MISP Objects

MISP Objects

Introduction

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

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

Funding and Support

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

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**.

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

MISP objects

ail-leak

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

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

Object attribute	MISP attribute type	Description	Disable correlation
last-seen	datetime	When the leak has been accessible or seen for the last time.	✔
type	text	Type of information leak as discovered and classified by an AIL module. ['Credential', 'CreditCards', 'Mail', 'Onion', 'Phone', 'Keys']	-
first-seen	datetime	When the leak has been accessible or seen for the first time.	✔
original-date	datetime	When the information available in the leak was created. It's usually before the first-seen.	✔
sensor	text	The AIL sensor uuid where the leak was processed and analysed.	-
text	text	A description of the leak which could include the potential victim(s) or description of the leak.	✔

Object attribute	MISP attribute type	Description	Disable correlation
origin	text	The link where the leak is (or was) accessible at first-seen.	-
raw-data	attachment	Raw data as received by the AIL sensor compressed and encoded in Base64.	✔
duplicate	text	Duplicate of the existing leaks.	-
duplicate_number	counter	Number of known duplicates.	-

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
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', 'BIND_NOTIFICATION_LISTENER_SERVICE', 'BIND_PRINT_SERVICE', 'BIND_QUICK_SETTINGS_TILE', 'BIND_REMOTEVIEWS', 'BIND_SCREENING_SERVICE', 'BIND_TELECOM_CONN	-

Object attribute	MISP attribute type	Description	Disable correlation
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
type	text	Type of the annotation ['Annotation', 'Executive Summary', 'Introduction', 'Conclusion', 'Disclaimer', 'Keywords', 'Acknowledgement', 'Other', 'Copyright', 'Authors', 'Logo']	✔
format	text	Format of the annotation ['text', 'markdown', 'asciidoctor', 'MultiMarkdown', 'GFM', 'pandoc', 'Fountain', 'CommonWork', 'kramdown-rfc2629', 'rfc7328', 'Extra']	✔
ref	link	Reference(s) to the annotation	-
text	text	Raw text of the annotation	-

Object attribute	MISP attribute type	Description	Disable correlation
modification-date	datetime	Last update of the annotation	-
creation-date	datetime	Initial creation of the annotation	-

asn

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

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

Object attribute	MISP attribute type	Description	Disable correlation
last-seen	datetime	Last time the ASN was seen	✔
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	-
country	text	Country code of the main location of the autonomous system	-
asn	AS	Autonomous System Number	-
import	text	The inbound IPv4 routing policy of the AS in RFC 2622 – Routing Policy Specification Language (RPSL) format	-

'INSTALL_LOCATION_PROVIDER',
'INSTALL_PACKAGES',
'INSTALL_SHORTCUT',
'INSTANT_APP_FOREGROUND_SERVICE',
'INTERNET',
'KILL_BACKGROUND_PROCESSES',
'LOCATION_HARDWARE',

'READ_PHONE_NUMBERS',
'READ_PHONE_STATE',

Object attribute	MISP attribute type	Description	Disable correlation
subnet-announced	ip-src	Subnet announced	-
first-seen	datetime	First time the ASN was seen	✔
export	text	The outbound routing policy of the AS in RFC 2622 – Routing Policy Specification Language (RPSL) format	-
description	text	Description of the autonomous system	-
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
software	text	Name of antivirus software	✔
signature	text	Name of detection signature	-

'SET_ALWAYS_FINISH', 'SET_ANIMATION_SCALE', 'SET_DEBUG_APP', 'SET_PREFERRED_APPLICATIONS', 'SET_PROCESS_LIMIT', 'SET_TIME', 'SET_TIME_ZONE', 'SET_WALLPAPER',

T', 'UPDATE_DEVICE_STAT

Object attribute	MISP attribute type	Description	Disable correlation
datetime	datetime	Datetime	✔
text	text	Free text value to attach to the file	✔

bank-account

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

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

Object attribute	MISP attribute type	Description	Disable correlation
comments	text	Comments about the bank account.	✔
account-name	text	A field to freely describe the bank account details.	-
status-code	text	Account status at the time of the transaction processed. ['A - Active', 'B - Inactive', 'C - Dormant']	✔
date-balance	datetime	When the balance was reported.	✔
swift	bic	SWIFT or BIC as defined in ISO 9362.	✔
text	text	A description of the bank account.	✔
branch	text	Branch code or name	✔
beneficiary	text	Final beneficiary of the bank account.	✔

