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	-	-
first-seen	datetime	-	✔
origin	url	-	-
original-date	datetime	-	✔
last-seen	datetime	-	✔

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
text	text	-	✔
software	text	-	-
signature	text	-	-
datetime	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
cookie-name	text	-	-
text	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']	-
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
cc-number	cc-number	-	-
card-security-code	text	-	-
expiration	datetime	-	-
issued	datetime	-	-
version	text	-	-
name	text	-	-
comment	comment	-	-

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

Object attribute	MISP attribute type	Description	Disable correlation
dst-port	port	-	-
text	text	-	-
ip-src	ip-src	-	-
ip-dst	ip-dst	-	-

domain-ip

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

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

Object attribute	MISP attribute type	Description	Disable correlation
first-seen	datetime	-	-
domain	domain	-	-
last-seen	datetime	-	-
text	text	-	-
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']	-
text	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
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
md5	md5	-	-
text	text	-	✔
sha224	sha224	-	-
sha512/256	sha512/256	-	-

'ECOG16', 'CR16', 'ETPU', 'SLE9X', 'L10M', 'K10M', 'AARCH64', 'AVR32', 'STM8', 'TILE64', 'TILEPRO', 'CUDA', 'TILEGX', 'CLOUDSHIELD', 'COREA_1ST',

'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	-	-

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	-	-
size-in-bytes	size-in-bytes	-	✔
entropy	float	-	✔
sha256	sha256	-	-
ssdeep	ssdeep	-	-
name	text	-	✔
sha512	sha512	-	-

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

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
sha512	sha512	-	-
tlsh	tlsh	-	-
sha224	sha224	-	-
malware-sample	malware-sample	-	-

Object attribute	MISP attribute type	Description	Disable correlation
sha512/256	sha512/256	-	-
authentihash	authentihash	-	-
sha512/224	sha512/224	-	-
filename	filename	-	-
sha1	sha1	-	-
pattern-in-file	pattern-in-file	-	-
mimetype	text	-	✔
sha384	sha384	-	-
entropy	float	-	✔
text	text	-	✔
size-in-bytes	size-in-bytes	-	✔
ssdeep	ssdeep	-	-
md5	md5	-	-
sha256	sha256	-	-

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
latitude	float	-	✔
last-seen	datetime	-	✔
text	text	-	✔
region	text	-	-
longitude	float	-	✔

Object attribute	MISP attribute type	Description	Disable correlation
first-seen	datetime	-	✔
city	text	-	-
altitude	float	-	-
country	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
text	text	-	✔
url	url	-	-
content-type	other	-	-
cookie	text	-	-
user-agent	user-agent	-	-
method	http-method	-	✔
host	hostname	-	-
uri	uri	-	-
proxy-password	text	-	-
basicauth-password	text	-	-
basicauth-user	text	-	-
proxy-user	text	-	-
referer	referer	-	-

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	-	-
text	text	-	-
ip	ip-dst	-	-
src-port	port	-	-
first-seen	datetime	-	-
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
last-seen	datetime	-	-
description	text	-	-
first-seen	datetime	-	-
ja3-fingerprint-md5	md5	-	-
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
number-sections	counter	-	✔
type	text	Type of Mach-O ['BUNDLE', 'CORE', 'DSYM', 'DYLIB', 'DYLIB_STUB', 'DYLINKER', 'EXECUTE', 'FVMLIB', 'KEXT_BUNDLE', 'OBJECT', 'PRELOAD']	-
text	text	-	✔
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
md5	md5	-	-
text	text	-	✔
sha224	sha224	-	-
sha512/256	sha512/256	-	-
sha512/224	sha512/224	-	-
sha1	sha1	-	-

Object attribute	MISP attribute type	Description	Disable correlation
sha384	sha384	-	-
size-in-bytes	size-in-bytes	-	✔
entropy	float	-	✔
sha256	sha256	-	-
ssdeep	ssdeep	-	-
name	text	-	✔
sha512	sha512	-	-

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

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

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
title	text	-	-
last-seen	datetime	-	✔
url	url	-	-
first-seen	datetime	-	✔
paste	text	-	-
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
impfuzzy	impfuzzy	-	-
imphash	imphash	-	-
internal-filename	filename	-	-
text	text	-	✔
pehash	pehash	-	-
entrypoint-address	text	-	✔
entrypoint-section-at-position	text	-	✔
file-description	text	-	✔

Object attribute	MISP attribute type	Description	Disable correlation
type	text	Type of PE ['exe', 'dll', 'driver', 'unknown']	✔
product-version	text	-	✔
legal-copyright	text	-	✔
compilation-timestamp	datetime	-	-
original-filename	filename	-	-
company-name	text	-	✔
product-name	text	-	✔
number-sections	counter	-	✔
file-version	text	-	✔
lang-id	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
md5	md5	-	-
text	text	-	✔
sha224	sha224	-	-
characteristic	text	Characteristic of the section ['read', 'write', 'executable']	-
sha512/256	sha512/256	-	-
sha512/224	sha512/224	-	-
sha1	sha1	-	-

