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
duplicate_number	counter	Number of known duplicates.	▬
raw-data	attachment	Raw data as received by the AIL sensor compressed and encoded in Base64.	✔
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.	▬
last-seen	datetime	When the leak has been accessible or seen for the last time.	✔
first-seen	datetime	When the leak has been accessible or seen for the first time.	✔
origin	text	The link where the leak is (or was) accessible at first-seen.	▬

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	text	Duplicate of the existing leaks.	▬
original-date	datetime	When the information available in the leak was created. It's usually before the first-seen.	✔

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	▬

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](#).

'ECTION_SERVICE',
'BIND_TEXT_SERVICE',
'BIND_TV_INPUT',
'BIND_VISUAL_VOICEM
AIL_SERVICE',
'BIND_VOICE_INTERAC
TION',
'BIND_VPN_SERVICE',

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

'DUMP',
'EXPAND_STATUS_BAR',
'FACTORY_TEST',

Object attribute	MISP attribute type	Description	Disable correlation
mp-import	text	The inbound IPv4 or IPv6 routing policy of the AS in RFC 4012 – Routing Policy Specification Language next generation (RPSLng), section 4.5. format	▬
subnet-announced	ip-src	Subnet announced	▬
description	text	Description of the autonomous system	▬
export	text	The outbound routing policy of the AS in RFC 2622 – Routing Policy Specification Language (RPSL) format	▬

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.

', 'MASTER_CLEAR', 'MEDIA_CONTENT_CONTROL', 'MODIFY_AUDIO_SETTINGS', 'MODIFY_PHONE_STAT MOUNT_FORMAT_FIL ESYSTEMS',

Object attribute	MISP attribute type	Description	Disable correlation
signature	text	Name of detection signature	▬
software	text	Name of antivirus software	✔
datetime	datetime	Datetime	✔
text	text	Free text value to attach to the file	✔

'READ_FRAME_BUFFER ', 'READ_INPUT_STATE', 'READ_LOGS', 'READ_PHONE_NUMBE RS', 'READ_PHONE_STATE',

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
address	btc	Address used as a payment destination in a cryptocurrency	▬
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	✔
text	text	Free text value	✔
first-seen	datetime	First 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	cookie	Full cookie	−
type	text	Type of cookie and how it's used in this specific object. ['Session management', 'Personalization', 'Tracking', 'Exfiltration', 'Malicious Payload', 'Beaconing']	−
text	text	A description of the cookie.	✔
cookie-name	text	Name of the cookie (if splitted)	−
cookie-value	text	Value of the cookie (if splitted)	−

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)	−
notification	text	Mention of any notification(s) towards the potential owner(s) of the credential(s) ['victim-notified', 'service-notified', 'none']	−

Object attribute	MISP attribute type	Description	Disable correlation
text	text	A description of the credential(s)	✔
format	text	Format of the password(s) ['clear-text', 'hashed', 'encrypted', 'unknown']	▬
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']	▬
password	text	Password	▬

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
comment	comment	A description of the card.	▬
expiration	datetime	Maximum date of validity	▬
cc-number	cc-number	credit-card number as encoded on the card.	▬

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

WRITE_SYNC_SETTING
S',
'WRITE_VOICEMAIL']

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
total-pps	counter	Packets per second	▬
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	▬
last-seen	datetime	End of the attack	✔
text	text	Description of the DDoS	✔
domain-dst	domain	Destination domain (victim)	▬

Object attribute	MISP attribute type	Description	Disable correlation
dst-port	port	Destination port of the attack	▬
ip-src	ip-src	IP address originating the attack	▬
total-bps	counter	Bits per second	▬
first-seen	datetime	Beginning of the attack	✔

domain-ip

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

ℹ️ 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	▬
last-seen	datetime	Last time the tuple has been seen	✔
domain	domain	Domain name	▬
text	text	A description of the tuple	✔
first-seen	datetime	First time the tuple has been seen	✔

elf

Object describing a Executable and Linkable Format.