Object attribute	MISP attribute type	Description	Disable correlation
personal-account-type	text	Account type. ['A - Business', 'B - Personal Current', 'C - Savings', 'D - Trust Account', 'E - Trading Account', 'O - Other']	✔
institution-code	text	Name of the bank or financial organisation.	✔
currency-code	text	Currency of the account. ['USD', 'EUR']	✔
closed	datetime	When the account was closed.	✔
account	bank-account-nr	Account number	-
iban	iban	IBAN of the bank account.	-
beneficiary-comment	text	Comment about the final beneficiary.	✔

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

Object attribute	MISP attribute type	Description	Disable correlation
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.	✔
client-_number	text	Client number as seen by the bank.	-

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
note	text	The text describing the purpose or significance of the alert message.	✔
sent	datetime	The time and date of the origination of the alert message.	✔
restriction	text	The text describing the rule for limiting distribution of the restricted alert message.	✔

Object attribute	MISP attribute type	Description	Disable correlation
references	text	The group listing identifying earlier message(s) referenced by the alert message. (1) The extended message identifier(s) (in the form sender,identifier,sent) of an earlier CAP message or messages referenced by this one. (2) If multiple messages are referenced, they SHALL be separated by whitespace.	✔
code	text	The code denoting the special handling of the alert message.	✔
source	text	The text identifying the source of the alert message. The particular source of this alert; e.g., an operator or a specific device.	✔
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.	✔

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

Object attribute	MISP attribute type	Description	Disable correlation
incident	text	The group listing naming the referent incident(s) of the alert message. (1) Used to collate multiple messages referring to different aspects of the same incident. (2) If multiple incident identifiers are referenced, they SHALL be separated by whitespace. Incident names including whitespace SHALL be surrounded by double-quotes.	✔
scope	text	The code denoting the intended distribution of the alert message. ['Public', 'Restricted', 'Private']	✔
status	text	The code denoting the appropriate handling of the alert message. ['Actual', 'Exercise', 'System', 'Test', 'Draft']	-

cap-info

Common Alerting Protocol Version (CAP) info object.

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

Object attribute	MISP attribute type	Description	Disable correlation
event	text	The text denoting the type of the subject event of the alert message.	✔

Object attribute	MISP attribute type	Description	Disable correlation
urgency	text	The code denoting the urgency of the subject event of the alert message. ['Immediate', 'Expected', 'Future', 'Past', 'Unknown']	✔
language	text	The code denoting the language of the info sub-element of the alert message.	✔
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.	✔
responseType	text	The code denoting the type of action recommended for the target audience. ['Shelter', 'Evacuate', 'Prepare', 'Execute', 'Avoid', 'Monitor', 'Assess', 'AllClear', 'None']	✔
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']	✔
description	text	The text describing the subject event of the alert message.	✔

Object attribute	MISP attribute type	Description	Disable correlation
senderName	text	The text naming the originator of the alert message.	✔
severity	text	The code denoting the severity of the subject event of the alert message. ['Extreme', 'Severe', 'Moderate', 'Minor', 'Unknown']	✔
expires	datetime	The expiry time of the information of the alert message.	✔
parameter	text	A system-specific additional parameter associated with the alert message.	✔
audience	text	The text describing the intended audience of the alert message.	✔
headline	text	The text headline of the alert message.	✔
web	link	The identifier of the hyperlink associating additional information with the alert message.	✔
onset	datetime	The expected time of the beginning of the subject event of the alert message.	✔

Object attribute	MISP attribute type	Description	Disable correlation
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']	✔
instruction	text	The text describing the recommended action to be taken by recipients of the alert message.	✔
contact	text	The text describing the contact for follow-up and confirmation of 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
derefUri	attachment	The base-64 encoded data content of the resource file.	✔
size	text	The integer indicating the size of the resource file.	✔
uri	link	The identifier of the hyperlink for the resource file.	-

Object attribute	MISP attribute type	Description	Disable correlation
resourceDesc	text	The text describing the type and content of the resource file.	✔
mimeType	mime-type	The identifier of the MIME content type and sub-type describing 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
first-seen	datetime	First time this payment destination address has been seen	✔
last-seen	datetime	Last time this payment destination address has been seen	✔

Object attribute	MISP attribute type	Description	Disable correlation
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']	✔
address	btc	Address used as a payment destination in a cryptocurrency	-
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
type	text	Type of cookie and how it's used in this specific object. ['Session management', 'Personalization', 'Tracking', 'Exfiltration', 'Malicious Payload', 'Beaconing']	-

Object attribute	MISP attribute type	Description	Disable correlation
cookie-value	text	Value of the cookie (if splitted)	-
cookie-name	text	Name of the cookie (if splitted)	-
cookie	cookie	Full cookie	-
text	text	A description of the cookie.	✔

