MISP Objects

MISP Objects

Introduction . . . 1
Funding and Support . . . 2
MISP objects . . . 3
ail-leak . . . 3
asn . . . 4
av-signature . . . 5
cookie . . . 6
credential . . . 7
credit-card . . . 8
ddos . . . 8
domain-ip . . . 9
elf . . . 10
elf-section . . . 12
email . . . 15
file . . . 16
geolocation . . . 18
http-request . . . 18
ip-port . . . 20
ja3 . . . 20
macho . . . 21
macho-section . . . 22
microblog . . . 23
netflow . . . 24
passive-dns . . . 25
paste . . . 26
pe . . . 27
pe-section . . . 29
person . . . 30
phone . . . 32
r2graphity . . . 34
regexp . . . 36
registry-key . . . 36
report . . . 37
rtir . . . 38
tor-node . . . 39
url . . . 40
victim . . . 41
virustotal-report . . . 43

vulnerability 43
whois 44
x509 44
yabin 46
Relationships 46

Introduction

[MISP logo] | *https://raw.githubusercontent.com/MISP/MISP/2.4/INSTALL/logos/misp-logo.png*

The MISP threat sharing platform is a free and open source software helping information sharing of threat intelligence including cyber security indicators, financial fraud or counter-terrorism information. The MISP project includes multiple sub-projects to support the operational requirements of analysts and improve the overall quality of information shared.

MISP objects are used in MISP (starting from version 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. The objects are just shared like any other attributes in MISP even if the other MISP instances don't have the template of the object. The following document is generated from the machine-readable JSON describing the MISP objects.

Funding and Support

The MISP project is financially and resource supported by CIRCL Computer Incident Response Center Luxembourg .

[CIRCL logo]

A CEF (Connecting Europe Facility) funding under CEF-TC-2016-3 - Cyber Security has been granted from 1st September 2017 until 31th August 2019 as **Improving MISP as building blocks for next-generation information sharing**.

[CEF funding]

If you are interested to co-fund projects around MISP, feel free to get in touch with us.

MISP objects

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
raw-data	text	Raw data as received by the AIL sensor compressed and encoded in Base64.	✔
type	text	Type of information leak as discovered and classified by an AIL module. ['Credential', 'CreditCards', 'Mail', 'Onion', 'Phone', 'Keys']	-
first-seen	datetime	When the leak has been accessible or seen for the first time.	✔
last-seen	datetime	When the leak has been accessible or seen for the last time.	✔
sensor	text	The AIL sensor uuid where the leak was processed and analysed.	-
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
origin	link	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.	✔

asn

Autonomous system object describing an autonomous system which can include one or more network operators management an entity (e.g. ISP) along with their routing policy, routing prefixes or alike..

asn 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
mp-export	text	This attribute performs the same function as the export attribute above. The difference is that mp-export allows both IPv4 and IPv6 address families to be specified. The export is described in RFC 4012 – Routing Policy Specification Language next generation (RPSLng), section 4.5. format	-
import	text	The inbound IPv4 routing policy of the AS in RFC 2622 – Routing Policy Specification Language (RPSL) format	-

Object attribute	MISP attribute type	Description	Disable correlation
asn	as	Autonomous System Number	-
first-seen	datetime	First time the ASN was seen	-
country	text	Country code of the main location of the autonomous system	-
last-seen	datetime	Last time the ASN was seen	-
subnet-announced	ip-src	Subnet announced	-
mp-import	text	The inbound IPv4 or IPv6 routing policy of the AS in RFC 4012 – Routing Policy Specification Language next generation (RPSLng), section 4.5. format	-
export	text	The outbound routing policy of the AS in RFC 2622 – Routing Policy Specification Language (RPSL) format	-
description	text	Description of the autonomous system	-

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	-
datetime	datetime	Datetime	✔
text	text	Free text value to attach to the file	✔

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	Name of the cookie (if splitted)	-
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	cookie	Full cookie	-
text	text	A description of the cookie.	✔

credential

Credential describes one or more credential(s) including password(s), api key(s) or decryption key(s)..

