

MISP Objects

MISP Objects

Introduction	1
Funding and Support	2
MISP objects	3
tsk-chats	3
tsk-web-bookmark	4
tsk-web-cookie	5
tsk-web-downloads	6
tsk-web-history	7
tsk-web-search-query	7
ail-leak	8
ais-info	10
android-permission	12
annotation	15
asn	16
av-signature	18
bank-account	19
bgp-hijack	23
cap-alert	23
cap-info	28
cap-resource	31
coin-address	32
cookie	34
cortex	35
cortex-taxonomy	36
course-of-action	36
cowrie	38
credential	40
credit-card	41
ddos	42
diameter-attack	43
domain-ip	45
elf	45
elf-section	48
email	51
exploit-poc	53
fail2ban	53
file	54
forensic-case	57

forensic-evidence	57
geolocation	59
gtp-attack	61
http-request	63
internal-reference	64
ip-api-address	65
ip-port	66
ja3	67
legal-entity	68
macho	68
macho-section	69
mactime-timeline-analysis	71
malware-config	71
microblog	72
mutex	74
netflow	74
network-connection	76
network-socket	77
original-imported-file	81
passive-dns	81
paste	83
pcap-metadata	85
pe	87
pe-section	89
person	90
phishing	93
phone	94
process	97
python-etvx-event-log	99
r2graphity	101
regexp	104
registry-key	105
regripper-NTUser	107
regripper-sam-hive-single-user	109
regripper-sam-hive-user-group	110
regripper-software-hive-BHO	111
regripper-software-hive-appInit-DLLS	112
regripper-software-hive-application-paths	113
regripper-software-hive-applications-installed	114
regripper-software-hive-command-shell	115
regripper-software-hive-windows-general-info	115

regripper-software-hive-software-run	117
regripper-software-hive-userprofile-winlogon	118
regripper-system-hive-firewall-configuration	121
regripper-system-hive-general-configuration	122
regripper-system-hive-network-information.	124
regripper-system-hive-services-drivers	126
report	128
rtir	129
sandbox-report	130
sb-signature	131
script	132
short-message-service	133
shortened-link	134
ss7-attack	134
stix2-pattern	137
suricata	138
target-system	138
threatgrid-report	139
timecode	139
timesketch-timeline	140
timesketch_message	141
timestamp	141
tor-node	142
tracking-id	144
transaction	144
url	146
vehicle	148
victim	149
virustotal-report	151
vulnerability	152
whois	153
x509	154
yabin	156
yara	157
Relationships	157

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](#).



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

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
message-type	text	the type of message extracted from the forensic-evidence. ['SMS', 'MMS', 'Instant Message (IM)', 'Voice Message']	✓	—
datetime-sent	datetime	date and the time when the message was sent.	✓	—
datetime-received	datetime	date and time when the message was received.	✓	✓
Source	text	Source of the message.(Contact details)	✓	—
destination	text	Destination of the message.(Contact details)	✓	—
app-used	text	Application used to send the message.	✓	—
subject	text	Subject of the message if any.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
message	text	Message exchanged.	—	—
attachments	link	External references	—	✓
additional-comments	text	Comments.	✓	—

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.	—	—
datetime-bookmarked	datetime	date and time when the URL was added to favorites.	✓	—
name	text	Book mark name.	✓	—
title	text	Title of the web page	—	—
browser	text	Browser used to access the URL. ['IE', 'Safari', 'Chrome', 'Firefox', 'Opera mini', 'Chromium']	✓	—
domain-name	text	Domain of the URL.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
domain-ip	ip-src	IP of the URL domain.	—	—
additional-comments	text	Comments.	✓	—

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.	—	—
datetime-created	datetime	date and time when the cookie was created.	✓	—
name	text	Name of the cookie	—	—
value	text	Value assigned to the cookie.	—	—
browser	text	Browser on which the cookie was created. ['IE', 'Safari', 'Chrome', 'Firefox', 'Opera mini', 'Chromium']	—	—
domain-name	text	Domain of the URL that created the cookie.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
domain-ip	ip-src	IP of the domain that created the URL.	—	—
additional-comments	text	Comments.	✓	—

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
url	url	The URL used to download the file.	—	—
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.	✓	—
attachment	attachment	The downloaded file itself.	✓	—
additional-comments	text	Comments.	✓	—

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.	—	—
datetime-accessed	datetime	date and the time when the URL was accessed.	✓	—
referrer	text	where the URL was referred from	✓	—
title	text	Title of the web page	—	—
domain-name	text	Domain of the URL.	—	—
domain-ip	ip-src	IP of the URL domain.	—	—
browser	text	Browser used to access the URL. ['IE', 'Safari', 'Chrome', 'Firefox', 'Opera mini', 'Chromium']	✓	—
additional-comments	text	Comments.	✓	—

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

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
sensor	text	The AIL sensor uuid where the leak was processed and analysed.	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
duplicate	text	Duplicate of the existing leaks.	–	✓
duplicate_number	counter	Number of known duplicates.	✓	–
origin	text	The link where the leak is (or was) accessible at first-seen.	–	–
text	text	A description of the leak which could include the potential victim(s) or description of the leak.	✓	–
original-date	datetime	When the information available in the leak was created. It's usually before the first-seen.	✓	–
last-seen	datetime	When the leak has been accessible or seen for the last time.	✓	–
first-seen	datetime	When the leak has been accessible or seen for the first time.	✓	–
raw-data	attachment	Raw data as received by the AIL sensor compressed and encoded in Base64.	✓	–

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
organisation	text	AIS Organisation Name.	—	—
administrative-area	text	AIS Administrative Area represented using ISO-3166-2.	—	—

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']	-	✓
country	text	AIS Country represented using ISO-3166-1_alpha-2.	-	-

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
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_SERVICE',	-	✓
14		'BIND_NFC_SERVICE'		

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

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](#).

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
text	text	Raw text of the annotation	—	—
ref	link	Reference(s) to the annotation	—	✓
type	text	Type of the annotation ['Annotation', 'Executive Summary', 'Introduction', 'Conclusion', 'Disclaimer', 'Keywords', 'Acknowledgement', 'Other', 'Copyright', 'Authors', 'Logo']	✓	—

'BIND_PRINT_SERVICE',
'BIND_QUICK_SETTINGS_TILE',
'BIND_REMOTEVIEW',
'BIND_SCREENING_SERVICE',
'BIND_TELECOM_CONNECTIONS'

'BROADCAST_SMS',
'BROADCAST_STICKY',
'BROADCAST_WAP_PUSH',
'CALL_PHONE',
'CALL_PRIVILEGED',
'CAMERA',
'CAPTURE_AUDIO_OUTPUT',
'CAPTURE_SECURE'

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
format	text	Format of the annotation ['text', 'markdown', 'asciidoc', 'MultiMarkdown', 'GFM', 'pandoc', 'Fountain', 'CommonWork', 'kramdown-rfc2629', 'rfc7328', 'Extra']	✓	—
creation-date	datetime	Initial creation of the annotation	—	—
modification-date	datetime	Last update of the annotation	—	—

asn

Autonomous system object describing an autonomous system which can include one or more network operators management an entity (as BGP) 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, automatically enabled in [MISP](#).