ℹ️ 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
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
text	text	Free text value to attach to the ELF	✔
entrypoint-address	text	Address of the entry point	✔
type	text	Type of ELF ['CORE', 'DYNAMIC', 'EXECUTABLE', 'HIPROC', 'LOPROC', 'NONE', 'RELOCATABLE']	▬
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']	▬

ARC_COMPACT2', 'OPEN8', 'RL78', 'VIDEOCORE5', 'ARCH_78KOR',

elf-section

Object describing a section of an Executable and Linkable Format. 'ARCH_5E800EX', 'BA1', 'BA2', 'XCORE',

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. 'MCHP_PIC', 'INTEL205', 'INTEL206', 'INTEL207', 'INTEL208', 'INTEL209',

Object attribute	MISP attribute type	Description	Disable correlation
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	▬
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	▬

Object attribute	MISP attribute type	Description	Disable correlation
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	▬
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	▬
md5	md5	[Insecure] MD5 hash (128 bits)	▬
name	text	Name of the section	✔
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	▬
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']	✔
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	▬
text	text	Free text value to attach to the section	✔
entropy	float	Entropy of the whole section	✔

Object attribute	MISP attribute type	Description	Disable correlation
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	▬
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)	▬
size-in-bytes	size-in-bytes	Size of the section, in bytes	✔

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
to	email-dst	Destination email address	—
subject	email-subject	Subject	—
cc	email-dst	Carbon copy	—
from	email-src	Sender email address	—
to-display-name	email-dst-display-name	Display name of the receiver	—
message-id	email-message-id	Message ID	—
x-mailer	email-x-mailer	X-Mailer generally tells the program that was used to draft and send the original email	—
from-display-name	email-src-display-name	Display name of the sender	—
mime-boundary	email-mime-boundary	MIME Boundary	—
thread-index	email-thread-index	Identifies a particular conversation thread	—
reply-to	email-reply-to	Email address the reply will be sent to	—
return-path	text	Message return path	—
screenshot	attachment	Screenshot of email	—
send-date	datetime	Date the email has been sent	✔
header	email-header	Full headers	—
attachment	email-attachment	Attachment	—

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
tlsh	tlsh	Fuzzy hash by Trend Micro: Locality Sensitive Hash	▬
certificate	x509-fingerprint-sha1	Certificate value if the binary is signed with another authentication scheme than authenticode	▬
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	▬
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	▬
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	▬
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	▬
state	text	State of the file ['Malicious', 'Harmless', 'Signed', 'Revoked', 'Expired', 'Trusted']	✔
md5	md5	[Insecure] MD5 hash (128 bits)	▬
pattern-in-file	pattern-in-file	Pattern that can be found in the file	▬

Object attribute	MISP attribute type	Description	Disable correlation
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	▬
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	▬
text	text	Free text value to attach to the file	✔
filename	filename	Filename on disk	▬
entropy	float	Entropy of the whole file	✔
authentihash	authentihash	Authenticode executable signature hash	▬
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	▬
malware-sample	malware-sample	The file itself (binary)	▬
mimetype	text	Mime type	✔
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	▬
size-in-bytes	size-in-bytes	Size of the file, in bytes	✔

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

http-request

A single HTTP request header.

ℹ️ 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
content-type	other	The MIME type of the body of the request	▬
referer	referer	This is the address of the previous web page from which a link to the currently requested page was followed	▬
basicauth-user	text	HTTP Basic Authentication Username	▬
proxy-user	text	HTTP Proxy Username	▬
cookie	text	An HTTP cookie previously sent by the server with Set-Cookie	▬
proxy-password	text	HTTP Proxy Password	▬
method	http-method	HTTP Method invoked (one of GET, POST, PUT, HEAD, DELETE, OPTIONS, CONNECT)	✔
basicauth-password	text	HTTP Basic Authentication Password	▬
host	hostname	The domain name of the server	▬
text	text	HTTP Request comment	✔
user-agent	user-agent	The user agent string of the user agent	▬
uri	uri	Request URI	▬
url	url	Full HTTP Request URL	▬

ip-port

An IP address and a port seen as a tuple (or as a triple) in a specific time frame..