credential 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	Origin of the credential(s) ['bruteforce-scanning', 'malware-analysis', 'memory-analysis', 'network-analysis', 'leak', 'unknown']	-
username	text	Username related to the password(s)	-
notification	text	Mention of any notification(s) towards the potential owner(s) of the credential(s) ['victim-notified', 'service-notified', 'none']	-
format	text	Format of the password(s) ['clear-text', 'hashed', 'encrypted', 'unknown']	-
type	text	Type of password(s) ['password', 'api-key', 'encryption-key', 'unknown']	-
text	text	A description of the credential(s)	✔
password	text	Password	-

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
issued	datetime	Initial date of validity or issued date.	-
version	text	Version of the card.	-
comment	comment	A description of the card.	-
card-security-code	text	Card security code (CSC, CVD, CVV, CVC and SPC) as embossed or printed on the card.	-
cc-number	cc-number	credit-card number as encoded on the card.	-
expiration	datetime	Maximum date of validity	-
name	text	Name of the card owner.	-

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	-

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

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
last-seen	datetime	Last time the tuple has been seen	-
domain	domain	Domain name	-
first-seen	datetime	First time the tuple has been seen	-
text	text	A description of the tuple	-

Object attribute	MISP attribute type	Description	Disable correlation
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
number-sections	counter	Number of sections	✔
entrypoint-address	text	Address of the entry point	✔

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

Object attribute	MISP attribute type	Description	Disable correlation
type	text	Type of ELF ['CORE', 'DYNAMIC', 'EXECUTABLE', 'HIPROC', 'LOPROC', 'NONE', 'RELOCATABLE']	-
text	text	Free text value to attach to the ELF	✔
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']	-

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 automatically enabled in MISP.

Object attribute	MISP attribute type	Description	Disable correlation
text	text	Free text value to attach to the section	✔
md5	md5	[Insecure] MD5 hash (128 bits)	-

Object attribute	MISP attribute type	Description	Disable correlation
type	text	Type of the section ['NULL', 'PROGBITS', 'SYMTAB', 'STRTAB', 'RELA', 'HASH', 'DYNAMIC', 'NOTE', 'NOBITS', 'REL', 'SHLIB', 'DYNSYM', 'INIT_ARRAY', 'FINI_ARRAY', 'PREINIT_ARRAY', 'GROUP', 'SYMTAB_SHNDX', 'LOOS', 'GNU_ATTRIBUTES', 'GNU_HASH', 'GNU_VERDEF', 'GNU_VERNEED', 'GNU_VERSYM', 'HIOS', 'LOPROC', 'ARM_EXIDX', 'ARM_PREEMPTMAP', 'HEX_ORDERED', 'X86_64_UNWIND', 'MIPS_REGINFO', 'MIPS_OPTIONS', 'MIPS_ABIFLAGS', 'HIPROC', 'LOUSER', 'HIUSER']	✔
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	-

Object attribute	MISP attribute type	Description	Disable correlation
flag	text	Flag of the section ['ALLOC', 'EXCLUDE', 'EXECINSTR', 'GROUP', 'HEX_GPREL', 'INFO_LINK', 'LINK_ORDER', 'MASKOS', 'MASKPROC', 'MERGE', 'MIPS_ADDR', 'MIPS_LOCAL', 'MIPS_MERGE', 'MIPS_NAMES', 'MIPS_NODUPES', 'MIPS_NOSTRIP', 'NONE', 'OS_NONCONFORMING', 'STRINGS', 'TLS', 'WRITE', 'XCORE_SHF_CP_SECTION']	✔
name	text	Name of the section	✔
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	-
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	-
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	-
size-in-bytes	size-in-bytes	Size of the section, in bytes	✔
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	-
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	-
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	-

Object attribute	MISP attribute type	Description	Disable correlation
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	-
entropy	float	Entropy of the whole section	✔

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
cc	email-dst	Carbon copy	-
to-display-name	email-dst-display-name	Display name of the receiver	-
to	email-dst	Destination email address	-
message-id	email-message-id	Message ID	-
screenshot	attachment	Screenshot of email	-
header	email-header	Full headers	-
return-path	text	Message return path	-
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	-
reply-to	email-reply-to	Email address the reply will be sent to	-