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
asn	AS	Autonomous System Number	—	—
description	text	Description of the autonomous system	—	—
country	text	Country code of the main location of the autonomous system	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
subnet-announced	ip-src	Subnet announced	–	✓
first-seen	datetime	First time the ASN was seen	✓	–
last-seen	datetime	Last time the ASN was seen	✓	–
import	text	The inbound IPv4 routing policy of the AS in RFC 2622 – Routing Policy Specification Language (RPSL) format	–	✓
export	text	The outbound routing policy of the AS in RFC 2622 – Routing Policy Specification Language (RPSL) 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	–	✓

'READ_PHONE_STATE', 'READ_SMS', 'READ_SYNC_SETTINGS', 'READ_SYNC_STATISTICS', 'READ_VOICEMAIL', 'REBOOT', 'RECEIVE_BOOT_COMPLETED', 'RECEIVE_MMS', 'RECEIVE_SMS',

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
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	–	✓

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
software	text	Name of antivirus software	✓	–
signature	text	Name of detection signature	–	–
text	text	Free text value to attach to the file	✓	–
datetime	datetime	Datetime	✓	–

VIA_MESSAGE',
'SEND_SMS',
'SET_ALARM',
'SET_ALWAYS_FINISH',
'SET_ANIMATION_SCALE',
'SET_DEBUG_APP',
'SET_PREFERRED'

TRANSMIT_IK,
'UNINSTALL_SHOW_RTCUT',
'UPDATE_DEVICE_STATS',

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
text	text	A description of the bank account.	✓	—
institution-name	text	Name of the bank or financial organisation.	✓	—
institution-code	text	Institution code of the bank.	✓	—
swift	bic	SWIFT or BIC as defined in ISO 9362.	✓	—
branch	text	Branch code or name	✓	—
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.	✓	—
account	bank-account-nr	Account number	—	—
currency-code	text	Currency of the account. ['USD', 'EUR']	✓	—
aba-rtn	aba-rtn	ABA routing transit number	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
account-name	text	A field to freely describe the bank account details.	—	—
iban	iban	IBAN of the bank account.	—	—
client-number	text	Client number as seen by the bank.	—	—
personal-account-type	text	Account type. ['A - Business', 'B - Personal Current', 'C - Savings', 'D - Trust Account', 'E - Trading Account', 'O - Other']	✓	—
opened	datetime	When the account was opened.	✓	—
closed	datetime	When the account was closed.	✓	—
balance	text	The balance of the account after the suspicious transaction was processed.	✓	—
date-balance	datetime	When the balance was reported.	✓	—
status-code	text	Account status at the time of the transaction processed. ['A - Active', 'B - Inactive', 'C - Dormant']	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
beneficiary	text	Final beneficiary of the bank account.	✓	—
beneficiary-comment	text	Comment about the final beneficiary.	✓	—
comments	text	Comments about the bank account.	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
report-code	text	<p>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']</p>	✓	–

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
expected-asn	AS	Expected Autonomous System Number	—	—
detected-asn	AS	Detected Autonomous System Number	—	—
description	text	BGP Hijack details	—	—
country	text	Country code of the main location of the attacking autonomous system	—	—
subnet-announced	ip-src	Subnet announced	—	✓
start	datetime	First time the Prefix hijack was seen	✓	—
end	datetime	Last time the Prefix hijack was seen	✓	—

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
identifier	text	The identifier of the alert message in a number or string uniquely identifying this message, assigned by the sender.	✓	—
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.	✓	—
status	text	The code denoting the appropriate handling of the alert message. ['Actual', 'Exercise', 'System', 'Test', 'Draft']	—	—
msgType	text	The code denoting the nature of the alert message. ['Alert', 'Update', 'Cancel', 'Ack', 'Error']	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
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.	✓	-
scope	text	The code denoting the intended distribution of the alert message. ['Public', 'Restricted', 'Private']	✓	-
restriction	text	The text describing the rule for limiting distribution of the restricted alert message.	✓	-

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
addresses	text	<p>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.</p>	✓	-
code	text	<p>The code denoting the special handling of the alert message.</p>	✓	-
note	text	<p>The text describing the purpose or significance of the alert message.</p>	✓	-

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
references	text	<p>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.</p>	✓	-
incident	text	<p>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.</p>	✓	-

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
language	text	The code denoting the language of the info sub-element 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']	✓	—
event	text	The text denoting the type of the subject event of 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']	✓	—

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']	✓	—
severity	text	The code denoting the severity of the subject event of the alert message. ['Extreme', 'Severe', 'Moderate', 'Minor', 'Unknown']	✓	—
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']	✓	—
audience	text	The text describing the intended audience of the alert message.	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
eventCode	text	A system-specific code identifying the event type of the alert message.	✓	—
effective	datetime	The effective time of the information of the alert message.	✓	—
onset	datetime	The expected time of the beginning of the subject event of the alert message.	✓	—
expires	datetime	The expiry time of the information of the alert message.	✓	—
senderName	text	The text naming the originator of the alert message.	✓	—
headline	text	The text headline of the alert message.	✓	—
description	text	The text describing the subject event of the alert message.	✓	—
instruction	text	The text describing the recommended action to be taken by recipients of the alert message.	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
web	link	The identifier of the hyperlink associating additional information with the alert message.	✓	—
contact	text	The text describing the contact for follow-up and confirmation of the alert message.	✓	—
parameter	text	A system-specific additional parameter associated 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
resourceDesc	text	The text describing the type and content of the resource file.	✓	—
contentType	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
size	text	The integer indicating the size of the resource file.	✓	—
uri	link	The identifier of the hyperlink for the resource file.	—	—
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).	—	—

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	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
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']	✓	—
last-seen	datetime	Last time this payment destination address has been seen	✓	—
first-seen	datetime	First time this payment destination address has been seen	✓	—
last-updated	datetime	Last time the balances and totals have been updated	✓	—
current-balance	float	Current balance of address	✓	—
total-transactions	text	Total transactions performed	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
total-received	float	Total balance received	✓	—
total-sent	float	Total balance sent	✓	—
text	text	Free text value	✓	—

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)	—	—
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
summary	text	Cortex summary object (summary) in JSON	—	—
full	text	Cortex report object (full report) in JSON	✓	—
start-date	datetime	When the Cortex analyser was started	✓	—
name	text	Cortex analyser/worker name	✓	—
server-name	text	Name of the cortex server	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
success	boolean	Result of the cortex job	✓	—

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
namespace	text	Cortex Taxonomy Namespace	✓	—
predicate	text	Cortex Taxonomy Predicate	✓	—
value	text	Cortex Taxonomy Value	✓	—
level	text	Cortex Taxonomy Level ['info', 'safe', 'suspicious', 'malicious']	✓	—
cortex_url	link	URL to the Cortex job	✓	—

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
name	text	The name used to identify the course of action.	✓	—
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']	✓	—
description	text	A description of the course of action.	✓	—
objective	text	The objective of the course of action.	✓	—
stage	text	The stage of the threat management lifecycle that the course of action is applicable to. ['Remedy', 'Response']	✓	—

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']	✓	—
impact	text	The estimated impact of applying the course of action. ['High', 'Medium', 'Low', 'None', 'Unknown']	✓	—
efficacy	text	The estimated efficacy of applying the course of action. ['High', 'Medium', 'Low', 'None', 'Unknown']	✓	—

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
eventid	text	Eventid of the session in the cowrie honeypot	✓	—
system	text	System origin in cowrie honeypot	✓	—
username	text	Username related to the password(s)	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
password	text	Password	—	✓
session	text	Session id	—	—
timestamp	datetime	When the event happened	✓	—
message	text	Message of the cowrie honeypot	✓	—
protocol	text	Protocol used in the cowrie honeypot	✓	—
sensor	text	Cowrie sensor name	✓	—
src_ip	ip-src	Source IP address of the session	—	—
dst_ip	ip-dst	Destination IP address of the session	✓	—
src_port	port	Source port of the session	✓	—
dst_port	port	Destination port of the session	✓	—
isError	text	isError	✓	—
input	text	Input of the session	—	—
macCS	text	SSH MAC supported in the session	✓	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
keyAlgs	text	SSH public-key algorithm supported in the session	✓	✓
encCS	text	SSH symmetric encryption algorithm supported in the session	✓	✓
compCS	text	SSH compression algorithm supported in the session	✓	✓