ℹ️ 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	✔
text	text	Description of the tuple	✔
first-seen	datetime	First time the tuple has been seen	✔
dst-port	port	Destination port	▬
src-port	port	Source port	▬
ip	ip-dst	IP Address	▬

ja3

JA3 is a new technique for creating SSL client fingerprints that are easy to produce and can be easily shared for threat intelligence. Fingerprints are composed of Client Hello packet; SSL Version, Accepted Ciphers, List of Extensions, Elliptic Curves, and Elliptic Curve Formats. https://github.com/salesforce/ja3.

ℹ️ 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
description	text	Type of detected software ie software, malware	▬
ip-dst	ip-dst	Destination IP address	▬
last-seen	datetime	Last seen of the SSL/TLS handshake	✔

Object attribute	MISP attribute type	Description	Disable correlation
first-seen	datetime	First seen of the SSL/TLS handshake	✔
ip-src	ip-src	Source IP Address	▬
ja3-fingerprint-md5	md5	Hash identifying source	▬

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
number-sections	counter	Number of sections	✔
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	✔
name	text	Binary's name	▬
entrypoint-address	text	Address of the entry point	✔

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
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	▬
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	▬
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	▬
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	▬
md5	md5	[Insecure] MD5 hash (128 bits)	▬
name	text	Name of the section	✔
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	▬
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	▬
text	text	Free text value to attach to the section	✔
entropy	float	Entropy of the whole section	✔
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	▬
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	▬
size-in-bytes	size-in-bytes	Size of the section, in bytes	✔

microblog

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

ℹ️ 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
url	url	Original URL location of the microblog post	▬
username	text	Username who posted the microblog post	▬
username-quoted	text	Username who are quoted into the microblog post	▬
creation-date	datetime	Initial creation of the microblog post	▬
link	url	Link into the microblog post	▬
modification-date	datetime	Last update of the microblog post	▬
removal-date	datetime	When the microblog post was removed	▬
type	text	Type of the microblog post ['Twitter', 'Facebook', 'LinkedIn', 'Reddit', 'Google+', 'Instagram', 'Forum', 'Other']	▬
post	text	Raw post	▬

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

Object attribute	MISP attribute type	Description	Disable correlation
dst-port	port	Destination port of the netflow	—
src-port	port	Source port of the netflow	—
first-packet-seen	datetime	First packet seen in this flow	—

passive-dns

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

ℹ️ 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_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	—
sensor_id	text	Sensor information where the record was seen	—
bailiwick	text	Best estimate of the apex of the zone where this data is authoritative	—
rdata	text	Resource records of the queried resource	—

Object attribute	MISP attribute type	Description	Disable correlation
rrname	text	Resource Record name of the queried resource	▬
rrtype	text	Resource Record type as seen by the passive DNS ['A', 'AAAA', 'CNAME', 'PTR', 'SOA', 'TXT', 'DNAME', 'NS', 'SRV', 'RP', 'NAPTR', 'HINFO', 'A6']	▬
text	text	▬	▬
time_last	datetime	Last time that the unique tuple (rrname, rrtype, rdata) record has been seen by the passive DNS	▬
zone_time_last	datetime	Last time that the unique tuple (rrname, rrtype, rdata) record has been seen via master file import	▬
origin	text	Origin of the Passive DNS response	▬
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	▬

paste

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

ℹ️ 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
url	url	Link to the original source of the paste or post.	—
last-seen	datetime	When the paste has been accessible or seen for the last time.	✔
title	text	Title of the paste or post.	—
paste	text	Raw text of the paste or post	—
first-seen	datetime	When the paste has been accessible or seen for the first time.	✔
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']	—

pe

Object describing a Portable Executable.

