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
original-date	datetime	When the information available in the leak was created. It's usually before the first-seen.	✔
type	text	Type of information leak as discovered and classified by an AIL module.	-
text	text	A description of the leak which could include the potential victim(s) or description of the leak.	✔
first-seen	datetime	When the leak has been accessible or seen for the first time.	✔

Object attribute	MISP attribute type	Description	Disable correlation
sensor	text	The AIL sensor uuid where the leak was processed and analysed.	-
origin	url	The link where the leak is (or was) accessible at first-seen.	-
last-seen	datetime	When the leak has been accessible or seen for the last time.	✔

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	A description of the cookie.	✔
type	text	Type of cookie and how it's used in this specific object.	-
cookie-name	text	Name of the cookie (if splitted)	-
cookie-value	text	Value of the cookie (if splitted)	-
cookie	cookie	Full cookie	-

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
dst-port	port	Destination port of the attack	-
total-bps	counter	Bits per second	-
text	text	Description of the DDoS	-
protocol	text	Protocol used for the attack	-
ip-dst	ip-dst	Destination ID (victim)	-
total-pps	counter	Packets per second	-
first-seen	datetime	Beginning of the attack	-
ip-src	ip-src	IP address originating the attack	-
src-port	port	Port originating the attack	-
last-seen	datetime	End of the attack	-

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	Domain name	-
first-seen	datetime	First time the tuple has been seen	-
text	text	A description of the tuple	-
last-seen	datetime	Last time the tuple has been seen	-
ip	ip-dst	IP Address	-

elf

Object describing a Executable and Linkable Format.

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

Object attribute	MISP attribute type	Description	Disable correlation
entrypoint-address	text	Address of the entry point	✔
type	text	Type of ELF	-
number-sections	counter	Number of sections	✔
os_abi	text	Header operating system application binary interface (ABI)	-
arch	text	Architecture of the ELF file	-
text	text	Free text value to attach to the ELF	✔

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	[Insecure] MD5 hash (128 bits)	-
text	text	Free text value to attach to the section	✔
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	-
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	-
size-in-bytes	size-in-bytes	Size of the section, in bytes	✔
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	-
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	-
type	text	Type of the section	-
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	-
flag	text	Flag of the section	-
entropy	float	Entropy of the whole section	✔
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	-
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	-
name	text	Name of the section	✔

Object attribute	MISP attribute type	Description	Disable correlation
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	-

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
to	email-dst	Destination email address	-
from	email-src	Sender email address	-
to-display-name	email-dst-display-name	Display name of the receiver	-
send-date	datetime	Date the email has been sent	✔
message-id	email-message-id	Message ID	-
reply-to	email-reply-to	Email address the reply will be sent to	-
header	email-header	Full headers	-
from-display-name	email-src-display-name	Display name of the sender	-
subject	email-subject	Subject	-
x-mailer	email-x-mailer	X-Mailer generally tells the program that was used to draft and send the original email	-
thread-index	email-thread-index	Identifies a particular conversation thread	-

Object attribute	MISP attribute type	Description	Disable correlation
mime-boundary	email-mime-boundary	MIME Boundary	-
attachment	email-attachment	Attachment	-

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
md5	md5	[Insecure] MD5 hash (128 bits)	-
text	text	Free text value to attach to the file	✔
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	-
mimetype	text	Mime type	✔
filename	filename	Filename on disk	-
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	-
size-in-bytes	size-in-bytes	Size of the file, in bytes	✔
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	-
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	-
malware-sample	malware-sample	The file itself (binary)	-
pattern-in-file	pattern-in-file	Pattern that can be found in the file	-

Object attribute	MISP attribute type	Description	Disable correlation
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	-
tlsh	tlsh	Fuzzy hash by Trend Micro: Locality Sensitive Hash	-
entropy	float	Entropy of the whole file	✔
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	-
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	-
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	-
authentihash	authentihash	Authenticode executable signature hash	-

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
longitude	float	The longitude is the decimal value of the longitude in the World Geodetic System 84 (WGS84) reference	✔
text	text	A generic description of the location.	✔