Object attribute	MISP attribute type	Description	Disable correlation
send-date	datetime	Date the email has been sent	✔
from	email-src	Sender email address	-
attachment	email-attachment	Attachment	-
thread-index	email-thread-index	Identifies a particular conversation thread	-
subject	email-subject	Subject	-
from-display-name	email-src-display-name	Display name of the sender	-

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)	-
md5	md5	[Insecure] MD5 hash (128 bits)	-
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	-
pattern-in-file	pattern-in-file	Pattern that can be found in the file	-
mimetype	text	Mime type	✔

Object attribute	MISP attribute type	Description	Disable correlation
text	text	Free text value to attach to the file	✔
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	-
state	text	State of the file ['Harmless', 'Signed', 'Revoked', 'Expired', 'Trusted']	-
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	-
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	-
size-in-bytes	size-in-bytes	Size of the file, in bytes	✔
tlsh	tlsh	Fuzzy hash by Trend Micro: Locality Sensitive Hash	-
filename	filename	Filename on disk	-
sha224	sha224	Secure Hash Algorithm 2 (224 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	-
entropy	float	Entropy of the whole file	✔

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	City.	-
first-seen	datetime	When the location was seen for the first time.	✔
altitude	float	The altitude is the decimal value of the altitude in the World Geodetic System 84 (WGS84) reference.	-
last-seen	datetime	When the location was seen for the last time.	✔
longitude	float	The longitude is the decimal value of the longitude in the World Geodetic System 84 (WGS84) reference	✔
country	text	Country.	-
latitude	float	The latitude is the decimal value of the latitude in the World Geodetic System 84 (WGS84) reference.	✔
text	text	A generic description of the location.	✔
region	text	Region.	-

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
cookie	text	An HTTP cookie previously sent by the server with Set-Cookie	-
url	url	Full HTTP Request URL	-
content-type	other	The MIME type of the body of the request	-
uri	uri	Request URI	-
host	hostname	The domain name of the server	-
proxy-password	text	HTTP Proxy Password	-
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	-
referer	referer	This is the address of the previous web page from which a link to the currently requested page was followed	-
proxy-user	text	HTTP Proxy Username	-
basicauth-user	text	HTTP Basic Authentication Username	-
basicauth-password	text	HTTP Basic Authentication Password	-

Object attribute	MISP attribute type	Description	Disable correlation
text	text	HTTP Request comment	✔

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

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-dst	ip-dst	Destination IP address	-
first-seen	datetime	First seen of the SSL/TLS handshake	-

Object attribute	MISP attribute type	Description	Disable correlation
ip-src	ip-src	Source IP Address	-
last-seen	datetime	Last seen of the SSL/TLS handshake	-
ja3-fingerprint-md5	md5	Hash identifying source	-
description	text	Type of detected software ie software, malware	-

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	Type of Mach-O ['BUNDLE', 'CORE', 'DSYM', 'DYLIB', 'DYLIB_STUB', 'DYLINKER', 'EXECUTE', 'FVMLIB', 'KEXT_BUNDLE', 'OBJECT', 'PRELOAD']	-
entrypoint-address	text	Address of the entry point	✔
name	text	Binary's name	-
number-sections	counter	Number of sections	✔
text	text	Free text value to attach to the Mach-O file	✔

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	Free text value to attach to the section	✔
md5	md5	[Insecure] MD5 hash (128 bits)	-
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	-
name	text	Name of the section	✔
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	-
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	-
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	-
size-in-bytes	size-in-bytes	Size of the section, in bytes	✔
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	-
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	-
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	-
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	-

Object attribute	MISP attribute type	Description	Disable correlation
entropy	float	Entropy of the whole section	✔

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

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

Object attribute	MISP attribute type	Description	Disable correlation
src-as	AS	Source AS number for this flow	-
flow-count	counter	Flows counted in this flow	✔
protocol	text	Protocol used for this flow ['TCP', 'UDP', 'ICMP', 'IP']	-
first-packet-seen	datetime	First packet seen in this flow	-

