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
origin	url	The link where the leak is (or was) accessible at first-seen.	−
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.	✓
original-date	datetime	When the information available in the leak was created. It's usually before the first-seen.	✓

Object attribute	MISP attribute type	Description	Disable correlation
last-seen	datetime	When the leak has been accessible or seen for the last time.	✓
type	text	Type of information leak as discovered and classified by an AIL module. ['Credential', 'CreditCards', 'Mail', 'Onion', 'Phone', 'Keys']	−
sensor	text	The AIL sensor uuid where the leak was processed and analysed.	−

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
software	text	Name of antivirus software	−
signature	text	Name of detection signature	−
text	text	Free text value to attach to the file	✓
datetime	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
text	text	A description of the cookie.	✓
cookie-value	text	Value of the cookie (if splitted)	—
type	text	Type of cookie and how it’s used in this specific object. ['Session management', 'Personalization', 'Tracking', 'Exfiltration', 'Malicious Payload', 'Beaconing']	—
cookie-name	text	Name of the cookie (if splitted)	—
cookie	cookie	Full 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
version	text	Version of the card.	—
cc-number	cc-number	credit-card number as encoded on the card.	—
name	text	Name of the card owner.	—
expiration	datetime	Maximum date of validity	—

Object attribute	MISP attribute type	Description	Disable correlation
issued	datetime	Initial date of validity or issued date.	−
card-security-code	text	Card security code (CSC, CVD, CVV, CVC and SPC) as embossed or printed on the card.	−
comment	comment	A description of the card.	−

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	End of the attack	−
text	text	Description of the DDoS	−
ip-dst	ip-dst	Destination ID (victim)	−
total-pps	counter	Packets per second	−
protocol	text	Protocol used for the attack ['TCP', 'UDP', 'ICMP', 'IP']	−
total-bps	counter	Bits per second	−
first-seen	datetime	Beginning of the attack	−
dst-port	port	Destination port of the attack	−
ip-src	ip-src	IP address originating the attack	−

Object attribute	MISP attribute type	Description	Disable correlation
src-port	port	Port originating 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
ip	ip-dst	IP Address	−
domain	domain	Domain name	−
text	text	A description of the tuple	−
first-seen	datetime	First time the tuple has been seen	−
last-seen	datetime	Last time the tuple has been seen	−

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	✓
text	text	Free text value to attach to the ELF	✓
number-sections	counter	Number of sections	✓

Object attribute	MISP attribute type	Description	Disable correlation
os_abi	text	Header operating system application binary interface (ABI) ['AIX', 'ARM', 'AROS', 'C6000_ELFABI', 'C6000_LINUX', 'CLOUDABI', 'FENIXOS', 'FREEBSD', 'GNU', 'HPUX', 'HURD', 'IRIX', 'MODESTO', 'NETBSD', 'NSK', 'OPENBSD', 'OPENVMS', 'SOLARIS', 'STANDALONE', 'SYSTEMV', 'TRU64']	▬
type	text	Type of ELF ['CORE', 'DYNAMIC', 'EXECUTABLE', 'HIPROC', 'LOPROC', 'NONE', 'RELOCATABLE']	▬

Object attribute	MISP attribute type	Description	Disable correlation
arch	text	Architecture of the ELF file ['None', 'M32', 'SPARC', 'i386', 'ARCH_68K', 'ARCH_88K', 'IAMCU', 'ARCH_860', 'MIPS', 'S370', 'MIPS_RS3_LE', 'PARISC', 'VPP500', 'SPARC32PLUS', 'ARCH_960', 'PPC', 'PPC64', 'S390', 'SPU', 'V800', 'FR20', 'RH32', 'RCE', 'ARM', 'ALPHA', 'SH', 'SPARCV9', 'TRICORE', 'ARC', 'H8_300', 'H8_300H', 'H8S', 'H8_500', 'IA_64', 'MIPS_X', 'COLDFIRE', 'ARCH_68HC12', 'MMA', 'PCP', 'NCPU', 'NDR1', 'STARCORE', 'ME16', 'ST100', 'TINYJ', 'x86_64', 'PDSP', 'PDP10', 'PDP11', 'FX66', 'ST9PLUS', 'ST7', 'ARCH_68HC16', 'ARCH_68HC11', 'ARCH_68HC08', 'ARCH_68HC05', 'SVX', 'ST19', 'VAX', 'CRIS', 'JAVELIN', 'FIREPATH', 'ZSP', 'MMIX', 'HUANY', 'PRISM', 'AVR', 'FR30', 'D10V', 'D30V', 'V850', 'M32R', 'MN10300', 'MN10200', 'PJ', 'OPENRISC', 'ARC_COMPACT', 'XTENSA', 'VIDEOCORE', 'TMM_GPP', 'NS32K', 'TPC', 'SNP1K', 'ST200', 'IP2K', 'MAX', 'CR', 'F2MC16', 'MSP430', 'BLACKFIN', 'SE_C33', 'SEP', 'ARCA', 'UNICORE', 'EXCESS', 'DXP', 'ALTERA_NIOS2', 'CRX', 'XGATE', 'C166',	-