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
text	text	A description of the credential(s)	✓	—
username	text	Username related to the password(s)	—	—
password	text	Password	—	✓
type	text	Type of password(s) ['password', 'api-key', 'encryption-key', 'unknown']	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
origin	text	Origin of the credential(s) ['bruteforce-scanning', 'malware-analysis', 'memory-analysis', 'network-analysis', 'leak', 'unknown']	—	—
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']	—	✓

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
version	text	Version of the card.	—	—
comment	comment	A description of the card.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
card-security-code	text	Card security code (CSC, CVD, CVV, CVC and SPC) as embossed or printed on the card.	—	—
name	text	Name of the card owner.	—	—
issued	datetime	Initial date of validity or issued date.	—	—
expiration	datetime	Maximum date of validity	—	—
cc-number	cc-number	credit-card number as encoded on the card.	—	—

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
total-bps	counter	Bits per second	—	—
text	text	Description of the DDoS	✓	—
domain-dst	domain	Destination domain (victim)	—	—

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

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
category	text	Category. ['Cat0', 'Cat1', 'Cat2', 'Cat3', 'CatSMS']	✓	—

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.	—	—
SessionId	text	Session-ID.	—	—
CmdCode	text	A decimal representation of the diameter Command Code.	✓	—
Origin-Host	text	Origin-Host.	—	✓
Destination-Host	text	Destination-Host.	—	✓
Origin-Realm	text	Origin-Realm.	—	✓
Destination-Realm	text	Destination-Realm.	—	✓
Username	text	Username (in this case, usually the IMSI).	—	✓
IdrFlags	text	IDR-Flags.	✓	—
text	text	A description of the attack seen.	✓	—
first-seen	datetime	When the attack has been seen for the first time.	✓	—

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
text	text	A description of the tuple	✓	—
last-seen	datetime	Last time the tuple has been seen	✓	—
first-seen	datetime	First time the tuple has been seen	✓	—
domain	domain	Domain name	—	✓
ip	ip-dst	IP Address	—	✓

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
entrypoint-address	text	Address of the entry point	✓	—
type	text	Type of ELF ['CORE', 'DYNAMIC', 'EXECUTABLE', 'HIPROC', 'LOPROC', 'NONE', 'RELOCATABLE']	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
number-sections	counter	Number of sections	✓	-

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
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	✓	—

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
md5	md5	[Insecure] MD5 hash (128 bits)	—	—
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)	—	—
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	—	—
entropy	float	Entropy of the whole section	✓	—
name	text	Name of the section	✓	—
size-in-bytes	size-in-bytes	Size of the section, in bytes	✓	—
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']	✓	-

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
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']	✓	✓

email

Email object describing an email with meta-information.



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
reply-to	email-reply-to	Email address the reply will be sent to	—	—
message-id	email-message-id	Message ID	✓	—
to	email-dst	Destination email address	✓	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
cc	email-dst	Carbon copy	✓	✓
to-display-name	email-dst-display-name	Display name of the receiver	—	✓
subject	email-subject	Subject	—	—
screenshot	attachment	Screenshot of email	✓	—
attachment	email-attachment	Attachment	—	✓
x-mailer	email-x-mailer	X-Mailer generally tells the program that was used to draft and send the original email	✓	—
header	email-header	Full headers	✓	✓
send-date	datetime	Date the email has been sent	✓	—
mime-boundary	email-mime-boundary	MIME Boundary	✓	—
thread-index	email-thread-index	Identifies a particular conversation thread	✓	—
from	email-src	Sender email address	—	—
return-path	email-src	Message return path	—	—
from-display-name	email-src-display-name	Display name of the sender	—	—
email-body	email-body	Body of the email	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
user-agent	text	User Agent of the sender	✓	—
eml	attachment	Full EML	✓	—

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
description	text	Description of the exploit - proof of concept	—	—
vulnerable_configuration	text	The vulnerable configuration described in CPE format where the exploit/proof of concept is valid	—	✓
author	text	Author of the exploit - proof of concept	✓	✓
references	link	External references	—	✓
poc	attachment	Proof of Concept or exploit (as a script, binary or described process)	✓	✓

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

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
md5	md5	[Insecure] MD5 hash (128 bits)	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
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)	—	—
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	—	—
authentihash	authentihash	Authenticode executable signature hash	—	—
size-in-bytes	size-in-bytes	Size of the file, in bytes	✓	—
entropy	float	Entropy of the whole file	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
pattern-in-file	pattern-in-file	Pattern that can be found in the file	–	✓
text	text	Free text value to attach to the file	✓	–
malware-sample	malware-sample	The file itself (binary)	–	–
filename	filename	Filename on disk	✓	✓
path	text	Path of the filename complete or partial	✓	✓
fullpath	text	Complete path of the filename including the filename	–	✓
tlsh	tlsh	Fuzzy hash by Trend Micro: Locality Sensitive Hash	–	–
certificate	x509-fingerprint-sha1	Certificate value if the binary is signed with another authentication scheme than authenticode	–	–
mimetype	mime-type	Mime type	✓	–
state	text	State of the file ['Malicious', 'Harmless', 'Signed', 'Revoked', 'Expired', 'Trusted']	✓	✓

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
case-number	text	Any unique number assigned to the case for unique identification.	—	—
case-name	text	Name to address the case.	—	—
name-of-the-analyst	text	Name(s) of the analyst assigned to the case.	✓	✓
references	link	External references	—	✓
analysis-start-date	datetime	Date when the analysis began.	✓	—
additional-comments	text	Comments.	✓	—

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
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.	–	–
type	text	Evidence type. ['Computer', 'Network', 'Mobile Device', 'Multimedia', 'Cloud', 'IoT', 'Other']	✓	✓
name	text	Name of the evidence acquired.	–	–
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']	✓	–

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']	✓	✓
references	link	External references	—	✓
additional-comments	text	Comments.	✓	—

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
first-seen	datetime	When the location was seen for the first time.	✓	—
last-seen	datetime	When the location was seen for the last time.	✓	—
text	text	A generic description of the location.	✓	—

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	✓	—
altitude	float	The altitude is the decimal value of the altitude in the World Geodetic System 84 (WGS84) reference.	✓	—
address	text	Address.	—	—
zipcode	text	Zip Code.	—	—
city	text	City.	—	—
region	text	Region.	—	—

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)	✓	—
country	text	Country.	—	—
epsg	text	EPSG Geodetic Parameter value. This is an integer value of the EPSG.	✓	—
spacial-reference	text	Default spacial or projection refence for this object. ['WGS84 EPSG:4326', 'Mercator EPSG:3857']	✓	—

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
GtpServingNetwork	text	GTP Serving Network.	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
GtpImei	text	GTP IMEI (International Mobile Equipment Identity).	—	—
GtpMsisdn	text	GTP MSISDN.	—	—
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.	✓	—
PortDest	text	Destination port.	✓	—
PortSrc	port	Source port.	✓	—
ipDest	ip-dst	IP destination address.	—	—
ipSrc	ip-src	IP source address.	—	—
GtpVersion	text	GTP version ['0', '1', '2']	✓	—
text	text	A description of the GTP attack.	✓	—
first-seen	datetime	When the attack has been seen for the first time.	✓	—

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
text	text	HTTP Request comment	✓	—
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	—	—
host	hostname	The domain name of the server	—	—
method	http-method	HTTP Method invoked (one of GET, POST, PUT, HEAD, DELETE, OPTIONS, CONNECT)	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
referer	other	This is the address of the previous web page from which a link to the currently requested page was followed	—	—
proxy-password	text	HTTP Proxy Password	—	—
proxy-user	text	HTTP Proxy Username	—	—
uri	uri	Request URI	—	—
url	url	Full HTTP Request URL	—	—
user-agent	user-agent	The user agent string of the user agent	—	—

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
identifier	text	Identifier of the reference. Should be unique in your system.	—	—
comment	comment	Comment associated to the identifier.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
type	text	Type of internal reference.	—	—
link	link	Link associated to the identifier.	—	—

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
ip-src	ip-src	Source IP address of the network connection.	—	—
asn	AS	Autonomous System Number	✓	—
organization	text	organization	✓	—
ISP	text	ISP.	✓	—
zipcode	text	Zip Code.	✓	—
city	text	City.	✓	—
state	text	State.	✓	—
country	text	Country name	✓	—
country code	text	Country code	✓	—
region	text	Region. example: California.	✓	—
region code	text	Region code. example: CA	✓	—

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	✓	—
first-seen	datetime	First time the ASN was seen	✓	—
last-seen	datetime	Last time the ASN was seen	✓	—

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
text	text	Description of the tuple	✓	—
last-seen	datetime	Last time the tuple has been seen	✓	—
first-seen	datetime	First time the tuple has been seen	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
src-port	port	Source port	—	—
dst-port	port	Destination port	✓	✓
domain	domain	Domain	—	✓
hostname	hostname	Hostname	—	✓
ip	ip-dst	IP Address	—	✓

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>.



