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

av-signature

Antivirus detection signature.

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

Object attribute	MISP attribute type	Description	Disable correlation
signature	text	-	-
datetime	datetime	-	✔
text	text	-	✔
software	text	-	-

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	-	-
cookie	cookie	-	-
cookie-name	text	-	-
text	text	-	✔
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
card-security-code	text	-	-
version	text	-	-
issued	datetime	-	-
name	text	-	-
cc-number	cc-number	-	-
comment	comment	-	-
expiration	datetime	-	-

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

Object attribute	MISP attribute type	Description	Disable correlation
total-pps	counter	-	-
text	text	-	-
src-port	port	-	-
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	-	-
last-seen	datetime	-	-
ip	ip-dst	-	-
text	text	-	-
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
text	text	-	✔
number-sections	counter	-	✔

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']	-
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
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
sha1	sha1	-	-
sha512/224	sha512/224	-	-
sha224	sha224	-	-
entropy	float	-	✔
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']	✔
sha512	sha512	-	-
size-in-bytes	size-in-bytes	-	✔
sha512/256	sha512/256	-	-

Object attribute	MISP attribute type	Description	Disable correlation
text	text	-	✔
name	text	-	✔
sha256	sha256	-	-
md5	md5	-	-
ssdeep	ssdeep	-	-
sha384	sha384	-	-
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']	✔

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

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
state	text	-	-
sha1	sha1	-	-

Object attribute	MISP attribute type	Description	Disable correlation
sha512/224	sha512/224	-	-
sha224	sha224	-	-
entropy	float	-	✔
pattern-in-file	pattern-in-file	-	-
tlsh	tlsh	-	-
sha512	sha512	-	-
size-in-bytes	size-in-bytes	-	✔
sha512/256	sha512/256	-	-
text	text	-	✔
authentihash	authentihash	-	-
malware-sample	malware-sample	-	-
sha256	sha256	-	-
md5	md5	-	-
ssdeep	ssdeep	-	-
sha384	sha384	-	-
mimetype	text	-	✔
filename	filename	-	-

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
text	text	-	✔
last-seen	datetime	-	✔

Object attribute	MISP attribute type	Description	Disable correlation
region	text	-	-
country	text	-	-
latitude	float	-	✔
city	text	-	-
altitude	float	-	-
first-seen	datetime	-	✔
longitude	float	-	✔

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

Object attribute	MISP attribute type	Description	Disable correlation
method	http-method	-	✔

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
last-seen	datetime	-	-
dst-port	port	-	-
ip	ip-dst	-	-
text	text	-	-
src-port	port	-	-
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
last-seen	datetime	-	-
description	text	-	-
ip-dst	ip-dst	-	-
ip-src	ip-src	-	-
first-seen	datetime	-	-

Object attribute	MISP attribute type	Description	Disable correlation
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
text	text	-	✔
number-sections	counter	-	✔
name	text	-	-
entrypoint-address	text	-	✔
type	text	Type of Mach-O ['BUNDLE', 'CORE', 'DSYM', 'DYLIB', 'DYLIB_STUB', 'DYLINKER', 'EXECUTE', 'FVMLIB', 'KEXT_BUNDLE', 'OBJECT', 'PRELOAD']	-

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
sha1	sha1	-	-
sha512/224	sha512/224	-	-
sha224	sha224	-	-
entropy	float	-	✔

Object attribute	MISP attribute type	Description	Disable correlation
sha512	sha512	-	-
size-in-bytes	size-in-bytes	-	✔
sha512/256	sha512/256	-	-
text	text	-	✔
name	text	-	✔
sha256	sha256	-	-
md5	md5	-	-
ssdeep	ssdeep	-	-
sha384	sha384	-	-

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
post	text	-	-
username-quoted	text	-	-
url	url	-	-
link	url	-	-
modification-date	datetime	-	-
removal-date	datetime	-	-
username	text	-	-
creation-date	datetime	-	-

Object attribute	MISP attribute type	Description	Disable correlation
type	text	Type of the microblog post ['Twitter', 'Facebook', 'LinkedIn', 'Reddit', 'Google+', 'Instagram', 'Forum', 'Other']	-

netflow

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

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

Object attribute	MISP attribute type	Description	Disable correlation
first-packet-seen	datetime	-	-
ip_version	counter	-	✔
byte-count	counter	-	✔
ip-dst	ip-dst	-	-
ip-protocol-number	size-in-bytes	-	✔
last-packet-seen	datetime	-	-
ip-src	ip-src	-	-
packet-count	counter	-	✔
src-port	port	-	-
src-as	AS	-	-
direction	text	Direction of this flow ['Ingress', 'Egress']	✔
flow-count	counter	-	✔
dst-port	port	-	-
tcp-flags	text	-	✔

Object attribute	MISP attribute type	Description	Disable correlation
dst-as	AS	-	-
icmp-type	text	-	✔
protocol	text	Protocol used for this flow ['TCP', 'UDP', 'ICMP', 'IP']	-

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	-	-
time_first	datetime	-	-
time_last	datetime	-	-
zone_time_last	datetime	-	-
text	text	-	-
origin	text	-	-
sensor_id	text	-	-
count	counter	-	-
bailiwick	text	-	-
rrname	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']	-

Object attribute	MISP attribute type	Description	Disable correlation
rdata	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
url	url	-	-
paste	text	-	-
last-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']	-
first-seen	datetime	-	✔
title	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
text	text	-	✔
original-filename	filename	-	-

