNS answers were received at the Passive DNS Server's collectors with exactly the given set of values as answers. ['ROGUE DNS', 'Unknown']	✓	−
timestamp	datetime	Last time that the rogue DNS value was seen.	✓	−

rtir

RTIR - Request Tracker for Incident Response.

rtir is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
classification	text	Classification of the RTIR ticket	−	✓
constituency	text	Constituency of the RTIR ticket	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
ip	ip-dst	IPs automatically extracted from the RTIR ticket	−	✓
queue	text	Queue of the RTIR ticket ['incident', 'investigations', 'blocks', 'incident reports']	−	−
status	text	Status of the RTIR ticket ['new', 'open', 'stalled', 'resolved', 'rejected', 'deleted']	✓	−
subject	text	Subject of the RTIR ticket	−	−
ticket-number	text	ticket-number of the RTIR ticket	−	−

sandbox-report

Sandbox report.

sandbox-report is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
on-premise-sandbox	text	The on-premise sandbox used ['cuckoo', 'symantec-cas-on-premise', 'bluecoat-maa', 'trendmicro-deep-discovery-analyzer', 'fireeye-ax', 'vmray', 'joe-sandbox-on-premise']	✓	−
permalink	link	Permalink reference	−	−
raw-report	text	Raw report from sandbox	✓	−
results	text	Freetext result values	✓	✓
saas-sandbox	text	A non-on-premise sandbox, also results are not publicly available ['forticloud-sandbox', 'joe-sandbox-cloud', 'symantec-cas-cloud']	✓	−
sandbox-file	attachment	File related to sandbox run	✓	✓
sandbox-type	text	The type of sandbox used ['on-premise', 'web', 'saas']	✓	−
score	text	Score	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
web-sandbox	text	A web sandbox where results are publicly available via an URL ['malwr', 'hybrid-analysis']	✓	−

sb-signature

Sandbox detection signature.

ℹ sb-signature is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
datetime	datetime	Datetime	✓	−
signature	text	Name of detection signature - set the description of the detection signature as a comment	−	✓
software	text	Name of Sandbox software	✓	−
text	text	Additional signature description	✓	−

scheduled-event

Event object template describing a gathering of individuals in meatspace.

ℹ scheduled-event is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
address	text	Postal address of the event.	−	✓
administrator	text	A user account who is an owner or admin of the event.	−	✓
archive	link	Archive of the original event (Internet Archive, Archive.is, etc).	−	✓
attachment	attachment	A screen capture or other attachment relevant to the event.	−	✓
e-mail	email-src	Email address of the event contact.	−	✓
embedded-link	url	Link embedded in the event description (potentially malicious).	−	✓
embedded-safe-link	link	Link embedded in the event description (supposed safe).	−	✓
event-alias	text	Aliases of event.	−	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
event-listing	text	Social media and other platforms on which the event is advertised. ['Twitter', 'Facebook', 'Meetup', 'Eventbrite', 'Other']	✓	✓
event-name	text	The name of the event.	−	−
fax-number	phone-number	Fax number of the event contact.	−	✓
hashtag	text	Hashtag used to identify or promote the event.	−	✓
link	link	Original link into the event (supposed harmless).	−	−
person-name	text	A person who is going to the event.	−	✓
phone-number	phone-number	Phone number of the event contact.	−	✓
scheduled-date	datetime	Initial creation of the microblog post	−	✓
url	url	Original URL location of the event (potentially malicious).	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
username	text	A user account who is going to the event.	−	✓

scrippsco2-c13-daily

Daily average C13 concentrations (ppm) derived from flask air samples.

scrippsco2-c13-daily is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
c13-value	float	C13 value (ppm) - C13 concentrations are measured on the '08A' Calibration Scale	✓	−
flag	counter	Flag (see taxonomy for details).	✓	−
number-flask	counter	Number of flasks used in daily average.	✓	−
sample-date-excel	float	M$Excel spreadsheet date format.	✓	−
sample-date-fractional	float	Decimal year and fractional year.	✓	−
sample-datetime	datetime	Datetime the sample has been taken	✓	−

scrippsco2-c13-monthly

Monthly average C13 concentrations (ppm) derived from flask air samples.

scrippsco2-c13-monthly is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
monthly-c13	float	Monthly C13 concentrations in micro-mol C13 per mole (ppm) reported on the 2008A SIO manometric mole fraction scale. This is the standard version of the data most often sought.	✓	−
monthly-c13-seasonal-adjustment	float	Same data after a seasonal adjustment to remove the quasi-regular seasonal cycle. The adjustment involves subtracting from the data a 4-harmonic fit with a linear gain factor.	✓	−
monthly-c13-smoothed	float	Smoothed version of the data generated from a stiff cubic spline function plus 4-harmonic functions with linear gain.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
monthly-c13-smoothed-seasonal-adjustment	float	Same smoothed version with the seasonal cycle removed.	✓	━
sample-date-excel	float	M$Excel spreadsheet date format.	✓	━
sample-date-fractional	float	Decimal year and fractional year.	✓	━
sample-datetime	datetime	The monthly values have been adjusted to 24:00 hours on the 15th of each month.	✓	━

scrippsco2-co2-daily

Daily average CO2 concentrations (ppm) derived from flask air samples.

scrippsco2-co2-daily is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
co2-value	float	CO2 value (ppm) - CO2 concentrations are measured on the '08A' Calibration Scale	✓	━
flag	counter	Flag (see taxonomy for details).	✓	━

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
number-flask	counter	Number of flasks used in daily average.	✓	−
sample-date-excel	float	M$Excel spreadsheet date format.	✓	−
sample-date-fractional	float	Decimal year and fractional year.	✓	−
sample-datetime	datetime	Datetime the sample has been taken	✓	−

scrippsco2-co2-monthly

Monthly average CO2 concentrations (ppm) derived from flask air samples.

scrippsco2-co2-monthly is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
monthly-co2	float	Monthly CO2 concentrations in micro-mol CO2 per mole (ppm) reported on the 2008A SIO manometric mole fraction scale. This is the standard version of the data most often sought.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
monthly-co2-seasonal-adjustment	float	Same data after a seasonal adjustment to remove the quasi-regular seasonal cycle. The adjustment involves subtracting from the data a 4-harmonic fit with a linear gain factor.	✓	−
monthly-co2-smoothed	float	Smoothed version of the data generated from a stiff cubic spline function plus 4-harmonic functions with linear gain.	✓	−
monthly-co2-smoothed-seasonal-adjustment	float	Same smoothed version with the seasonal cycle removed.	✓	−
sample-date-excel	float	M$Excel spreadsheet date format.	✓	−
sample-date-fractional	float	Decimal year and fractional year.	✓	−
sample-datetime	datetime	The monthly values have been adjusted to 24:00 hours on the 15th of each month.	✓	−

scrippsco2-o18-daily

Daily average O18 concentrations (ppm) derived from flask air samples.