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
ja3-fingerprint-md5	md5	Hash identifying source	—	—
description	text	Type of detected software ie software, malware	—	—
ip-src	ip-src	Source IP Address	—	—
ip-dst	ip-dst	Destination IP address	—	—
first-seen	datetime	First seen of the SSL/TLS handshake	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
last-seen	datetime	Last seen of the SSL/TLS handshake	✓	—

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
text	text	A description of the entity.	✓	—
name	text	Name of an entity.	—	—
commercial-name	text	Commercial name of an entity.	—	—
legal-form	text	Legal form of an entity.	—	—
registration-number	text	Registration number of an entity in the relevant authority.	—	—
business	text	Business area of an entity.	—	—
phone-number	phone-number	Phone number of an entity.	—	—

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	✓	—
type	text	Type of Mach-O ['BUNDLE', 'CORE', 'DSYM', 'DYLIB', 'DYLIB_STUB', 'DYLINKER', 'EXECUTE', 'FVMLIB', 'KEXT_BUNDLE', 'OBJECT', 'PRELOAD']	—	—
number-sections	counter	Number of sections	✓	—
name	text	Binary's name	—	—
text	text	Free text value to attach to the Mach-O file	✓	—

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
md5	md5	[Insecure] MD5 hash (128 bits)	—	—
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)	—	—
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	—	—
entropy	float	Entropy of the whole section	✓	—
name	text	Name of the section	✓	—
size-in-bytes	size-in-bytes	Size of the section, in bytes	✓	—
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
file-path	text	Location of the file on the disc	—	—
datetime	datetime	Date and time when the operation was conducted on the file	✓	—
file_size	text	Determines the file size in bytes	✓	—
activityType	text	Determines the type of activity conducted on the file at a given time ['Accessed', 'Created', 'Changed', 'Modified', 'Other']	✓	—
filePermissions	text	Describes permissions assigned the file	✓	—
file	attachment	Mactime output file	✓	—

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.	—	—
format	text	Original format of the malware configuration. ['JSON', 'yaml', 'INI', 'other']	✓	—
encrypted	text	Encrypted or encoded text of the malware configuration in base64.	—	—
password	text	Password or encryption key used to encrypt the malware configuration.	—	—
last-seen	datetime	When the malware configuration has been seen for the last time.	✓	—
first-seen	datetime	When the malware configuration has been seen for the first time.	✓	—

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
post	text	Raw post	—	—
url	url	Original URL location of the microblog post	—	—
type	text	Type of the microblog post ['Twitter', 'Facebook', 'LinkedIn', 'Reddit', 'Google+', 'Instagram', 'Forum', 'Other']	✓	—
username	text	Username who posted the microblog post (without the @ prefix)	—	—
creation-date	datetime	Initial creation of the microblog post	—	—
modification-date	datetime	Last update of the microblog post	—	—
link	url	Link into the microblog post	—	✓
removal-date	datetime	When the microblog post was removed	—	—
username-quoted	text	Username who are quoted into the microblog post	—	✓

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	—	—
operating-system	text	Operating system where the mutex has been seen ['Windows', 'Unix']	—	—
name	text	name of the mutex	—	—

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
ip-dst	ip-dst	IP address destination of the netflow	—	—
ip-src	ip-src	IP address source of the netflow	—	—
dst-port	port	Destination port of the netflow	—	—
src-port	port	Source port of the netflow	—	—
tcp-flags	text	TCP flags of the flow	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
icmp-type	text	ICMP type of the flow (if the traffic is ICMP)	✓	—
ip-protocol-number	size-in-bytes	IP protocol number of this flow	✓	—
protocol	text	Protocol used for this flow ['TCP', 'UDP', 'ICMP', 'IP']	—	—
src-as	AS	Source AS number for this flow	—	—
dst-as	AS	Destination AS number for this flow	—	—
ip_version	counter	IP version of this flow	✓	—
direction	text	Direction of this flow ['Ingress', 'Egress']	✓	—
flow-count	counter	Flows counted in this flow	✓	—
packet-count	counter	Packets counted in this flow	✓	—
byte-count	counter	Bytes counted in this flow	✓	—
first-packet-seen	datetime	First packet seen in this flow	—	—
last-packet-seen	datetime	Last packet seen in this 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
ip-src	ip-src	Source IP address of the network connection.	—	—
ip-dst	ip-dst	Destination IP address of the network connection.	—	—
src-port	port	Source port of the network connection.	—	—
dst-port	port	Destination port of the network connection.	—	—
hostname-src	hostname	Source hostname of the network connection.	—	—
hostname-dst	hostname	Destination hostname of the network 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']	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
layer7-protocol	text	Layer 7 protocol of the network connection. ['HTTP', 'HTTPS', 'FTP']	✓	—
first-packet-seen	datetime	Datetime of the first packet seen.	—	—

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
ip-src	ip-src	Source (local) IP address 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.	—	—
hostname-dst	hostname	Destination hostname of the network socket connection.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
src-port	port	Source (local) port of the network socket connection.	—	—
dst-port	port	Destination port of the network socket connection.	—	—
protocol	text	Protocol used by the network socket. ['TCP', 'UDP', 'ICMP', 'IP']	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
address-family	text	<p>Address family who specifies the address family type (AF_*) of the socket connection.</p> <p>['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',</p>	-	-

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
domain-family	text	<p>Domain family who specifies the communication domain (PF_*) of the socket connection.</p> <p>['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',</p>	-	-
80				

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
state	text	State of the socket connection. ['blocking', 'listening']	—	✓
option	text	Option on the socket connection.	—	✓

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
imported-sample	attachment	The original imported file itself (binary).	—	—
format	text	Format of data imported. ['STIX 1.0', 'STIX 1.1', 'STIX 1.2', 'STIX 2.0', 'OpenIOC']	✓	—
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
zone_time_last	datetime	Last time that the unique tuple (rrname, rrtype, rdata) record has been seen via master file import.	✓	—
text	text	Description of the passive DNS record.	✓	—
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.	✓	—
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']	✓	—
rdata	text	Resource records of the queried resource	—	—

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	✓	—
origin	text	Origin of the Passive DNS response	✓	—
time_last	datetime	Last time that the unique tuple (rrname, rrtype, rdata) record has been seen by the passive DNS	✓	—
time_first	datetime	First time that the unique tuple (rrname, rrtype, rdata) has been seen by the passive DNS	✓	—
bailiwick	text	Best estimate of the apex of the zone where this data is authoritative	✓	—
sensor_id	text	Sensor information where the record was seen	✓	—