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
type	text	Type of password(s) ['password', 'api-key', 'encryption-key', 'unknown']	-
format	text	Format of the password(s) ['clear-text', 'hashed', 'encrypted', 'unknown']	-
username	text	Username related to the password(s)	-
password	text	Password	-
origin	text	Origin of the credential(s) ['bruteforce-scanning', 'malware-analysis', 'memory-analysis', 'network-analysis', 'leak', 'unknown']	-

Object attribute	MISP attribute type	Description	Disable correlation
text	text	A description of the credential(s)	✔
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
issued	datetime	Initial date of validity or issued date.	-
cc-number	cc-number	credit-card number as encoded on the card.	-
expiration	datetime	Maximum date of validity	-
comment	comment	A description of the card.	-
version	text	Version of the card.	-
name	text	Name of the card owner.	-
card-security-code	text	Card security code (CSC, CVD, CVV, CVC and SPC) as embossed or printed 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
last-seen	datetime	End of the attack	✔
total-bps	counter	Bits per second	-
domain-dst	domain	Destination domain (victim)	-
dst-port	port	Destination port of the attack	-
ip-src	ip-src	IP address originating the attack	-
total-pps	counter	Packets per second	-
text	text	Description of the DDoS	✔
first-seen	datetime	Beginning of the attack	✔
protocol	text	Protocol used for the attack ['TCP', 'UDP', 'ICMP', 'IP']	-
ip-dst	ip-dst	Destination IP (victim)	-
src-port	port	Port originating 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
CmdCode	text	A decimal representation of the diameter Command Code.	✔
Origin-Host	text	Origin-Host.	-
text	text	A description of the attack seen.	✔
first-seen	datetime	When the attack has been seen for the first time.	✔
category	text	Category. ['Cat0', 'Cat1', 'Cat2', 'Cat3', 'CatSMS']	✔
ApplicationId	text	Application-ID is used to identify for which Diameter application the message is applicable. Application-ID is a decimal representation.	-
Destination-Realm	text	Destination-Realm.	-
Origin-Realm	text	Origin-Realm.	-
SessionId	text	Session-ID.	-
IdrFlags	text	IDR-Flags.	✔
Destination-Host	text	Destination-Host.	-
Username	text	Username (in this case, usually the IMSI).	-

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

elf

Object describing a Executable and Linkable Format.

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

Object attribute	MISP attribute type	Description	Disable correlation
type	text	Type of ELF ['CORE', 'DYNAMIC', 'EXECUTABLE', 'HIPROC', 'LOPROC', 'NONE', 'RELOCATABLE']	-
number-sections	counter	Number of sections	✔

Object attribute	MISP attribute type	Description	Disable correlation
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', 'ARC_COMPACT', 'XTENSA', 'VIDEOCORE', 'TMM_GPP', 'NS32K', 'TPC', 'SNP1K', 'ST200', 'IP2K', 'MAX', 'CR', 'F2MC16', 'MSP430', 'BLACKFIN', 'SE_C33', 'SEP', 'ARCA', 'UNICORE', 'EXCESS', 'DXP', 'ALTERA_NIOS2', 'CRX', 'XGATE', 'C166',	✔

Object attribute	MISP attribute type	Description	Disable correlation
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	✔
entrypoint-address	text	Address of the entry point	✔

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

'K10M', 'AARCH64', 'AVR32', 'STM8', 'TILE64', 'TILEPRO', 'CUDA', 'TILEGX', 'CLOUDSHIELD', 'COREA_1ST', 'COREA_2ND', 'ARC_COMPACT2', 'OPEN8', 'RL78', 'MCHP_PIC', 'INTEL205', 'INTEL206', 'INTEL207', 'INTEL208', 'INTEL209', 'KM32', 'KMX32', 'KMX16', 'KMX8', 'KVARC', 'CDP', 'COGE', 'COOL', 'NORC', 'CSR_KALIMBA', 'AMDGPU']

Object attribute	MISP attribute type	Description	Disable correlation
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']	✔
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	-
text	text	Free text value to attach to the section	✔
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	-
size-in-bytes	size-in-bytes	Size of the section, in bytes	✔
entropy	float	Entropy of the whole section	✔
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	-

Object attribute	MISP attribute type	Description	Disable correlation
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']	✔
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	-
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	-
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	-
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	-
name	text	Name of the section	✔

Object attribute	MISP attribute type	Description	Disable correlation
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	-

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
from	email-src	Sender email address	-
email-body	email-body	Body of the email	-
to	email-dst	Destination email address	-
attachment	email-attachment	Attachment	-
return-path	text	Message return path	-
screenshot	attachment	Screenshot of email	-
reply-to	email-reply-to	Email address the reply will be sent to	-
cc	email-dst	Carbon copy	-
x-mailer	email-x-mailer	X-Mailer generally tells the program that was used to draft and send the original email	-
thread-index	email-thread-index	Identifies a particular conversation thread	-
mime-boundary	email-mime-boundary	MIME Boundary	-
message-id	email-message-id	Message ID	-