scrippsco2-o18-daily is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
flag	counter	Flag (see taxonomy for details).	✓	━
number-flask	counter	Number of flasks used in daily average.	✓	━
o18-value	float	O18 value (ppm) - O18 concentrations are measured on the '08A' Calibration Scale	✓	━
sample-date-excel	float	M$Excel spreadsheet date format.	✓	━
sample-date-fractional	float	Decimal year and fractional year.	✓	━
sample-datetime	datetime	Datetime the sample has been taken	✓	━

scrippsco2-o18-monthly

Monthly average O18 concentrations (ppm) derived from flask air samples.

scrippsco2-o18-monthly is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
monthly-o18	float	Monthly O18 concentrations in micro-mol O18 per mole (ppm) reported on the 2008A SIO manometric mole fraction scale. This is the standard version of the data most often sought.	✓	−
monthly-o18-seasonal-adjustment	float	Same data after a seasonal adjustment to remove the quasi-regular seasonal cycle. The adjustment involves subtracting from the data a 4-harmonic fit with a linear gain factor.	✓	−
monthly-o18-smoothed	float	Smoothed version of the data generated from a stiff cubic spline function plus 4-harmonic functions with linear gain.	✓	−
monthly-o18-smoothed-seasonal-adjustment	float	Same smoothed version with the seasonal cycle removed.	✓	−
sample-date-excel	float	M$Excel spreadsheet date format.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
sample-date-fractional	float	Decimal year and fractional year.	✓	−
sample-datetime	datetime	The monthly values have been adjusted to 24:00 hours on the 15th of each month.	✓	−

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.

script is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
comment	text	Comment associated to the script.	−	−
filename	filename	Filename used for the script.	✓	✓
language	text	Scripting language used for the script. ['PowerShell', 'VBScript', 'Bash', 'Lua', 'JavaScript', 'AppleScript', 'AWK', 'Python', 'Perl', 'Ruby', 'Winbatch', 'AutoIt', 'PHP', 'Nim']	✓	−
script	text	Free text of the script.	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
script-as-attachment	attachment	Attachment of the script.	—	—
state	text	Known state of the script. ['Malicious', 'Unknown', 'Harmless', 'Trusted']	✓	✓

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.

shell-commands is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
comment	text	Comment associated to the shell commands executed.	—	—
language	text	Scripting language used for the shell commands executed. ['PowerShell', 'VBScript', 'Bash', 'Lua', 'JavaScript', 'AppleScript', 'AWK', 'Python', 'Perl', 'Ruby', 'Winbatch', 'AutoIt', 'PHP']	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
script	text	Free text of the script if available which executed the shell commands.	-	-
shell-command	text	-	-	✓
state	text	Known state of the script. ['Malicious', 'Unknown', 'Harmless', 'Trusted']	✓	✓

shodan-report

Shodan Report for a given IP.

shodan-report is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
banner	text	server banner reported	-	-
hostname	domain	Hostnames found	-	✓
ip	ip-dst	IP Address Queried	-	-
org	text	Associated Organization	-	-
port	port	Listening Port	-	-
text	text	A description of the report	-	-

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.

short-message-service is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
body	text	Message body of the SMS	−	−
from	phone-number	Phone number used to send the SMS	−	✓
name	text	Sender name	−	−
received-date	datetime	Received date of the SMS	✓	−
sent-date	datetime	Initial sent date of the SMS	✓	−
smsc	phone-number	SMS Message Center	−	−
to	phone-number	Phone number receiving the SMS	−	✓
url-rfc5724	url	url representing SMS using RFC 5724 (not url contained in the SMS which should use an url object)	−	−

shortened-link

Shortened link and its redirect target.

shortened-link is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
credential	text	Credential (username, password)	−	−
domain	domain	Full domain	−	−
first-seen	datetime	First time this shortened URL has been seen	✓	−
redirect-url	url	Redirected to URL	−	−
shortened-url	url	Shortened URL	−	−
text	text	Description and context of the shortened URL	−	−

social-media-group

Social media group object template describing a public or private group or channel.

social-media-group is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
administrator	text	A user account who is an owner or admin of the group.	−	✓
archive	link	Archive of the original group (Internet Archive, Archive.is, etc).	✓	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
attachment	attachment	A screen capture or exported list of contacts, group members, etc.	−	✓
description	text	A description of the group, channel or community.	−	−
embedded-link	url	Link embedded in the group description (potentially malicious).	−	✓
embedded-safe-link	link	Link embedded in the group description (supposed safe).	−	✓
group-alias	text	Aliases of group, channel or community.	−	✓
group-name	text	The name of the group, channel or community.	−	−
hashtag	text	Hashtag used to identify or promote the group.	−	✓
link	link	Original link into the group (supposed harmless).	−	−
person-name	text	A person who is a member of the group.	−	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
platform	text	The social media platform used. ['Facebook', 'Twitter']	✓	✓
url	url	Original URL location of the group (potentially malicious).	−	−
username	text	A user account who is a member of the group.	−	✓

splunk

Splunk / Splunk ES object.

splunk is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
description	comment	Description	✓	−
drill-down	text	Drilldown	✓	✓
earliest	text	Earliest time	✓	−
latest	text	Latest time	✓	−
response-action	text	Response action ['notable', 'risk']	✓	✓
schedule	other	Schedule	✓	−
search	text	Search / Correlation search	✓	−

