MISP Objects

MISP Objects

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

MISP MISP objects to be used in MISP (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.

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
sensor	text	-	-
first-seen	datetime	-	✔
origin	url	-	-
original-date	datetime	-	✔
text	text	-	✔
type	text	Type of information leak as discovered and classified by an AIL module. ['Credential', 'CreditCards', 'Mail', 'Onion', 'Phone', 'Keys']	-
last-seen	datetime	-	✔

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
text	text	-	✔
cookie-value	text	-	-
type	text	Type of cookie and how it's used in this specific object. ['Session management', 'Personalization', 'Tracking', 'Exfiltration', 'Malicious Payload', 'Beaconing']	-
cookie-name	text	-	-
cookie	cookie	-	-

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
expiration	datetime	-	-
version	text	-	-
issued	datetime	-	-

Object attribute	MISP attribute type	Description	Disable correlation
comment	comment	-	-
card-security-code	text	-	-
cc-number	cc-number	-	-
name	text	-	-

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
first-seen	datetime	-	-
last-seen	datetime	-	-
protocol	text	Protocol used for the attack ['TCP', 'UDP', 'ICMP', 'IP']	-
ip-dst	ip-dst	-	-
text	text	-	-
total-bps	counter	-	-
src-port	port	-	-
ip-src	ip-src	-	-
total-pps	counter	-	-
dst-port	port	-	-

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
text	text	-	-
first-seen	datetime	-	-
domain	domain	-	-
last-seen	datetime	-	-
ip	ip-dst	-	-

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
text	text	-	✔
number-sections	counter	-	✔
type	text	Type of ELF ['CORE', 'DYNAMIC', 'EXECUTABLE', 'HIPROC', 'LOPROC', 'NONE', 'RELOCATABLE']	-

Object attribute	MISP attribute type	Description	Disable correlation
arch	text	Architecture of the ELF file ['None', 'M32', 'SPARC', 'i386', 'ARCH_68K', 'ARCH_88K', 'IAMCU', 'ARCH_860', 'MIPS', 'S370', 'MIPS_RS3_LE', 'PARISC', 'VPP500', 'SPARC32PLUS', 'ARCH_960', 'PPC', 'PPC64', 'S390', 'SPU', 'V800', 'FR20', 'RH32', 'RCE', 'ARM', 'ALPHA', 'SH', 'SPARCV9', 'TRICORE', 'ARC', 'H8_300', 'H8_300H', 'H8S', 'H8_500', 'IA_64', 'MIPS_X', 'COLDFIRE', 'ARCH_68HC12', 'MMA', 'PCP', 'NCPU', 'NDR1', 'STARCORE', 'ME16', 'ST100', 'TINYJ', 'x86_64', 'PDSP', 'PDP10', 'PDP11', 'FX66', 'ST9PLUS', 'ST7', 'ARCH_68HC16', 'ARCH_68HC11', 'ARCH_68HC08', 'ARCH_68HC05', 'SVX', 'ST19', 'VAX', 'CRIS', 'JAVELIN', 'FIREPATH', 'ZSP', 'MMIX', 'HUANY', 'PRISM', 'AVR', 'FR30', 'D10V', 'D30V', 'V850', 'M32R', 'MN10300', 'MN10200', 'PJ', 'OPENRISC', 'ARC_COMPACT', 'XTENSA', 'VIDEOCORE', 'TMM_GPP', 'NS32K', 'TPC', 'SNP1K', 'ST200', 'IP2K', 'MAX', 'CR', 'F2MC16', 'MSP430', 'BLACKFIN', 'SE_C33', 'SEP', 'ARCA', 'UNICORE', 'EXCESS', 'DXP', 'ALTERA_NIOS2', 'CRX', 'XGATE', 'C166',	-