Object attribute	MISP attribute type	Description	Disable correlation
subject	email-subject	Subject	-
header	email-header	Full headers	-
to-display-name	email-dst-display-name	Display name of the receiver	-
from-display-name	email-src-display-name	Display name of the sender	-
send-date	datetime	Date the email has been sent	✔

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
md5	md5	[Insecure] MD5 hash (128 bits)	-
certificate	x509-fingerprint-sha1	Certificate value if the binary is signed with another authentication scheme than authenticode	-
malware-sample	malware-sample	The file itself (binary)	-
authentihash	authentihash	Authenticode executable signature hash	-
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	-
text	text	Free text value to attach to the file	✔

Object attribute	MISP attribute type	Description	Disable correlation
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	-
tlsh	tlsh	Fuzzy hash by Trend Micro: Locality Sensitive Hash	-
size-in-bytes	size-in-bytes	Size of the file, in bytes	✔
mimetype	mime-type	Mime type	✔
entropy	float	Entropy of the whole file	✔
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	-
filename	filename	Filename on disk	✔
pattern-in-file	pattern-in-file	Pattern that can be found in the file	-
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	-
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	-
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	-
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	-
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	-
state	text	State of the file ['Malicious', 'Harmless', 'Signed', 'Revoked', 'Expired', 'Trusted']	✔

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
latitude	float	The latitude is the decimal value of the latitude in the World Geodetic System 84 (WGS84) reference.	✔
last-seen	datetime	When the location was seen for the last time.	✔
country	text	Country.	-
city	text	City.	-
zipcode	text	Zip Code.	-
address	text	Address.	-
text	text	A generic description of the location.	✔
first-seen	datetime	When the location was seen for the first time.	✔
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.	-
region	text	Region.	-

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
GtpImsi	text	GTP IMSI (International mobile subscriber identity).	-
PortSrc	port	Source port.	✔
GtpServingNetwork	text	GTP Serving Network.	✔
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.	✔
text	text	A description of the GTP attack.	✔
first-seen	datetime	When the attack has been seen for the first time.	✔
GtpMsisdn	text	GTP MSISDN.	-
GtpInterface	text	GTP interface. ['S5', 'S11', 'S10', 'S8', 'Gn', 'Gp']	✔
GtpVersion	text	GTP version ['0', '1', '2']	✔
ipSrc	ip-src	IP source address.	-
PortDest	text	Destination port.	✔
ipDest	ip-dst	IP destination address.	-

Object attribute	MISP attribute type	Description	Disable correlation
GtpImei	text	GTP IMEI (International Mobile Equipment Identity).	-

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
host	hostname	The domain name of the server	-
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	-
basicauth-password	text	HTTP Basic Authentication Password	-
uri	uri	Request URI	-
text	text	HTTP Request comment	✔
user-agent	user-agent	The user agent string of the user agent	-
method	http-method	HTTP Method invoked (one of GET, POST, PUT, HEAD, DELETE, OPTIONS, CONNECT)	✔
proxy-user	text	HTTP Proxy Username	-

Object attribute	MISP attribute type	Description	Disable correlation
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	-
url	url	Full HTTP Request URL	-
basicauth-user	text	HTTP Basic Authentication Username	-

ip-port

An IP address (or domain) 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
last-seen	datetime	Last time the tuple has been seen	✔
dst-port	port	Destination port	-
text	text	Description of the tuple	✔
first-seen	datetime	First time the tuple has been seen	✔
ip	ip-dst	IP Address	-
src-port	port	Source port	-
domain	domain	Domain	-

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
ja3-fingerprint-md5	md5	Hash identifying source	-
ip-dst	ip-dst	Destination IP address	-
last-seen	datetime	Last seen of the SSL/TLS handshake	✔
ip-src	ip-src	Source IP Address	-
description	text	Type of detected software ie software, malware	-
first-seen	datetime	First 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
phone-number	phone-number	Phone number of an entity.	-
commercial-name	text	Commercial name of an entity.	-
text	text	A description of the entity.	✔
business	text	Business area of an entity.	-

Object attribute	MISP attribute type	Description	Disable correlation
legal-form	text	Legal form of an entity.	-
name	text	Name of an entity.	-
registration-number	text	Registration number of an entity in the relevant authority.	-