ss7-attack

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

ss7-attack is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
Category	text	Category ['Cat0', 'Cat1', 'Cat2.1', 'Cat2.2', 'Cat3.1', 'Cat3.2', 'Cat3.3', 'CatSMS', 'CatSpoofing']	✓	✓
MapApplicationContext	text	MAP application context in OID format.	✓	−
MapGmlc	text	MAP GMLC. Phone number.	−	−
MapGsmscfGT	text	MAP GSMSCF GT. Phone number.	−	−
MapImsi	text	MAP IMSI. Phone number starting with MCC/MNC.	−	✓
MapMscGT	text	MAP MSC GT. Phone number.	−	−
MapMsisdn	text	MAP MSISDN. Phone number.	−	✓
MapOpCode	text	MAP operation codes - Decimal value between 0-99.	✓	−
MapSmsTP-DCS	text	MAP SMS TP-DCS.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
MapSmsTP-OA	text	MAP SMS TP-OA. Phone number.	–	–
MapSmsTP-PID	text	MAP SMS TP-PID.	✓	–
MapSmsText	text	MAP SMS Text. Important indicators in SMS text.	–	–
MapSmsTypeNumber	text	MAP SMS TypeNumber.	✓	–
MapSmscGT	text	MAP SMSC. Phone number.	–	✓
MapUssdCoding	text	MAP USSD Content.	✓	–
MapUssdContent	text	MAP USSD Content.	–	–
MapVersion	text	Map version. ['1', '2', '3']	✓	–
MapVlrGT	text	MAP VLR GT. Phone number.	–	–
SccpCdGT	text	Signaling Connection Control Part (SCCP) CdGT - Phone number.	–	–
SccpCdPC	text	Signaling Connection Control Part (SCCP) CdPC - Phone number.	–	–

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
SccpCdSSN	text	Signaling Connection Control Part (SCCP) - Decimal value between 0-255.	✓	−
SccpCgGT	text	Signaling Connection Control Part (SCCP) CgGT - Phone number.	−	✓
SccpCgPC	text	Signaling Connection Control Part (SCCP) CgPC - Phone number.	−	✓
SccpCgSSN	text	Signaling Connection Control Part (SCCP) - Decimal value between 0-255.	✓	−
first-seen	datetime	When the attack has been seen for the first time.	✓	−
text	text	A description of the attack seen via SS7 logging.	✓	✓

ssh-authorized-keys

An object to store ssh authorized keys file.

ssh-authorized-keys is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
first-seen	datetime	First time the ssh authorized keys file has been seen	✓	−
full-line	text	One full-line of the authorized key file	−	✓
hostname	hostname	hostname	−	✓
ip	ip-dst	IP Address	−	✓
key	text	Public key in base64 as found in the authorized key file	−	✓
key-id	text	Key-id and option part of the public key line	−	✓
last-seen	datetime	Last time the ssh authorized keys file has been seen	✓	−
text	text	A description of the ssh authorized keys	✓	−

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.

stix2-pattern is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
comment	comment	A description of the stix2-pattern.	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
stix2-pattern	stix2-pattern	STIX 2 pattern	−	−
version	text	Version of STIX 2 pattern. ['stix 2.0']	−	−

suricata

An object describing one or more Suricata rule(s) along with version and contextual information.

suricata is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
comment	comment	A description of the Suricata rule(s).	−	−
ref	link	Reference to the Suricata rule such as origin of the rule or alike.	−	−
suricata	snort	Suricata rule.	−	✓
version	text	Version of the Suricata rule depending where the suricata rule is known to work as expected.	−	−

target-system

Description about an targeted system, this could potentially be a compromissed internal system.

target-system is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
targeted_ip_of_system	ip-src	Targeted system IP address	✓	−
targeted_machine	target-machine	Targeted system	✓	−
timestamp_seen	datetime	Registered date and time	✓	−

threatgrid-report

ThreatGrid report.

threatgrid-report is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
analysis_submitted_at	text	Submission date	−	−
heuristic_raw_score	text	heuristic_raw_score	✓	−
heuristic_score	text	heuristic_score	−	−
id	text	ThreatGrid ID	−	−
iocs	text	iocs	−	✓
original_filename	text	Original filename	−	−
permalink	text	permalink	−	−
threat_score	text	threat_score	✓	−

timecode

Timecode object to describe a start of video sequence (e.g. CCTV evidence) and the end of the video sequence.

timecode is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
description	text	Description of the video sequence	−	−
end-marker-timecode	text	End marker timecode in the format hh:mm:ss;ff	−	✓
end-timecode	text	End marker timecode in the format hh:mm:ss.mms	−	✓
recording-date	datetime	Date of recording of the video sequence	−	✓
start-marker-timecode	text	Start marker timecode in the format hh:mm:ss;ff	−	✓
start-timecode	text	Start marker timecode in the format hh:mm:ss.mms	−	✓

timesketch-timeline

A timesketch timeline object based on mandatory field in timesketch to describe a log entry.

timesketch-timeline is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
datetime	datetime	When the log entry was seen	—	—
message	text	Informative message of the event	—	—
timestamp	text	When the log entry was seen in microseconds since Unix epoch	—	—
timestamp_desc	text	Text explaining what type of timestamp is it	—	—

timesketch_message

A timesketch message entry.

timesketch_message is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
datetime	datetime	datetime of the message	✓	—
message	text	message	✓	—

timestamp

A generic timestamp object to represent time including first time and last time seen. Relationship will then define the kind of time relationship.

timestamp is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
first-seen	datetime	First time that the linked object or attribute has been seen.	✓	━
last-seen	datetime	First time that the linked object or attribute has been seen.	✓	━
precision	text	Timestamp precision represents the precision given to first_seen and/or last_seen in this object. ['year', 'month', 'day', 'hour', 'minute', 'full']	✓	━
text	text	Description of the time object.	✓	━

tor-hiddenservice

Tor hidden service (onion service) object.

tor-hiddenservice is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
address	text	onion address of the Tor node seen.	━	━
description	text	Tor onion service comment.	✓	━

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
first-seen	datetime	When the Tor hidden service was been seen for the first time.	✓	−
last-seen	datetime	When the Tor hidden service was seen for the last time.	✓	−

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.

tor-node is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
address	ip-src	IP address of the Tor node seen.	−	−
description	text	Tor node description.	✓	−
document	text	Raw document from the consensus.	✓	−
fingerprint	text	router's fingerprint.	−	−
first-seen	datetime	When the Tor node designed by the IP address has been seen for the first time.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
flags	text	list of flag associated with the node.	−	−
last-seen	datetime	When the Tor node designed by the IP address has been seen for the last time.	✓	−
nickname	text	router’s nickname.	−	−
published	datetime	router’s publication time. This can be different from first-seen and last-seen.	✓	−
text	text	Tor node comment.	✓	−
version	text	parsed version of tor, this is None if the relay’s using a new versioning scheme.	−	−
version_line	text	versioning information reported by the node.	−	−

tracking-id

Analytics and tracking ID such as used in Google Analytics or other analytic platform.