elf-section

'M16C', 'DSPIC30F', 'CE', 'M32C', 'TSK3000', 'RS08', 'SHARC', 'ECOG2', 'SCORE7', 'DSP24', 'VIDEOCORE3', 'LATTICEMICO32',

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
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	−
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	−
md5	md5	[Insecure] MD5 hash (128 bits)	−
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']	✓

'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']	✓
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	−
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	−
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	−
text	text	Free text value to attach to the section	✓
name	text	Name of the section	✓
entropy	float	Entropy of the whole section	✓

Object attribute	MISP attribute type	Description	Disable correlation
size-in-bytes	size-in-bytes	Size of the section, in bytes	✓
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	−
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	−
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 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
mime-boundary	email-mime-boundary	MIME Boundary	−
x-mailer	email-x-mailer	X-Mailer generally tells the program that was used to draft and send the original email	−
from-display-name	email-src-display-name	Display name of the sender	−
to-display-name	email-dst-display-name	Display name of the receiver	−
message-id	email-message-id	Message ID	−
return-path	text	Message return path	−
reply-to	email-reply-to	Email address the reply will be sent to	−
subject	email-subject	Subject	−

Object attribute	MISP attribute type	Description	Disable correlation
send-date	datetime	Date the email has been sent	✔
thread-index	email-thread-index	Identifies a particular conversation thread	−
cc	email-dst	Carbon copy	−
to	email-dst	Destination email address	−
attachment	email-attachment	Attachment	−
header	email-header	Full headers	−
from	email-src	Sender email address	−

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	The file itself (binary)	−
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	−
tlsh	tlsh	Fuzzy hash by Trend Micro: Locality Sensitive Hash	−
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	−
md5	md5	[Insecure] MD5 hash (128 bits)	−

Object attribute	MISP attribute type	Description	Disable correlation
pattern-in-file	pattern-in-file	Pattern that can be found in the file	−
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	−
mimetype	text	Mime type	✓
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	−
authentihash	authentihash	Authenticode executable signature hash	−
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	−
text	text	Free text value to attach to the file	✓
entropy	float	Entropy of the whole file	✓
size-in-bytes	size-in-bytes	Size of the file, in bytes	✓
state	text	State of the file ['Harmless', 'Signed', 'Revoked', 'Expired', 'Trusted']	−
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	−
filename	filename	Filename on disk	−
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	−
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	−

geolocation

An object to describe a geographic location..

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

Object attribute	MISP attribute type	Description	Disable correlation
text	text	A generic description of the location.	✓
longitude	float	The longitude is the decimal value of the longitude in the World Geodetic System 84 (WGS84) reference	✓
region	text	Region.	—
latitude	float	The latitude is the decimal value of the latitude in the World Geodetic System 84 (WGS84) reference.	✓
last-seen	datetime	When the location was seen for the last time.	✓
first-seen	datetime	When the location was seen for the first time.	✓
country	text	Country.	—
altitude	float	The altitude is the decimal value of the altitude in the World Geodetic System 84 (WGS84) reference.	—
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
user-agent	user-agent	The user agent string of the user agent	−
uri	uri	Request URI	−
proxy-user	text	HTTP Proxy Username	−
content-type	other	The MIME type of the body of the request	−
basicauth-password	text	HTTP Basic Authentication Password	−
url	url	Full HTTP Request URL	−
referer	referer	This is the address of the previous web page from which a link to the currently requested page was followed	−
host	hostname	The domain name of the server	−
proxy-password	text	HTTP Proxy Password	−
text	text	HTTP Request comment	✓
basicauth-user	text	HTTP Basic Authentication Username	−
method	http-method	HTTP Method invoked (one of GET, POST, PUT, HEAD, DELETE, OPTIONS, CONNECT)	✓

