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
type	text	Type of information leak as discovered and classified by an AIL module. ['Credential', 'CreditCards', 'Mail', 'Onion', 'Phone', 'Keys']	-
duplicate_number	counter	Number of known duplicates.	-
raw-data	attachment	Raw data as received by the AIL sensor compressed and encoded in Base64.	✔
last-seen	datetime	When the leak has been accessible or seen for the last time.	✔
text	text	A description of the leak which could include the potential victim(s) or description of the leak.	✔
sensor	text	The AIL sensor uuid where the leak was processed and analysed.	-

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

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
comment	comment	Comment about the set of android permission(s)	-

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	-

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
text	text	Raw text of the annotation	-
modification-date	datetime	Last update of the annotation	-
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	-
creation-date	datetime	Initial creation of the annotation	-

ECTION_SERVICE', 'BIND_TEXT_SERVICE', 'BIND_TV_INPUT', 'BIND_VISUAL_VOICEMAIL_SERVICE', 'BIND_VOICE_INTERACTION', 'DIAGNOSTIC', 'DISABLE_KEYGUARD', 'DUMP', 'EXPAND_STATUS_BAR', 'FACTORY_TEST',

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
asn	AS	Autonomous System Number	-
last-seen	datetime	Last time the ASN was seen	✔
subnet-announced	ip-src	Subnet announced	-
export	text	The outbound routing policy of the AS in RFC 2622 – Routing Policy Specification Language (RPSL) format	-
country	text	Country code of the main location of the autonomous system	-
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	-

Object attribute	MISP attribute type	Description	Disable correlation
first-seen	datetime	First time the ASN was seen	✔
import	text	The inbound IPv4 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	-

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
text	text	Free text value to attach to the file	✔
datetime	datetime	Datetime	✔
signature	text	Name of detection signature	-
software	text	Name of antivirus software	✔

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
branch	text	Branch code or name	✔
text	text	A description of the bank account.	✔
institution-code	text	Name of the bank or financial organisation.	✔
iban	iban	IBAN of the bank account.	-
account-name	text	A field to freely describe the bank account details.	-
date-balance	datetime	When the balance was reported.	✔
personal-account-type	text	Account type. ['A - Business', 'B - Personal Current', 'C - Savings', 'D - Trust Account', 'E - Trading Account', 'O - Other']	✔
comments	text	Comments about the bank account.	✔
beneficiary	text	Final beneficiary of the bank account.	✔
account	bank-account-nr	Account number	-
status-code	text	Account status at the time of the transaction processed. ['A - Active', 'B - Inactive', 'C - Dormant']	✔

READ_SMS',
'READ_SYNC_SETTINGS
OW', 'TRANSMIT_IR',
'UNINSTALL_SHORTCU
T',
'UPDATE_DEVICE_STAT

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']	✔
swift	bic	SWIFT or BIC as defined in ISO 9362.	✔
currency-code	text	Currency of the account. ['USD', 'EUR']	✔
balance	text	The balance of the account after the suspicious transaction was processed.	✔

Object attribute	MISP attribute type	Description	Disable correlation
opened	datetime	When the account was opened.	✔
beneficiary-comment	text	Comment about the final beneficiary.	✔
closed	datetime	When the account was closed.	✔
client-_number	text	Client number as seen by the bank.	-
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.	✔

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
text	text	Free text value	✔
address	btc	Address used as a payment destination in a cryptocurrency	-
first-seen	datetime	First 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']	✔
last-seen	datetime	Last time this payment destination address has been seen	✔

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
cookie-name	text	Name of the cookie (if splitted)	-
text	text	A description of the cookie.	✔
cookie-value	text	Value of the cookie (if splitted)	-

