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
origin	url	—	—
last-seen	datetime	—	✓
text	text	—	✓
original-date	datetime	—	✓
type	text	—	—
sensor	text	—	—
first-seen	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
text	text	—	✓
cookie	cookie	—	—
cookie-name	text	—	—
cookie-value	text	—	—
type	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
comment	comment	—	—
expiration	datetime	—	—
name	text	—	—
issued	datetime	—	—
cc-number	cc-number	—	—
version	comment	—	—
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
text	text	-	-
ip-dst	ip-dst	-	-
src-port	port	-	-
protocol	text	Protocol used for the attack ['TCP', 'UDP', 'ICMP', 'IP']	-
ip-src	ip-src	-	-
total-pps	counter	-	-
total-bps	counter	-	-
last-seen	datetime	-	-
dst-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	-	-
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
text	text	−	✓
os_abi	text	−	−
entrypoint-address	text	−	✓
number-sections	counter	−	✓
arch	text	−	−
type	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
entropy	float	−	✓
sha512/224	sha512/224	−	−
sha384	sha384	−	−
sha512/256	sha512/256	−	−
type	text	−	✓
ssdeep	ssdeep	−	−
sha256	sha256	−	−
flag	text	−	✓
md5	md5	−	−
name	text	−	✓
sha224	sha224	−	−

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

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
thread-index	email-thread-index	−	−
subject	email-subject	−	−
reply-to	email-reply-to	−	−
attachment	email-attachment	−	−
mime-boundary	email-mime-boundary	−	−
from	email-src	−	−
from-display-name	email-src-display-name	−	−
message-id	email-message-id	−	−
to-display-name	email-dst-display-name	−	−
to	email-dst	−	−
send-date	datetime	−	✓
header	email-header	−	−
x-mailer	email-x-mailer	−	−

file

File object describing a file with meta-information.

> ℹ 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
entropy	float	−	✓
authentihash	authentihash	−	−
sha512/224	sha512/224	−	−
filename	filename	−	−
tlsh	tlsh	−	−
sha384	sha384	−	−
sha512/256	sha512/256	−	−
ssdeep	ssdeep	−	−
sha256	sha256	−	−
pattern-in-file	pattern-in-file	−	−
md5	md5	−	−
malware-sample	malware-sample	−	−
sha224	sha224	−	−
sha512	sha512	−	−
sha1	sha1	−	−
mimetype	text	−	✓
text	text	−	✓
size-in-bytes	size-in-bytes	−	✓

geolocation

An object to describe a geographic location..

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

Object attribute	MISP attribute type	Description	Disable correlation
region	text	−	−
country	text	−	−
city	text	−	−
altitude	float	−	−
latitude	float	−	✓
text	text	−	✓
last-seen	datetime	−	✓
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
user-agent	user-agent	−	−
cookie	text	−	−
proxy-user	text	−	−
url	url	−	−
method	http-method	−	✓
proxy-password	text	−	−
host	hostname	−	−
basicauth-user	text	−	−

Object attribute	MISP attribute type	Description	Disable correlation
uri	uri	−	−
basicauth-password	text	−	−
text	text	−	✓
content-type	other	−	−
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	−	−
ip	ip-dst	−	−
dst-port	port	−	−
last-seen	datetime	−	−
text	text	−	−
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
name	text	−	−
entrypoint-address	text	−	✓
type	text	−	−

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

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
time_first	datetime	—	—
sensor_id	text	—	—
rrname	text	—	—
rrtype	text	—	—
zone_time_first	datetime	—	—
rdata	text	—	—
origin	text	—	—
bailiwick	text	—	—
text	text	—	—
count	counter	—	—
zone_time_last	datetime	—	—
time_last	datetime	—	—

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
company-name	text	—	✓
entrypoint-section-at-position	text	—	✓
compilation-timestamp	datetime	—	—
impfuzzy	impfuzzy	—	—
file-description	text	—	✓
product-name	text	—	✓
original-filename	filename	—	—

