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

cookie

An HTTP cookie (web cookie, browser cookie) is a small piece of data that a server sends to the user's web browser. The browser may store it and send it back with the next request to the same server. Typically, it's used to tell if two requests came from the same browser — keeping a user logged-in, for example. It remembers stateful information for the stateless HTTP protocol. (as defined by the Mozilla foundation..

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

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

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
version	text	-	-
comment	comment	-	-
cc-number	cc-number	-	-

Object attribute	MISP attribute type	Description	Disable correlation
name	text	-	-
expiration	datetime	-	-
issued	datetime	-	-
card-security-code	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
src-port	port	-	-
dst-port	port	-	-
ip-dst	ip-dst	-	-
text	text	-	-
first-seen	datetime	-	-
ip-src	ip-src	-	-
last-seen	datetime	-	-
total-bps	counter	-	-
total-pps	counter	-	-
protocol	text	Protocol used for the attack ['TCP', 'UDP', 'ICMP', 'IP']	-

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
last-seen	datetime	-	-
text	text	-	-
first-seen	datetime	-	-
domain	domain	-	-
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
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
text	text	-	✔
entrypoint-address	text	-	✔
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']	-
number-sections	counter	-	✔

elf-section

Object describing a section of an Executable and Linkable Format.

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

Object attribute	MISP attribute type	Description	Disable correlation
type	text	Type of the section ['NULL', 'PROGBITS', 'SYMTAB', 'STRTAB', 'RELA', 'HASH', 'DYNAMIC', 'NOTE', 'NOBITS', 'REL', 'SHLIB', 'DYNSYM', 'INIT_ARRAY', 'FINI_ARRAY', 'PREINIT_ARRAY', 'GROUP', 'SYMTAB_SHNDX', 'LOOS', 'GNU_ATTRIBUTES', 'GNU_HASH', 'GNU_VERDEF', 'GNU_VERNEED', 'GNU_VERSYM', 'HIOS', 'LOPROC', 'ARM_EXIDX', 'ARM_PREEMPTMAP', 'HEX_ORDERED', 'X86_64_UNWIND', 'MIPS_REGINFO', 'MIPS_OPTIONS', 'MIPS_ABIFLAGS', 'HIPROC', 'LOUSER', 'HIUSER']	✔
sha384	sha384	-	-
sha224	sha224	-	-
entropy	float	-	✔

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	-	-
sha512	sha512	-	-
size-in-bytes	size-in-bytes	-	✔
text	text	-	✔
sha512/224	sha512/224	-	-
sha512/256	sha512/256	-	-
name	text	-	✔
md5	md5	-	-
ssdeep	ssdeep	-	-
sha256	sha256	-	-

email

Email object describing an email with meta-information.

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

Object attribute	MISP attribute type	Description	Disable correlation
from-display-name	email-src-display-name	-	-
cc	email-dst	-	-
thread-index	email-thread-index	-	-
return-path	text	-	-
message-id	email-message-id	-	-
to-display-name	email-dst-display-name	-	-
subject	email-subject	-	-
mime-boundary	email-mime-boundary	-	-
to	email-dst	-	-
send-date	datetime	-	✔
x-mailer	email-x-mailer	-	-
attachment	email-attachment	-	-
header	email-header	-	-
reply-to	email-reply-to	-	-
from	email-src	-	-

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
authentihash	authentihash	-	-
sha384	sha384	-	-

Object attribute	MISP attribute type	Description	Disable correlation
sha224	sha224	-	-
entropy	float	-	✔
mimetype	text	-	✔
filename	filename	-	-
pattern-in-file	pattern-in-file	-	-
malware-sample	malware-sample	-	-
tlsh	tlsh	-	-
sha1	sha1	-	-
sha512	sha512	-	-
text	text	-	✔
sha512/224	sha512/224	-	-
sha512/256	sha512/256	-	-
md5	md5	-	-
sha256	sha256	-	-
ssdeep	ssdeep	-	-
size-in-bytes	size-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	-	✔
country	text	-	-
text	text	-	✔

Object attribute	MISP attribute type	Description	Disable correlation
first-seen	datetime	-	✔
altitude	float	-	-
last-seen	datetime	-	✔
latitude	float	-	✔
region	text	-	-
city	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
user-agent	user-agent	-	-
content-type	other	-	-
referer	referer	-	-
basicauth-password	text	-	-
basicauth-user	text	-	-
proxy-user	text	-	-
url	url	-	-
cookie	text	-	-
host	hostname	-	-
text	text	-	✔
proxy-password	text	-	-
method	http-method	-	✔
uri	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
src-port	port	-	-
dst-port	port	-	-
text	text	-	-
first-seen	datetime	-	-
last-seen	datetime	-	-
ip	ip-dst	-	-

ja3

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

ja3 is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

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

macho

Object describing a file in Mach-O format..