Object attribute	MISP attribute type	Description	Disable correlation
latitude	float	The latitude is the decimal value of the latitude in the World Geodetic System 84 (WGS84) reference.	✔
altitude	float	The altitude is the decimal value of the altitude in the World Geodetic System 84 (WGS84) reference.	-
region	text	Region.	-
first-seen	datetime	When the location was seen for the first time.	✔
country	text	Country.	-
last-seen	datetime	When the location was seen for the last time.	✔
city	text	City.	-

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	Request URI	-
text	text	HTTP Request comment	✔
basicauth-user	text	HTTP Basic Authentication Username	-

Object attribute	MISP attribute type	Description	Disable correlation
basicauth-password	text	HTTP Basic Authentication Password	-
proxy-user	text	HTTP Proxy Username	-
method	http-method	HTTP Method invoked (one of GET, POST, PUT, HEAD, DELETE, OPTIONS, CONNECT)	✔
user-agent	user-agent	The user agent string of the user agent	-
content-type	other	The MIME type of the body of the request	-
referer	referer	This is the address of the previous web page from which a link to the currently requested page was followed	-
cookie	text	An HTTP cookie previously sent by the server with Set-Cookie	-
proxy-password	text	HTTP Proxy Password	-
host	hostname	The domain name of the server	-
url	url	Full HTTP Request URL	-

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
dst-port	text	Destination port	-
text	text	Description of the tuple	-
ip	ip-dst	IP Address	-
first-seen	datetime	First time the tuple has been seen	-
src-port	text	Source port	-
last-seen	datetime	Last time the tuple has been seen	-

macho

Object describing a file in Mach-O format..

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

Object attribute	MISP attribute type	Description	Disable correlation
entrypoint-address	text	Address of the entry point	✔
type	text	Type of Mach-O	-
text	text	Free text value to attach to the Mach-O file	✔
number-sections	counter	Number of sections	✔
name	text	Binary's name	-

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	[Insecure] MD5 hash (128 bits)	-
text	text	Free text value to attach to the section	✔
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	-
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	-
size-in-bytes	size-in-bytes	Size of the section, in bytes	✔
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	-
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	-
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	-
entropy	float	Entropy of the whole section	✔
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	-
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	-
name	text	Name of the section	✔
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	-

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	Resource Record name of the queried resource	-
text	text	-	-
sensor_id	text	Sensor information where the record was seen	-
zone_time_first	datetime	First time that the unique tuple (rrname, rrtype, rdata) record has been seen via master file import	-
rrtype	text	Resource Record type as seen by the passive DNS	-
rdata	text	Resource records of the queried resource	-
bailiwick	text	Best estimate of the apex of the zone where this data is authoritative	-
time_first	datetime	First time that the unique tuple (rrname, rrtype, rdata) has been seen by the passive DNS	-
count	counter	How many authoritative DNS answers were received at the Passive DNS Server's collectors with exactly the given set of values as answers	-

Object attribute	MISP attribute type	Description	Disable correlation
time_last	datetime	Last time that the unique tuple (rrname, rrtype, rdata) record has been seen by the passive DNS	-
zone_time_last	datetime	Last time that the unique tuple (rrname, rrtype, rdata) record has been seen via master file import	-
origin	text	Origin of the Passive DNS response	-

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
product-name	text	ProductName in the resources	✔
pehash	pehash	Hash of the structural information about a sample. See https://www.usenix.org/legacy/event/leet09/tech/full_papers/wicherski/wicherski_html/	-
text	text	Free text value to attach to the PE	✔
file-version	text	FileVersion in the resources	✔

