MISP Objects

MISP Objects

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

MISP MISP objects to be used in MISP (2.4.80 (TBC)) 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	-	✔
type	text	-	-
text	text	-	✔
first-seen	datetime	-	✔
original-date	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-name	text	-	-
text	text	-	✔
cookie-value	text	-	-
type	text	-	-
cookie	cookie	-	-

credit-card

A payment card like credit card, debit card or any similar cards which can be used for financial transactions..

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

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

elf

Object describing a Executable and Linkable Format.

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

Object attribute	MISP attribute type	Description	Disable correlation
number-sections	counter	-	✔
arch	text	-	-
type	text	-	-
text	text	-	✔
entrypoint-address	text	-	✔
os_abi	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
text	text	-	✔
type	text	-	✔
sha512	sha512	-	-
sha256	sha256	-	-
sha512/224	sha512/224	-	-
sha512/256	sha512/256	-	-
entropy	float	-	✔
sha1	sha1	-	-
sha384	sha384	-	-
md5	md5	-	-
sha224	sha224	-	-

Object attribute	MISP attribute type	Description	Disable correlation
flag	text	-	✔
name	text	-	✔
size-in-bytes	size-in-bytes	-	✔
ssdeep	ssdeep	-	-

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	-	-
header	email-header	-	-
from	email-src	-	-
to-display-name	email-dst-display-name	-	-
thread-index	email-thread-index	-	-
from-display-name	email-src-display-name	-	-
send-date	datetime	-	✔
to	email-dst	-	-
mime-boundary	email-mime-boundary	-	-
attachment	email-attachment	-	-
reply-to	email-reply-to	-	-
message-id	email-message-id	-	-
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
malware-sample	malware-sample	-	-
tlsh	tlsh	-	-
text	text	-	✔
sha512	sha512	-	-
pattern-in-file	pattern-in-file	-	-
sha256	sha256	-	-
sha512/224	sha512/224	-	-
sha512/256	sha512/256	-	-
filename	filename	-	-
entropy	float	-	✔
mimetype	text	-	✔
sha1	sha1	-	-
sha384	sha384	-	-
md5	md5	-	-
sha224	sha224	-	-
authentihash	authentihash	-	-
size-in-bytes	size-in-bytes	-	✔
ssdeep	ssdeep	-	-

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	-	-
last-seen	datetime	-	✔
region	text	-	-
altitude	float	-	-
text	text	-	✔
first-seen	datetime	-	✔
latitude	float	-	✔
country	text	-	-
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
host	hostname	-	-
uri	uri	-	-
text	text	-	✔
basicauth-password	text	-	-
cookie	text	-	-
proxy-password	text	-	-
url	url	-	-
user-agent	user-agent	-	-

Object attribute	MISP attribute type	Description	Disable correlation
content-type	other	-	-
method	http-method	-	✔
proxy-user	text	-	-
basicauth-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
src-port	port	-	-
last-seen	datetime	-	-
dst-port	port	-	-
ip	ip-dst	-	-
text	text	-	-
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
ip-src	ip-src	-	-

Object attribute	MISP attribute type	Description	Disable correlation
last-seen	datetime	-	-
ja3-fingerprint-md5	md5	-	-
description	text	-	-
first-seen	datetime	-	-
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
type	text	-	-
text	text	-	✔
entrypoint-address	text	-	✔
number-sections	counter	-	✔
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
text	text	-	✔
sha512	sha512	-	-
sha256	sha256	-	-
sha512/224	sha512/224	-	-

Object attribute	MISP attribute type	Description	Disable correlation
sha512/256	sha512/256	-	-
entropy	float	-	✔
sha1	sha1	-	-
sha384	sha384	-	-
md5	md5	-	-
sha224	sha224	-	-
name	text	-	✔
size-in-bytes	size-in-bytes	-	✔
ssdeep	ssdeep	-	-

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
rrname	text	-	-
time_first	datetime	-	-
time_last	datetime	-	-
rdata	text	-	-
zone_time_first	datetime	-	-
origin	text	-	-
sensor_id	text	-	-
text	text	-	-
count	counter	-	-
zone_time_last	datetime	-	-