Object attribute	MISP attribute type	Description	Disable correlation
sha384	sha384	-	-
size-in-bytes	size-in-bytes	-	✔
entropy	float	-	✔
sha256	sha256	-	-
ssdeep	ssdeep	-	-
name	text	Name of the section ['.rsrc', '.reloc', '.rdata', '.data', '.text']	✔
sha512	sha512	-	-

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

Object attribute	MISP attribute type	Description	Disable correlation
passport-number	passport-number	-	-
nationality	nationality	-	-
passport-expiration	passport-expiration	-	-

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

Object attribute	MISP attribute type	Description	Disable correlation
callback-average	counter	-	✔
ratio-functions	float	-	✔
gml	attachment	-	✔
callback-largest	counter	-	✔
dangling-strings	counter	-	✔
create-thread	counter	-	✔
shortest-path-to-create-thread	counter	-	✔
referenced-strings	counter	-	✔
miss-api	counter	-	✔
callbacks	counter	-	✔
total-functions	counter	-	✔
total-api	counter	-	✔
ratio-string	float	-	✔
not-referenced-strings	counter	-	✔
r2-commit-version	text	-	✔
local-references	counter	-	✔
refsglobalvar	counter	-	✔
memory-allocations	counter	-	✔
get-proc-address	counter	-	✔
ratio-api	float	-	✔
unknown-references	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-type	text	Type of the regular expression syntax. ['PCRE', 'PCRE2', 'POSIX BRE', 'POSIX ERE']	✔
regexp	text	-	-
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
data	reg-data	-	-
key	reg-key	-	-
last-modified	datetime	-	-

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']	-
hive	reg-hive	-	-
name	reg-name	-	-

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']	-
subject	text	-	-
ip	ip-dst	-	-
constituency	text	-	-
ticket-number	text	-	-

Object attribute	MISP attribute type	Description	Disable correlation
classification	text	-	-
status	text	Status of the RTIR ticket ['new', 'open', 'stalled', 'resolved', 'rejected', 'deleted']	-

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
last-seen	datetime	-	✔
text	text	-	✔
first-seen	datetime	-	✔
version_line	text	-	-
nickname	text	-	-
flags	text	-	-
address	ip-src	-	-
published	datetime	-	✔
document	text	-	✔
fingerprint	text	-	-
description	text	-	✔
version	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
domain	domain	-	-
last-seen	datetime	-	-
text	text	-	-
url	url	-	-
host	hostname	-	-
query_string	text	-	-
first-seen	datetime	-	-
tld	text	-	-
credential	text	-	-
scheme	text	Scheme ['http', 'https', 'ftp', 'gopher', 'sip']	-
fragment	text	-	-
port	port	-	-
resource_path	text	-	-
subdomain	text	-	-
domain_without_tld	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
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']	-
roles	text	-	-
description	text	-	-
name	text	-	-
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
last-submission	datetime	-	-
detection-ratio	text	-	✔
community-score	text	-	✔
permalink	link	-	-
first-submission	datetime	-	-

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

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	-	-
text	text	-	-
registrant-email	whois-registrant-email	-	-
modification-date	datetime	-	-
registrant-name	whois-registrant-name	-	-
domain	domain	-	-
registrant-phone	whois-registrant-phone	-	-
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
text	text	-	-
x509-fingerprint-sha1	sha1	-	-
version	text	-	-
issuer	text	-	-
pubkey-info-modulus	text	-	-
subject	text	-	-
raw-base64	text	-	-
serial-number	text	-	-

Object attribute	MISP attribute type	Description	Disable correlation
validity-not-before	datetime	-	-
pubkey-info-size	text	-	-
validity-not-after	datetime	-	-
x509-fingerprint-md5	md5	-	-
pubkey-info-exponent	text	-	-
x509-fingerprint-sha256	sha256	-	-
pubkey-info-algorithm	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	yara	-	✔
whitelist	comment	-	-
comment	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']

Name of relationship	Description	Format
duplicate-of	The referenced source and target objects are semantically duplicates of each other.	['misp', 'stix-2.0']
related-to	The referenced source is related to the target object.	['misp', 'stix-2.0']
attributed-to	This referenced source is attributed to the target object.	['misp', 'stix-2.0']
targets	This relationship describes that the source object targets the target object.	['misp', 'stix-2.0']
uses	This relationship describes the use by the source object of the target object.	['misp', 'stix-2.0']
indicates	This relationships describes that the source object indicates the target object.	['misp', 'stix-2.0']
mitigates	This relationship describes a source object which mitigates the target object.	['misp', 'stix-2.0']
variant-of	This relationship describes a source object which is a variant of the target object	['misp', 'stix-2.0']
impersonates	This relationship describe a source object which impersonates the target object	['misp', 'stix-2.0']
authored-by	This relationship describes the author of a specific object.	['misp']
located	This relationship describes the location (of any type) of a specific object.	['misp']
included-in	This relationship describes an object included in another object.	['misp']
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']

Name of relationship	Description	Format
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']
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']