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

Object attribute	MISP attribute type	Description	Disable correlation
type	text	Type of Mach-O ['BUNDLE', 'CORE', 'DSYM', 'DYLIB', 'DYLIB_STUB', 'DYLINKER', 'EXECUTE', 'FVMLIB', 'KEXT_BUNDLE', 'OBJECT', 'PRELOAD']	-
name	text	-	-
number-sections	counter	-	✔
text	text	-	✔
entrypoint-address	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
sha384	sha384	-	-
sha224	sha224	-	-
entropy	float	-	✔
sha1	sha1	-	-
sha512	sha512	-	-
size-in-bytes	size-in-bytes	-	✔

Object attribute	MISP attribute type	Description	Disable correlation
text	text	-	✔
sha512/224	sha512/224	-	-
sha512/256	sha512/256	-	-
name	text	-	✔
md5	md5	-	-
ssdeep	ssdeep	-	-
sha256	sha256	-	-

microblog

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

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

Object attribute	MISP attribute type	Description	Disable correlation
type	text	Type of the microblog post ['Twitter', 'Facebook', 'LinkedIn', 'Reddit', 'Google+', 'Instagram', 'Forum', 'Other']	-
creation-date	datetime	-	-
url	url	-	-
link	url	-	-
modification-date	datetime	-	-
removal-date	datetime	-	-
username	text	-	-
post	text	-	-
username-quoted	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
sensor_id	text	-	-
rdata	text	-	-
rrname	text	-	-
count	counter	-	-
time_first	datetime	-	-
text	text	-	-
bailiwick	text	-	-
zone_time_first	datetime	-	-
rrtype	text	Resource Record type as seen by the passive DNS ['A', 'AAAA', 'CNAME', 'PTR', 'SOA', 'TXT', 'DNAME', 'NS', 'SRV', 'RP', 'NAPTR', 'HINFO', 'A6']	-
zone_time_last	datetime	-	-
time_last	datetime	-	-
origin	text	-	-

paste

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

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

Object attribute	MISP attribute type	Description	Disable correlation
first-seen	datetime	-	✔
title	text	-	-
paste	text	-	-
last-seen	datetime	-	✔
url	url	-	-
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.

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
original-filename	filename	-	-
type	text	Type of PE ['exe', 'dll', 'driver', 'unknown']	✔
entrypoint-address	text	-	✔
legal-copyright	text	-	✔
file-version	text	-	✔
internal-filename	filename	-	-
lang-id	text	-	✔

Object attribute	MISP attribute type	Description	Disable correlation
company-name	text	-	✔
pehash	pehash	-	-
impfuzzy	impfuzzy	-	-
text	text	-	✔
entrypoint-section-at-position	text	-	✔
compilation-timestamp	datetime	-	-
product-name	text	-	✔
number-sections	counter	-	✔
imphash	imphash	-	-
product-version	text	-	✔
file-description	text	-	✔

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
sha384	sha384	-	-
sha224	sha224	-	-
entropy	float	-	✔
sha1	sha1	-	-
sha512	sha512	-	-
size-in-bytes	size-in-bytes	-	✔
text	text	-	✔
sha512/224	sha512/224	-	-

Object attribute	MISP attribute type	Description	Disable correlation
sha512/256	sha512/256	-	-
name	text	Name of the section ['.rsrc', '.reloc', '.rdata', '.data', '.text']	✔
md5	md5	-	-
ssdeep	ssdeep	-	-
characteristic	text	Characteristic of the section ['read', 'write', 'executable']	-
sha256	sha256	-	-

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

Object attribute	MISP attribute type	Description	Disable correlation
passport-country	passport-country	-	-
passport-number	passport-number	-	-
middle-name	middle-name	-	-