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']	-
cookie	cookie	Full 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
username	text	Username related to the password(s)	-
text	text	A description of the credential(s)	✔
password	text	Password	-
origin	text	Origin of the credential(s) ['bruteforce-scanning', 'malware-analysis', 'memory-analysis', 'network-analysis', 'leak', 'unknown']	-
type	text	Type of password(s) ['password', 'api-key', 'encryption-key', 'unknown']	-

Object attribute	MISP attribute type	Description	Disable correlation
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
name	text	Name of the card owner.	-
expiration	datetime	Maximum date of validity	-
comment	comment	A description of the card.	-
version	text	Version of the card.	-
card-security-code	text	Card security code (CSC, CVD, CVV, CVC and SPC) as embossed or printed on the card.	-
issued	datetime	Initial date of validity or issued date.	-

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

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
text	text	A description of the attack seen.	✔
Destination-Realm	text	Destination-Realm.	-
Destination-Host	text	Destination-Host.	-
Origin-Realm	text	Origin-Realm.	-
IdrFlags	text	IDR-Flags.	✔
first-seen	datetime	When the attack has been seen for the first time.	✔
CmdCode	text	A decimal representation of the diameter Command Code.	✔
Origin-Host	text	Origin-Host.	-
ApplicationId	text	Application-ID is used to identify for which Diameter application the message is applicable. Application-ID is a decimal representation.	-
category	text	Category. ['Cat0', 'Cat1', 'Cat2', 'Cat3', 'CatSMS']	✔
SessionId	text	Session-ID.	-

Object attribute	MISP attribute type	Description	Disable correlation
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
ip	ip-dst	IP Address	-
text	text	A description of the tuple	✔
first-seen	datetime	First time the tuple has been seen	✔
last-seen	datetime	Last time the tuple has been seen	✔
domain	domain	Domain name	-

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
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
number-sections	counter	Number of sections	✔
text	text	Free text value to attach to the ELF	✔
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']	✔
type	text	Type of ELF ['CORE', 'DYNAMIC', 'EXECUTABLE', 'HIPROC', 'LOPROC', 'NONE', 'RELOCATABLE']	-
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
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']	✔
text	text	Free text value to attach to the section	✔
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	-
name	text	Name of the section	✔

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']	✔
entropy	float	Entropy of the whole section	✔
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	-
md5	md5	[Insecure] MD5 hash (128 bits)	-
size-in-bytes	size-in-bytes	Size of the section, in bytes	✔
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	-
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	-
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	-
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	-

Object attribute	MISP attribute type	Description	Disable correlation
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	-
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	-

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
header	email-header	Full headers	-
to	email-dst	Destination email address	-
mime-boundary	email-mime-boundary	MIME Boundary	-
message-id	email-message-id	Message ID	-
from-display-name	email-src-display-name	Display name of the sender	-
attachment	email-attachment	Attachment	-
send-date	datetime	Date the email has been sent	✔
x-mailer	email-x-mailer	X-Mailer generally tells the program that was used to draft and send the original email	-
subject	email-subject	Subject	-
screenshot	attachment	Screenshot of email	-

Object attribute	MISP attribute type	Description	Disable correlation
to-display-name	email-dst-display-name	Display name of the receiver	-
cc	email-dst	Carbon copy	-
return-path	text	Message return path	-
reply-to	email-reply-to	Email address the reply will be sent to	-
from	email-src	Sender email address	-
thread-index	email-thread-index	Identifies a particular conversation thread	-

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
certificate	x509-fingerprint-sha1	Certificate value if the binary is signed with another authentication scheme than authenticode	-
text	text	Free text value to attach to the file	✔
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	-
state	text	State of the file ['Malicious', 'Harmless', 'Signed', 'Revoked', 'Expired', 'Trusted']	✔
mimetype	text	Mime type	✔