Object attribute	MISP attribute type	Description	Disable correlation
impfuzzy	impfuzzy	Fuzzy Hash (ssdeep) calculated from the import table	-
entrypoint-section-at-position	text	Name of the section and position of the section in the PE	✔
original-filename	filename	OriginalFilename in the resources	-
lang-id	text	Lang ID in the resources	✔
legal-copyright	text	LegalCopyright in the resources	✔
company-name	text	CompanyName in the resources	✔
entrypoint-address	text	Address of the entry point	✔
type	text	Type of PE	✔
number-sections	counter	Number of sections	✔
file-description	text	FileDescription in the resources	✔
product-version	text	ProductVersion in the resources	✔
internal-filename	filename	InternalFilename in the resources	-
imphash	imphash	Hash (md5) calculated from the import table	-
compilation-timestamp	datetime	Compilation timestamp defined in the PE header	-

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	[Insecure] MD5 hash (128 bits)	-
text	text	Free text value to attach to the section	✔
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	-
characteristic	text	Characteristic of the section	-
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	-
size-in-bytes	size-in-bytes	Size of the section, in bytes	✔
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	-
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	-
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	-
entropy	float	Entropy of the whole section	✔
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	-

Object attribute	MISP attribute type	Description	Disable correlation
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	-
name	text	Name of the section	✔
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	-

phone

A phone or mobile phone object which describe a phone..

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

Object attribute	MISP attribute type	Description	Disable correlation
imei	text	International Mobile Equipment Identity (IMEI) is a number, usually unique, to identify 3GPP and iDEN mobile phones, as well as some satellite phones.	-
serial-number	text	Serial Number.	-
gummei	text	Globally Unique MME Identifier (GUMMEI) is composed from MCC, MNC and MME Identifier (MMEI).	-
tmsi	text	Temporary Mobile Subscriber Identities (TMSI) to visiting mobile subscribers can be allocated.	-

Object attribute	MISP attribute type	Description	Disable correlation
guti	text	Globally Unique Temporary UE Identity (GUTI) is a temporary identification to not reveal the phone (user equipment in 3GPP jargon) composed of GUMMEI and the M-TMSI.	✗
first-seen	datetime	When the phone has been accessible or seen for the first time.	✓
text	text	A description of the phone.	✓
last-seen	datetime	When the phone has been accessible or seen for the last time.	✓
imsi	text	A usually unique International Mobile Subscriber Identity (IMSI) is allocated to each mobile subscriber in the GSM/UMTS/EPS system. IMSI can also refer to International Mobile Station Identity in the ITU nomenclature.	✗

Object attribute	MISP attribute type	Description	Disable correlation
msisdn	text	MSISDN (pronounced as /'em es ai es di en/ or misden) is a number uniquely identifying a subscription in a GSM or a UMTS mobile network. Simply put, it is the mapping of the telephone number to the SIM card in a mobile/cellular phone. This abbreviation has a several interpretations, the most common one being Mobile Station International Subscriber Directory Number.	-

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
create-thread	counter	Amount of calls to CreateThread	✔
unknown-references	counter	Amount of API calls not ending in a function (Radare2 bug, probalby)	✔
total-functions	counter	Total amount of functions in the file.	✔
memory-allocations	counter	Amount of memory allocations	✔
callback-largest	counter	Largest callback	✔

Object attribute	MISP attribute type	Description	Disable correlation
total-api	counter	Total amount of API calls	✔
ratio-functions	float	Ratio: amount of functions per kilobyte of code section	✔
callback-average	counter	Average size of a callback	✔
miss-api	counter	Amount of API call reference that does not resolve to a function offset	✔
dangling-strings	counter	Amount of dangling strings (string with a code cross reference, that is not within a function. Radare2 failed to detect that function.)	✔
get-proc-address	counter	Amount of calls to GetProcAddress	✔
referenced-strings	counter	Amount of referenced strings	✔
text	text	Description of the r2graphity object	✔
gml	attachment	Graph export in G>raph Modelling Language format	✔
r2-commit-version	text	Radare2 commit ID used to generate this object	✔
local-references	counter	Amount of API calls inside a code section	✔