Object attribute	MISP attribute type	Description	Disable correlation
os_abi	text	Header operating system application binary interface (ABI) ['AIX', 'ARM', 'AROS', 'C6000_ELFABI', 'C6000_LINUX', 'CLOUDABI', 'FENIXOS', 'FREEBSD', 'GNU', 'HPUX', 'HURD', 'IRIX', 'MODESTO', 'NETBSD', 'NSK', 'OPENBSD', 'OPENVMS', 'SOLARIS', 'STANDALONE', 'SYSTEMV', 'TRU64']	-
entrypoint-address	text	-	✔

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
size-in-bytes	size-in-bytes	-	✔
sha512/256	sha512/256	-	-

'METAG', 'MCST_ELBRUS', 'ECOG16', 'CR16', 'ETPU', 'SLE9X', 'L10M', 'K10M', 'AARCH64', 'AVR32', 'STM8', 'TILE64', 'TILEPRO', 'CUDA', 'TILEGX', 'CLOUDSHIELD', 'ARCH_78KOR', 'ARCH_56800EX', 'BA1', 'BA2', 'XCORE', 'MCHP_PIC', 'INTEL205', 'INTEL206', 'INTEL207', 'INTEL208', 'INTEL209', 'KM32', 'KMX32', 'KMX16', 'KMX8', 'KVARC', 'CDP', 'COGE', 'COOL', 'NORC', 'CSR_KALIMBA', 'AMDGPU']

Object attribute	MISP attribute type	Description	Disable correlation
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']	✔
sha512/224	sha512/224	-	-
text	text	-	✔
entropy	float	-	✔
sha256	sha256	-	-
sha512	sha512	-	-
sha224	sha224	-	-
ssdeep	ssdeep	-	-
md5	md5	-	-

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']	✔
sha1	sha1	-	-
sha384	sha384	-	-
name	text	-	✔

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	-	-
reply-to	email-reply-to	-	-
subject	email-subject	-	-
mime-boundary	email-mime-boundary	-	-
header	email-header	-	-

Object attribute	MISP attribute type	Description	Disable correlation
thread-index	email-thread-index	-	-
x-mailer	email-x-mailer	-	-
to-display-name	email-dst-display-name	-	-
send-date	datetime	-	✔
from	email-src	-	-
message-id	email-message-id	-	-
from-display-name	email-src-display-name	-	-
attachment	email-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
size-in-bytes	size-in-bytes	-	✔
sha512/256	sha512/256	-	-
filename	filename	-	-
sha512/224	sha512/224	-	-
pattern-in-file	pattern-in-file	-	-
tlsh	tlsh	-	-
malware-sample	malware-sample	-	-
mimetype	text	-	✔
entropy	float	-	✔
sha256	sha256	-	-
sha512	sha512	-	-

Object attribute	MISP attribute type	Description	Disable correlation
sha224	sha224	-	-
ssdeep	ssdeep	-	-
md5	md5	-	-
sha1	sha1	-	-
sha384	sha384	-	-
text	text	-	✔
authentihash	authentihash	-	-

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
altitude	float	-	-
text	text	-	✔
city	text	-	-
latitude	float	-	✔
country	text	-	-
first-seen	datetime	-	✔
last-seen	datetime	-	✔
longitude	float	-	✔
region	text	-	-

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
proxy-user	text	-	-
method	http-method	-	✔
text	text	-	✔
host	hostname	-	-
content-type	other	-	-
basicauth-user	text	-	-
proxy-password	text	-	-
referer	referer	-	-
url	url	-	-
basicauth-password	text	-	-
user-agent	user-agent	-	-
uri	uri	-	-
cookie	text	-	-

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
first-seen	datetime	-	-
ip	ip-dst	-	-
text	text	-	-
last-seen	datetime	-	-

Object attribute	MISP attribute type	Description	Disable correlation
src-port	port	-	-
dst-port	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
description	text	-	-
ja3-fingerprint-md5	md5	-	-
first-seen	datetime	-	-
last-seen	datetime	-	-
ip-src	ip-src	-	-
ip-dst	ip-dst	-	-