Object attribute	MISP attribute type	Description	Disable correlation
entropy	float	Entropy of the whole file	✔
pattern-in-file	pattern-in-file	Pattern that can be found in the file	-
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	-
md5	md5	[Insecure] MD5 hash (128 bits)	-
size-in-bytes	size-in-bytes	Size of the file, in bytes	✔
authentihash	authentihash	Authenticode executable signature hash	-
tlsh	tlsh	Fuzzy hash by Trend Micro: Locality Sensitive Hash	-
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	-
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	-
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	-
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	-
malware-sample	malware-sample	The file itself (binary)	-
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	-
filename	filename	Filename on disk	✔

Object attribute	MISP attribute type	Description	Disable correlation
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	-

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

Object attribute	MISP attribute type	Description	Disable correlation
longitude	float	The longitude is the decimal value of the longitude in the World Geodetic System 84 (WGS84) reference	✔

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).	-
text	text	A description of the GTP attack.	✔
ipSrc	ip-src	IP source address.	-
GtpMsisdn	text	GTP MSISDN.	-
GtpImei	text	GTP IMEI (International Mobile Equipment Identity).	-
ipDest	ip-dst	IP destination address.	-
GtpServingNetwork	text	GTP Serving Network.	✔
first-seen	datetime	When the attack has been seen for the first time.	✔
GtpInterface	text	GTP interface. ['S5', 'S11', 'S10', 'S8', 'Gn', 'Gp']	✔
GtpVersion	text	GTP version ['0', '1', '2']	✔

Object attribute	MISP attribute type	Description	Disable correlation
PortSrc	port	Source port.	✔
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.	✔

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
text	text	HTTP Request comment	✔
uri	uri	Request URI	-
basicauth-user	text	HTTP Basic Authentication Username	-
cookie	text	An HTTP cookie previously sent by the server with Set-Cookie	-
basicauth-password	text	HTTP Basic Authentication Password	-
host	hostname	The domain name of the server	-

Object attribute	MISP attribute type	Description	Disable correlation
method	http-method	HTTP Method invoked (one of GET, POST, PUT, HEAD, DELETE, OPTIONS, CONNECT)	✔
user-agent	user-agent	The user agent string of the user agent	-
referer	referer	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	-
content-type	other	The MIME type of the body of the request	-
url	url	Full HTTP Request URL	-
proxy-user	text	HTTP Proxy Username	-

ip-port

An IP address 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
text	text	Description of the tuple	✔
last-seen	datetime	Last time the tuple has been seen	✔
dst-port	port	Destination port	-
ip	ip-dst	IP Address	-
first-seen	datetime	First time the tuple has been seen	✔

Object attribute	MISP attribute type	Description	Disable correlation
src-port	port	Source port	-

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
ip-dst	ip-dst	Destination IP address	-
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	✔
ja3-fingerprint-md5	md5	Hash identifying source	-
last-seen	datetime	Last seen of the SSL/TLS handshake	✔

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']	-
text	text	Free text value to attach to the Mach-O file	✔
entrypoint-address	text	Address of the entry point	✔
name	text	Binary's name	-
number-sections	counter	Number of sections	✔

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
text	text	Free text value to attach to the section	✔
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	-
name	text	Name of the section	✔
entropy	float	Entropy of the whole section	✔
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	-

Object attribute	MISP attribute type	Description	Disable correlation
md5	md5	[Insecure] MD5 hash (128 bits)	-
size-in-bytes	size-in-bytes	Size of the section, in bytes	✔
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	-
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	-
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	-
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	-
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	-
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	-

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
type	text	Type of the microblog post ['Twitter', 'Facebook', 'LinkedIn', 'Reddit', 'Google+', 'Instagram', 'Forum', 'Other']	✔

Object attribute	MISP attribute type	Description	Disable correlation
removal-date	datetime	When the microblog post was removed	-
modification-date	datetime	Last update of the microblog post	-
link	url	Link into the microblog post	-
post	text	Raw post	-
username-quoted	text	Username who are quoted into the microblog post	-
username	text	Username who posted the microblog post	-
url	url	Original URL location of the microblog post	-
creation-date	datetime	Initial creation of 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
name	text	name of the mutex	-
description	text	Description	-
operating-system	text	Operating system where the mutex has been seen ['Windows', 'Unix']	-