Object attribute	MISP attribute type	Description	Disable correlation
shortest-path-to-create-thread	counter	Shortest path to the first time the binary calls CreateThread	✔
ratio-string	float	Ratio: amount of referenced strings per kilobyte of code section	✔
ratio-api	float	Ratio: amount of API calls per kilobyte of code section	✔
not-referenced-strings	counter	Amount of not referenced strings	✔
refsglobalvar	counter	Amount of API calls outside of code section (glob var, dynamic API)	✔
callbacks	counter	Amount of callbacks (functions started as thread)	✔

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	-
last-modified	datetime	Last time the registry key has been modified	-
hive	reg-hive	Hive used to store the registry key (file on disk)	-
key	reg-key	Full key path	-

Object attribute	MISP attribute type	Description	Disable correlation
data	reg-data	Data stored in the registry key	-
name	reg-name	Name of the registry key	-

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	list of flag associated with the node.	-
text	text	Tor node comment.	✔
nickname	text	router's nickname.	-
first-seen	datetime	When the Tor node designed by the IP address has been seen for the first time.	✔
version	text	parsed version of tor, this is None if the relay's using a new versioning scheme.	-
document	text	Raw document from the consensus.	✔
published	datetime	router's publication time. This can be different from first-seen and last-seen.	✔
description	text	Tor node description.	✔

Object attribute	MISP attribute type	Description	Disable correlation
version_line	text	versioning information reported by the node.	-
last-seen	datetime	When the Tor node designed by the IP address has been seen for the last time.	✔
fingerprint	text	router's fingerprint.	-
address	ip-src	IP address of the Tor node seen.	-

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	text	Port number	-
tld	text	Top-Level Domain	-
first-seen	datetime	First time this URL has been seen	-
subdomain	text	Subdomain	-
resource_path	text	Path (between hostname:port and query)	-
fragment	text	Fragment identifier is a short string of characters that refers to a resource that is subordinate to another, primary resource.	-

Object attribute	MISP attribute type	Description	Disable correlation
credential	text	Credential (username, password)	-
text	text	Description of the URL	-
query_string	text	Query (after path, preceded by '?')	-
last-seen	datetime	Last time this URL has been seen	-
scheme	text	Scheme	-
domain	domain	Full domain	-
host	hostname	Full hostname	-
url	url	Full URL	-
domain_without_tld	text	Domain without Top-Level Domain	-

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
vulnerable_configuration	text	The vulnerable configuration is described in CPE format	-
id	vulnerability	Vulnerability ID (generally CVE, but not necessarely)	-
text	text	Description of the vulnerability	-

Object attribute	MISP attribute type	Description	Disable correlation
references	link	External references	-
modified	datetime	Last modification date	-
published	datetime	Initial publication date	-
summary	text	Summary of the vulnerability	-

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
modification-date	datetime	Last update of the whois entry	-
text	text	Full whois entry	-
domain	domain	Domain of the whois entry	-
expiration-date	datetime	Expiration of the whois entry	-
registrant-phone	whois-registrant-phone	Registrant phone number	-
creation-date	datetime	Initial creation of the whois entry	-
registar	whois-registar	Registar of the whois entry	-
registrant-name	whois-registrant-name	Registrant name	-
registrant-email	whois-registrant-email	Registrant email address	-

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
raw-base64	text	Raw certificate base64 encoded	-
x509-fingerprint-sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	-
text	text	Free text description of hte certificate	-
pubkey-info-algorithm	text	Algorithm of the public key	-
validity-not-before	datetime	Certificate invalid before that date	-
x509-fingerprint-sha256	sha256	Secure Hash Algorithm 2 (256 bits)	-
validity-not-after	datetime	Certificate invalid after that date	-
pubkey-info-exponent	text	Exponent of the public key	-
x509-fingerprint-md5	md5	[Insecure] MD5 hash (128 bits)	-
issuer	text	Issuer of the certificate	-
pubkey-info-size	text	Length of the public key (in bits)	-
subject	text	Subject of the certificate	-

Object attribute	MISP attribute type	Description	Disable correlation
pubkey-info-modulus	text	Modulus of the public key	-
version	text	Version of the certificate	-
serial-number	text	Serial number of the certificate	-