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
paste	text	Raw text of the paste or post	—	—
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']	✓	—
title	text	Title of the paste or post.	—	—
username	text	User who posted the post.	—	—
url	url	Link to the original source of the paste or post (when used maliciously).	—	—
link	link	Link to the original source of the source or post (when used legitimately for OSINT source or alike).	—	—
last-seen	datetime	When the paste has been accessible or seen for the last time.	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
first-seen	datetime	When the paste has been accessible or seen for the first time.	✓	—

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-length	text	Capture length set on the captured interface.	✓	—
capture-interface	text	Interface name where the packet capture was running.	✓	—

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_RADIO_TAP', '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.	✓	—
first-packet-seen	datetime	When the first packet has been seen.	✓	—
last-packet-seen	datetime	When the last packet has been seen.	✓	—

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 applications if it is automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
pehash	pehash	Hash of the structural information about a sample. See https://www.usenix.org/legacy/event/leet09/tech/full_papers/wicherski/wicherski_html/	—	—
impfuzzy	impfuzzy	Fuzzy Hash (ssdeep) calculated from the import table	—	—
internal-filename	filename	InternalFilename in the resources	✓	—

'P',
'NETTL_RAW_ICM
PV6', 'GPRS_LLC',
'JUNIPER_ATM1',
'JUNIPER_ATM2',
'REDBACK',
'NETTL_RAW_ICM',
'POLICY_ENGINE',
'T',
'JUNIPER_VP',
'USB_FREEBSD',
'IEEE802_16_MAC_
CPS',
'NETTL_RAW_TEL

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
original-filename	filename	OriginalFilename in the resources	✓	—
number-sections	counter	Number of sections	✓	—
text	text	Free text value to attach to the PE	✓	—
type	text	Type of PE ['exe', 'dll', 'driver', 'unknown']	✓	—
imphash	imphash	Hash (md5) calculated from the import table	—	—
compilation-timestamp	datetime	Compilation timestamp defined in the PE header	—	—
entrypoint-section-at-position	text	Name of the section and position of the section in the PE	✓	—
entrypoint-address	text	Address of the entry point	✓	—
file-description	text	FileDescription in the resources	✓	—
file-version	text	FileVersion in the resources	✓	—
lang-id	text	Lang ID in the resources	✓	—
product-name	text	ProductName in the resources	✓	—

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

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
product-version	text	ProductVersion in the resources	✓	—
company-name	text	CompanyName in the resources	✓	—
legal-copyright	text	LegalCopyright in the resources	✓	—

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
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)	—	—

'RTAC_SERIAL',
 'BLUETOOTH_LE_LL',
 'WIRESHARK_UPP
 'STANAG_4607',
 'STANAG_3066_D
 'BLUETOOTH_LIN
 'VSOCK',
 'NORDIC_BLE',
 'NETMON_NET_N
 ETEVENT',

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)	—	—
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	—	—
entropy	float	Entropy of the whole section	✓	—
name	text	Name of the section ['.rsrc', '.reloc', '.rdata', '.data', '.text']	✓	—
size-in-bytes	size-in-bytes	Size of the section, in bytes	✓	—
text	text	Free text value to attach to the section	✓	—
characteristic	text	Characteristic of the section ['read', 'write', 'executable']	—	—

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
text	text	A description of the person or identity.	✓	—
last-name	last-name	Last name of a natural person.	—	—
middle-name	middle-name	Middle name of a natural person.	—	—
first-name	first-name	First name of a natural person.	✓	—
mothers-name	text	Mother name, father, second name or other names following country's regulation.	—	—
title	text	Title of the natural person such as Dr. or equivalent.	✓	—
alias	text	Alias name or known as.	—	✓
date-of-birth	date-of-birth	Date of birth of a natural person (in YYYY-MM-DD format).	—	—
place-of-birth	place-of-birth	Place of birth of a natural person.	✓	—
gender	gender	The gender of a natural person. ['Male', 'Female', 'Other', 'Prefer not to say']	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
identity-card-number	identity-card-number	The identity card number of a natural person.	—	—
passport-number	passport-number	The passport number of a natural person.	—	—
passport-country	passport-country	The country in which the passport was issued.	✓	—
passport-expiration	passport-expiration	The expiration date of a passport.	✓	—
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.	—	—
social-security-number	text	Social security number.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
birth-certificate-number	text	Birth Certificate Number	—	—
ofac-identification-number	text	ofac-identification Number	—	—
nationality	nationality	The nationality of a natural person.	✓	✓
nic-hdl	text	NIC Handle (Network Information Centre handle) of the person.	—	✓
phone-number	phone-number	Phone number of the person.	—	✓
fax-number	phone-number	Fax number of the person.	—	✓
address	text	Postal address of the person.	—	✓
e-mail	email-src	Email address of the person.	—	✓

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
url	url	Original url of the phishing website	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
phishtank-id	text	Phishtank ID of the reported phishing	-	-
phishtank-detail-url	link	Phishtank detail URL to the reported phishing	-	-
submission-time	datetime	When the phishing was submitted and/or reported	-	-
verified	text	The phishing has been verified by the team handling the phishing ['No', 'Yes']	✓	-
verification-time	datetime	When the phishing was verified	✓	-
online	text	If the phishing is online and operational, by default is yes ['Yes', 'No']	✓	-
takedown-time	datetime	When the phishing was taken down	✓	-
target	text	Targeted organisation by the phishing	-	-

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
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.	—	—
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.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
msisdn	text	<p>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.</p>	-	-
tmsi	text	<p>Temporary Mobile Subscriber Identities (TMSI) to visiting mobile subscribers can be allocated.</p>	-	-
gummei	text	<p>Globally Unique MME Identifier (GUMMEI) is composed from MCC, MNC and MME Identifier (MMEI).</p>	-	-

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
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.	—	—
serial-number	text	Serial Number.	—	—
text	text	A description of the phone.	✓	—
last-seen	datetime	When the phone has been accessible or seen for the last time.	✓	—
first-seen	datetime	When the phone has been accessible or seen for the first time.	✓	—

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
creation-time	datetime	Local date/time at which the process was created.	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
start-time	datetime	Local date/time at which the process was started.	✓	—
name	text	Name of the process	—	—
pid	text	Process ID of the process.	✓	—
parent-pid	text	Process ID of the parent process.	✓	—
child-pid	text	Process ID of the child(ren) process.	✓	✓
port	src-port	Port(s) owned by the process.	✓	✓
command-line	text	Command line of the process	—	—
current-directory	filename	Current working directory of the process	✓	—
image	filename	Path of process image	—	—
parent-command-line	text	Command line of the parent process	—	—
parent-image	filename	Path of parent process image	—	—
user	text	User context of the process	✓	—
integrity-level	text	Integrity level 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
event-id	text	A unique number which identifies the event.	✓	—
name	text	Name of the event.	✓	—
event-channel	text	Channel through which the event occurred ['Application', 'System', 'Security', 'Setup', 'other']	✓	—
event-type	text	Event-type assigned to the event ['Admin', 'Operational', 'Audit', 'Analytic', 'Debug', 'other']	✓	—
source	text	The source of the event log - application/software that logged the event.	—	—
event-date-time	datetime	Date and time when the event was logged.	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
level	text	Determines the event severity. ['Information', 'Warning', 'Error', 'Critical', 'Success Audit', 'Failure Audit']	—	—
Computer	text	Computer name on which the event occurred	✓	—
User	text	Name or the User ID the event is associated with.	✓	—
Operational-code	text	The opcode (numeric value or name) associated with the activity carried out by the event.	✓	—
log	text	Log file where the event was recorded.	✓	—
task-category	text	Activity by the event publisher	✓	—
Keywords	text	Tags used for the event for the purpose of filtering or searching. ['Network', 'Security', 'Resource not found', 'other']	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
Processor-ID	text	ID of the processor that processed the event.	✓	-
Thread-ID	text	Thread id that generated the event.	✓	-
Session-ID	text	Terminal server session ID.	✓	-
Correlation-ID	text	Unique activity identity which relates the event to a process.	-	-
Relative-Correlation-ID	text	Related activity ID which identity similar activities which occurred as a part of the event.	✓	-
kernel-time	datetime	Execution time of the kernel mode instruction.	✓	-
user-time	datetime	Date and time when the user instruction was executed.	✓	-
Event-data	text	Event data description.	✓	-
comment	text	Additional comments.	✓	-

r2graphity

Indicators extracted from files using radare2 and graphml.