Object attribute	MISP attribute type	Description	Disable correlation
cookie	text	An HTTP cookie previously sent by the server with Set-Cookie	–

ip-port

An IP address and a port seen as a tuple (or as a triple) in a specific time frame..

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

ℹ 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
ja3-fingerprint-md5	md5	Hash identifying source	–

Object attribute	MISP attribute type	Description	Disable correlation
ip-src	ip-src	Source IP Address	−
description	text	Type of detected software ie software, malware	−
last-seen	datetime	Last seen of the SSL/TLS handshake	−
first-seen	datetime	First seen of the SSL/TLS handshake	−
ip-dst	ip-dst	Destination IP address	−

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	✓
text	text	Free text value to attach to the Mach-O file	✓
type	text	Type of Mach-O ['BUNDLE', 'CORE', 'DSYM', 'DYLIB', 'DYLIB_STUB', 'DYLINKER', 'EXECUTE', 'FVMLIB', 'KEXT_BUNDLE', 'OBJECT', 'PRELOAD']	−
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
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	−
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	−
md5	md5	[Insecure] MD5 hash (128 bits)	−
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	−
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	−
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	−
text	text	Free text value to attach to the section	✓
name	text	Name of the section	✓
entropy	float	Entropy of the whole section	✓
size-in-bytes	size-in-bytes	Size of the section, in bytes	✓
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	−
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	−

Object attribute	MISP attribute type	Description	Disable correlation
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	−

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
removal-date	datetime	When the microblog post was removed	−
post	text	Raw post	−
modification-date	datetime	Last update of the microblog post	−
username	text	Username who posted the microblog post	−
creation-date	datetime	Initial creation of the microblog post	−
url	url	Original URL location of the microblog post	−
link	url	Link into the microblog post	−
type	text	Type of the microblog post ['Twitter', 'Facebook', 'LinkedIn', 'Reddit', 'Google+', 'Instagram', 'Forum', 'Other']	−
username-quoted	text	Username who are quoted into the microblog post	−

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
src-as	AS	Source AS number for this flow	−
ip_version	counter	IP version of this flow	✓
icmp-type	text	ICMP type of the flow (if the traffic is ICMP)	✓
ip-protocol-number	size-in-bytes	IP protocol number of this flow	✓
protocol	text	Protocol used for this flow ['TCP', 'UDP', 'ICMP', 'IP']	−
dst-port	port	Destination port of the netflow	−
ip-dst	ip-dst	IP address destination of the netflow	−
tcp-flags	text	TCP flags of the flow	✓
direction	text	Direction of this flow ['Ingress', 'Egress']	✓
dst-as	AS	Destination AS number for this flow	−
byte-count	counter	Bytes counted in this flow	✓
first-packet-seen	datetime	First packet seen in this flow	−

Object attribute	MISP attribute type	Description	Disable correlation
packet-count	counter	Packets counted in this flow	✓
flow-count	counter	Flows counted in this flow	✓
last-packet-seen	datetime	Last packet seen in this flow	−
ip-src	ip-src	IP address source of the netflow	−
src-port	port	Source port of the netflow	−

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
rrtype	text	Resource Record type as seen by the passive DNS ['A', 'AAAA', 'CNAME', 'PTR', 'SOA', 'TXT', 'DNAME', 'NS', 'SRV', 'RP', 'NAPTR', 'HINFO', 'A6']	−
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	−
rdata	text	Resource records of the queried resource	−