tracking-id is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
description	text	Description of the tracking id	−	−
first-seen	datetime	First time the tracking code was seen	✓	−
hostname	hostname	hostname where the tracking id was found	−	✓
id	text	Tracking code	−	−
last-seen	datetime	Last time the tracking code was seen	✓	−
tracker	text	Name of the tracker - organisation doing the tracking and/or analytics ['Google Analytics', 'Piwik', 'Kissmetrics', 'Woopra', 'Chartbeat']	−	−
url	url	URL where the tracking id was found	−	✓

transaction

An object to describe a financial transaction.

transaction is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
amount	text	The value of the transaction in local currency.	−	−
authorized	text	Person who autorized the transaction.	−	−
date	datetime	Date and time of the transaction.	−	−
date-posting	datetime	Date of posting, if different from date of transaction.	−	−
from-country	text	Origin country of a transaction.	−	−
from-funds-code	text	Type of funds used to initiate a transaction. ['A Deposit', 'C Currency exchange', 'D Casino chips', 'E Bank draft', 'F Money order', 'G Traveler’s cheques', 'H Life insurance policy', 'I Real estate', 'J Securities', 'K Cash', 'O Other', 'P Cheque']	✓	−
location	text	Location where the transaction took place.	−	−
teller	text	Person who conducted the transaction.	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
text	text	A description of the transaction.	✓	—
to-country	text	Target country of a transaction.	—	—
to-funds-code	text	Type of funds used to finalize a transaction. ['A Deposit', 'C Currency exchange', 'D Casino chips', 'E Bank draft', 'F Money order', 'G Traveler’s cheques', 'H Life insurance policy', 'I Real estate', 'J Securities', 'K Cash', 'O Other', 'P Cheque']	✓	—
transaction-number	text	A unique number identifying a transaction.	—	—
transmode-code	text	How the transaction was conducted.	—	—
transmode-comment	text	Comment describing transmode-code, if needed.	—	—

translation

Used to keep a text and its translation.

ℹ translation is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
original-language	text	Language of the original text ['Mandarin (language family)', 'Spanish', 'English', 'Hindi', 'Bengali', 'Portuguese', 'Russian', 'Japanese', 'Western Punjabi', 'Marathi', 'Telugu', 'Wu (language family)', 'Turkish', 'Korean', 'French', 'German', 'Vietnamese', 'Tamil', 'Yue (language family)', 'Urdu', 'Javanese', 'Italian', 'Egyptian Arabic', 'Gujarati', 'Iranian Persian', 'Bhojpuri', 'Min Nan (language family)', 'Hakka', 'Jinyu', 'Hausa', 'Kannada', 'Indonesian (Indonesian Malay)', 'Polish', 'Yoruba', 'Xiang Chinese (language family)', 'Malayalam', 'Odia', 'Maithili', 'Burmese', 'Eastern Punjabi', 'Sunda', 'Sudanese Arabic', 'Algerian Arabic', 'Moroccan Arabic', 'Ukrainian', 'Igbo', 'Northern Uzbek', 'Sindhi', 'North Levantine Arabic', 'Romanian', 'Tagalog', 'Dutch', 'Saʿidi Arabic',	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
original-text	text	Original text	-	-
translated-text	text	Text after translation	-	-

'Somali', 'Malay (Malaysian Malay)', 'Cebuano', 'Nepali', 'Mesopotamian Arabic', 'Assamese', 'Sinhala', 'Northern Kurdish', 'Hejazi Arabic', 'Nigerian Fulfulde', 'South Azerbaijani', 'Greek', 'Chittagonian', 'Kazakh', 'Deccan', 'Hungarian', 'Kinyarwanda', 'Zulu', 'South Levantine Arabic', 'Tunisian Arabic', 'Sanaani Spoken Arabic', 'Min Bei Chinese (language family)', 'Southern Pashto', 'Rundi', 'Czech', 'Taʽizzi-Adeni Arabic', 'Uyghur', 'Min Dong Chinese (language family)', 'Sylheti ']

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
translation-language	text	Language of translation ['Mandarin (language family)', 'Spanish', 'English', 'Hindi', 'Bengali', 'Portuguese', 'Russian', 'Japanese', 'Western Punjabi', 'Marathi', 'Telugu', 'Wu (language family)', 'Turkish', 'Korean', 'French', 'German', 'Vietnamese', 'Tamil', 'Yue (language family)', 'Urdu', 'Javanese', 'Italian', 'Egyptian Arabic', 'Gujarati', 'Iranian Persian', 'Bhojpuri', 'Min Nan (language family)', 'Hakka', 'Jinyu', 'Hausa', 'Kannada', 'Indonesian (Indonesian Malay)', 'Polish', 'Yoruba', 'Xiang Chinese (language family)', 'Malayalam', 'Odia', 'Maithili', 'Burmese', 'Eastern Punjabi', 'Sunda', 'Sudanese Arabic', 'Algerian Arabic', 'Moroccan Arabic', 'Ukrainian', 'Igbo', 'Northern Uzbek', 'Sindhi', 'North Levantine Arabic', 'Romanian', 'Tagalog', 'Dutch', 'Saʽidi Arabic',	-	-

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
translation-service	text	translation service used for the translation ['Google Translate', 'Microsoft Translator', 'Babelfish', 'Reverso', 'Dict.cc', 'Linguee', 'unknown']	—	—
translation-type	text	type of translation ['Automated translation', 'Manual translation']	—	—

'Greek', 'Chittagonian', 'Kazakh', 'Deccan', 'Hungarian', 'Kinyarwanda', 'Zulu', 'South Levantine Arabic', 'Tunisian Arabic', 'Sanaani Spoken

trustar_report

TruStar Report.

trustar_report is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
BITCOIN_ADDRESS	btc	A bitcoin address is an identifier of 26-35 alphanumeric characters, beginning with the number 1 or 3, that represents a possible destination for a bitcoin payment.	—	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
CIDR_BLOCK	ip-src	CIDR (Classless Inter-Domain Routing) identifies a range of IP addresses, and was introduced as a way to allow more flexible allocation of Internet Protocol (IP) addresses than was possible with the original system of IP address classes.	−	✓
CVE	vulnerability	The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures.	−	✓
EMAIL_ADDRESS	email-src	An email address is a unique identifier for an email account.	−	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
IP	ip-dst	An Internet Protocol address (IP address) is a numerical label assigned to each device participating in a computer network that uses the Internet Protocol for communication.	−	✓
MALWARE	malware-type	Names of software that are intended to damage or disable computers and computer systems.	−	✓
MD5	md5	The MD5 algorithm is a widely used hash function producing a 128-bit hash value.	−	✓
REGISTRY_KEY	regkey	The registry is a hierarchical database that contains data that is critical for the operation of Windows and the applications and services that run on Windows.	−	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
SHA1	sha1	SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest - typically rendered as a hexadecimal number, 40 digits long. SHA-1 is prone to length extension attacks.	−	✓
SHA256	sha256	SHA-256 is a member of the SHA-2 cryptographic hash functions designed by the NSA, which are the successors to SHA-1. It is represented as a 64-character hexadecimal string.	−	✓
SOFTWARE	filename	The name of a file on a filesystem.	−	✓
URL	url	A Uniform Resource Locator (URL) is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.	−	✓

tsk-chats

An Object Template to gather information from evidential or interesting exchange of messages identified during a digital forensic investigation.