ℹ️ 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
number-sections	counter	Number of sections	✔
legal-copyright	text	LegalCopyright in the resources	✔

Object attribute	MISP attribute type	Description	Disable correlation
internal-filename	filename	InternalFilename in the resources	▬
entrypoint-section-at-position	text	Name of the section and position of the section in the PE	✔
entrypoint-address	text	Address of the entry point	✔
lang-id	text	Lang ID in the resources	✔
file-version	text	FileVersion in the resources	✔
product-version	text	ProductVersion in the resources	✔
pehash	pehash	Hash of the structural information about a sample. See https://www.usenix.org /legacy/event/leet09/ tech/full_papers/ wicherski/ wicherski_html/	▬
file-description	text	FileDescription in the resources	✔
compilation-timestamp	datetime	Compilation timestamp defined in the PE header	▬
text	text	Free text value to attach to the PE	✔
company-name	text	CompanyName in the resources	✔
product-name	text	ProductName in the resources	✔

Object attribute	MISP attribute type	Description	Disable correlation
impfuzzy	impfuzzy	Fuzzy Hash (ssdeep) calculated from the import table	▬
type	text	Type of PE ['exe', 'dll', 'driver', 'unknown']	✔
imphash	imphash	Hash (md5) calculated from the import table	▬
original-filename	filename	OriginalFilename in the resources	▬

pe-section

Object describing a section of a Portable Executable.

> ℹ 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
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	▬
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	▬
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	▬
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	▬
md5	md5	[Insecure] MD5 hash (128 bits)	▬
name	text	Name of the section ['.rsrc', '.reloc', '.rdata', '.data', '.text']	✔

Object attribute	MISP attribute type	Description	Disable correlation
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	▬
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	▬
characteristic	text	Characteristic of the section ['read', 'write', 'executable']	▬
text	text	Free text value to attach to the section	✔
entropy	float	Entropy of the whole section	✔
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	▬
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	▬
size-in-bytes	size-in-bytes	Size of the section, in bytes	✔

person

An person which describes a person or an identity..

ℹ️ 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
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
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.	▬
place-of-birth	place-of-birth	Place of birth of a natural person.	▬
middle-name	middle-name	Middle name of a natural person	▬
gender	gender	The gender of a natural person. ['Male', 'Female', 'Other', 'Prefer not to say']	▬
last-name	last-name	Last name of a natural person.	▬
nationality	nationality	The nationality of a natural person.	▬
text	text	A description of the person or identity.	✔
passport-expiration	passport-expiration	The expiration date of a passport.	▬

Object attribute	MISP attribute type	Description	Disable correlation
first-name	first-name	First name of a natural person.	—
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
gummei	text	Globally Unique MME Identifier (GUMMEI) is composed from MCC, MNC and MME Identifier (MMEI).	—
guti	text	Globally Unique Temporary UE Identity (GUTI) is a temporary identification to not reveal the phone (user equipment in 3GPP jargon) composed of GUMMEI and the M-TMSI.	—
imei	text	International Mobile Equipment Identity (IMEI) is a number, usually unique, to identify 3GPP and iDEN mobile phones, as well as some satellite phones.	—
last-seen	datetime	When the phone has been accessible or seen for the last time.	✔

Object attribute	MISP attribute type	Description	Disable correlation
text	text	A description of the phone.	✔
first-seen	datetime	When the phone has been accessible or seen for the first time.	✔
serial-number	text	Serial Number.	▬
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.	▬
tmsi	text	Temporary Mobile Subscriber Identities (TMSI) to visiting mobile subscribers can be allocated.	▬

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.	—

r2graphity

Indicators extracted from files using radare2 and graphml.

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

Object attribute	MISP attribute type	Description	Disable correlation
callback-average	counter	Average size of a callback	✔
not-referenced-strings	counter	Amount of not referenced strings	✔
miss-api	counter	Amount of API call reference that does not resolve to a function offset	✔
callbacks	counter	Amount of callbacks (functions started as thread)	✔

Object attribute	MISP attribute type	Description	Disable correlation
memory-allocations	counter	Amount of memory allocations	✔
ratio-api	float	Ratio: amount of API calls per kilobyte of code section	✔
local-references	counter	Amount of API calls inside a code section	✔
referenced-strings	counter	Amount of referenced strings	✔
ratio-string	float	Ratio: amount of referenced strings per kilobyte of code section	✔
r2-commit-version	text	Radare2 commit ID used to generate this object	✔
total-functions	counter	Total amount of functions in the file.	✔
total-api	counter	Total amount of API calls	✔
shortest-path-to-create-thread	counter	Shortest path to the first time the binary calls CreateThread	✔
get-proc-address	counter	Amount of calls to GetProcAddress	✔
gml	attachment	Graph export in G>raph Modelling Language format	✔
create-thread	counter	Amount of calls to CreateThread	✔