Object attribute	MISP attribute type	Description	Disable correlation
zone_time_first	datetime	First time that the unique tuple (rrname, rrtype, rdata) record has been seen via master file import	▬
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	▬
rrname	text	Resource Record name of the queried resource	▬
text	text	▬	▬
sensor_id	text	Sensor information where the record was seen	▬
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	▬
time_last	datetime	Last time that the unique tuple (rrname, rrtype, rdata) record has been seen by the passive DNS	▬

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
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']	−
paste	text	Raw text of the paste or post	−
url	url	Link to the original source of the paste or post.	−
last-seen	datetime	When the paste has been accessible or seen for the last time.	✓
first-seen	datetime	When the paste has been accessible or seen for the first time.	✓
title	text	Title of the paste or post.	−

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
pehash	pehash	Hash of the structural information about a sample. See https://www.usenix.org/legacy/event/leet09/tech/full_papers/wicherski/wicherski_html/	−
product-name	text	ProductName in the resources	✓
compilation-timestamp	datetime	Compilation timestamp defined in the PE header	−
product-version	text	ProductVersion in the resources	✓
type	text	Type of PE ['exe', 'dll', 'driver', 'unknown']	✓
company-name	text	CompanyName in the resources	✓
legal-copyright	text	LegalCopyright in the resources	✓
entrypoint-address	text	Address of the entry point	✓
lang-id	text	Lang ID in the resources	✓
text	text	Free text value to attach to the PE	✓
internal-filename	filename	InternalFilename in the resources	−
original-filename	filename	OriginalFilename in the resources	−

Object attribute	MISP attribute type	Description	Disable correlation
number-sections	counter	Number of sections	✓
impfuzzy	impfuzzy	Fuzzy Hash (ssdeep) calculated from the import table	−
file-description	text	FileDescription in the resources	✓
imphash	imphash	Hash (md5) calculated from the import table	−
entrypoint-section-at-position	text	Name of the section and position of the section in the PE	✓
file-version	text	FileVersion in the resources	✓

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
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	−
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	−
md5	md5	[Insecure] MD5 hash (128 bits)	−
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	−

Object attribute	MISP attribute type	Description	Disable correlation
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	−
characteristic	text	Characteristic of the section ['read', 'write', 'executable']	−
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	−
text	text	Free text value to attach to the section	✓
name	text	Name of the section ['.rsrc', '.reloc', '.rdata', '.data', '.text']	✓
entropy	float	Entropy of the whole section	✓
size-in-bytes	size-in-bytes	Size of the section, in bytes	✓
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	−
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	−
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	−

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
middle-name	middle-name	Middle name of a natural person	−

Object attribute	MISP attribute type	Description	Disable correlation
nationality	nationality	The nationality of a natural person.	−
last-name	last-name	Last name of a natural person.	−
redress-number	redress-number	The Redress Control Number is the record identifier for people who apply for redress through the DHS Travel Redress Inquiry Program (DHS TRIP). DHS TRIP is for travelers who have been repeatedly identified for additional screening and who want to file an inquiry to have erroneous information corrected in DHS systems.	−
passport-number	passport-number	The passport number of a natural person.	−
first-name	first-name	First name of a natural person.	−
text	text	A description of the person or identity.	✓
passport-expiration	passport-expiration	The expiration date of a passport.	−
gender	gender	The gender of a natural person. ['Male', 'Female', 'Other', 'Prefer not to say']	−
passport-country	passport-country	The country in which the passport was issued.	−

Object attribute	MISP attribute type	Description	Disable correlation
date-of-birth	date-of-birth	Date of birth of a natural person (in YYYY-MM-DD format).	−
place-of-birth	place-of-birth	Place of birth of a natural person.	−

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	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.	−
last-seen	datetime	When the phone has been accessible or seen for the last time.	✓
text	text	A description of the phone.	✓

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.	−
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.	−
gummei	text	Globally Unique MME Identifier (GUMMEI) is composed from MCC, MNC and MME Identifier (MMEI).	−
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.	−