tsk-chats is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
Source	text	Source of the message.(Contact details)	✓	—
additional-comments	text	Comments.	✓	—
app-used	text	Application used to send the message.	✓	—
attachments	link	External references	—	✓
datetime-received	datetime	date and time when the message was received.	✓	✓
datetime-sent	datetime	date and the time when the message was sent.	✓	—
destination	text	Destination of the message.(Contact details)	✓	—
message	text	Message exchanged.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
message-type	text	the type of message extracted from the forensic-evidence. ['SMS', 'MMS', 'Instant Message (IM)', 'Voice Message']	✓	−
subject	text	Subject of the message if any.	−	−

tsk-web-bookmark

An Object Template to add evidential bookmarks identified during a digital forensic investigation.

tsk-web-bookmark is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
URL	link	The URL saved as bookmark.	−	−
additional-comments	text	Comments.	✓	−
browser	text	Browser used to access the URL. ['IE', 'Safari', 'Chrome', 'Firefox', 'Opera mini', 'Chromium']	✓	−
datetime-bookmarked	datetime	date and time when the URL was added to favorites.	✓	−
domain-ip	ip-src	IP of the URL domain.	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
domain-name	text	Domain of the URL.	−	−
name	text	Book mark name.	✓	−
title	text	Title of the web page	−	−

tsk-web-cookie

An TSK-Autopsy Object Template to represent cookies identified during a forensic investigation.

tsk-web-cookie is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
URL	link	The website URL that created the cookie.	−	−
additional-comments	text	Comments.	✓	−
browser	text	Browser on which the cookie was created. ['IE', 'Safari', 'Chrome', 'Firefox', 'Opera mini', 'Chromium']	−	−
datetime-created	datetime	date and time when the cookie was created.	✓	−
domain-ip	ip-src	IP of the domain that created the URL.	−	−
domain-name	text	Domain of the URL that created the cookie.	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
name	text	Name of the cookie	−	−
value	text	Value assigned to the cookie.	−	−

tsk-web-downloads

An Object Template to add web-downloads.

tsk-web-downloads is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
additional-comments	text	Comments.	✓	−
attachment	attachment	The downloaded file itself.	✓	−
datetime-accessed	datetime	date and time when the file was downloaded.	✓	−
name	text	Name of the file downloaded.	−	−
path-downloadedTo	text	Location the file was downloaded to.	−	−
pathID	text	Id of the attribute file where the information is gathered from.	✓	−
url	url	The URL used to download the file.	−	−

tsk-web-history

An Object Template to share web history information.

tsk-web-history is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
URL	link	The URL accessed.	−	−
additional-comments	text	Comments.	✓	−
browser	text	Browser used to access the URL. ['IE', 'Safari', 'Chrome', 'Firefox', 'Opera mini', 'Chromium']	✓	−
datetime-accessed	datetime	date and the time when the URL was accessed.	✓	−
domain-ip	ip-src	IP of the URL domain.	−	−
domain-name	text	Domain of the URL.	−	−
referrer	text	where the URL was referred from	✓	−
title	text	Title of the web page	−	−

tsk-web-search-query

An Object Template to share web search query information.

tsk-web-search-query is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
additional-comments	text	Comments.	✓	−
browser	text	Browser used. ['IE', 'Safari', 'Chrome', 'Firefox', 'Opera mini', 'Chromium']	✓	−
datetime-searched	datetime	date and time when the search was conducted.	✓	−
domain	link	The domain of the search engine. ['Google', 'Yahoo', 'Bing', 'Alta Vista', 'MSN']	✓	−
text	text	the search word or sentence.	−	−
username	text	User name or ID associated with the search.	✓	−

url

url object describes an url along with its normalized field (like extracted using faup parsing library) and its metadata.

url is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
credential	text	Credential (username, password)	−	−
domain	domain	Full domain	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
domain_without_tld	text	Domain without Top-Level Domain	−	−
first-seen	datetime	First time this URL has been seen	✓	−
fragment	text	Fragment identifier is a short string of characters that refers to a resource that is subordinate to another, primary resource.	−	✓
host	hostname	Full hostname	−	−
ip	ip-dst	Better type when the host is an IP.	−	−
last-seen	datetime	Last time this URL has been seen	✓	−
port	port	Port number	✓	−
query_string	text	Query (after path, preceded by '?')	−	✓
resource_path	text	Path (between hostname:port and query)	−	✓
scheme	text	Scheme ['http', 'https', 'ftp', 'gopher', 'sip']	✓	−
subdomain	text	Subdomain	✓	−
text	text	Description of the URL	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
tld	text	Top-Level Domain	✓	−
url	url	Full URL	−	−

user-account

.

ℹ user-account is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
account-type	text	Type of the account. ['facebook', 'ldap', 'nis', 'openid', 'radius', 'skype', 'tacacs', 'twitter', 'unix', 'windows-local', 'windows-domain']	−	−
can_escalate_privs	boolean	Specifies if the account has the ability to escalate privileges.	✓	−
created	datetime	Creation time of the account.	✓	−
disabled	boolean	Specifies if the account is desabled.	✓	−
display-name	text	Display name of the account.	−	−
expires	datetime	Expiration time of the account	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
first_login	datetime	First time someone logged in to the account.	✓	−
group	text	UNIX group(s) the account is member of.	✓	✓
group-id	text	Identifier of the primary group of the account, in case of a UNIX account.	✓	−
home_dir	text	Home directory of the UNIX account.	✓	−
is_service_account	boolean	Specifies if the account is associated with a network service.	✓	−
last_login	datetime	Last time someone logged in to the account.	✓	−
link	link	Original link into the account page (Supposed harmless)	−	−
password	text	Password related to the username.	−	−
password_last_changed	datetime	Last time the password has been changed.	✓	−
privileged	boolean	Specifies if the account has privileges such as root rights.	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
shell	text	UNIX command shell of the account.	✓	−
text	text	A description of the user account.	✓	−
user-avatar	attachment	A user profile picture or avatar.	−	✓
user-id	text	Identifier of the account.	−	−
username	text	Username related to the password.	−	−

vehicle

Vehicle object template to describe a vehicle information and registration.