Object attribute	MISP attribute type	Description	Disable correlation
refsglobalvar	counter	Amount of API calls outside of code section (glob var, dynamic API)	✔
callback-largest	counter	Largest callback	✔
text	text	Description of the r2graphity object	✔
unknown-references	counter	Amount of API calls not ending in a function (Radare2 bug, probalby)	✔
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.)	✔
ratio-functions	float	Ratio: amount of functions per kilobyte of code section	✔

regexp

An object describing a regular expression (regex or regexp). The object can be linked via a relationship to other attributes or objects to describe how it can be represented as a regular expression..

ℹ️ 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
comment	comment	A description of the regular expression.	▬
regexp	text	regexp	▬

Object attribute	MISP attribute type	Description	Disable correlation
regexp-type	text	Type of the regular expression syntax. ['PCRE', 'PCRE2', 'POSIX BRE', 'POSIX ERE']	✔

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	reg-datatype	Registry value type ['REG_NONE', 'REG_SZ', 'REG_EXPAND_SZ', 'REG_BINARY', 'REG_DWORD', 'REG_DWORD_LITTLE_ENDIAN', 'REG_DWORD_BIG_EN DIAN', 'REG_LINK', 'REG_MULTI_SZ', 'REG_RESOURCE_LIST', 'REG_FULL_RESOURCE _DESCRIPTOR', 'REG_RESOURCE_REQU IREMENTS_LIST', 'REG_QWORD', 'REG_QWORD_LITTLE_ ENDIAN']	▬
data	reg-data	Data stored in the registry key	▬
hive	reg-hive	Hive used to store the registry key (file on disk)	▬
last-modified	datetime	Last time the registry key has been modified	▬

Object attribute	MISP attribute type	Description	Disable correlation
name	reg-name	Name of the registry key	—
key	reg-key	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
summary	text	Free text summary of the report	—
case-number	text	Case number	—

rtir

RTIR - Request Tracker for Incident Response.

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

Object attribute	MISP attribute type	Description	Disable correlation
constituency	text	Constituency of the RTIR ticket	—
ticket-number	text	ticket-number of the RTIR ticket	—
subject	text	Subject of the RTIR ticket	—
status	text	Status of the RTIR ticket ['new', 'open', 'stalled', 'resolved', 'rejected', 'deleted']	—

Object attribute	MISP attribute type	Description	Disable correlation
ip	ip-dst	IPs automatically extracted from the RTIR ticket	▬
classification	text	Classification of the RTIR ticket	▬
queue	text	Queue of the RTIR ticket ['incident', 'investigations', 'blocks', 'incident reports']	▬

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
nickname	text	router's nickname.	▬
fingerprint	text	router's fingerprint.	▬
flags	text	list of flag associated with the node.	▬
published	datetime	router's publication time. This can be different from first-seen and last-seen.	✔
document	text	Raw document from the consensus.	✔
address	ip-src	IP address of the Tor node seen.	▬
description	text	Tor node description.	✔

Object attribute	MISP attribute type	Description	Disable correlation
last-seen	datetime	When the Tor node designed by the IP address has been seen for the last time.	✔
version_line	text	versioning information reported by the node.	▬
text	text	Tor node comment.	✔
first-seen	datetime	When the Tor node designed by the IP address has been seen for the first time.	✔
version	text	parsed version of tor, this is None if the relay's using a new versioning scheme.	▬

url

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

ℹ️   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
resource_path	text	Path (between hostname:port and query)	▬
domain_without_tld	text	Domain without Top-Level Domain	▬
tld	text	Top-Level Domain	✔
credential	text	Credential (username, password)	▬

Object attribute	MISP attribute type	Description	Disable correlation
fragment	text	Fragment identifier is a short string of characters that refers to a resource that is subordinate to another, primary resource.	▬
url	url	Full URL	▬
port	port	Port number	✔
last-seen	datetime	Last time this URL has been seen	✔
domain	domain	Full domain	▬
text	text	Description of the URL	▬
first-seen	datetime	First time this URL has been seen	✔
subdomain	text	Subdomain	✔
host	hostname	Full hostname	▬
scheme	text	Scheme ['http', 'https', 'ftp', 'gopher', 'sip']	✔
query_string	text	Query (after path, preceded by '?')	▬

victim

Victim object describes the target of an attack or abuse..