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	✓	—
callbacks	counter	Amount of callbacks (functions started as thread)	✓	—
shortest-path-to-create-thread	counter	Shortest path to the first time the binary calls CreateThread	✓	—
create-thread	counter	Amount of calls to CreateThread	✓	—
memory-allocations	counter	Amount of memory allocations	✓	—
get-proc-address	counter	Amount of calls to GetProcAddress	✓	—
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.)	✓	—
referenced-strings	counter	Amount of referenced strings	✓	—
callback-largest	counter	Largest callback	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
gml	attachment	Graph export in G>raph Modelling Language format	✓	—
r2-commit-version	text	Radare2 commit ID used to generate this object	✓	—
text	text	Description of the r2graphity object	✓	—
miss-api	counter	Amount of API call reference that does not resolve to a function offset	✓	—
total-api	counter	Total amount of API calls	✓	—
unknown-references	counter	Amount of API calls not ending in a function (Radare2 bug, probalby)	✓	—
refsglobalvar	counter	Amount of API calls outside of code section (glob var, dynamic API)	✓	—
local-references	counter	Amount of API calls inside a code section	✓	—
total-functions	counter	Total amount of functions in the file.	✓	—
not-referenced-strings	counter	Amount of not referenced strings	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
ratio-functions	float	Ratio: amount of functions per kilobyte of code section	✓	—
ratio-api	float	Ratio: amount of API calls per kilobyte of code section	✓	—
ratio-string	float	Ratio: amount of referenced strings per kilobyte of code section	✓	—

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-type	text	Type of the regular expression syntax. ['PCRE', 'PCRE2', 'POSIX BRE', 'POSIX ERE']	✓	—
regexp	text	regexp	—	—

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
last-modified	datetime	Last time the registry key has been modified	—	—

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']	✓	—
data	text	Data stored in the registry key	—	—
name	text	Name of the registry key	—	—
key	regkey	Full key path	—	—
hive	text	Hive used to store the registry key (file on disk)	✓	—

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
key	text	Registry key where the information is retrieved from.	—	—
key-last-write-time	datetime	Date and time when the key was last updated.	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
logon-user-name	text	Name assigned to the user profile.	—	—
recent-folders-accessed	text	List of recent folders accessed by the user.	—	✓
recent-files-accessed	text	List of recent files accessed by the user.	—	✓
typed-urls	text	Urls typed by the user in internet explorer	—	✓
applications-installed	text	List of applications installed.	—	✓
applications-run	text	List of applications set to run on the system.	—	✓
external-devices	text	List of external devices connected to the system by the user.	—	✓
user-init	text	Applications or processes set to run when the user logs onto the windows system.	—	✓
nukeOnDelete	boolean	Determines if the Recycle bin option has been disabled.	✓	—
network-connected-to	text	List of networks the user connected the system to.	—	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
mount-points	text	Details of the mount points created on the system.	✓	✓
comments	text	Additional information related to the user profile	✓	—

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
key	text	Registry key where the information is retrieved from.	—	—
key-last-write-time	datetime	Date and time when the key was last updated.	✓	—
user-name	text	User name assigned to the user profile.	—	—
full-user-name	text	Full name assigned to the user profile.	—	—
last-login-time	datetime	Date and time when the user last logged onto the system.	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
pwd-reset-time	datetime	Date and time when the password was last reset.	✓	—
pwd-fail-date	datetime	Date and time when a password last failed for this user profile.	✓	—
login-count	counter	Number of times the user logged-in onto the system.	✓	—
comments	text	Full 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
key	text	Registry key where the information is retrieved from.	—	—
key-last-write-time	datetime	Date and time when the key was last updated.	✓	—
group-name	text	Name assigned to the profile.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
full-name	text	Full name assigned to the profile.	–	–
last-write-date-time	datetime	Date and time when the group key was updated.	✓	–
group-comment	text	Any group comment added.	✓	–
group-users	text	Users belonging to the group	–	✓

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
key	text	Software hive key where the information is retrieved from.	–	–
last-write-time	datetime	Date and time when the key was last updated.	✓	–
BHO-name	text	Name of the browser helper object.	–	–
BHO-key-last-write-time	datetime	Date and time when the BHO key was last updated.	✓	–

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
class	text	Class to which the BHO belongs to.	✓	—
module	text	DLL module the BHO belongs to.	✓	—
comments	text	Additional comments.	✓	—
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
key	text	Software hive key where the information is retrieved from.	—	—
last-write-time	datetime	Date and time when the key was last updated.	✓	—
DLL-name	text	Name of the DLL file.	—	—
DLL-path	text	Path where the DLL file is stored.	—	—
DLL-last-write-time	datetime	Date and time when the DLL file was last updated.	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
comments	text	Additional comments.	✓	—
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
key	text	Software hive key where the information is retrieved from.	—	—
last-write-time	datetime	Date and time when the key was last updated.	✓	—
executable-file-name	text	Name of the executable file.	—	✓
path	text	Path of the executable file.	—	✓
comments	text	Additional comments.	✓	—
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
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.	✓	—
app-name	text	Name of the application.	—	—
app-last-write-time	datetime	Date and time when the application key was last updated.	✓	—
version	text	Version of the application.	—	—
comments	text	Additional comments.	✓	—
references	link	References to the application installed.	—	✓

regripper-software-hive-command-shell

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



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
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.	—	—
command	text	Command executed.	—	—
comments	text	Additional comments.	✓	—

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
win-cv-path	text	key where the windows information is retrieved from	—	—
last-write-time	datetime	Date and time when the key was last updated.	✓	—
RegisteredOrganization	text	Name of the registered organization.	—	—
RegisteredOwner	text	Name of the registered owner.	—	—
CurrentVersion	text	Current version of windows	✓	—
CurrentBuild	text	Build number of the windows OS.	—	—
SoftwareType	text	Software type of windows. ['System', 'Application', 'other']	✓	—
InstallationType	text	Type of windows installation.	✓	—
InstallDate	datetime	Date when windows was installed.	✓	—
SystemRoot	text	Root directory.	✓	—
PathName	text	Path to the root directory.	✓	—
EditionID	text	Windows edition.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
ProductName	text	Name of the windows version.	—	—
ProductID	text	ID of the product version.	—	—
CSDVersion	text	Version of the service pack installed.	—	—
CurrentBuildType	text	Current build type of the OS.	—	—
BuildLab	text	Windows BuildLab string.	—	—
BuildGUID	text	Build ID.	—	—
BuildLabEx	text	Windows BuildLabEx string.	—	—
comment	comment	Additional comments.	✓	—

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
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.	✓	—
application-name	text	Name of the application run.	—	✓
application-path	text	Path where the application is installed.	—	✓
comments	text	Additional comments.	✓	—
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
user-profile-key-path	text	key where the user-profile information is retrieved from.	✓	—
user-profile-key-last-write-time	datetime	Date and time when the key was last updated.	✓	—
user-profile-path	text	Path of the user profile on the system	✓	—
SID	text	Security identifier assigned to the user profile.	✓	—
user-profile-last-write-time	datetime	Date and time when the user profile was last updated.	✓	—
winlogon-key-path	text	winlogon key referred in order to retrieve default user information	✓	—
winlogon-key-last-write-time	datetime	Date and time when the winlogon key was last updated.	✓	—
DefaultUserName	text	user-name of the default user.	✓	—
Shell	text	Shell set to run when the user logs onto the system.	✓	✓