vehicle is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
date-first-registration	text	Date of first registration	−	✓
description	text	Description of the vehicle	✓	−
dyno-power	text	Dyno power output	−	✓
exterior color	text	Exterior color of the vehicule	✓	−
gearbox	text	Gearbox	−	✓
image	attachment	Image of the vehicle.	−	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
image-url	text	Image URL	−	✓
indicative-value	text	Indicative value	−	✓
interior color	text	Interior color of the vehicule	✓	−
license-plate-number	text	License plate number	−	✓
make	text	Manufacturer of the vehicle	✓	−
model	text	Model of the vehicle	✓	−
state	text	State of the vehicule (stolen or recovered)	✓	−
type	text	Type of the vehicule ['car', 'bus', 'caravan', 'bicycle', 'boat', 'taxi', 'camper van', 'motorcycle', 'truck', 'scooter', 'tractor', 'trailer', 'van']	✓	−
vin	text	Vehicle identification number (VIN)	−	−

victim

Victim object describes the target of an attack or abuse.

victim is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
classification	text	The type of entity being targeted. ['individual', 'group', 'organization', 'class', 'unknown']	✓	−
description	text	Description of the victim	−	−
domain	domain	Domain name of the organisation targeted.	−	✓
email	target-email	The email address(es) of the user targeted.	−	✓
external	target-external	External target organisations affected by this attack.	−	✓
ip-address	ip-dst	IP address(es) of the node targeted.	−	✓
name	target-org	The name of the department(s) or organisation(s) targeted.	−	✓
node	target-machine	Name(s) of node that was targeted.	−	✓
reference	text	External reference to the victim/case.	−	✓
regions	target-location	The list of regions or locations from the victim targeted. ISO 3166 should be used.	−	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
roles	text	The list of roles targeted within the victim.	−	✓
sectors	text	The list of sectors that the victim belong to ['agriculture', 'aerospace', 'automotive', 'communications', 'construction', 'defence', 'education', 'energy', 'engineering', 'entertainment', 'financial services', 'government national', 'government regional', 'government local', 'government public services', 'healthcare', 'hospitality leisure', 'infrastructure', 'insurance', 'manufacturing', 'mining', 'non profit', 'pharmaceuticals', 'retail', 'technology', 'telecommunications', 'transportation', 'utilities']	−	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
user	target-user	The username(s) of the user targeted.	—	✓

virustotal-graph

VirusTotal graph.

virustotal-graph is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
access	text	Access to the VirusTotal graph ['Private', 'Public']	✓	—
comment	text	Comment related to this VirusTotal graph	✓	✓
permalink	link	Permalink Reference to the VirusTotal graph	—	—
screenshot	attachment	Screenshot of the VirusTotal graph	✓	—

virustotal-report

VirusTotal report.

virustotal-report is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
comment	text	Comment related to this hash	—	✓
community-score	text	Community Score	✓	—
detection-ratio	text	Detection Ratio	✓	—
first-submission	datetime	First Submission	—	—
last-submission	datetime	Last Submission	—	—
permalink	link	Permalink Reference	—	—

vulnerability

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

ℹ vulnerability is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
created	datetime	First time when the vulnerability was discovered	✓	—
credit	text	Who reported/found the vulnerability such as an organisation, person or nickname.	✓	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
cvss-score	float	Score of the Common Vulnerability Scoring System (version 3).	✓	−
cvss-string	text	String of the Common Vulnerability Scoring System (version 3).	✓	−
description	text	Description of the vulnerability	−	−
id	text	Vulnerability ID (generally CVE, but not necessarely). The id is not required as the object itself has an UUID and the CVE id can be update or assigned later.	−	✓
modified	datetime	Last modification date	✓	−
published	datetime	Initial publication date	✓	−
references	link	External references	−	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
state	text	State of the vulnerability. A vulnerability can have multiple states depending of the current actions performed. ['Published', 'Embargo', 'Reviewed', 'Vulnerability ID Assigned', 'Reported', 'Fixed']	✓	✓
summary	text	Summary of the vulnerability	−	−
vulnerable-configuration	text	The vulnerable configuration is described in CPE format	−	✓

weakness

Weakness object describing a common weakness enumeration which can describe usable, incomplete, draft or deprecated weakness for software, equipment of hardware.

weakness is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
description	text	Description of the weakness.	−	−
id	text	Weakness ID (generally CWE).	−	−
name	text	Name of the weakness.	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
status	text	Status of the weakness. ['Incomplete', 'Deprecated', 'Draft', 'Usable']	✓	−
weakness-abs	text	Abstraction of the weakness. ['Class', 'Base', 'Variant']	✓	−

whois

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

whois is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
comment	text	Comment of the whois entry	−	−
creation-date	datetime	Initial creation of the whois entry	✓	−
domain	domain	Domain of the whois entry	−	✓
expiration-date	datetime	Expiration of the whois entry	✓	−
ip-address	ip-src	IP address of the whois entry	−	✓
modification-date	datetime	Last update of the whois entry	✓	−
nameserver	hostname	Nameserver	✓	✓
registrant-email	whois-registrant-email	Registrant email address	−	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
registrant-name	whois-registrant-name	Registrant name	−	−
registrant-org	whois-registrant-org	Registrant organisation	−	−
registrant-phone	whois-registrant-phone	Registrant phone number	−	−
registrar	whois-registrar	Registrar of the whois entry	−	−
text	text	Full whois entry	✓	−

x509

x509 object describing a X.509 certificate.

x509 is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
dns_names	hostname	Subject Alternative Name - DNS names	−	✓
email	email-dst	Subject Alternative Name - emails	−	✓
ip	ip-dst	Subject Alternative Name - IP	−	✓
is_ca	boolean	CA certificate	✓	−
issuer	text	Issuer of the certificate	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
pem	text	Raw certificate in PEM formati (Unix-like newlines)	−	−
pubkey-info-algorithm	text	Algorithm of the public key	✓	−
pubkey-info-exponent	text	Exponent of the public key - in decimal	−	−
pubkey-info-modulus	text	Modulus of the public key - in Hexadecimal - no 0x, no :	−	−
pubkey-info-size	text	Length of the public key (in bits expressed in decimal: eg. 256 bits)	✓	−
raw-base64	text	Raw certificate base64 encoded (DER format)	−	−
rid	text	Subject Alternative Name - RID	−	✓
self_signed	boolean	Self-signed certificate	✓	−
serial-number	text	Serial number of the certificate	−	−
signature_algorithm	text	Signature algorithm ['SHA1_WITH_RSA_ENCRYPTION', 'SHA256_WITH_RSA_ENCRYPTION']	✓	−