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
type	text	Type of Mach-O ['BUNDLE', 'CORE', 'DSYM', 'DYLIB', 'DYLIB_STUB', 'DYLINKER', 'EXECUTE', 'FVMLIB', 'KEXT_BUNDLE', 'OBJECT', 'PRELOAD']	-
name	text	Binary's name	-
number-sections	counter	Number of sections	✔
entrypoint-address	text	Address of the entry point	✔
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
md5	md5	[Insecure] MD5 hash (128 bits)	-
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	-
text	text	Free text value to attach to the section	✔
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	-
size-in-bytes	size-in-bytes	Size of the section, in bytes	✔
entropy	float	Entropy of the whole section	✔
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	-
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	-
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	-
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	-
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	-
name	text	Name of the section	✔
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	-

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
username-quoted	text	Username who are quoted into the microblog post	-
type	text	Type of the microblog post ['Twitter', 'Facebook', 'LinkedIn', 'Reddit', 'Google+', 'Instagram', 'Forum', 'Other']	✔
removal-date	datetime	When the microblog post was removed	-
modification-date	datetime	Last update of the microblog post	-
username	text	Username who posted the microblog post	-
url	url	Original URL location of the microblog post	-
link	url	Link into the microblog post	-
creation-date	datetime	Initial creation of the microblog post	-
post	text	Raw 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
name	text	name of the mutex	-
operating-system	text	Operating system where the mutex has been seen ['Windows', 'Unix']	-
description	text	Description	-

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
first-packet-seen	datetime	First packet seen in this flow	-
protocol	text	Protocol used for this flow ['TCP', 'UDP', 'ICMP', 'IP']	-
last-packet-seen	datetime	Last packet seen in this flow	-
ip-src	ip-src	IP address source of the netflow	-
dst-as	AS	Destination AS number for this flow	-
src-as	AS	Source AS number for this flow	-
direction	text	Direction of this flow ['Ingress', 'Egress']	✔

Object attribute	MISP attribute type	Description	Disable correlation
src-port	port	Source port of the netflow	-
ip-protocol-number	size-in-bytes	IP protocol number of this flow	✔
flow-count	counter	Flows counted in this flow	✔
ip-dst	ip-dst	IP address destination of the netflow	-
dst-port	port	Destination port of the netflow	-
icmp-type	text	ICMP type of the flow (if the traffic is ICMP)	✔
packet-count	counter	Packets counted in this flow	✔
tcp-flags	text	TCP flags of the flow	✔
byte-count	counter	Bytes counted in this flow	✔
ip_version	counter	IP version of this flow	✔

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
zone_time_last	datetime	Last time that the unique tuple (rrname, rrtype, rdata) record has been seen via master file import.	✔

Object attribute	MISP attribute type	Description	Disable correlation
rrtype	text	Resource Record type as seen by the passive DNS. ['A', 'AAAA', 'CNAME', 'PTR', 'SOA', 'TXT', 'DNAME', 'NS', 'SRV', 'RP', 'NAPTR', 'HINFO', 'A6']	✔
bailiwick	text	Best estimate of the apex of the zone where this data is authoritative	✔
text	text	Description of the passive DNS record.	✔
zone_time_first	datetime	First time that the unique tuple (rrname, rrtype, rdata) record has been seen via master file import	✔
rdata	text	Resource records of the queried resource	-
sensor_id	text	Sensor information where the record was seen	✔
count	counter	How many authoritative DNS answers were received at the Passive DNS Server's collectors with exactly the given set of values as answers.	✔
origin	text	Origin of the Passive DNS response	✔

Object attribute	MISP attribute type	Description	Disable correlation
time_first	datetime	First time that the unique tuple (rrname, rrtype, rdata) has been seen by the passive DNS	✔
rrname	text	Resource Record name of the queried resource.	-
time_last	datetime	Last time that the unique tuple (rrname, rrtype, rdata) record has been seen by the passive DNS	✔

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
last-seen	datetime	When the paste has been accessible or seen for the last time.	✔
first-seen	datetime	When the paste has been accessible or seen for the first time.	✔
paste	text	Raw text of the paste or post	-

Object attribute	MISP attribute type	Description	Disable correlation
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']	-
title	text	Title of the paste or post.	-
url	url	Link to the original source of the paste or post.	-

pe

Object describing a Portable Executable.

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

Object attribute	MISP attribute type	Description	Disable correlation
legal-copyright	text	LegalCopyright in the resources	✔
product-name	text	ProductName in the resources	✔
number-sections	counter	Number of sections	✔
entrypoint-address	text	Address of the entry point	✔
text	text	Free text value to attach to the PE	✔

