MISP Objects

MISP Objects

Introduction . . . 10
- Funding and Support . . . 11

MISP objects . . . 12
- ADS . . . 12
- abuseipdb . . . 14
- ai-chat-prompt . . . 14
- ail-leak . . . 15
- ais . . . 17
- ais-info . . . 19
- android-app . . . 21
- android-permission . . . 21
- annotation . . . 23
- anonymisation . . . 24
- apivoid-email-verification . . . 28
- artifact . . . 30
- asn . . . 33
- attack-pattern . . . 35
- attack-step . . . 36
- attacker-infra . . . 37
- authentication-failure-report . . . 39
- authenticode-signerinfo . . . 40
- av-signature . . . 41
- availability-impact . . . 41
- bank-account . . . 43
- bgp-hijack . . . 46
- bgp-ranking . . . 47
- blog . . . 47
- boleto . . . 49
- btc-transaction . . . 50
- btc-wallet . . . 51
- c2-list . . . 51
- cap-alert . . . 52
- cap-info . . . 55
- cap-resource . . . 58
- cert-pl-phishing . . . 59
- cloth . . . 60

coin-address . . . 61
command . . . 63
command-line . . . 64
concordia-mtmf-intrusion-set . . . 64
confidentiality-impact . . . 65
cookie . . . 67
cortex . . . 68
cortex-taxonomy . . . 69
course-of-action . . . 69
covid19-csse-daily-report . . . 71
covid19-dxy-live-city . . . 73
covid19-dxy-live-province . . . 74
cowrie . . . 74
cpe-asset . . . 76
credential . . . 86
credit-card . . . 87
crowdsec-ip-context . . . 88
crowdstrike-report . . . 90
crypto-material . . . 91
cryptocurrency-transaction . . . 93
cs-beacon-config . . . 95
ctf-challenge . . . 97
cytomic-orion-file . . . 98
cytomic-orion-machine . . . 98
dark-pattern-item . . . 99
ddos . . . 100
ddos-claim . . . 102
ddos-config . . . 103
device . . . 104
diameter-attack . . . 107
diamond-event . . . 108
directory . . . 110
dkim . . . 112
dns-record . . . 112
url . . . 113
domain-crawled . . . 114
domain-ip . . . 114
edr-report . . . 115
elf . . . 116
elf-section . . . 119
email . . . 122

employee . . . 124
error-message . . . 125
event . . . 126
exploit . . . 128
exploit-poc . . . 130
external-impact . . . 130
facebook-account . . . 132
facebook-group . . . 133
facebook-page . . . 134
facebook-post . . . 136
facebook-reaction . . . 138
facial-composite . . . 138
fail2ban . . . 139
favicon . . . 140
file . . . 140
flowintel-cm-case . . . 145
flowintel-cm-task . . . 146
flowintel-cm-task-note . . . 146
forensic-case . . . 147
forensic-evidence . . . 147
forged-document . . . 149
ftm-Airplane . . . 150
ftm-Assessment . . . 152
ftm-Asset . . . 153
ftm-Associate . . . 154
ftm-Audio . . . 155
ftm-BankAccount . . . 157
ftm-Call . . . 158
ftm-Company . . . 159
ftm-Contract . . . 163
ftm-ContractAward . . . 164
ftm-CourtCase . . . 166
ftm-CourtCaseParty . . . 167
ftm-Debt . . . 168
ftm-Directorship . . . 168
ftm-Document . . . 169
ftm-Documentation . . . 171
ftm-EconomicActivity . . . 172
ftm-Email . . . 174
ftm-Event . . . 176
ftm-Family . . . 178

ftm-Folder . . . 178
ftm-HyperText . . . 180
ftm-Image . . . 183
ftm-Land . . . 185
ftm-LegalEntity . . . 186
ftm-License . . . 188
ftm-Membership . . . 190
ftm-Message . . . 191
ftm-Organization . . . 193
ftm-Ownership . . . 195
ftm-Package . . . 196
ftm-Page . . . 198
ftm-Pages . . . 199
ftm-Passport . . . 201
ftm-Payment . . . 202
ftm-Person . . . 203
ftm-PlainText . . . 205
ftm-PublicBody . . . 207
ftm-RealEstate . . . 209
ftm-Representation . . . 211
ftm-Row . . . 212
ftm-Sanction . . . 212
ftm-Succession . . . 213
ftm-Table . . . 214
ftm-TaxRoll . . . 216
ftm-UnknownLink . . . 217
ftm-UserAccount . . . 218
ftm-Vehicle . . . 219
ftm-Vessel . . . 220
ftm-Video . . . 222
ftm-Workbook . . . 224
game-cheat . . . 226
Generalizing Persuasion Framework . . . 228
geolocation . . . 231
git-vuln-finder . . . 233
github-repo . . . 235
github-user . . . 236
gitlab-user . . . 238
google-safe-browsing . . . 238
google-threat-intelligence-report . . . 239
greynoise-ip . . . 239