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
subject	text	Subject of the certificate	−	−
text	text	Free text description of the certificate	−	−
uri	uri	Subject Alternative Name - URI	−	✓
validity-not-after	datetime	Certificate invalid after that date	✓	−
validity-not-before	datetime	Certificate invalid before that date	✓	−
version	text	Version of the certificate	✓	−
x509-fingerprint-md5	x509-fingerprint-md5	[Insecure] MD5 hash (128 bits)	−	−
x509-fingerprint-sha1	x509-fingerprint-sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	−	−
x509-fingerprint-sha256	x509-fingerprint-sha256	Secure Hash Algorithm 2 (256 bits)	−	−

yabin

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

yabin is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
comment	comment	A description of Yara rule generated.	—	—
version	comment	yabin.py and regex.txt version used for the generation of the yara rules.	—	—
whitelist	comment	Whitelist name used to generate the rules.	—	—
yara	yara	Yara rule generated from -y.	✓	—
yara-hunt	yara	Wide yara rule generated from -yh.	✓	—

yara

An object describing a YARA rule (or a YARA rule name) along with its version.

yara is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
comment	comment	A description of the YARA rule.	—	—
context	text	Context where the YARA rule can be applied ['all', 'disk', 'memory', 'network']	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
version	text	Version of the YARA rule depending where the yara rule is known to work as expected. ['3.7.1']	−	−
yara	yara	YARA rule.	−	−
yara-rule-name	text	YARA rule name.	−	−

Relationships

Default type of relationships in MISP objects.

Relationships are part of MISP object and available in JSON format at this location. The JSON format can be freely reused in your application or automatically enabled in MISP.

Name of relationship	Description	Format
derived-from	The information in the target object is based on information from the source object.	['misp', 'stix-2.0', 'alfred']
executes	This relationship describes an object which executes another object	['misp']
duplicate-of	The referenced source and target objects are semantically duplicates of each other.	['misp', 'stix-2.0']
related-to	The referenced source is related to the target object.	['misp', 'stix-2.0', 'alfred']
connected-to	The referenced source is connected to the target object.	['misp', 'stix-1.1']
connected-from	The referenced source is connected from the target object.	['misp', 'stix-1.1']
contains	The referenced source is containing the target object.	['misp', 'stix-1.1', 'alfred']
contained-by	The referenced source is contained by the target object.	['misp', 'stix-1.1']
contained-within	The referenced source is contained within the target object.	['misp', 'stix-1.1']

Name of relationship	Description	Format
characterized-by	The referenced source is characterized by the target object.	['misp', 'stix-1.1']
characterizes	The referenced source is characterizing the target object.	['misp', 'stix-1.1']
properties-queried	The referenced source has queried the target object.	['misp', 'stix-1.1']
properties-queried-by	The referenced source is queried by the target object.	['misp', 'stix-1.1']
extracted-from	The referenced source is extracted from the target object.	['misp', 'stix-1.1']
supra-domain-of	The referenced source is a supra domain of the target object.	['misp', 'stix-1.1']
sub-domain-of	The referenced source is a sub domain of the target object.	['misp', 'stix-1.1']
dropped	The referenced source has dropped the target object.	['misp', 'stix-1.1']
dropped-by	The referenced source is dropped by the target object.	['misp', 'stix-1.1']
downloaded	The referenced source has downloaded the target object.	['misp', 'stix-1.1']
downloaded-from	The referenced source has been downloaded from the target object.	['misp', 'stix-1.1']
resolved-to	The referenced source is resolved to the target object.	['misp', 'stix-1.1']
attributed-to	This referenced source is attributed to the target object.	['misp', 'stix-2.0']
targets	This relationship describes that the source object targets the target object.	['misp', 'stix-2.0']
uses	This relationship describes the use by the source object of the target object.	['misp', 'stix-2.0', 'alfred']
indicates	This relationship describes that the source object indicates the target object.	['misp', 'stix-2.0']
mentions	This relationship describes that the source object mentions the target object.	['misp']
mitigates	This relationship describes a source object which mitigates the target object.	['misp', 'stix-2.0']

Name of relationship	Description	Format
variant-of	This relationship describes a source object which is a variant of the target object	['misp', 'stix-2.0', 'alfred']
impersonates	This relationship describes a source object which impersonates the target object	['misp', 'stix-2.0']
retrieved-from	This relationship describes an object retrieved from the target object.	['misp']
authored-by	This relationship describes the author of a specific object.	['misp']
is-author-of	This relationship describes an object being author by someone.	['misp']
located	This relationship describes the location (of any type) of a specific object.	['misp']
included-in	This relationship describes an object included in another object.	['misp']
includes	This relationship describes an object that includes an other object.	['misp']
analysed-with	This relationship describes an object analysed by another object.	['misp']
claimed-by	This relationship describes an object claimed by another object.	['misp']
communicates-with	This relationship describes an object communicating with another object.	['misp']
drops	This relationship describes an object which drops another object	['misp']
executed-by	This relationship describes an object executed by another object.	['misp']
affects	This relationship describes an object affected by another object.	['misp', 'alfred']
beacons-to	This relationship describes an object beaconing to another object.	['misp', 'alfred']

Name of relationship	Description	Format
abuses	This relationship describes an object which abuses another object.	['misp']
exfiltrates-to	This relationship describes an object exfiltrating to another object.	['misp', 'alfred']
identifies	This relationship describes an object which identifies another object.	['misp', 'alfred']
intercepts	This relationship describes an object which intercepts another object.	['misp', 'alfred']
calls	This relationship describes an object which calls another objects.	['misp']
detected-as	This relationship describes an object which is detected as another object.	['misp']
followed-by	This relationship describes an object which is followed by another object. This can be used when a time reference is missing but a sequence is known.	['misp']
preceding-by	This relationship describes an object which is preceded by another object. This can be used when a time reference is missing but a sequence is known.	['misp']
triggers	This relationship describes an object which triggers another object.	['misp']
vulnerability-of	This relationship describes an object which is a vulnerability of another object.	['cert-eu']
works-like	This relationship describes an object which works like another object.	['cert-eu']
seller-of	This relationship describes an object which is selling another object.	['cert-eu']
seller-on	This relationship describes an object which is selling on another object.	['cert-eu']