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

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

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
paste	text	Raw text of the paste or post	-
first-seen	datetime	When the paste has been accessible or seen for the first time.	✔
url	url	Link to the original source of the paste or post.	-
title	text	Title of the paste or post.	-
last-seen	datetime	When the paste has been accessible or seen for the last time.	✔
origin	text	Original source of the paste or post. ['pastebin.com', 'pastebin.com_pro', 'pastie.org', 'slexy.org', 'gist.github.com', 'codepad.org', 'safebin.net', 'hastebin.com', 'ghostbin.com']	-

pe

Object describing a Portable Executable.

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

Object attribute	MISP attribute type	Description	Disable correlation
legal-copyright	text	LegalCopyright in the resources	✔

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

Object attribute	MISP attribute type	Description	Disable correlation
product-name	text	ProductName in the resources	✔
file-version	text	FileVersion in the resources	✔
entrypoint-section-at-position	text	Name of the section and position of the section in the PE	✔
type	text	Type of PE ['exe', 'dll', 'driver', 'unknown']	✔
text	text	Free text value to attach to the PE	✔

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	Free text value to attach to the section	✔
md5	md5	[Insecure] MD5 hash (128 bits)	-
characteristic	text	Characteristic of the section ['read', 'write', 'executable']	-
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	-
name	text	Name of the section ['.rsrc', '.reloc', '.rdata', '.data', '.text']	✔

Object attribute	MISP attribute type	Description	Disable correlation
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	-
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	-
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	-
size-in-bytes	size-in-bytes	Size of the section, in bytes	✔
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	-
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	-
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	-
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	-
entropy	float	Entropy of the whole section	✔

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
last-name	last-name	Last name of a natural person.	-
passport-expiration	passport-expiration	The expiration date of a passport.	-

Object attribute	MISP attribute type	Description	Disable correlation
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.	-
first-name	first-name	First name of a natural person.	-
place-of-birth	place-of-birth	Place of birth of a natural person.	-
middle-name	middle-name	Middle name of a natural person	-
passport-country	passport-country	The country in which the passport was issued.	-
date-of-birth	date-of-birth	Date of birth of a natural person (in YYYY-MM-DD format).	-
passport-number	passport-number	The passport number of a natural person.	-
nationality	nationality	The nationality of a natural person.	-

Object attribute	MISP attribute type	Description	Disable correlation
gender	gender	The gender of a natural person. ['Male', 'Female', 'Other', 'Prefer not to say']	-
text	text	A description of the person or identity.	✔

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

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.	-
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.	-
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.	-
gummei	text	Globally Unique MME Identifier (GUMMEI) is composed from MCC, MNC and MME Identifier (MMEI).	-
serial-number	text	Serial Number.	-

Object attribute	MISP attribute type	Description	Disable correlation
tmsi	text	Temporary Mobile Subscriber Identities (TMSI) to visiting mobile subscribers can be allocated.	-

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
total-functions	counter	Total amount of functions in the file.	✔
ratio-api	float	Ratio: amount of API calls per kilobyte of code section	✔
callback-average	counter	Average size of a callback	✔
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	✔
total-api	counter	Total amount of API calls	✔
callbacks	counter	Amount of callbacks (functions started as thread)	✔

Object attribute	MISP attribute type	Description	Disable correlation
not-referenced-strings	counter	Amount of not referenced strings	✔
unknown-references	counter	Amount of API calls not ending in a function (Radare2 bug, probalby)	✔
create-thread	counter	Amount of calls to CreateThread	✔
refsglobalvar	counter	Amount of API calls outside of code section (glob var, dynamic API)	✔
miss-api	counter	Amount of API call reference that does not resolve to a function offset	✔
ratio-string	float	Ratio: amount of referenced strings per kilobyte of code section	✔
r2-commit-version	text	Radare2 commit ID used to generate this object	✔
local-references	counter	Amount of API calls inside a code section	✔
gml	attachment	Graph export in G>raph Modelling Language format	✔
text	text	Description of the r2graphity object	✔
ratio-functions	float	Ratio: amount of functions per kilobyte of code section	✔
referenced-strings	counter	Amount of referenced strings	✔

