MISP Objects

MISP Objects

Generated from https://github.com/MISP/misp-objects.

MISP MISP objects to be used in MISP (2.4.80 (TBC)) 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.

ail-leak

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

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

Object attribute	MISP attribute type	Description	Disable correlation
last-seen	datetime	When the leak has been accessible or seen for the last time.	✔
text	text	A description of the leak which could include the potential victim(s) or description of the leak.	✔
original-date	datetime	When the information available in the leak was created. It's usually before the first-seen.	✔
first-seen	datetime	When the leak has been accessible or seen for the first time.	✔

Object attribute	MISP attribute type	Description	Disable correlation
origin	url	The link where the leak is (or was) accessible at first-seen.	-
type	text	Type of information leak as discovered and classified by an AIL module.	-
sensor	text	The AIL sensor uuid where the leak was processed and analysed.	-

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)	-
type	text	Type of cookie and how it's used in this specific object.	-
cookie-value	text	Value of the cookie (if splitted)	-
cookie	cookie	Full cookie	-
text	text	A description of the cookie.	✔

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
ip-dst	ip-dst	Destination ID (victim)	-
last-seen	datetime	End of the attack	-
total-bps	counter	Bits per second	-
dst-port	port	Destination port of the attack	-
text	text	Description of the DDoS	-
protocol	text	Protocol used for the attack	-
ip-src	ip-src	IP address originating the attack	-
first-seen	datetime	Beginning of the attack	-
total-pps	counter	Packets per second	-
src-port	port	Port originating the attack	-

domain|ip

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

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

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

elf

Object describing a Executable and Linkable Format.

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

Object attribute	MISP attribute type	Description	Disable correlation
os_abi	text	Header operating system application binary interface (ABI)	-
number-sections	counter	Number of sections	✔
text	text	Free text value to attach to the ELF	✔
entrypoint-address	text	Address of the entry point	✔
arch	text	Architecture of the ELF file	-
type	text	Type of ELF	-

elf-section

Object describing a section of an Executable and Linkable Format.

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

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

Object attribute	MISP attribute type	Description	Disable correlation
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
attachment	email-attachment	Attachment	-
from	email-src	Sender email address	-
reply-to	email-reply-to	Email address the reply will be sent to	-
from-display-name	email-src-display-name	Display name of the sender	-
x-mailer	email-x-mailer	X-Mailer generally tells the program that was used to draft and send the original email	-
header	email-header	Full headers	-
thread-index	email-thread-index	Identifies a particular conversation thread	-
send-date	datetime	Date the email has been sent	✔
to	email-dst	Destination email address	-
to-display-name	email-dst-display-name	Display name of the receiver	-

Object attribute	MISP attribute type	Description	Disable correlation
message-id	email-message-id	Message ID	-
subject	email-subject	Subject	-
mime-boundary	email-mime-boundary	MIME Boundary	-

file

File object describing a file with meta-information.

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

Object attribute	MISP attribute type	Description	Disable correlation
md5	md5	[Insecure] MD5 hash (128 bits)	-
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	-
authentihash	authentihash	Authenticode executable signature hash	-
text	text	Free text value to attach to the file	✔
entropy	float	Entropy of the whole file	✔
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	-
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	-
malware-sample	malware-sample	The file itself (binary)	-
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	-

Object attribute	MISP attribute type	Description	Disable correlation
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	-
size-in-bytes	size-in-bytes	Size of the file, in bytes	✔
pattern-in-file	pattern-in-file	Pattern that can be found in the file	-
tlsh	tlsh	Fuzzy hash by Trend Micro: Locality Sensitive Hash	-
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	-
mimetype	text	Mime type	✔
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	-
filename	filename	Filename on disk	-
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
city	text	City.	-
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
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.	✔
text	text	A generic description of the location.	✔
first-seen	datetime	When the location was seen for the first time.	✔
longitude	float	The longitude is the decimal value of the longitude in the World Geodetic System 84 (WGS84) reference	✔
region	text	Region.	-
country	text	Country.	-

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
content-type	other	The MIME type of the body of the request	-
text	text	HTTP Request comment	✔
basicauth-user	text	HTTP Basic Authentication Username	-

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

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
ip	ip-dst	IP Address	-

Object attribute	MISP attribute type	Description	Disable correlation
text	text	Description of the tuple	-
last-seen	datetime	Last time the tuple has been seen	-
first-seen	datetime	First time the tuple has been seen	-
src-port	text	Source port	-
dst-port	text	Destination port	-

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

passive-dns

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

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

Object attribute	MISP attribute type	Description	Disable correlation
zone_time_first	datetime	First time that the unique tuple (rrname, rrtype, rdata) record has been seen via master file import	-
rrname	text	Resource Record name of the queried resource	-
rrtype	text	Resource Record type as seen by the passive DNS	-
rdata	text	Resource records of the queried resource	-
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	-
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_first	datetime	First time that the unique tuple (rrname, rrtype, rdata) has been seen by the passive DNS	-

Object attribute	MISP attribute type	Description	Disable correlation
sensor_id	text	Sensor information where the record was seen	-
origin	text	Origin of the Passive DNS response	-
text	text	-	-
time_last	datetime	Last time that the unique tuple (rrname, rrtype, rdata) record has been seen by the passive DNS	-

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
imphash	imphash	Hash (md5) calculated from the import table	-
pehash	pehash	Hash of the structural information about a sample. See https://www.usenix.org/legacy/event/leet09/tech/full_papers/wicherski/wicherski_html/	-
text	text	Free text value to attach to the PE	✔
file-description	text	FileDescription in the resources	✔

Object attribute	MISP attribute type	Description	Disable correlation
original-filename	filename	OriginalFilename in the resources	-
internal-filename	filename	InternalFilename in the resources	-
product-version	text	ProductVersion in the resources	✔
company-name	text	CompanyName in the resources	✔
compilation-timestamp	datetime	Compilation timestamp defined in the PE header	-
lang-id	text	Lang ID in the resources	✔
product-name	text	ProductName in the resources	✔
number-sections	counter	Number of sections	✔
entrypoint-section-at-position	text	Name of the section and position of the section in the PE	✔
entrypoint-address	text	Address of the entry point	✔
file-version	text	FileVersion in the resources	✔
type	text	Type of PE	✔
impfuzzy	impfuzzy	Fuzzy Hash (ssdeep) calculated from the import table	-
legal-copyright	text	LegalCopyright in the resources	✔

pe-section

Object describing a section of a Portable Executable.