Name of relationship	Description	Format
trying-to-obtain-the-exploit	This relationship describes an object which is trying to obtain the exploit described by another object	['cert-eu']
used-by	This relationship describes an object which is used by another object.	['cert-eu']
affiliated	This relationship describes an object which is affiliated with another object.	['cert-eu']
alleged-founder-of	This relationship describes an object which is the alleged founder of another object.	['cert-eu']
attacking-other-group	This relationship describes an object which attacks another object.	['cert-eu']
belongs-to	This relationship describes an object which belongs to another object.	['cert-eu']
business-relations	This relationship describes an object which has business relations with another object.	['cert-eu']
claims-to-be-the-founder-of	This relationship describes an object which claims to be the founder of another object.	['cert-eu']
cooperates-with	This relationship describes an object which cooperates with another object.	['cert-eu']
former-member-of	This relationship describes an object which is a former member of another object.	['cert-eu']
successor-of	This relationship describes an object which is a successor of another object.	['cert-eu']
has-joined	This relationship describes an object which has joined another object.	['cert-eu']
member-of	This relationship describes an object which is a member of another object.	['cert-eu']
primary-member-of	This relationship describes an object which is a primary member of another object.	['cert-eu']

Name of relationship	Description	Format
administrator-of	This relationship describes an object which is an administrator of another object.	['cert-eu']
is-in-relation-with	This relationship describes an object which is in relation with another object,	['cert-eu']
provide-support-to	This relationship describes an object which provides support to another object.	['cert-eu']
regional-branch	This relationship describes an object which is a regional branch of another object.	['cert-eu']
similar	This relationship describes an object which is similar to another object.	['cert-eu']
subgroup	This relationship describes an object which is a subgroup of another object.	['cert-eu']
suspected-link	This relationship describes an object which is suspected to be linked with another object.	['misp']
same-as	This relationship describes an object which is the same as another object.	['misp']
creator-of	This relationship describes an object which is the creator of another object.	['cert-eu']
developer-of	This relationship describes an object which is a developer of another object.	['cert-eu']
uses-for-recon	This relationship describes an object which uses another object for recon.	['cert-eu']
operator-of	This relationship describes an object which is an operator of another object.	['cert-eu']
overlaps	This relationship describes an object which overlaps another object.	['cert-eu']
owner-of	This relationship describes an object which owns another object.	['cert-eu', 'alfred']
publishes-method-for	This relationship describes an object which publishes method for another object.	['cert-eu']

Name of relationship	Description	Format
recommends-use-of	This relationship describes an object which recommends the use of another object.	['cert-eu']
released-source-code	This relationship describes an object which released source code of another object.	['cert-eu']
released	This relationship describes an object which release another object.	['cert-eu']
exploits	This relationship describes an object (like a PoC/exploit) which exploits another object (such as a vulnerability object).	['misp']
signed-by	This relationship describes an object signed by another object.	['misp']
delivered-by	This relationship describes an object by another object (such as exploit kit, dropper).	['misp']
controls	This relationship describes an object which controls another object.	['misp']
annotates	This relationships describes an object which annotates another object.	['misp']
references	This relationships describes an object which references another object or attribute.	['misp']
child-of	A child semantic link to a parent.	['alfred']
compromised	Represents the semantic link of having compromised something.	['alfred']
connects	The initiator of a connection.	['alfred']
connects-to	The destination or target of a connection.	['alfred']
cover-term-for	Represents the semantic link of one thing being the cover term for another.	['alfred']
disclosed-to	Semantic link indicating where information is disclosed to.	['alfred']
downloads	Represents the semantic link of one thing downloading another.	['alfred']

Name of relationship	Description	Format
downloads-from	Represents the semantic link of malware being downloaded from a location.	['alfred']
generated	Represents the semantic link of an alert generated from a signature.	['alfred']
implements	One data object implements another.	['alfred']
initiates	Represents the semantic link of a communication initiating an event.	['alfred']
instance-of	Represents the semantic link between a FILE and FILE_BINARY.	['alfred']
issuer-of	Represents the semantic link of being the issuer of something.	['alfred']
linked-to	Represents the semantic link of being associated with something.	['alfred']
not-relevant-to	Represents the semantic link of a comm that is not relevant to an EVENT.	['alfred']
part-of	Represents the semantic link that defines one thing to be part of another in a hierachial structure from the child to the parent.	['alfred']
processed-by	Represents the semantic link of something has been processed by another program.	['alfred']
produced	Represents the semantic link of something having produced something else.	['alfred']
queried-for	The IP Address or domain being queried for.	['alfred']
query-returned	The IP Address or domain returned as the result of a query.	['alfred']
registered	Represents the semantic link of someone registered some thing.	['alfred']
registered-to	Represents the semantic link of something being registered to.	['alfred']

Name of relationship	Description	Format
relates	Represents the semantic link between HBS Comms and communication addresses.	['alfred']
relevant-to	Represents the semantic link of a comm that is relevant to an EVENT.	['alfred']
resolves-to	Represents the semantic link of resolving to something.	['alfred']
responsible-for	Represents the semantic link of some entity being responsible for something.	['alfred']
seeded	Represents the semantic link of a seeded domain redirecting to another site.	['alfred']
sends	A sends semantic link meaning 'who sends what'.	['alfred']
sends-as-bcc-to	A sends to as BCC semantic link meaning 'what sends to who as BCC'.	['alfred']
sends-as-cc-to	A sends to as CC semantic link meaning 'what sends to who as CC'.	['alfred']
sends-to	A sends to semantic link meaning 'what sends to who'.	['alfred']
spoofer-of	The represents the semantic link of having spoofed something.	['alfred']
subdomain-of	Represents a domain being a subdomain of another.	['alfred']
supersedes	One data object supersedes another.	['alfred']
triggered-on	Represents the semantic link of an alert triggered on an event.	['alfred']
uploads	Represents the semantic link of one thing uploading another.	['alfred']
user-of	The represents the semantic link of being the user of something.	['alfred']
works-for	Represents the semantic link of working for something.	['alfred']
witness-of	Represents an object being a witness of something.	['misp']
injects-into	Represents an object injecting something into something	['misp']

Name of relationship	Description	Format
injected-into	Represents an object which is injected something into something	['misp']
creates	Represents an object that creates something.	['misp', 'haxpak']
screenshot-of	Represents an object being the screenshot of something.	['misp']
knows	Represents an object having the knowledge of another object.	['misp']