gtp-attack . . . 240
hashlookup . . . 241
hhhash . . . 243
http-request . . . 244
identity . . . 245
ilr-impact . . . 249
ilr-notification-incident . . . 249
image . . . 252
impersonation . . . 252
imsi-catcher . . . 254
incident . . . 255
infrastructure . . . 258
instagram-account . . . 260
instant-message . . . 261
instant-message-group . . . 263
integrity-impact . . . 265
intel471-vulnerability-intelligence . . . 267
intelmq_event . . . 270
intelmq_report . . . 286
internal-reference . . . 287
interpol-notice . . . 288
intrusion-set . . . 290
iot-device . . . 295
iot-firmware . . . 297
ip-api-address . . . 298
ip-port . . . 299
irc . . . 300
ja3 . . . 301
ja3s . . . 302
ja4-plus . . . 303
jarm . . . 304
keybase-account . . . 304
language-content . . . 305
leaked-document . . . 307
legal-entity . . . 308
lnk . . . 309
macho . . . 312
macho-section . . . 313
mactime-timeline-analysis . . . 314
malware . . . 314
malware-analysis . . . 318

malware-config . . . 320
meme-image . . . 321
microblog . . . 323
monetary-impact . . . 325
mutex . . . 327
narrative . . . 328
netflow . . . 329
network-connection . . . 330
network-profile . . . 332
network-socket . . . 335
network-traffic . . . 340
news-agency . . . 342
news-media . . . 343
open-data-security . . . 345
opentide . . . 347
organization . . . 348
original-imported-file . . . 351
paloalto-threat-event . . . 351
parler-account . . . 352
parler-comment . . . 354
parler-post . . . 355
passive-dns . . . 357
passive-dns-dnsdbflex . . . 360
passive-ssh . . . 360
paste . . . 361
pcap-metadata . . . 363
pe . . . 365
pe-optional-header . . . 368
pe-section . . . 373
Deception PersNOna . . . 375
person . . . 376
personification . . . 381
pgp-meta . . . 384
phishing . . . 385
phishing-kit . . . 386
phone . . . 387
phone-number . . . 390
physical-impact . . . 391
postal-address . . . 393
probabilistic-data-structure . . . 394
process . . . 395

publication . . . 397
python-etvx-event-log . . . 399
query . . . 402
r2graphity . . . 402
ransom-negotiation . . . 404
ransomware-group-post . . . 406
reddit-account . . . 408
reddit-comment . . . 409
reddit-post . . . 411
reddit-subreddit . . . 413
regexp . . . 415
registry-key . . . 416
registry-key-value . . . 418
regripper-NTUser . . . 419
regripper-sam-hive-single-user . . . 421
regripper-sam-hive-user-group . . . 422
regripper-software-hive-BHO . . . 423
regripper-software-hive-appInit-DLLS . . . 423
regripper-software-hive-application-paths . . . 424
regripper-software-hive-applications-installed . . . 425
regripper-software-hive-command-shell . . . 426
regripper-software-hive-software-run . . . 426
regripper-software-hive-userprofile-winlogon . . . 427
regripper-software-hive-windows-general-info . . . 430
regripper-system-hive-firewall-configuration . . . 432
regripper-system-hive-general-configuration . . . 432
regripper-system-hive-network-information . . . 434
regripper-system-hive-services-drivers . . . 435
report . . . 437
research-scanner . . . 438
risk-assessment-report . . . 439
rmm . . . 440
rogue-dns . . . 441
rtir . . . 442
sandbox-report . . . 443
sb-signature . . . 444
scan-result . . . 445
scheduled-event . . . 447
scheduled-task . . . 449
scrippsco2-c13-daily . . . 450
scrippsco2-c13-monthly . . . 451