Object attribute	MISP attribute type	Description	Disable correlation
memory-allocations	counter	Amount of memory allocations	✔
callback-largest	counter	Largest callback	✔
shortest-path-to-create-thread	counter	Shortest path to the first time the binary calls CreateThread	✔

regexp

An object describing a regular expression (regex or regexp). The object can be linked via a relationship to other attributes or objects to describe how it can be represented as a regular expression..

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

Object attribute	MISP attribute type	Description	Disable correlation
regexp-type	text	Type of the regular expression syntax. ['PCRE', 'PCRE2', 'POSIX BRE', 'POSIX ERE']	✔
comment	comment	A description of the regular expression.	-
regexp	text	regexp	-

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 ['REG_NONE', 'REG_SZ', 'REG_EXPAND_SZ', 'REG_BINARY', 'REG_DWORD', 'REG_DWORD_LITTLE_ENDIAN', 'REG_DWORD_BIG_ENDIAN', 'REG_LINK', 'REG_MULTI_SZ', 'REG_RESOURCE_LIST', 'REG_FULL_RESOURCE_DESCRIPTOR', 'REG_RESOURCE_REQUIREMENTS_LIST', 'REG_QWORD', 'REG_QWORD_LITTLE_ENDIAN']	-
hive	reg-hive	Hive used to store the registry key (file on disk)	-
data	reg-data	Data stored in the registry key	-
key	reg-key	Full key path	-
name	reg-name	Name of the registry key	-
last-modified	datetime	Last time the registry key has been modified	-

report

Metadata used to generate an executive level report.

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
summary	text	Free text summary of the report	-
case-number	text	Case number	-

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
classification	text	Classification of the RTIR ticket	-
status	text	Status of the RTIR ticket ['new', 'open', 'stalled', 'resolved', 'rejected', 'deleted']	-
ticket-number	text	ticket-number of the RTIR ticket	-
ip	ip-dst	IPs automatically extracted from the RTIR ticket	-
subject	text	Subject 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..

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
document	text	Raw document from the consensus.	✔
address	ip-src	IP address of the Tor node seen.	-
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.	-
published	datetime	router's publication time. This can be different from first-seen and last-seen.	✔
fingerprint	text	router's fingerprint.	-
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.	✔

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.	-

url

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

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

Object attribute	MISP attribute type	Description	Disable correlation
domain	domain	Full domain	-
query_string	text	Query (after path, preceded by '?')	-
first-seen	datetime	First time this URL has been seen	-
url	url	Full URL	-
tld	text	Top-Level Domain	✔
subdomain	text	Subdomain	✔
port	port	Port number	✔
scheme	text	Scheme ['http', 'https', 'ftp', 'gopher', 'sip']	✔
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
host	hostname	Full hostname	-
credential	text	Credential (username, password)	-
domain_without_tld	text	Domain without Top-Level Domain	-
last-seen	datetime	Last time this URL has been seen	-
text	text	Description of the URL	-
resource_path	text	Path (between hostname:port and query)	-

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.	-
classification	text	The type of entity being targeted. ['individual', 'group', 'organization', 'class', 'unknown']	-

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']	-
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.	-
description	text	Description of the victim	-

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
first-submission	datetime	First Submission	-
community-score	text	Community Score	✔
detection-ratio	text	Detection Ratio	✔
last-submission	datetime	Last Submission	-
permalink	link	Permalink Reference	-

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
id	vulnerability	Vulnerability ID (generally CVE, but not necessarely)	-
summary	text	Summary of the vulnerability	-
published	datetime	Initial publication date	-
references	link	External references	-
vulnerable_configuration	text	The vulnerable configuration is described in CPE format	-

Object attribute	MISP attribute type	Description	Disable correlation
text	text	Description of the vulnerability	-
modified	datetime	Last modification date	-

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

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

Object attribute	MISP attribute type	Description	Disable correlation
validity-not-before	datetime	Certificate invalid before that date	-

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

Relationships

Default type of relationships in MISP objects.