Object attribute	MISP attribute type	Description	Disable correlation
first-seen	datetime	When the phone has been accessible or seen for the first time.	✓
tmsi	text	Temporary Mobile Subscriber Identities (TMSI) to visiting mobile subscribers can be allocated.	−
serial-number	text	Serial 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
memory-allocations	counter	Amount of memory allocations	✓
referenced-strings	counter	Amount of referenced strings	✓
ratio-functions	float	Ratio: amount of functions per kilobyte of code section	✓
total-api	counter	Total amount of API calls	✓
ratio-api	float	Ratio: amount of API calls per kilobyte of code section	✓
not-referenced-strings	counter	Amount of not referenced strings	✓

Object attribute	MISP attribute type	Description	Disable correlation
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.)	✓
text	text	Description of the r2graphity object	✓
create-thread	counter	Amount of calls to CreateThread	✓
total-functions	counter	Total amount of functions in the file.	✓
unknown-references	counter	Amount of API calls not ending in a function (Radare2 bug, probalby)	✓
shortest-path-to-create-thread	counter	Shortest path to the first time the binary calls CreateThread	✓
callbacks	counter	Amount of callbacks (functions started as thread)	✓
r2-commit-version	text	Radare2 commit ID used to generate this object	✓
get-proc-address	counter	Amount of calls to GetProcAddress	✓
callback-average	counter	Average size of a callback	✓
gml	attachment	Graph export in G>raph Modelling Language format	✓

Object attribute	MISP attribute type	Description	Disable correlation
miss-api	counter	Amount of API call reference that does not resolve to a function offset	✓
local-references	counter	Amount of API calls inside a code section	✓
callback-largest	counter	Largest callback	✓
refsglobalvar	counter	Amount of API calls outside of code section (glob var, dynamic API)	✓
ratio-string	float	Ratio: amount of referenced strings per kilobyte of code section	✓

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	text	regexp	−
regexp-type	text	Type of the regular expression syntax. ['PCRE', 'PCRE2', 'POSIX BRE', 'POSIX ERE']	✓
comment	comment	A description of the regular expression.	−

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	Full key path	−
name	reg-name	Name of the registry key	−
data	reg-data	Data stored in the registry key	−
hive	reg-hive	Hive used to store the registry key (file on disk)	−
last-modified	datetime	Last time the registry key has been modified	−
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']	−

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
subject	text	Subject of the RTIR ticket	−
status	text	Status of the RTIR ticket ['new', 'open', 'stalled', 'resolved', 'rejected', 'deleted']	−
ip	ip-dst	IPs automatically extracted from the RTIR ticket	−
classification	text	Classification of the RTIR ticket	−
ticket-number	text	ticket-number of the RTIR ticket	−
constituency	text	Constituency of the RTIR ticket	−
queue	text	Queue of the RTIR ticket ['incident', 'investigations', 'blocks', 'incident reports']	−

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..

ℹ 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
version	text	parsed version of tor, this is None if the relay's using a new versioning scheme.	−

Object attribute	MISP attribute type	Description	Disable correlation
published	datetime	router’s publication time. This can be different from first-seen and last-seen.	✓
version_line	text	versioning information reported by the node.	−
description	text	Tor node description.	✓
last-seen	datetime	When the Tor node designed by the IP address has been seen for the last time.	✓
first-seen	datetime	When the Tor node designed by the IP address has been seen for the first time.	✓
fingerprint	text	router’s fingerprint.	−
nickname	text	router’s nickname.	−
flags	text	list of flag associated with the node.	−
text	text	Tor node comment.	✓
document	text	Raw document from the consensus.	✓
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
resource_path	text	Path (between hostname:port and query)	−
scheme	text	Scheme ['http', 'https', 'ftp', 'gopher', 'sip']	−
text	text	Description of the URL	−
first-seen	datetime	First time this URL has been seen	−
last-seen	datetime	Last time this URL has been seen	−
domain	domain	Full domain	−
credential	text	Credential (username, password)	−
subdomain	text	Subdomain	−
url	url	Full URL	−
port	port	Port number	−
domain_without_tld	text	Domain without Top-Level Domain	−
host	hostname	Full hostname	−
tld	text	Top-Level Domain	−
fragment	text	Fragment identifier is a short string of characters that refers to a resource that is subordinate to another, primary resource.	−
query_string	text	Query (after path, preceded by '?')	−