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
first-seen	datetime	-	✔
gummei	text	-	-
text	text	-	✔
serial-number	text	-	-
tmsi	text	-	-
last-seen	datetime	-	✔
guti	text	-	-
imsi	text	-	-
imei	text	-	-
msisdn	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
shortest-path-to-create-thread	counter	-	✔
create-thread	counter	-	✔
referenced-strings	counter	-	✔
unknown-references	counter	-	✔
gml	attachment	-	✔
dangling-strings	counter	-	✔
total-functions	counter	-	✔
ratio-api	float	-	✔
local-references	counter	-	✔
miss-api	counter	-	✔
callbacks	counter	-	✔
callback-average	counter	-	✔
ratio-functions	float	-	✔
callback-largest	counter	-	✔
r2-commit-version	text	-	✔
get-proc-address	counter	-	✔
text	text	-	✔
memory-allocations	counter	-	✔
total-api	counter	-	✔
ratio-string	float	-	✔
not-referenced-strings	counter	-	✔
refsglobalvar	counter	-	✔

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

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
last-modified	datetime	-	-
name	reg-name	-	-
key	reg-key	-	-
data	reg-data	-	-
hive	reg-hive	-	-

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_ENDIAN', 'REG_LINK', 'REG_MULTI_SZ', 'REG_RESOURCE_LIST', 'REG_FULL_RESOURCE_DESCRIPTOR', 'REG_RESOURCE_REQUIREMENTS_LIST', 'REG_QWORD', 'REG_QWORD_LITTLE_ENDIAN']	-

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
queue	text	Queue of the RTIR ticket ['incident', 'investigations', 'blocks', 'incident reports']	-
classification	text	-	-
status	text	Status of the RTIR ticket ['new', 'open', 'stalled', 'resolved', 'rejected', 'deleted']	-
constituency	text	-	-
ticket-number	text	-	-

Object attribute	MISP attribute type	Description	Disable correlation
subject	text	-	-
ip	ip-dst	-	-

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	text	-	-
published	datetime	-	✔
nickname	text	-	-
document	text	-	✔
address	ip-src	-	-
version_line	text	-	-
flags	text	-	-
first-seen	datetime	-	✔
fingerprint	text	-	-
description	text	-	✔
text	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	-	-
domain	domain	-	-
query_string	text	-	-
fragment	text	-	-
resource_path	text	-	-
scheme	text	Scheme ['http', 'https', 'ftp', 'gopher', 'sip']	-
host	hostname	-	-
domain_without_tld	text	-	-
url	url	-	-
text	text	-	-
first-seen	datetime	-	-
subdomain	text	-	-
last-seen	datetime	-	-
port	port	-	-
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
name	text	-	-

Object attribute	MISP attribute type	Description	Disable correlation
regions	text	-	-
classification	text	The type of entity being targeted. ['individual', 'group', 'organization', 'class', 'unknown']	-
description	text	-	-
roles	text	-	-
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']	-

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

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

Object attribute	MISP attribute type	Description	Disable correlation
creation-date	datetime	-	-

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

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	-	-
comment	comment	-	-
yara	yara	-	✔
whitelist	comment	-	-
yara-hunt	yara	-	✔

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']

Name of relationship	Description	Format
variant-of	This relationship describes a source object which is a variant of the target object	['misp', 'stix-2.0']
impersonates	This relationship describe a source object which impersonates the target object	['misp', 'stix-2.0']
authored-by	This relationship describes the author of a specific object.	['misp']
located	This relationship describes the location (of any type) of a specific object.	['misp']
included-in	This relationship describes an object included in another object.	['misp']
analysed-with	This relationship describes an object analysed by another object.	['misp']
claimed-by	This relationship describes an object claimed by another object.	['misp']
communicates-with	This relationship describes an object communicating with another object.	['misp']
dropped-by	This relationship describes an object dropped by another object.	['misp']
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']

Name of relationship	Description	Format
intercepts	This relationship describes an object which intercepts another object.	['misp']
calls	This relationship describes an object which calls another objects.	['misp']
detected-as	This relationship describes an object which is detected as another object.	['misp']
triggers	This relationship describes an object which triggers another object.	['misp']