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
text	text	-	✔

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']	-
number-sections	counter	-	✔
entrypoint-address	text	-	✔
name	text	-	-

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
size-in-bytes	size-in-bytes	-	✔
sha512/256	sha512/256	-	-
sha512/224	sha512/224	-	-
text	text	-	✔
entropy	float	-	✔
sha256	sha256	-	-
sha512	sha512	-	-
sha224	sha224	-	-
ssdeep	ssdeep	-	-
md5	md5	-	-
sha1	sha1	-	-

Object attribute	MISP attribute type	Description	Disable correlation
sha384	sha384	-	-
name	text	-	✔

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
count	counter	-	-
time_last	datetime	-	-
text	text	-	-
zone_time_first	datetime	-	-
origin	text	-	-
rdata	text	-	-
zone_time_last	datetime	-	-
time_first	datetime	-	-
sensor_id	text	-	-
rrtype	text	Resource Record type as seen by the passive DNS ['A', 'AAAA', 'CNAME', 'PTR', 'SOA', 'TXT', 'DNAME', 'NS', 'SRV', 'RP', 'NAPTR', 'HINFO', 'A6']	-
bailiwick	text	-	-
rrname	text	-	-

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
company-name	text	-	✔
legal-copyright	text	-	✔
number-sections	counter	-	✔
impfuzzy	impfuzzy	-	-
internal-filename	filename	-	-
entrypoint-section-at-position	text	-	✔
text	text	-	✔
product-name	text	-	✔
entrypoint-address	text	-	✔
compilation-timestamp	datetime	-	-
product-version	text	-	✔
pehash	pehash	-	-
file-description	text	-	✔
lang-id	text	-	✔
imphash	imphash	-	-
type	text	Type of PE ['exe', 'dll', 'driver', 'unknown']	✔
file-version	text	-	✔
original-filename	filename	-	-

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
size-in-bytes	size-in-bytes	-	✔
sha512/256	sha512/256	-	-
sha512/224	sha512/224	-	-
text	text	-	✔
entropy	float	-	✔
characteristic	text	Characteristic of the section ['read', 'write', 'executable']	-
sha256	sha256	-	-
sha512	sha512	-	-
sha224	sha224	-	-
ssdeep	ssdeep	-	-
md5	md5	-	-
sha1	sha1	-	-
sha384	sha384	-	-
name	text	Name of the section ['.rsrc', '.reloc', '.rdata', '.data', '.text']	✔

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
place-of-birth	place-of-birth	-	-
first-name	first-name	-	-
passport-country	passport-country	-	-
text	text	-	✔
redress-number	redress-number	-	-
nationality	nationality	-	-
gender	gender	The gender of a natural person. ['Male', 'Female', 'Other', 'Prefer not to say']	-
passport-expiration	passport-expiration	-	-
middle-name	middle-name	-	-
last-name	last-name	-	-
passport-number	passport-number	-	-
date-of-birth	date-of-birth	-	-

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	-	✔
last-seen	datetime	-	✔
first-seen	datetime	-	✔
msisdn	text	-	-
imei	text	-	-

Object attribute	MISP attribute type	Description	Disable correlation
gummei	text	-	-
imsi	text	-	-
serial-number	text	-	-
tmsi	text	-	-
guti	text	-	-

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
referenced-strings	counter	-	✔
text	text	-	✔
callback-largest	counter	-	✔
gml	attachment	-	✔
callback-average	counter	-	✔
dangling-strings	counter	-	✔
miss-api	counter	-	✔
shortest-path-to-create-thread	counter	-	✔
not-referenced-strings	counter	-	✔
memory-allocations	counter	-	✔
ratio-string	float	-	✔
create-thread	counter	-	✔
r2-commit-version	text	-	✔
unknown-references	counter	-	✔