> ℹ 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.	▬

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

Object attribute	MISP attribute type	Description	Disable correlation
ip-address	ip-dst	IP address(es) of the node targeted.	▬
classification	text	The type of entity being targeted. ['individual', 'group', 'organization', 'class', 'unknown']	✔
name	target-org	The name of the department(s) or organisation(s) targeted.	▬
node	target-machine	Name(s) of node that was targeted.	▬

virustotal-report

VirusTotal report.

ℹ 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
permalink	link	Permalink Reference	▬
first-submission	datetime	First Submission	▬
community-score	text	Community Score	✔
detection-ratio	text	Detection Ratio	✔
last-submission	datetime	Last Submission	▬

vulnerability

Vulnerability object describing common vulnerability enumeration.

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

Object attribute	MISP attribute type	Description	Disable correlation
references	link	External references	▬
modified	datetime	Last modification date	▬
text	text	Description of the vulnerability	▬
vulnerable_configuration	text	The vulnerable configuration is described in CPE format	▬
published	datetime	Initial publication date	▬
summary	text	Summary of the vulnerability	▬
id	vulnerability	Vulnerability ID (generally CVE, but not necessarely)	▬

whois

Whois records information for a domain name..

> ℹ️ 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
text	text	Full whois entry	▬
registrant-name	whois-registrant-name	Registrant name	▬
creation-date	datetime	Initial creation of the whois entry	▬
registrant-email	whois-registrant-email	Registrant email address	▬
domain	domain	Domain of the whois entry	▬

Object attribute	MISP attribute type	Description	Disable correlation
registrant-phone	whois-registrant-phone	Registrant phone number	▬
modification-date	datetime	Last update of the whois entry	▬
registrar	whois-registrar	Registrar of the whois entry	▬
expiration-date	datetime	Expiration 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
x509-fingerprint-sha256	sha256	Secure Hash Algorithm 2 (256 bits)	▬
pubkey-info-size	text	Length of the public key (in bits)	▬
subject	text	Subject of the certificate	▬
pubkey-info-exponent	text	Exponent of the public key	▬
serial-number	text	Serial number of the certificate	▬
x509-fingerprint-md5	md5	[Insecure] MD5 hash (128 bits)	▬
pubkey-info-algorithm	text	Algorithm of the public key	▬
issuer	text	Issuer of the certificate	▬

Object attribute	MISP attribute type	Description	Disable correlation
validity-not-before	datetime	Certificate invalid before that date	▬
validity-not-after	datetime	Certificate invalid after that date	▬
x509-fingerprint-sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	▬
text	text	Free text description of hte certificate	▬
raw-base64	text	Raw certificate base64 encoded	▬
version	text	Version of the certificate	▬
pubkey-info-modulus	text	Modulus of the public key	▬

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
version	comment	yabin.py and regex.txt version used for the generation of the yara rules.	▬
comment	comment	A description of Yara rule generated.	▬
whitelist	comment	Whitelist name used to generate the rules.	▬

Object attribute	MISP attribute type	Description	Disable correlation
yara	yara	Yara rule generated from -y.	✔
yara-hunt	yara	Wide yara rule generated from -yh.	✔

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']
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']
calls	This relationship describes an object which calls another objects.	['misp']

Name of relationship	Description	Format
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']
attacking-other-group	This relationship describes an object which attacks another object.	['cert-eu']

Name of relationship	Description	Format
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']
subgroup	This relationship describes an object which is a subgroup of another object.	['cert-eu']

Name of relationship	Description	Format
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']