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).	–	✓
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.	✓	✓
PreCreateKnownFolders	text	create known folders key	✓	–
ReportBootOk	boolean	Flag to check if the reboot was successful.	✓	–
AutoRestartShell	boolean	Value of the flag set to auto restart the shell if it crashes or shuts down automatically.	✓	–
PasswordExpiryWarning	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.	✓	–

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
ShutdownWithout Logon	boolean	Value of the flag set to enable shutdown without requiring a user to login.	✓	—
WinStationsDisabled	boolean	Flag value set to enable/disable logons to the system.	✓	—
DisableCAD	boolean	Flag to determine if user login is enabled by pressing Ctrl+ALT+Delete.	✓	—
AutoAdminLogon	boolean	Flag value to determine if autologon is enabled for a user without entering the password.	✓	—
CachedLogonCount	counter	Number of times the user has logged into the system.	✓	—
ShutdownFlags	counter	Number of times shutdown is initiated from a process when the user is logged-in.	✓	—
Comments	text	Additional comments.	✓	—

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

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
computer-name	text	name of the computer under analysis	–	–
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-last-write-time	datetime	Date and time when the timezone key was last updated.	✓	–
timezone-bias	text	Offset in minutes from UTC. Offset added to the local time to get a UTC value.	✓	–
timezone-standard-name	text	Timezone standard name used during non-daylight saving months.	✓	–
timezone-standard-date	datetime	Standard date - non daylight saving months	✓	–
timezone-standard-bias	text	value in minutes to be added to the value of timezone-bias to generate the bias used during standard time.	✓	–

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
timezone-daylight-name	text	Timezone name used during daylight saving months.	✓	—
timezone-daylight-date	datetime	Daylight date - daylight saving months	✓	—
timezone-daylight-bias	text	value in minutes to be added to the value of timezone-bias to generate the bias used during daylight time.	✓	—
fDenyTSConnections:	boolean	Specifies whether remote connections are enabled or disabled on the system.	✓	—
comment		Additional comments.	✓	—

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
network-key	text	Registry key assigned to the network	—	—

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

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
name	text	name of the key	—	—
last-write-time	datetime	Date and time when the key was last updated.	✓	—
display	text	Display name/information of the service or the driver.	—	—
image-path	text	Path of the service/driver	—	—

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

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']	✓	—
comment		Additional comments.	✓	—

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
summary	text	Free text summary of the report	—	✓
case-number	text	Case number	—	—

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	—	✓
ip	ip-dst	IPs automatically extracted from the RTIR ticket	—	✓
constituency	text	Constituency of the RTIR ticket	—	—
queue	text	Queue of the RTIR ticket ['incident', 'investigations', 'blocks', 'incident reports']	—	—
subject	text	Subject of the RTIR ticket	—	—
status	text	Status of the RTIR ticket ['new', 'open', 'stalled', 'resolved', 'rejected', 'deleted']	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
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
permalink	link	Permalink reference	—	—
score	text	Score	✓	—
results	text	Freetext result values	✓	✓
raw-report	text	Raw report from sandbox	✓	—
sandbox-file	attachment	File related to sandbox run	✓	✓
sandbox-type	text	The type of sandbox used ['on-premise', 'web', 'saas']	✓	—

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']	✓	—
web-sandbox	text	A web sandbox where results are publicly available via an URL ['malwr', 'hybrid-analysis']	✓	—
saas-sandbox	text	A non-on-premise sandbox, also results are not publicly available ['forticloud-sandbox', 'joe-sandbox-cloud', 'symantec-cas-cloud']	✓	—

sb-signature

Sandbox detection signature.



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
software	text	Name of Sandbox software	✓	—

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

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
script	text	Free text of the script.	—	—
comment	text	Comment associated to the script.	—	—
language	text	Scripting language used for the script. ['PowerShell', 'VBScript', 'Bash', 'Lua', 'JavaScript', 'AppleScript', 'AWK', 'Python', 'Perl', 'Ruby', 'Winbatch', 'AutoIt']	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
filename	filename	Filename used for the script.	✓	✓
state	text	Known state of the script. ['Malicious', 'Unknown', 'Harmless', 'Trusted']	✓	✓

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	—	—
url-rfc5724	url	url representing SMS using RFC 5724 (not url contained in the SMS which should use an url object)	—	—
from	phone-number	Phone number used to send the SMS	—	✓
to	phone-number	Phone number receiving the SMS	—	✓
sent-date	datetime	Initial sent date of the SMS	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
received-date	datetime	Received date of the SMS	✓	—

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
first-seen	datetime	First time this shortened URL has been seen	✓	—
redirect-url	url	Redirected to URL	—	—
shortened-url	url	Shortened URL	—	—
domain	domain	Full domain	—	—
credential	text	Credential (username, password)	—	—
text	text	Description and context of the shortened URL	—	—

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']	✓	✓
MapVersion	text	Map version. ['1', '2', '3']	✓	-
SccpCgGT	text	Signaling Connection Control Part (SCCP) CgGT - Phone number.	-	✓
SccpCdGT	text	Signaling Connection Control Part (SCCP) CdGT - Phone number.	-	-
SccpCgPC	text	Signaling Connection Control Part (SCCP) CgPC - Phone number.	-	✓
SccpCdPC	text	Signaling Connection Control Part (SCCP) CdPC - Phone number.	-	-
SccpCgSSN	text	Signaling Connection Control Part (SCCP) - Decimal value between 0-255.	✓	-

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
SccpCdSSN	text	Signaling Connection Control Part (SCCP) - Decimal value between 0-255.	✓	—
MapOpCode	text	MAP operation codes - Decimal value between 0-99.	✓	—
MapApplicationContext	text	MAP application context in OID format.	✓	—
MapImsi	text	MAP IMSI. Phone number starting with MCC/MNC.	—	✓
MapMsisdn	text	MAP MSISDN. Phone number.	—	✓
MapMscGT	text	MAP MSC GT. Phone number.	—	—
MapGsmScfGT	text	MAP GSMSCF GT. Phone number.	—	—
MapVlrGT	text	MAP VLR GT. Phone number.	—	—
MapGmlc	text	MAP GMLC. Phone number.	—	—
MapSmscGT	text	MAP SMSC. Phone number.	—	✓
MapSmsTP-OA	text	MAP SMS TP-OA. Phone number.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
MapSmsText	text	MAP SMS Text. Important indicators in SMS text.	—	—
MapSmsTP-PID	text	MAP SMS TP-PID.	✓	—
MapSmsTP-DCS	text	MAP SMS TP-DCS.	✓	—
MapSmsTypeNumber	text	MAP SMS TypeNumber.	✓	—
MapUssdContent	text	MAP USSD Content.	—	—
MapUssdCoding	text	MAP USSD Content.	✓	—
text	text	A description of the attack seen via SS7 logging.	✓	✓
first-seen	datetime	When the attack has been seen for the first time.	✓	—

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.	—	—
stix2-pattern	stix2-pattern	STIX 2 pattern	—	—

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

target-system

Description about an targeted system, this could potentially be a compromised 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_machine	target-machine	Targeted system	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
targeted_ip_of_system	ip-src	Targeted system IP address	✓	—
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
threat_score	text	threat_score	✓	—
heuristic_raw_score	text	heuristic_raw_score	✓	—
heuristic_score	text	heuristic_score	—	—
analysis_submitted_at	text	Submission date	—	—
original_filename	text	Original filename	—	—
permalink	text	permalink	—	—
id	text	ThreatGrid ID	—	—
iocs	text	iocs	—	✓