Object attribute	MISP attribute type	Description	Disable correlation
type	text	—	✓
pehash	pehash	—	—
file-version	text	—	✓
legal-copyright	text	—	✓
entrypoint-address	text	—	✓
lang-id	text	—	✓
text	text	—	✓
internal-filename	filename	—	—
number-sections	counter	—	✓
imphash	imphash	—	—
product-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
entropy	float	—	✓
sha512/224	sha512/224	—	—
characteristic	text	—	—
sha384	sha384	—	—
sha512/256	sha512/256	—	—
ssdeep	ssdeep	—	—
sha256	sha256	—	—
md5	md5	—	—

Object attribute	MISP attribute type	Description	Disable correlation
name	text	−	✓
sha224	sha224	−	−
sha512	sha512	−	−
sha1	sha1	−	−
text	text	−	✓
size-in-bytes	size-in-bytes	−	✓

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

Object attribute	MISP attribute type	Description	Disable correlation
passport-number	passport-number	—	—

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
imsi	text	—	—
msisdn	text	—	—
imei	text	—	—
tmsi	text	—	—
gummei	text	—	—
text	text	—	✓
serial-number	text	—	—
last-seen	datetime	—	✓
first-seen	datetime	—	✓
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
callback-average	counter	—	✓
memory-allocations	counter	—	✓
get-proc-address	counter	—	✓

Object attribute	MISP attribute type	Description	Disable correlation
r2-commit-version	text	−	✓
total-api	counter	−	✓
refsglobalvar	counter	−	✓
referenced-strings	counter	−	✓
miss-api	counter	−	✓
ratio-string	float	−	✓
text	text	−	✓
callbacks	counter	−	✓
ratio-api	float	−	✓
unknown-references	counter	−	✓
local-references	counter	−	✓
not-referenced-strings	counter	−	✓
callback-largest	counter	−	✓
gml	attachment	−	✓
total-functions	counter	−	✓
shortest-path-to-create-thread	counter	−	✓
ratio-functions	float	−	✓
dangling-strings	counter	−	✓
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
data	reg-data	–	–
last-modified	datetime	–	–
hive	reg-hive	–	–
name	reg-name	–	–
key	reg-key	–	–
data-type	reg-datatype	–	–

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	–	✓
flags	text	–	–

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

url

url object describes an url along with its normalized field (like extracted using faup parsing library) and its metadata..

ℹ 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	−	−
url	url	−	−
port	port	−	−
tld	text	−	−
first-seen	datetime	−	−
host	hostname	−	−
scheme	text	−	−
resource_path	text	−	−

Object attribute	MISP attribute type	Description	Disable correlation
credential	text	–	–
domain_without_tld	text	–	–
subdomain	text	–	–
fragment	text	–	–
text	text	–	–
last-seen	datetime	–	–
query_string	text	–	–

vulnerability

Vulnerability object describing common vulnerability enumeration.

ℹ 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
modified	datetime	–	–
id	vulnerability	–	–
references	link	–	–
vulnerable_configuration	text	–	–
summary	text	–	–
text	text	–	–
published	datetime	–	–

whois

Whois records information for a domain name..

ℹ 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
expiration-date	datetime	–	–
modification-date	datetime	–	–
registrant-name	whois-registrant-name	–	–
registrant-phone	whois-registrant-phone	–	–
creation-date	datetime	–	–
text	text	–	–
registrant-email	whois-registrant-email	–	–
registar	whois-registar	–	–
domain	domain	–	–

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
issuer	text	–	–
x509-fingerprint-md5	md5	–	–
raw-base64	text	–	–
subject	text	–	–
x509-fingerprint-sha1	sha1	–	–
x509-fingerprint-sha256	sha256	–	–
pubkey-info-exponent	text	–	–
validity-not-before	datetime	–	–
version	text	–	–
pubkey-info-modulus	text	–	–

Object attribute	MISP attribute type	Description	Disable correlation
pubkey-info-size	text	−	−
pubkey-info-algorithm	text	−	−
text	text	−	−
serial-number	text	−	−
validity-not-after	datetime	−	−

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	−	−
whitelist	comment	−	−
yara-hunt	yara	−	✓
yara	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']