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
ip_version	counter	IP version of this flow	✔
dst-port	port	Destination port of the netflow	-
ip-protocol-number	size-in-bytes	IP protocol number of this flow	✔
ip-dst	ip-dst	IP address destination of the netflow	-
ip-src	ip-src	IP address source of the netflow	-
tcp-flags	text	TCP flags of the flow	✔
first-packet-seen	datetime	First packet seen in this flow	-
packet-count	counter	Packets counted in this flow	✔
src-port	port	Source port of the netflow	-
direction	text	Direction of this flow ['Ingress', 'Egress']	✔
dst-as	AS	Destination AS number for this flow	-
flow-count	counter	Flows counted in this flow	✔
icmp-type	text	ICMP type of the flow (if the traffic is ICMP)	✔

Object attribute	MISP attribute type	Description	Disable correlation
src-as	AS	Source AS number for this flow	-
last-packet-seen	datetime	Last packet seen in this flow	-
byte-count	counter	Bytes counted in this flow	✔
protocol	text	Protocol used for this flow ['TCP', 'UDP', 'ICMP', 'IP']	-

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
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.	✔
time_last	datetime	Last time that the unique tuple (rrname, rrtype, rdata) record has been seen by the passive DNS	✔

Object attribute	MISP attribute type	Description	Disable correlation
rrtype	text	Resource Record type as seen by the passive DNS. ['A', 'AAAA', 'CNAME', 'PTR', 'SOA', 'TXT', 'DNAME', 'NS', 'SRV', 'RP', 'NAPTR', 'HINFO', 'A6']	✔
zone_time_last	datetime	Last time that the unique tuple (rrname, rrtype, rdata) record has been seen via master file import.	✔
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	✔
rdata	text	Resource records of the queried resource	✘
origin	text	Origin of the Passive DNS response	✔
rrname	text	Resource Record name of the queried resource.	✘
zone_time_first	datetime	First time that the unique tuple (rrname, rrtype, rdata) record has been seen via master file import	✔
time_first	datetime	First time that the unique tuple (rrname, rrtype, rdata) 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.	✔
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']	-
first-seen	datetime	When the paste has been accessible or seen for the first time.	✔
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
internal-filename	filename	InternalFilename in the resources	✔
number-sections	counter	Number of sections	✔
pehash	pehash	Hash of the structural information about a sample. See https://www.usenix.org/legacy/event/leet09/tech/full_papers/wicherski/wicherski_html/	-
company-name	text	CompanyName in the resources	✔
compilation-timestamp	datetime	Compilation timestamp defined in the PE header	-
imphash	imphash	Hash (md5) calculated from the import table	-
lang-id	text	Lang ID in the resources	✔
text	text	Free text value to attach to the PE	✔
product-version	text	ProductVersion in the resources	✔
original-filename	filename	OriginalFilename in the resources	✔
entrypoint-section-at-position	text	Name of the section and position of the section in the PE	✔
legal-copyright	text	LegalCopyright in the resources	✔

Object attribute	MISP attribute type	Description	Disable correlation
file-version	text	FileVersion in the resources	✔
product-name	text	ProductName in the resources	✔
impfuzzy	impfuzzy	Fuzzy Hash (ssdeep) calculated from the import table	-
type	text	Type of PE ['exe', 'dll', 'driver', 'unknown']	✔
entrypoint-address	text	Address of the entry point	✔
file-description	text	FileDescription 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
text	text	Free text value to attach to the section	✔
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	-
name	text	Name of the section ['.rsrc', '.reloc', '.rdata', '.data', '.text']	✔
entropy	float	Entropy of the whole section	✔
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	-