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	—	—
start-marker-timecode	text	Start marker timecode in the format hh:mm:ss;ff	—	✓
end-marker-timecode	text	End marker timecode in the format hh:mm:ss;ff	—	✓
start-timecode	text	Start marker timecode in the format hh:mm:ss.mms	—	✓
end-timecode	text	End marker timecode in the format hh:mm:ss.mms	—	✓
recording-date	datetime	Date of recording of the video sequence	—	✓

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
message	text	Informative message of the event	—	—

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

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
text	text	Description of the time object.	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
precision	text	Timestamp precision represents the precision given to first_seen and/or last_seen in this object. ['year', 'month', 'day', 'hour', 'minute', 'full']	✓	—
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.	✓	—

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
description	text	Tor node description.	✓	—
nickname	text	router's nickname.	—	—
fingerprint	text	router's fingerprint.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
text	text	Tor node comment.	✓	—
address	ip-src	IP address of the Tor node seen.	—	—
flags	text	list of flag associated with the node.	—	—
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.	—	—
published	datetime	router's publication time. This can be different from first-seen and last-seen.	✓	—
last-seen	datetime	When the Tor node designed by the IP address has been seen for the last time.	✓	—
first-seen	datetime	When the Tor node designed by the IP address has been seen for the first time.	✓	—
document	text	Raw document from the consensus.	✓	—

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

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
text	text	A description of the transaction.	✓	—
transaction-number	text	A unique number identifying a transaction.	—	—
location	text	Location where the transaction took place.	—	—
transmode-code	text	How the transaction was conducted.	—	—
transmode-comment	text	Comment describing transmode-code, if needed.	—	—
teller	text	Person who conducted the transaction.	—	—
authorized	text	Person who authorized the transaction.	—	—
date	datetime	Date and time of the transaction.	—	—
amount	text	The value of the transaction in local currency.	—	—
date-posting	datetime	Date of posting, if different from date of transaction.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
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']	✓	—
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']	✓	—
from-country	text	Origin country of a transaction.	—	—
to-country	text	Target country of a transaction.	—	—

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
fragment	text	Fragment identifier is a short string of characters that refers to a resource that is subordinate to another, primary resource.	—	✓
tld	text	Top-Level Domain	✓	—
port	port	Port number	✓	—
scheme	text	Scheme ['http', 'https', 'ftp', 'gopher', 'sip']	✓	—
first-seen	datetime	First time this URL has been seen	✓	—
resource_path	text	Path (between hostname:port and query)	—	✓
query_string	text	Query (after path, preceded by '?')	—	✓
url	url	Full URL	—	—
domain_without_tld	text	Domain without Top-Level Domain	—	—
domain	domain	Full domain	—	—
subdomain	text	Subdomain	✓	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
credential	text	Credential (username, password)	—	—
text	text	Description of the URL	—	—
last-seen	datetime	Last time this URL has been seen	✓	—
host	hostname	Full hostname	—	—

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
description	text	Description of the vehicle	✓	—
year	text	Year of manufacturing of the vehicle	✓	—
make	text	Manufacturer of the vehicle	✓	—
model	text	Model of the vehicle	✓	—
vin	text	Vehicle identification number (VIN)	—	—
license-plate-number	text	License plate number	—	✓

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
description	text	Description of the victim	—	—
name	target-org	The name of the department(s) or organisation(s) targeted.	—	✓
external	target-external	External target organisations affected by this attack.	—	✓
classification	text	The type of entity being targeted. ['individual', 'group', 'organization', 'class', 'unknown']	✓	—
roles	text	The list of roles targeted within the victim.	—	✓

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
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']	-	✓
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
user	target-user	The username(s) of the user targeted.	—	✓
email	target-email	The email address(es) of the user targeted.	—	✓
node	target-machine	Name(s) of node that was targeted.	—	✓
ip-address	ip-dst	IP address(es) of the node targeted.	—	✓

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
community-score	text	Community Score	✓	—
detection-ratio	text	Detection Ratio	✓	—
first-submission	datetime	First Submission	—	—
last-submission	datetime	Last Submission	—	—
permalink	link	Permalink Reference	—	—
comment	text	Comment related to this hash	—	✓

vulnerability

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



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
id	text	Vulnerability ID (generally CVE, but not necessarily). The id is not required as the object itself has an UUID and the CVE id can be update or assigned later.	-	✓
description	text	Description of the vulnerability	-	-
summary	text	Summary of the vulnerability	-	-
vulnerable_configuration	text	The vulnerable configuration is described in CPE format	-	✓
modified	datetime	Last modification date	✓	-
published	datetime	Initial publication date	✓	-
created	datetime	First time when the vulnerability was discovered	✓	-
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']	✓	✓
cvss-score	float	Score of the Common Vulnerability Scoring System (version 3).	✓	—
cvss-string	text	String of the Common Vulnerability Scoring System (version 3).	✓	—
credit	text	Who reported/found the vulnerability such as an organisation, person or nickname.	✓	✓

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
text	text	Full whois entry	✓	—
registrar	whois-registrar	Registrar of the whois entry	—	—
registrant-name	whois-registrant-name	Registrant name	—	—
registrant-phone	whois-registrant-phone	Registrant phone number	—	—
registrant-email	whois-registrant-email	Registrant email address	—	—
registrant-org	whois-registrant-org	Registrant organisation	—	—
creation-date	datetime	Initial creation of the whois entry	✓	—
modification-date	datetime	Last update of the whois entry	✓	—
expiration-date	datetime	Expiration of the whois entry	✓	—
nameserver	hostname	Nameserver	✓	✓
domain	domain	Domain of the whois entry	—	✓
comment	text	Comment of the whois entry	—	—
ip-address	ip-src	IP address of the 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
subject	text	Subject of the certificate	—	—
pubkey-info-algorithm	text	Algorithm of the public key	—	—
pubkey-info-size	text	Length of the public key (in bits)	—	—
pubkey-info-exponent	text	Exponent of the public key	—	—
pubkey-info-modulus	text	Modulus of the public key	—	—
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)	—	—
raw-base64	text	Raw certificate base64 encoded (DER format)	—	—
pem	text	Raw certificate in PEM format (Unix-like newlines)	—	—
text	text	Free text description of the certificate	—	—
validity-not-before	datetime	Certificate invalid before that date	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
validity-not-after	datetime	Certificate invalid after that date	—	—
issuer	text	Issuer of the certificate	—	—
serial-number	text	Serial number of the certificate	—	—
version	text	Version of the certificate	—	—
self_signed	boolean	Self-signed certificate	—	—
is_ca	boolean	CA certificate	—	—
dns_names	text	DNS names	—	✓

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
version	comment	yabin.py and regex.txt version used for the generation of the yara rules.	—	—
comment	comment	A description of Yara rule generated.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
whitelist	comment	Whitelist name used to generate the rules.	—	—
yara-hunt	yara	Wide yara rule generated from -yh.	✓	—
yara	yara	Yara rule generated from -y.	✓	—

yara

An object describing a YARA rule 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.	—	—
yara	yara	YARA rule.	—	—
version	text	Version of the YARA rule depending where the yara rule is known to work as expected. ['3.7.1']	—	—
context	text	Context where the YARA rule can be applied ['all', 'disk', 'memory', 'network']	—	—

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']
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']
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']

Name of relationship	Description	Format
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']
mitigates	This relationship describes a source object which mitigates the target object.	['misp', 'stix-2.0']
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']
authored-by	This relationship describes the author of a specific object.	['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']
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']

Name of relationship	Description	Format
dropped-by	This relationship describes an object dropped by 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']
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']

Name of relationship	Description	Format
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']
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']

Name of relationship	Description	Format
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']
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']

Name of relationship	Description	Format
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']
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']

Name of relationship	Description	Format
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']
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']

Name of relationship	Description	Format
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']
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']
spoofed-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']

Name of relationship	Description	Format
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']