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
original-date	datetime	−	✓
sensor	text	−	−
text	text	−	✓
last-seen	datetime	−	✓
type	text	Type of information leak as discovered and classified by an AIL module. ['Credential', 'CreditCards', 'Mail', 'Onion', 'Phone', 'Keys']	−
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
cookie-value	text	−	−
text	text	−	✓
cookie-name	text	−	−
cookie	cookie	−	−
type	text	Type of cookie and how it’s used in this specific object. ['Session management', 'Personalization', 'Tracking', 'Exfiltration', 'Malicious Payload', 'Beaconing']	−

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
issued	datetime	−	−
expiration	datetime	−	−
comment	comment	−	−

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

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

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
entrypoint-address	text	—	✓

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

'COREA_1ST', 'COREA_2ND', 'ARC_COMPACT2', 'OPEN8', 'RL78', 'VIDEOCORE5', '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']

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
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']	✓
sha256	sha256	−	−
sha512/224	sha512/224	−	−
entropy	float	−	✓
sha224	sha224	−	−
text	text	−	✓
name	text	−	✓
sha384	sha384	−	−
sha512/256	sha512/256	−	−
md5	md5	−	−
ssdeep	ssdeep	−	−
sha512	sha512	−	−
size-in-bytes	size-in-bytes	−	✓

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']	✓
sha1	sha1	−	−

email

Email object describing an email with meta-information.

ℹ 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
send-date	datetime	−	✓
subject	email-subject	−	−
header	email-header	−	−

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

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
filename	filename	−	−
sha256	sha256	−	−
pattern-in-file	pattern-in-file	−	−
sha512/224	sha512/224	−	−
entropy	float	−	✓
sha224	sha224	−	−
text	text	−	✓

Object attribute	MISP attribute type	Description	Disable correlation
sha384	sha384	−	−
sha512/256	sha512/256	−	−
md5	md5	−	−
ssdeep	ssdeep	−	−
mimetype	text	−	✓
tlsh	tlsh	−	−
authentihash	authentihash	−	−
sha512	sha512	−	−
size-in-bytes	size-in-bytes	−	✓
malware-sample	malware-sample	−	−
sha1	sha1	−	−

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	−	−
altitude	float	−	−
country	text	−	−
latitude	float	−	✓
longitude	float	−	✓
text	text	−	✓
last-seen	datetime	−	✓
first-seen	datetime	−	✓

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

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
ja3-fingerprint-md5	md5	-	-
description	text	-	-
ip-dst	ip-dst	-	-
ip-src	ip-src	-	-
last-seen	datetime	-	-
first-seen	datetime	-	-

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
entrypoint-address	text	—	✓
text	text	—	✓
name	text	—	—
type	text	Type of Mach-O ['BUNDLE', 'CORE', 'DSYM', 'DYLIB', 'DYLIB_STUB', 'DYLINKER', 'EXECUTE', 'FVMLIB', 'KEXT_BUNDLE', 'OBJECT', 'PRELOAD']	—
number-sections	counter	—	✓

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
sha256	sha256	—	—
sha512/224	sha512/224	—	—
entropy	float	—	✓
sha224	sha224	—	—
text	text	—	✓
name	text	—	✓
sha384	sha384	—	—
sha512/256	sha512/256	—	—
md5	md5	—	—
ssdeep	ssdeep	—	—

Object attribute	MISP attribute type	Description	Disable correlation
sha512	sha512	━	━
size-in-bytes	size-in-bytes	━	✓
sha1	sha1	━	━

microblog

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

ℹ 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
link	url	━	━
removal-date	datetime	━	━
url	url	━	━
modification-date	datetime	━	━
username-quoted	text	━	━
creation-date	datetime	━	━
post	text	━	━
type	text	Type of the microblog post ['Twitter', 'Facebook', 'LinkedIn', 'Reddit', 'Google+', 'Instagram', 'Forum', 'Other']	━
username	text	━	━

netflow

Netflow object describes an network object based on the Netflowv5/v9 minimal definition.

ℹ 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
src-port	port	–	–
last-packet-seen	datetime	–	–
protocol	text	Protocol used for this flow ['TCP', 'UDP', 'ICMP', 'IP']	–
dst-port	port	–	–
src-as	AS	–	–
ip-src	ip-src	–	–
dst-as	AS	–	–
flow-count	counter	–	✓
first-packet-seen	datetime	–	–
tcp-flags	text	–	✓
ip-protocol-number	size-in-bytes	–	✓
byte-count	counter	–	✓
ip_version	counter	–	✓
direction	text	Direction of this flow ['Ingress', 'Egress']	✓
packet-count	counter	–	✓
ip-dst	ip-dst	–	–
icmp-type	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
bailiwick	text	➖	➖
count	counter	➖	➖
time_first	datetime	➖	➖
text	text	➖	➖
rdata	text	➖	➖
origin	text	➖	➖
rrname	text	➖	➖
time_last	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	➖	➖
sensor_id	text	➖	➖
zone_time_first	datetime	➖	➖

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
url	url	➖	➖
last-seen	datetime	➖	✓
title	text	➖	➖
paste	text	➖	➖