Object attribute	MISP attribute type	Description	Disable correlation
md5	md5	[Insecure] MD5 hash (128 bits)	-
size-in-bytes	size-in-bytes	Size of the section, in bytes	✔
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	-
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	-
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	-
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	-
characteristic	text	Characteristic of the section ['read', 'write', 'executable']	-
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	-
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	-

person

An person 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
last-name	last-name	Last name of a natural person.	-

Object attribute	MISP attribute type	Description	Disable correlation
text	text	A description of the person or identity.	✔
place-of-birth	place-of-birth	Place of birth of a natural person.	✔
mothers-name	text	Mother name, father, second name or other names following country's regulation.	-
social-security-number	text	Social security number	-
alias	text	Alias name or known as.	-
title	text	Title of the natural person such as Dr. or equivalent.	✔
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.	-
passport-number	passport-number	The passport number of a natural person.	-
passport-expiration	passport-expiration	The expiration date of a passport.	✔
nationality	nationality	The nationality of a natural person.	✔
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).	-

Object attribute	MISP attribute type	Description	Disable correlation
passport-country	passport-country	The country in which the passport was issued.	✔
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.	-

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
text	text	A description of the phone.	✔
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
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.	✗
first-seen	datetime	When the phone has been accessible or seen for the first time.	✓
gummei	text	Globally Unique MME Identifier (GUMMEI) is composed from MCC, MNC and MME Identifier (MMEI).	✗
serial-number	text	Serial Number.	✗
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.	✗

Object attribute	MISP attribute type	Description	Disable correlation
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.	-
tmsi	text	Temporary Mobile Subscriber Identities (TMSI) to visiting mobile subscribers can be allocated.	-
last-seen	datetime	When the phone has been accessible or seen for the last time.	✔

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
local-references	counter	Amount of API calls inside a code section	✔
callbacks	counter	Amount of callbacks (functions started as thread)	✔
miss-api	counter	Amount of API call reference that does not resolve to a function offset	✔

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.)	✔
memory-allocations	counter	Amount of memory allocations	✔
refsglobalvar	counter	Amount of API calls outside of code section (glob var, dynamic API)	✔
shortest-path-to-create-thread	counter	Shortest path to the first time the binary calls CreateThread	✔
create-thread	counter	Amount of calls to CreateThread	✔
referenced-strings	counter	Amount of referenced strings	✔
total-functions	counter	Total amount of functions in the file.	✔
text	text	Description of the r2graphity object	✔
gml	attachment	Graph export in G>raph Modelling Language format	✔
callback-average	counter	Average size of a callback	✔
ratio-api	float	Ratio: amount of API calls per kilobyte of code section	✔

Object attribute	MISP attribute type	Description	Disable correlation
r2-commit-version	text	Radare2 commit ID used to generate this object	✔
not-referenced-strings	counter	Amount of not referenced strings	✔
unknown-references	counter	Amount of API calls not ending in a function (Radare2 bug, probalby)	✔
ratio-functions	float	Ratio: amount of functions per kilobyte of code section	✔
ratio-string	float	Ratio: amount of referenced strings per kilobyte of code section	✔
callback-largest	counter	Largest callback	✔
total-api	counter	Total amount of API calls	✔
get-proc-address	counter	Amount of calls to GetProcAddress	✔

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
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']	-
regexp	text	regexp	-
regexp-type	text	Type of the regular expression syntax. ['PCRE', 'PCRE2', 'POSIX BRE', 'POSIX ERE']	✔
comment	comment	A description of the regular expression.	-

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
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']	✔
name	text	Name of the registry key	-
last-modified	datetime	Last time the registry key has been modified	-
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']	✔
hive	text	Hive used to store the registry key (file on disk)	✔

Object attribute	MISP attribute type	Description	Disable correlation
data	text	Data stored in the registry key	-
key	regkey	Full key path	-

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
constituency	text	Constituency of the RTIR ticket	-
subject	text	Subject 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	-