Object attribute	MISP attribute type	Description	Disable correlation
callbacks	counter	-	✔
local-references	counter	-	✔
ratio-api	float	-	✔
total-api	counter	-	✔
get-proc-address	counter	-	✔
total-functions	counter	-	✔
refsglobalvar	counter	-	✔
ratio-functions	float	-	✔

regexp

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

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

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

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	-	-
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_ENDIAN', 'REG_LINK', 'REG_MULTI_SZ', 'REG_RESOURCE_LIST', 'REG_FULL_RESOURCE_DESCRIPTOR', 'REG_RESOURCE_REQUIREMENTS_LIST', 'REG_QWORD', 'REG_QWORD_LITTLE_ENDIAN']	-
key	reg-key	-	-
last-modified	datetime	-	-
data	reg-data	-	-
name	reg-name	-	-

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
version_line	text	-	-
version	text	-	-
nickname	text	-	-

Object attribute	MISP attribute type	Description	Disable correlation
text	text	-	✔
document	text	-	✔
address	ip-src	-	-
description	text	-	✔
published	datetime	-	✔
flags	text	-	-
first-seen	datetime	-	✔
fingerprint	text	-	-
last-seen	datetime	-	✔

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
tld	text	-	-
fragment	text	-	-
query_string	text	-	-
text	text	-	-
host	hostname	-	-
port	port	-	-
scheme	text	Scheme ['http', 'https', 'ftp', 'gopher', 'sip']	-
resource_path	text	-	-
first-seen	datetime	-	-

Object attribute	MISP attribute type	Description	Disable correlation
last-seen	datetime	-	-
url	url	-	-
subdomain	text	-	-
domain	domain	-	-
domain_without_tld	text	-	-
credential	text	-	-

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
roles	text	-	-
regions	text	-	-
description	text	-	-

Object attribute	MISP attribute type	Description	Disable correlation
sectors	text	The list of sectors that the victim belong to ['agriculture', 'aerospace', 'automotive', 'communications', 'construction', 'defence', 'education', 'energy', 'engineering', 'entertainment', 'financial\xadservices', 'government\xadnational', 'government\xadregional', 'government\xadlocal', 'government\xadpublic\xadservices', 'healthcare', 'hospitality\xadleisure', 'infrastructure', 'insurance', 'manufacturing', 'mining', 'non\xadprofit', 'pharmaceuticals', 'retail', 'technology', 'telecommunications', 'transportation', 'utilities']	-
classification	text	The type of entity being targeted. ['individual', 'group', 'organization', 'class', 'unknown']	-
name	text	-	-

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
id	vulnerability	-	-
published	datetime	-	-
text	text	-	-
vulnerable_configuration	text	-	-
references	link	-	-
modified	datetime	-	-
summary	text	-	-

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-phone	whois-registrant-phone	-	-
registrant-name	whois-registrant-name	-	-
expiration-date	datetime	-	-
modification-date	datetime	-	-
text	text	-	-
domain	domain	-	-
registrant-email	whois-registrant-email	-	-
creation-date	datetime	-	-
registar	whois-registrar	-	-

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
subject	text	-	-
x509-fingerprint-sha256	sha256	-	-
pubkey-info-size	text	-	-
text	text	-	-
pubkey-info-modulus	text	-	-
x509-fingerprint-sha1	sha1	-	-
pubkey-info-exponent	text	-	-
serial-number	text	-	-
validity-not-after	datetime	-	-
pubkey-info-algorithm	text	-	-
x509-fingerprint-md5	md5	-	-
version	text	-	-
issuer	text	-	-
raw-base64	text	-	-
validity-not-before	datetime	-	-

yabin

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

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

Object attribute	MISP attribute type	Description	Disable correlation
yara	yara	-	✔

Object attribute	MISP attribute type	Description	Disable correlation
whitelist	comment	-	-
version	comment	-	-
yara-hunt	yara	-	✔
comment	comment	-	-

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