Object attribute	MISP attribute type	Description	Disable correlation
first-seen	datetime	−	✓
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
compilation-timestamp	datetime	−	−
entrypoint-address	text	−	✓
company-name	text	−	✓
impfuzzy	impfuzzy	−	−
product-name	text	−	✓
internal-filename	filename	−	−
number-sections	counter	−	✓
text	text	−	✓
entrypoint-section-at-position	text	−	✓
original-filename	filename	−	−
imphash	imphash	−	−
legal-copyright	text	−	✓

Object attribute	MISP attribute type	Description	Disable correlation
pehash	pehash	−	−
product-version	text	−	✓
lang-id	text	−	✓
type	text	Type of PE ['exe', 'dll', 'driver', 'unknown']	✓
file-description	text	−	✓
file-version	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
characteristic	text	Characteristic of the section ['read', 'write', 'executable']	−
sha256	sha256	−	−
sha512/224	sha512/224	−	−
entropy	float	−	✓
sha224	sha224	−	−
text	text	−	✓
name	text	Name of the section ['.rsrc', '.reloc', '.rdata', '.data', '.text']	✓
sha384	sha384	−	−
sha512/256	sha512/256	−	−
md5	md5	−	−

Object attribute	MISP attribute type	Description	Disable correlation
ssdeep	ssdeep	−	−
sha512	sha512	−	−
size-in-bytes	size-in-bytes	−	✓
sha1	sha1	−	−

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	−	−
passport-expiration	passport-expiration	−	−
text	text	−	✓
middle-name	middle-name	−	−
passport-number	passport-number	−	−
redress-number	redress-number	−	−
gender	gender	The gender of a natural person. ['Male', 'Female', 'Other', 'Prefer not to say']	−
place-of-birth	place-of-birth	−	−
first-name	first-name	−	−
passport-country	passport-country	−	−
last-name	last-name	−	−
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
imei	text	−	−
tmsi	text	−	−
imsi	text	−	−
guti	text	−	−
msisdn	text	−	−
text	text	−	✓
last-seen	datetime	−	✓
gummei	text	−	−
first-seen	datetime	−	✓
serial-number	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
memory-allocations	counter	−	✓
local-references	counter	−	✓
r2-commit-version	text	−	✓
gml	attachment	−	✓
unknown-references	counter	−	✓

Object attribute	MISP attribute type	Description	Disable correlation
text	text	−	✓
total-functions	counter	−	✓
ratio-string	float	−	✓
miss-api	counter	−	✓
not-referenced-strings	counter	−	✓
callback-average	counter	−	✓
total-api	counter	−	✓
dangling-strings	counter	−	✓
get-proc-address	counter	−	✓
shortest-path-to-create-thread	counter	−	✓
ratio-api	float	−	✓
callback-largest	counter	−	✓
refsglobalvar	counter	−	✓
referenced-strings	counter	−	✓
ratio-functions	float	−	✓
create-thread	counter	−	✓
callbacks	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
regexp	text	−	−

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']	✓

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	reg-data	−	−
hive	reg-hive	−	−
name	reg-name	−	−
key	reg-key	−	−
last-modified	datetime	−	−
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
constituency	text	−	−
subject	text	−	−
ticket-number	text	−	−
status	text	Status of the RTIR ticket ['new', 'open', 'stalled', 'resolved', 'rejected', 'deleted']	−
classification	text	−	−
ip	ip-dst	−	−
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
description	text	−	✓
fingerprint	text	−	−
published	datetime	−	✓

Object attribute	MISP attribute type	Description	Disable correlation
version	text	−	−
version_line	text	−	−
text	text	−	✓
flags	text	−	−
first-seen	datetime	−	✓
document	text	−	✓
last-seen	datetime	−	✓
address	ip-src	−	−
nickname	text	−	−

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
subdomain	text	−	−
url	url	−	−
fragment	text	−	−
scheme	text	Scheme ['http', 'https', 'ftp', 'gopher', 'sip']	−
domain	domain	−	−
text	text	−	−
last-seen	datetime	−	−
resource_path	text	−	−
tld	text	−	−

Object attribute	MISP attribute type	Description	Disable correlation
port	port	—	—
credential	text	—	—
host	hostname	—	—
first-seen	datetime	—	—
domain_without_tld	text	—	—
query_string	text	—	—

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
description	text	—	—
regions	text	—	—
name	text	—	—
roles	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']	━

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
references	link	-	-
modified	datetime	-	-
summary	text	-	-
id	vulnerability	-	-
text	text	-	-
published	datetime	-	-
vulnerable_configuration	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
registar	whois-registrar	-	-
creation-date	datetime	-	-
registrant-email	whois-registrant-email	-	-
registrant-name	whois-registrant-name	-	-
expiration-date	datetime	-	-
domain	domain	-	-
text	text	-	-
registrant-phone	whois-registrant-phone	-	-
modification-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
pubkey-info-exponent	text	-	-
subject	text	-	-
version	text	-	-
raw-base64	text	-	-
x509-fingerprint-sha1	sha1	-	-
text	text	-	-
validity-not-after	datetime	-	-
serial-number	text	-	-
pubkey-info-modulus	text	-	-
issuer	text	-	-
pubkey-info-algorithm	text	-	-
validity-not-before	datetime	-	-
x509-fingerprint-md5	md5	-	-
pubkey-info-size	text	-	-
x509-fingerprint-sha256	sha256	-	-

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
whitelist	comment	-	-

Object attribute	MISP attribute type	Description	Disable correlation
comment	comment	−	−
version	comment	−	−
yara	yara	−	✓
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']
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']