Object attribute	MISP attribute type	Description	Disable correlation
ip	ip-dst	IPs automatically extracted from the RTIR ticket	-
classification	text	Classification 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
score	text	Score	✔
web-sandbox	text	A web sandbox where results are publicly available via an URL ['malwr', 'hybrid-analysis']	✔
results	text	Freetext result values	✔
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']	✔

Object attribute	MISP attribute type	Description	Disable correlation
sandbox-type	text	The type of sandbox used ['on-premise', 'web', 'saas']	✔
raw-report	text	Raw report from sandbox	✔
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']	✔

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
text	text	Additional signature description	✔
datetime	datetime	Datetime	✔
signature	text	Name of detection signature - set the description of the detection signature as a comment	-
software	text	Name of Sandbox software	✔

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
MapVersion	text	Map version. ['1', '2', '3']	✔
MapGsmscfGT	text	MAP GSMSCF GT. Phone number.	-
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.	✔
MapVlrGT	text	MAP VLR GT. Phone number.	-
MapUssdContent	text	MAP USSD Content.	-
MapSmsText	text	MAP SMS Text. Important indicators in SMS text.	-
MapSmsTypeNumber	text	MAP SMS TypeNumber.	✔
MapSmsTP-DCS	text	MAP SMS TP-DCS.	✔
MapMscGT	text	MAP MSC GT. Phone number.	-
MapMsisdn	text	MAP MSISDN. Phone number.	-

Object attribute	MISP attribute type	Description	Disable correlation
SccpCgPC	text	Signaling Connection Control Part (SCCP) CgPC - Phone number.	-
text	text	A description of the attack seen via SS7 logging.	✔
MapSmsTP-OA	text	MAP SMS TP-OA. Phone number.	-
MapSmscGT	text	MAP SMSC. Phone number.	-
MapUssdCoding	text	MAP USSD Content.	✔
first-seen	datetime	When the attack has been seen for the first time.	✔
SccpCgGT	text	Signaling Connection Control Part (SCCP) CgGT - Phone number.	-
SccpCdGT	text	Signaling Connection Control Part (SCCP) CdGT - Phone number.	-
MapImsi	text	MAP IMSI. Phone number starting with MCC/MNC.	-
MapGmlc	text	MAP GMLC. Phone number.	-
Category	text	Category ['Cat0', 'Cat1', 'Cat2.1', 'Cat2.2', 'Cat3.1', 'Cat3.2', 'Cat3.3', 'CatSMS', 'CatSpoofing']	✔
MapSmsTP-PID	text	MAP SMS TP-PID.	✔

Object attribute	MISP attribute type	Description	Disable correlation
SccpCdPC	text	Signaling Connection Control Part (SCCP) CdPC - 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.	✔
published	datetime	router's publication time. This can be different from first-seen and last-seen.	✔

Object attribute	MISP attribute type	Description	Disable correlation
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.	-
description	text	Tor node description.	✔
version_line	text	versioning information reported by the node.	-
nickname	text	router's nickname.	-
fingerprint	text	router's fingerprint.	-
document	text	Raw document from the consensus.	✔
first-seen	datetime	When the Tor node designed by the IP address has been seen for the first time.	✔
address	ip-src	IP address of the Tor node seen.	-
last-seen	datetime	When the Tor node designed by the IP address has been seen for the last time.	✔

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

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
external	target-external	External target organisations affected by this attack.	-
node	target-machine	Name(s) of node that was targeted.	-
sectors	text	The list of sectors that the victim belong to ['agriculture', 'aerospace', 'automotive', 'communications', 'construction', 'defence', 'education', 'energy', 'engineering', 'entertainment', 'financial services', 'government national', 'government regional', 'government local', 'government public services', 'healthcare', 'hospitality leisure', 'infrastructure', 'insurance', 'manufacturing', 'mining', 'non profit', 'pharmaceuticals', 'retail', 'technology', 'telecommunications', 'transportation', 'utilities']	-