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
regions	text	The list of regions or locations from the victim targeted. ISO 3166 should be used.	−
name	text	The name of the victim targeted. The name can be an organisation or a group of organisations.	−
roles	text	The list of roles targeted within the victim.	−
classification	text	The type of entity being targeted. ['individual', 'group', 'organization', 'class', 'unknown']	−
description	text	Description of the victim	−

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']	–

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
community-score	text	Community Score	✓
detection-ratio	text	Detection Ratio	✓

Object attribute	MISP attribute type	Description	Disable correlation
permalink	link	Permalink Reference	−
last-submission	datetime	Last Submission	−
first-submission	datetime	First Submission	−

vulnerability

Vulnerability object describing common vulnerability enumeration.

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

Object attribute	MISP attribute type	Description	Disable correlation
published	datetime	Initial publication date	−
id	vulnerability	Vulnerability ID (generally CVE, but not necessarely)	−
text	text	Description of the vulnerability	−
summary	text	Summary of the vulnerability	−
vulnerable_configuration	text	The vulnerable configuration is described in CPE format	−
modified	datetime	Last modification date	−
references	link	External references	−

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

x509

x509 object describing a X.509 certificate.

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

Object attribute	MISP attribute type	Description	Disable correlation
version	text	Version of the certificate	—
raw-base64	text	Raw certificate base64 encoded	—
x509-fingerprint-sha256	sha256	Secure Hash Algorithm 2 (256 bits)	—

Object attribute	MISP attribute type	Description	Disable correlation
validity-not-after	datetime	Certificate invalid after that date	−
pubkey-info-exponent	text	Exponent of the public key	−
pubkey-info-size	text	Length of the public key (in bits)	−
pubkey-info-algorithm	text	Algorithm of the public key	−
validity-not-before	datetime	Certificate invalid before that date	−
subject	text	Subject of the certificate	−
text	text	Free text description of hte certificate	−
x509-fingerprint-sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	−
pubkey-info-modulus	text	Modulus of the public key	−
serial-number	text	Serial number of the certificate	−
x509-fingerprint-md5	md5	[Insecure] MD5 hash (128 bits)	−
issuer	text	Issuer of the certificate	−

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	yabin.py and regex.txt version used for the generation of the yara rules.	−
yara	yara	Yara rule generated from -y.	✓
whitelist	comment	Whitelist name used to generate the rules.	−
comment	comment	A description of Yara rule generated.	−
yara-hunt	yara	Wide yara rule generated from -yh.	✓

Relationships

Default type of relationships in MISP objects.

Relationships are part of MISP object and available in JSON format at this location. The JSON format can be freely reused in your application or automatically enabled in MISP.

Name of relationship	Description	Format
derived-from	The information in the target object is based on information from the source object.	['misp', 'stix-2.0']
duplicate-of	The referenced source and target objects are semantically duplicates of each other.	['misp', 'stix-2.0']
related-to	The referenced source is related to the target object.	['misp', 'stix-2.0']
attributed-to	This referenced source is attributed to the target object.	['misp', 'stix-2.0']
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']

Name of relationship	Description	Format
indicates	This relationships describes that the source object indicates the target object.	['misp', 'stix-2.0']
mitigates	This relationship describes a source object which mitigates the target object.	['misp', 'stix-2.0']
variant-of	This relationship describes a source object which is a variant of the target object	['misp', 'stix-2.0']
impersonates	This relationship describe a source object which impersonates the target object	['misp', 'stix-2.0']
authored-by	This relationship describes the author of a specific object.	['misp']
located	This relationship describes the location (of any type) of a specific object.	['misp']
included-in	This relationship describes an object included in another object.	['misp']
analysed-with	This relationship describes an object analysed by another object.	['misp']
claimed-by	This relationship describes an object claimed by another object.	['misp']
communicates-with	This relationship describes an object communicating with another object.	['misp']
dropped-by	This relationship describes an object dropped by another object.	['misp']
executed-by	This relationship describes an object executed by another object.	['misp']
affects	This relationship describes an object affected by another object.	['misp']
beacons-to	This relationship describes an object beaconing to another object.	['misp']
abuses	This relationship describes an object which abuses another object.	['misp']

Name of relationship	Description	Format
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']