Object attribute	MISP attribute type	Description	Disable correlation
entrypoint-section-at-position	text	Name of the section and position of the section in the PE	✔
internal-filename	filename	InternalFilename in the resources	✔
compilation-timestamp	datetime	Compilation timestamp defined in the PE header	-
type	text	Type of PE ['exe', 'dll', 'driver', 'unknown']	✔
pehash	pehash	Hash of the structural information about a sample. See https://www.usenix.org/legacy/event/leet09/tech/full_papers/wicherski/wicherski_html/	-
original-filename	filename	OriginalFilename in the resources	✔
imphash	imphash	Hash (md5) calculated from the import table	-
product-version	text	ProductVersion in the resources	✔
company-name	text	CompanyName in the resources	✔
impfuzzy	impfuzzy	Fuzzy Hash (ssdeep) calculated from the import table	-
file-version	text	FileVersion in the resources	✔
file-description	text	FileDescription in the resources	✔

Object attribute	MISP attribute type	Description	Disable correlation
lang-id	text	Lang ID 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
md5	md5	[Insecure] MD5 hash (128 bits)	-
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	-
text	text	Free text value to attach to the section	✔
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	-
size-in-bytes	size-in-bytes	Size of the section, in bytes	✔
entropy	float	Entropy of the whole section	✔
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	-
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	-
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	-
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	-

Object attribute	MISP attribute type	Description	Disable correlation
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	-
characteristic	text	Characteristic of the section ['read', 'write', 'executable']	-
name	text	Name of the section ['.rsrc', '.reloc', '.rdata', '.data', '.text']	✔
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	-

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
first-name	first-name	First name of a natural person.	✔
date-of-birth	date-of-birth	Date of birth of a natural person (in YYYY-MM-DD format).	-
alias	text	Alias name or known as.	-
nationality	nationality	The nationality of a natural person.	✔
passport-expiration	passport-expiration	The expiration date of a passport.	✔
text	text	A description of the person or identity.	✔

Object attribute	MISP attribute type	Description	Disable correlation
identity-card-number	identity-card-number	The identity card number of a natural person.	-
title	text	Title of the natural person such as Dr. or equivalent.	✔
mothers-name	text	Mother name, father, second name or other names following country's regulation.	-
social-security-number	text	Social security number	-
place-of-birth	place-of-birth	Place of birth of a natural person.	✔
last-name	last-name	Last name of a natural person.	-
gender	gender	The gender of a natural person. ['Male', 'Female', 'Other', 'Prefer not to say']	✔
middle-name	middle-name	Middle name of a natural person.	-

Object attribute	MISP attribute type	Description	Disable correlation
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.	-
passport-country	passport-country	The country in which the passport was issued.	✔
passport-number	passport-number	The passport number of a natural person.	-

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
imei	text	International Mobile Equipment Identity (IMEI) is a number, usually unique, to identify 3GPP and iDEN mobile phones, as well as some satellite phones.	-

Object attribute	MISP attribute type	Description	Disable correlation
tmsi	text	Temporary Mobile Subscriber Identities (TMSI) to visiting mobile subscribers can be allocated.	✗
first-seen	datetime	When the phone has been accessible or seen for the first time.	✓
last-seen	datetime	When the phone has been accessible or seen for the last time.	✓
gummei	text	Globally Unique MME Identifier (GUMMEI) is composed from MCC, MNC and MME Identifier (MMEI).	✗
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.	✗
text	text	A description of the phone.	✓
serial-number	text	Serial Number.	✗

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

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
create-thread	counter	Amount of calls to CreateThread	✔
not-referenced-strings	counter	Amount of not referenced strings	✔

Object attribute	MISP attribute type	Description	Disable correlation
local-references	counter	Amount of API calls inside a code section	✔
r2-commit-version	text	Radare2 commit ID used to generate this object	✔
callbacks	counter	Amount of callbacks (functions started as thread)	✔
callback-largest	counter	Largest callback	✔
ratio-string	float	Ratio: amount of referenced strings per kilobyte of code section	✔
ratio-api	float	Ratio: amount of API calls per kilobyte of code section	✔
refsglobalvar	counter	Amount of API calls outside of code section (glob var, dynamic API)	✔
ratio-functions	float	Ratio: amount of functions per kilobyte of code section	✔
get-proc-address	counter	Amount of calls to GetProcAddress	✔
referenced-strings	counter	Amount of referenced strings	✔
memory-allocations	counter	Amount of memory allocations	✔
text	text	Description of the r2graphity object	✔

Object attribute	MISP attribute type	Description	Disable correlation
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.)	✔
miss-api	counter	Amount of API call reference that does not resolve to a function offset	✔
total-functions	counter	Total amount of functions in the file.	✔
shortest-path-to-create-thread	counter	Shortest path to the first time the binary calls CreateThread	✔
gml	attachment	Graph export in G>raph Modelling Language format	✔
unknown-references	counter	Amount of API calls not ending in a function (Radare2 bug, probalby)	✔
callback-average	counter	Average size of a callback	✔
total-api	counter	Total amount of API calls	✔