Object attribute	MISP attribute type	Description	Disable correlation
name	target-org	The name of the department(s) or organisation(s) targeted.	-
ip-address	ip-dst	IP address(es) of the node targeted.	-
roles	text	The list of roles targeted within the victim.	-
description	text	Description of the victim	-
classification	text	The type of entity being targeted. ['individual', 'group', 'organization', 'class', 'unknown']	✔
user	target-user	The username(s) of the user targeted.	-
regions	target-location	The list of regions or locations from the victim targeted. ISO 3166 should be used.	-
email	target-email	The email address(es) of the user 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
community-score	text	Community Score	✔

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

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
text	text	Description of the vulnerability	-
published	datetime	Initial publication date	✔
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.	-
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']	✔

Object attribute	MISP attribute type	Description	Disable correlation
modified	datetime	Last modification date	✔
vulnerable_configuration	text	The vulnerable configuration is described in CPE format	-
created	datetime	First time when the vulnerability was discovered	✔
summary	text	Summary of the vulnerability	-
references	link	External references	-

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
registrant-org	whois-registrant-org	Registrant organisation	-
text	text	Full whois entry	✔
registrar	whois-registrar	Registrar of the whois entry	-
expiration-date	datetime	Expiration of the whois entry	✔
registrant-name	whois-registrant-name	Registrant name	-
nameserver	hostname	Nameserver	✔
modification-date	datetime	Last update of the whois entry	✔

Object attribute	MISP attribute type	Description	Disable correlation
registrant-email	whois-registrant-email	Registrant email address	-
domain	domain	Domain of the whois entry	-
registrant-phone	whois-registrant-phone	Registrant phone number	-
creation-date	datetime	Initial creation 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
text	text	Free text description of hte certificate	-
pubkey-info-algorithm	text	Algorithm of the public key	-
validity-not-before	datetime	Certificate invalid before that date	-
pubkey-info-size	text	Length of the public key (in bits)	-
validity-not-after	datetime	Certificate invalid after that date	-
x509-fingerprint-sha1	x509-fingerprint-sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	-
x509-fingerprint-md5	x509-fingerprint-md5	[Insecure] MD5 hash (128 bits)	-

Object attribute	MISP attribute type	Description	Disable correlation
pubkey-info-modulus	text	Modulus of the public key	-
pubkey-info-exponent	text	Exponent of the public key	-
serial-number	text	Serial number of the certificate	-
subject	text	Subject of the certificate	-
x509-fingerprint-sha256	x509-fingerprint-sha256	Secure Hash Algorithm 2 (256 bits)	-
raw-base64	text	Raw certificate base64 encoded	-
issuer	text	Issuer of the certificate	-
version	text	Version of the certificate	-

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-hunt	yara	Wide yara rule generated from -yh.	✔
version	comment	yabin.py and regex.txt version used for the generation of the yara rules.	-
whitelist	comment	Whitelist name used to generate the rules.	-

Object attribute	MISP attribute type	Description	Disable correlation
comment	comment	A description of Yara rule generated.	-
yara	yara	Yara rule generated from -y.	✔

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']
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']

Name of relationship	Description	Format
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']
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']

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

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

Name of relationship	Description	Format
subgroup	This relationship describes an object which is a subgroup of another object.	['cert-eu']
suspected-link	This relationship describes an object which is suspected to be linked with another object.	['misp']
same-as	This relationship describes an object which is the same as another object.	['misp']
creator-of	This relationship describes an object which is the creator of another object.	['cert-eu']
developer-of	This relationship describes an object which is a developer of another object.	['cert-eu']
uses-for-recon	This relationship describes an object which uses another object for recon.	['cert-eu']
operator-of	This relationship describes an object which is an operator of another object.	['cert-eu']
overlaps	This relationship describes an object which overlaps another object.	['cert-eu']
owner-of	This relationship describes an object which owns another object.	['cert-eu']
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']