Object attribute	MISP attribute type	Description	Disable correlation
bailiwick	text	-	-
rrtype	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
lang-id	text	-	✔
number-sections	counter	-	✔
product-version	text	-	✔
internal-filename	filename	-	-
impfuzzy	impfuzzy	-	-
type	text	-	✔
entrypoint-address	text	-	✔
company-name	text	-	✔
legal-copyright	text	-	✔
pehash	pehash	-	-
entrypoint-section-at-position	text	-	✔
file-version	text	-	✔
file-description	text	-	✔
original-filename	filename	-	-
imphash	imphash	-	-
product-name	text	-	✔
compilation-timestamp	datetime	-	-

Object attribute	MISP attribute type	Description	Disable correlation
text	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
text	text	-	✔
sha512	sha512	-	-
sha256	sha256	-	-
sha512/224	sha512/224	-	-
sha512/256	sha512/256	-	-
characteristic	text	-	-
entropy	float	-	✔
sha1	sha1	-	-
sha384	sha384	-	-
md5	md5	-	-
sha224	sha224	-	-
name	text	-	✔
size-in-bytes	size-in-bytes	-	✔
ssdeep	ssdeep	-	-

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

Object attribute	MISP attribute type	Description	Disable correlation
tmsi	text	-	-
msisdn	text	-	-
first-seen	datetime	-	✔
imsi	text	-	-
guti	text	-	-

r2graphity

Indicators extracted from files using radare2 and graphml.

r2graphity is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
gml	attachment	-	✔
total-functions	counter	-	✔
total-api	counter	-	✔
ratio-string	float	-	✔
unknown-references	counter	-	✔
callback-largest	counter	-	✔
referenced-strings	counter	-	✔
ratio-functions	float	-	✔
r2-commit-version	text	-	✔
text	text	-	✔
miss-api	counter	-	✔
not-referenced-strings	counter	-	✔
create-thread	counter	-	✔
callbacks	counter	-	✔

Object attribute	MISP attribute type	Description	Disable correlation
callback-average	counter	-	✔
local-references	counter	-	✔
dangling-strings	counter	-	✔
memory-allocations	counter	-	✔
ratio-api	float	-	✔
get-proc-address	counter	-	✔
refsglobalvar	counter	-	✔
shortest-path-to-create-thread	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	text	-	-
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
key	reg-key	-	-
name	reg-name	-	-
data-type	reg-datatype	-	-
data	reg-data	-	-
last-modified	datetime	-	-
hive	reg-hive	-	-

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
flags	text	-	-
published	datetime	-	✔
address	ip-src	-	-
last-seen	datetime	-	✔
nickname	text	-	-
document	text	-	✔
version_line	text	-	-
fingerprint	text	-	-
version	text	-	-
text	text	-	✔
description	text	-	✔
first-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
port	port	-	-
last-seen	datetime	-	-
host	hostname	-	-
scheme	text	-	-
fragment	text	-	-
url	url	-	-
subdomain	text	-	-
tld	text	-	-
credential	text	-	-
resource_path	text	-	-
text	text	-	-
domain_without_tld	text	-	-
query_string	text	-	-
first-seen	datetime	-	-
domain	domain	-	-

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	-	-
name	text	-	-
sectors	text	-	-
description	text	-	-
regions	text	-	-
roles	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
summary	text	-	-
vulnerable_configuration	text	-	-
references	link	-	-
text	text	-	-
id	vulnerability	-	-
published	datetime	-	-
modified	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
domain	domain	-	-
registrant-phone	whois-registrant-phone	-	-
expiration-date	datetime	-	-
registrant-email	whois-registrant-email	-	-
creation-date	datetime	-	-
text	text	-	-
registrant-name	whois-registrant-name	-	-
modification-date	datetime	-	-
registar	whois-registrar	-	-

x509

x509 object describing a X.509 certificate.

x509 is a MISP object available in JSON format at **this location** The JSON format can be freely reused in your application or automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
subject	text	-	-
serial-number	text	-	-
pubkey-info-size	text	-	-
x509-fingerprint-md5	md5	-	-
version	text	-	-
validity-not-after	datetime	-	-
pubkey-info-exponent	text	-	-
validity-not-before	datetime	-	-
x509-fingerprint-sha256	sha256	-	-
pubkey-info-modulus	text	-	-

Object attribute	MISP attribute type	Description	Disable correlation
raw-base64	text	-	-
issuer	text	-	-
x509-fingerprint-sha1	sha1	-	-
text	text	-	-
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
comment	comment	-	-
version	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']

Name of relationship	Description	Format
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']
dropped-by	This relationship describes an object dropped by another object.	['misp']

Name of relationship	Description	Format
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']