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

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

Object attribute	MISP attribute type	Description	Disable correlation
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	-
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	-

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
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.	-
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.	-
gummei	text	Globally Unique MME Identifier (GUMMEI) is composed from MCC, MNC and MME Identifier (MMEI).	-

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

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

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
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.)	✔
text	text	Description of the r2graphity object	✔
ratio-string	float	Ratio: amount of referenced strings per kilobyte of code section	✔
referenced-strings	counter	Amount of referenced strings	✔
refsglobalvar	counter	Amount of API calls outside of code section (glob var, dynamic API)	✔
ratio-api	float	Ratio: amount of API calls per kilobyte of code section	✔

Object attribute	MISP attribute type	Description	Disable correlation
get-proc-address	counter	Amount of calls to GetProcAddress	✔
memory-allocations	counter	Amount of memory allocations	✔
r2-commit-version	text	Radare2 commit ID used to generate this object	✔
gml	attachment	Graph export in G>raph Modelling Language format	✔
callback-average	counter	Average size of a callback	✔
create-thread	counter	Amount of calls to CreateThread	✔
callbacks	counter	Amount of callbacks (functions started as thread)	✔
not-referenced-strings	counter	Amount of not referenced strings	✔
local-references	counter	Amount of API calls inside a code section	✔
callback-largest	counter	Largest callback	✔
ratio-functions	float	Ratio: amount of functions per kilobyte of code section	✔
miss-api	counter	Amount of API call reference that does not resolve to a function offset	✔

Object attribute	MISP attribute type	Description	Disable correlation
unknown-references	counter	Amount of API calls not ending in a function (Radare2 bug, probalby)	✔
shortest-path-to-create-thread	counter	Shortest path to the first time the binary calls CreateThread	✔
total-api	counter	Total amount of API calls	✔
total-functions	counter	Total amount of functions in the file.	✔

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
hive	reg-hive	Hive used to store the registry key (file on disk)	-
data-type	reg-datatype	Registry value type	-
name	reg-name	Name of the registry key	-
data	reg-data	Data stored in the registry key	-
key	reg-key	Full key path	-
last-modified	datetime	Last time the registry key has been modified	-

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.	-
published	datetime	router's publication time. This can be different from first-seen and last-seen.	✔
text	text	Tor node comment.	✔
flags	text	list of flag associated with the node.	-
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.	-
description	text	Tor node description.	✔
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.	✔
fingerprint	text	router's fingerprint.	-

Object attribute	MISP attribute type	Description	Disable correlation
version_line	text	versioning information reported by the node.	-
document	text	Raw document from the consensus.	✔

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
query_string	text	Query (after path, preceded by '?')	-
port	text	Port number	-
first-seen	datetime	First time this URL has been seen	-
host	hostname	Full hostname	-
tld	text	Top-Level Domain	-
credential	text	Credential (username, password)	-
domain_without_tld	text	Domain without Top-Level Domain	-
fragment	text	Fragment identifier is a short string of characters that refers to a resource that is subordinate to another, primary resource.	-
last-seen	datetime	Last time this URL has been seen	-

Object attribute	MISP attribute type	Description	Disable correlation
resource_path	text	Path (between hostname:port and query)	-
domain	domain	Full domain	-
text	text	Description of the URL	-
url	url	Full URL	-
subdomain	text	Subdomain	-
scheme	text	Scheme	-

vulnerability

Vulnerability object describing common vulnerability enumeration.

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

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

Object attribute	MISP attribute type	Description	Disable correlation
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
creation-date	datetime	Initial creation of the whois entry	-
expiration-date	datetime	Expiration of the whois entry	-
registar	whois-registar	Registar of the whois entry	-
text	text	Full whois entry	-
registrant-name	whois-registrant-name	Registrant name	-
domain	domain	Domain of the whois entry	-
registrant-email	whois-registrant-email	Registrant email address	-
registrant-phone	whois-registrant-phone	Registrant phone number	-
modification-date	datetime	Last update 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
validity-not-before	datetime	Certificate invalid before that date	-
validity-not-after	datetime	Certificate invalid after that date	-
pubkey-info-algorithm	text	Algorithm of the public key	-
text	text	Free text description of hte certificate	-
x509-fingerprint-sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	-
pubkey-info-size	text	Length of the public key (in bits)	-
issuer	text	Issuer of the certificate	-
serial-number	text	Serial number of the certificate	-
version	text	Version of the certificate	-
x509-fingerprint-md5	md5	[Insecure] MD5 hash (128 bits)	-
pubkey-info-exponent	text	Exponent of the public key	-
subject	text	Subject of the certificate	-
x509-fingerprint-sha256	sha256	Secure Hash Algorithm 2 (256 bits)	-
pubkey-info-modulus	text	Modulus of the public key	-
raw-base64	text	Raw certificate base64 encoded	-

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']
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']

Name of relationship	Description	Format
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']