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

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
sha1	sha1	-	-
sha512/224	sha512/224	-	-

Object attribute	MISP attribute type	Description	Disable correlation
sha224	sha224	-	-
entropy	float	-	✔
characteristic	text	Characteristic of the section ['read', 'write', 'executable']	-
sha512	sha512	-	-
size-in-bytes	size-in-bytes	-	✔
sha512/256	sha512/256	-	-
text	text	-	✔
name	text	Name of the section ['.rsrc', '.reloc', '.rdata', '.data', '.text']	✔
sha256	sha256	-	-
md5	md5	-	-
ssdeep	ssdeep	-	-
sha384	sha384	-	-

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
first-name	first-name	-	-
redress-number	redress-number	-	-
nationality	nationality	-	-
place-of-birth	place-of-birth	-	-

Object attribute	MISP attribute type	Description	Disable correlation
text	text	-	✔
gender	gender	The gender of a natural person. ['Male', 'Female', 'Other', 'Prefer not to say']	-
passport-expiration	passport-expiration	-	-
date-of-birth	date-of-birth	-	-
passport-number	passport-number	-	-
middle-name	middle-name	-	-
last-name	last-name	-	-
passport-country	passport-country	-	-

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
last-seen	datetime	-	✔
first-seen	datetime	-	✔
imei	text	-	-
tmsi	text	-	-
imsi	text	-	-
guti	text	-	-
msisdn	text	-	-
gummei	text	-	-
serial-number	text	-	-

Object attribute	MISP attribute type	Description	Disable correlation
text	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
total-functions	counter	-	✔
dangling-strings	counter	-	✔
memory-allocations	counter	-	✔
ratio-api	float	-	✔
referenced-strings	counter	-	✔
text	text	-	✔
r2-commit-version	text	-	✔
get-proc-address	counter	-	✔
refsglobalvar	counter	-	✔
callback-largest	counter	-	✔
create-thread	counter	-	✔
not-referenced-strings	counter	-	✔
callbacks	counter	-	✔
ratio-string	float	-	✔
callback-average	counter	-	✔
total-api	counter	-	✔
local-references	counter	-	✔
gml	attachment	-	✔

Object attribute	MISP attribute type	Description	Disable correlation
shortest-path-to-create-thread	counter	-	✔
miss-api	counter	-	✔
unknown-references	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
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
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']	-
name	reg-name	-	-
key	reg-key	-	-
last-modified	datetime	-	-
data	reg-data	-	-
hive	reg-hive	-	-

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
classification	text	-	-
subject	text	-	-

Object attribute	MISP attribute type	Description	Disable correlation
queue	text	Queue of the RTIR ticket ['incident', 'investigations', 'blocks', 'incident reports']	-
status	text	Status of the RTIR ticket ['new', 'open', 'stalled', 'resolved', 'rejected', 'deleted']	-
ticket-number	text	-	-
ip	ip-dst	-	-
constituency	text	-	-

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	-	-
version	text	-	-
flags	text	-	-
first-seen	datetime	-	✔
text	text	-	✔
last-seen	datetime	-	✔
description	text	-	✔
version_line	text	-	-
published	datetime	-	✔

Object attribute	MISP attribute type	Description	Disable correlation
document	text	-	✔
address	ip-src	-	-
fingerprint	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
text	text	-	-
domain_without_tld	text	-	-
tld	text	-	-
subdomain	text	-	-
url	url	-	-
host	hostname	-	-
port	port	-	-
scheme	text	Scheme ['http', 'https', 'ftp', 'gopher', 'sip']	-
first-seen	datetime	-	-
last-seen	datetime	-	-
query_string	text	-	-
domain	domain	-	-
fragment	text	-	-
credential	text	-	-
resource_path	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
classification	text	The type of entity being targeted. ['individual', 'group', 'organization', 'class', 'unknown']	-
description	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']	-
regions	text	-	-

virustotal-report

VirusTotal report.

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

Object attribute	MISP attribute type	Description	Disable correlation
detection-ratio	text	-	✔

Object attribute	MISP attribute type	Description	Disable correlation
permalink	link	-	-
last-submission	datetime	-	-
first-submission	datetime	-	-
community-score	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
published	datetime	-	-
references	link	-	-
modified	datetime	-	-
id	vulnerability	-	-
vulnerable_configuration	text	-	-
text	text	-	-
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
domain	domain	-	-
registrant-phone	whois-registrant-phone	-	-

Object attribute	MISP attribute type	Description	Disable correlation
registrant-name	whois-registrant-name	-	-
registrant-email	whois-registrant-email	-	-
modification-date	datetime	-	-
registar	whois-registrar	-	-
text	text	-	-
creation-date	datetime	-	-
expiration-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	-	-
x509-fingerprint-sha256	sha256	-	-
subject	text	-	-
validity-not-before	datetime	-	-
pubkey-info-size	text	-	-
pubkey-info-exponent	text	-	-
pubkey-info-algorithm	text	-	-
text	text	-	-
x509-fingerprint-sha1	sha1	-	-
x509-fingerprint-md5	md5	-	-
pubkey-info-modulus	text	-	-
issuer	text	-	-

Object attribute	MISP attribute type	Description	Disable correlation
raw-base64	text	-	-
validity-not-after	datetime	-	-
serial-number	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	-	-
yara-hunt	yara	-	✔
comment	comment	-	-
yara	yara	-	✔
whitelist	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']

Name of relationship	Description	Format
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']
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']

Name of relationship	Description	Format
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']
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']