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
regexp-type	text	Type of the regular expression syntax. ['PCRE', 'PCRE2', 'POSIX BRE', 'POSIX ERE']	✔
regexp	text	regexp	-
comment	comment	A description of the regular expression.	-
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
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']	✔
last-modified	datetime	Last time the registry key has been modified	-
data	text	Data stored in the registry key	-
key	regkey	Full key path	-
name	text	Name of the registry key	-

Object attribute	MISP attribute type	Description	Disable correlation
data-type	text	Registry value type ['REG_NONE', 'REG_SZ', 'REG_EXPAND_SZ', 'REG_BINARY', 'REG_DWORD', 'REG_DWORD_LITTLE_ENDIAN', 'REG_DWORD_BIG_ENDIAN', 'REG_LINK', 'REG_MULTI_SZ', 'REG_RESOURCE_LIST', 'REG_FULL_RESOURCE_DESCRIPTOR', 'REG_RESOURCE_REQUIREMENTS_LIST', 'REG_QWORD', 'REG_QWORD_LITTLE_ENDIAN']	✔
hive	text	Hive used to store the registry key (file on disk)	✔

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

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

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
web-sandbox	text	A web sandbox where results are publicly available via an URL ['malwr', 'hybrid-analysis']	✔

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

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
software	text	Name of Sandbox software	✔

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

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
MapVlrGT	text	MAP VLR GT. Phone number.	-
MapSmscGT	text	MAP SMSC. Phone number.	-
text	text	A description of the attack seen via SS7 logging.	✔
SccpCgGT	text	Signaling Connection Control Part (SCCP) CgGT - Phone number.	-
MapSmsTP-PID	text	MAP SMS TP-PID.	✔
first-seen	datetime	When the attack has been seen for the first time.	✔
SccpCgPC	text	Signaling Connection Control Part (SCCP) CgPC - Phone number.	-

Object attribute	MISP attribute type	Description	Disable correlation
MapMsisdn	text	MAP MSISDN. Phone number.	-
MapSmsTP-OA	text	MAP SMS TP-OA. Phone number.	-
MapSmsTP-DCS	text	MAP SMS TP-DCS.	✔
MapSmsTypeNumber	text	MAP SMS TypeNumber.	✔
MapImsi	text	MAP IMSI. Phone number starting with MCC/MNC.	-
MapSmsText	text	MAP SMS Text. Important indicators in SMS text.	-
MapMscGT	text	MAP MSC GT. Phone number.	-
MapUssdCoding	text	MAP USSD Content.	✔
Category	text	Category ['Cat0', 'Cat1', 'Cat2.1', 'Cat2.2', 'Cat3.1', 'Cat3.2', 'Cat3.3', 'CatSMS', 'CatSpoofing']	✔
MapApplicationContext	text	MAP application context in OID format.	✔
MapOpCode	text	MAP operation codes - Decimal value between 0-99.	✔
MapVersion	text	Map version. ['1', '2', '3']	✔
MapGmlc	text	MAP GMLC. Phone number.	-

Object attribute	MISP attribute type	Description	Disable correlation
SccpCdPC	text	Signaling Connection Control Part (SCCP) CdPC - Phone number.	-
MapUssdContent	text	MAP USSD Content.	-
SccpCdSSN	text	Signaling Connection Control Part (SCCP) - Decimal value between 0-255.	✔
MapGsmscfGT	text	MAP GSMSCF GT. Phone number.	-
SccpCdGT	text	Signaling Connection Control Part (SCCP) CdGT - Phone number.	-
SccpCgSSN	text	Signaling Connection Control Part (SCCP) - Decimal value between 0-255.	✔

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
stix2-pattern	stix2-pattern	STIX 2 pattern	-
comment	comment	A description of the stix2-pattern.	-

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
text	text	Tor node comment.	✔
version	text	parsed version of tor, this is None if the relay's using a new versioning scheme.	-
first-seen	datetime	When the Tor node designed by the IP address has been seen for the first time.	✔
flags	text	list of flag associated with the node.	-
nickname	text	router's nickname.	-
last-seen	datetime	When the Tor node designed by the IP address has been seen for the last time.	✔
document	text	Raw document from the consensus.	✔
address	ip-src	IP address of the Tor node seen.	-
description	text	Tor node description.	✔
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.	✔
fingerprint	text	router's fingerprint.	-

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
transmode-code	text	How the transaction was conducted.	-
from-country	text	Origin country of a transaction.	-
transmode-comment	text	Comment describing transmode-code, if needed.	-
teller	text	Person who conducted the transaction.	-
text	text	A description of the transaction.	✔
from-funds-code	text	Type of funds used to initiate a transaction. ['A Deposit', 'C Currency exchange', 'D Casino chips', 'E Bank draft', 'F Money order', 'G Traveler's cheques', 'H Life insurance policy', 'I Real estate', 'J Securities', 'K Cash', 'O Other', 'P Cheque']	✔
amount	text	The value of the transaction in local currency.	-
location	text	Location where the transaction took place.	-