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

Name of relationship	Description	Format
derived-from	The information in the target object is based on information from the source object.	['misp', 'stix-2.0']

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

Name of relationship	Description	Format
dropped-by	This relationship describes an object dropped by another object.	['misp']
executed-by	This relationship describes an object executed by another object.	['misp']
affects	This relationship describes an object affected by another object.	['misp']
beacons-to	This relationship describes an object beaconing to another object.	['misp']
abuses	This relationship describes an object which abuses another object.	['misp']
exfiltrates-to	This relationship describes an object exfiltrating to another object.	['misp']
identifies	This relationship describes an object which identifies another object.	['misp']
intercepts	This relationship describes an object which intercepts another object.	['misp']
calls	This relationship describes an object which calls another objects.	['misp']
detected-as	This relationship describes an object which is detected as another object.	['misp']
triggers	This relationship describes an object which triggers another object.	['misp']
vulnerability-of	This relationship describes an object which is a vulnerability of another object.	['cert-eu']
works-like	This relationship describes an object which works like another object.	['cert-eu']
seller-of	This relationship describes an object which is selling another object.	['cert-eu']
seller-on	This relationship describes an object which is selling on another object.	['cert-eu']

Name of relationship	Description	Format
trying-to-obtain-the-exploit	This relationship describes an object which is trying to obtain the exploit described by another object	['cert-eu']
used-by	This relationship describes an object which is used by another object.	['cert-eu']
affiliated	This relationship describes an object which is affiliated with another object.	['cert-eu']
alleged-founder-of	This relationship describes an object which is the alleged founder of another object.	['cert-eu']
attacking-other-group	This relationship describes an object which attacks another object.	['cert-eu']
belongs-to	This relationship describes an object which belongs to another object.	['cert-eu']
business-relations	This relationship describes an object which has business relations with another object.	['cert-eu']
claims-to-be-the-founder-of	This relationship describes an object which claims to be the founder of another object.	['cert-eu']
cooperates-with	This relationship describes an object which cooperates with another object.	['cert-eu']
former-member-of	This relationship describes an object which is a former member of another object.	['cert-eu']
successor-of	This relationship describes an object which is a successor of another object.	['cert-eu']
has-joined	This relationship describes an object which has joined another object.	['cert-eu']
member-of	This relationship describes an object which is a member of another object.	['cert-eu']
primary-member-of	This relationship describes an object which is a primary member of another object.	['cert-eu']

Name of relationship	Description	Format
administrator-of	This relationship describes an object which is an administrator of another object.	['cert-eu']
is-in-relation-with	This relationship describes an object which is in relation with another object,	['cert-eu']
provide-support-to	This relationship describes an object which provides support to another object.	['cert-eu']
regional-branch	This relationship describes an object which is a regional branch of another object.	['cert-eu']
similar	This relationship describes an object which is similar to another object.	['cert-eu']
subgroup	This relationship describes an object which is a subgroup of another object.	['cert-eu']
suspected-link	This relationship describes an object which is suspected to be linked with another object.	['misp']
same-as	This relationship describes an object which is the same as another object.	['misp']
creator-of	This relationship describes an object which is the creator of another object.	['cert-eu']
developer-of	This relationship describes an object which is a developer of another object.	['cert-eu']
uses-for-recon	This relationship describes an object which uses another object for recon.	['cert-eu']
operator-of	This relationship describes an object which is an operator of another object.	['cert-eu']
overlaps	This relationship describes an object which overlaps another object.	['cert-eu']
owner-of	This relationship describes an object which owns another object.	['cert-eu']
publishes-method-for	This relationship describes an object which publishes method for another object.	['cert-eu']

Name of relationship	Description	Format
recommends-use-of	This relationship describes an object which recommends the use of another object.	['cert-eu']
released-source-code	This relationship describes an object which released source code of another object.	['cert-eu']
released	This relationship describes an object which release another object.	['cert-eu']