Object attribute	MISP attribute type	Description	Disable correlation
transaction-number	text	A unique number identifying a transaction.	-
to-country	text	Target country of a transaction.	-
to-funds-code	text	Type of funds used to finalize a transaction. ['A Deposit', 'C Currency exchange', 'D Casino chips', 'E Bank draft', 'F Money order', 'G Traveler's cheques', 'H Life insurance policy', 'I Real estate', 'J Securities', 'K Cash', 'O Other', 'P Cheque']	✔
authorized	text	Person who autorized the transaction.	-
date	datetime	Date and time of the transaction.	-
date-posting	datetime	Date of posting, if different from date of transaction.	-

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
last-seen	datetime	Last time this URL has been seen	✔
host	hostname	Full hostname	-

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

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
classification	text	The type of entity being targeted. ['individual', 'group', 'organization', 'class', 'unknown']	✔
description	text	Description of the victim	-
node	target-machine	Name(s) of node that was targeted.	-
regions	target-location	The list of regions or locations from the victim targeted. ISO 3166 should be used.	-
user	target-user	The username(s) of the user targeted.	-

Object attribute	MISP attribute type	Description	Disable correlation
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']	-
email	target-email	The email address(es) of the user targeted.	-
roles	text	The list of roles targeted within the victim.	-
external	target-external	External target organisations affected by this attack.	-
name	target-org	The name of the department(s) or organisation(s) targeted.	-

Object attribute	MISP attribute type	Description	Disable correlation
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
last-submission	datetime	Last Submission	-
permalink	link	Permalink Reference	-
community-score	text	Community Score	✔
detection-ratio	text	Detection Ratio	✔
first-submission	datetime	First Submission	-

vulnerability

Vulnerability object describing a common vulnerability enumeration which can describe 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
published	datetime	Initial publication date	✔
summary	text	Summary of the vulnerability	-

Object attribute	MISP attribute type	Description	Disable correlation
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']	✔
references	link	External references	-
text	text	Description of the vulnerability	-
modified	datetime	Last modification date	✔
created	datetime	First time when the vulnerability was discovered	✔
vulnerable_configuration	text	The vulnerable configuration is described in CPE format	-
id	vulnerability	Vulnerability ID (generally CVE, but not necessarely). The id is not required as the object itself has an UUID and the CVE id can updated later.	-

whois

Whois records information for a domain name..

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
registrar	whois-registrar	Registrar of the whois entry	-
registrant-phone	whois-registrant-phone	Registrant phone number	-
modification-date	datetime	Last update of the whois entry	✔
registrant-name	whois-registrant-name	Registrant name	-
text	text	Full whois entry	✔
creation-date	datetime	Initial creation of the whois entry	✔
registrant-org	whois-registrant-org	Registrant organisation	-
expiration-date	datetime	Expiration of the whois entry	✔
registrant-email	whois-registrant-email	Registrant email address	-
domain	domain	Domain of the whois entry	-
nameserver	hostname	Nameserver	✔

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
x509-fingerprint-sha1	x509-fingerprint-sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	-

Object attribute	MISP attribute type	Description	Disable correlation
pubkey-info-algorithm	text	Algorithm of the public key	-
raw-base64	text	Raw certificate base64 encoded	-
text	text	Free text description of hte certificate	-
serial-number	text	Serial number of the certificate	-
version	text	Version of the certificate	-
validity-not-after	datetime	Certificate invalid after that date	-
validity-not-before	datetime	Certificate invalid before that date	-
pubkey-info-modulus	text	Modulus of the public key	-
x509-fingerprint-sha256	x509-fingerprint-sha256	Secure Hash Algorithm 2 (256 bits)	-
pubkey-info-exponent	text	Exponent of the public key	-
issuer	text	Issuer of the certificate	-
subject	text	Subject of the certificate	-
pubkey-info-size	text	Length of the public key (in bits)	-
x509-fingerprint-md5	x509-fingerprint-md5	[Insecure] MD5 hash (128 bits)	-

yabin

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

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

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

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']
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']
attributed-to	This referenced source is attributed to the target object.	['misp', 'stix-2.0']

Name of relationship	Description	Format
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']
indicates	This relationships 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']
impersonates	This relationship describe 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']
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']

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

Name of relationship	Description	Format
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']
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']

Name of relationship	Description	Format
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']
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']

Name of relationship	Description	Format
owner-of	This relationship describes an object which owns another object.	['cert-eu']
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']