scrippsco2-co2-daily . . . 452
scrippsco2-co2-monthly . . . 453
scrippsco2-o18-daily . . . 454
scrippsco2-o18-monthly . . . 455
script . . . 457
security-playbook . . . 458
shadowserver-malware-url-report . . . 463
shadowserver-scan-http-proxy . . . 465
shell-commands . . . 468
shodan-report . . . 469
short-message-service . . . 469
shortened-link . . . 470
sigma . . . 471
sigmf-archive . . . 471
sigmf-expanded-recording . . . 472
sigmf-recording . . . 475
social-media-group . . . 475
software . . . 477
spambee-report . . . 478
spearphishing-attachment . . . 479
spearphishing-link . . . 481
splunk . . . 482
ss7-attack . . . 482
ssh-authorized-keys . . . 489
stairwell . . . 490
stix2-pattern . . . 491
stock . . . 492
submarine . . . 496
summariser-output . . . 498
suricata . . . 499
target-system . . . 500
task . . . 500
tattoo . . . 502
telegram-account . . . 504
telegram-bot . . . 504
temporal-event . . . 505
thaicert-group-cards . . . 506
threatgrid-report . . . 507
timecode . . . 507
timesketch-timeline . . . 508
timesketch_message . . . 509

timestamp . . . 509
tor-hiddenservice . . . 510
tor-node . . . 511
traceability-impact . . . 512
tracking-id . . . 513
transaction . . . 514
translation . . . 516
transport-ticket . . . 521
trustar_report . . . 522
tsk-chats . . . 526
tsk-web-bookmark . . . 527
tsk-web-cookie . . . 528
tsk-web-downloads . . . 528
tsk-web-history . . . 529
tsk-web-search-query . . . 530
twitter-account . . . 531
twitter-list . . . 533
twitter-post . . . 534
typosquatting-finder . . . 536
typosquatting-finder-result . . . 537
url . . . 538
user-account . . . 539
user-action . . . 541
vehicle . . . 542
victim . . . 543
virustotal-graph . . . 546
virustotal-report . . . 546
virustotal-submission . . . 547
vulnerability . . . 547
weakness . . . 549
whois . . . 550
windows-service . . . 551
x-header . . . 553
x509 . . . 553
yabin . . . 555
yara . . . 556
youtube-channel . . . 557
youtube-comment . . . 558
youtube-playlist . . . 559
youtube-video . . . 560
Relationships . . . 561

Introduction

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.lu
Computer Incident
Response Center
LUXEMBOURG

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**.

Co-financed by the European Union
Connecting Europe Facility

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

MISP objects

ADS

An object defining ADS - Alerting and Detection Strategy by PALANTIR. Can be used for detection engineering.

ADS 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	Multiple
acd-element	text	lists the steps required to generate a representative true positive event which triggers this alert.	—	—
additional_resources	url	Any other internal, external, or technical references that may be useful for understanding the ADS.	—	✔
blind_spots_and_assumptions	text	Recognized issues, assumptions, and areas where an ADS may not fire.	—	—
categorization	text	Provides a mapping of the ADS to the relevant entry in the Att&CK.	—	✔
categorization_others	text	Provides a mapping of the ADS to the relevant entry in the Att&CK if 'categorization is not sufficient'.	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
date	datetime	Enter date, when ADS has been created or edited.	—	—
false_positives	text	Known instances of an ADS misfiring due to a misconfiguration, idiosyncrasy in the environment, or other non-malicious scenario.	—	—
goal	text	Short, plaintext description of the type of behavior the ADS is supposed to detect.	—	—
priority	text	Describes the various alerting levels that an ADS may be tagged with.	—	—
responses	text	General response steps in the event that this alert fired.	—	—
sigma_rule	sigma	Rule in SIGMA format.	—	—
strategy_abstract	text	High-level walkthrough of how the ADS functions.	—	—
technical_context	text	Detailed information and background needed for a responder to understand all components of the alert.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
validation	text	lists the steps required to generate a representative true positive event which triggers this alert.	—	—

abuseipdb

AbuseIPDB checks an ip address, domain name, or subnet against a central blacklist.

abuseipdb 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	Multiple
abuse-confidence-score	integer	Rating (0-100) of how confident AbuseIPDB is that an IP address is entirely malicious	—	—
is-malicious	boolean	If the IP is malicious based on the abuse-confidence-score and threshold	—	—
is-public	boolean	If an IP is public	—	—
is-tor	boolean	If Tor (The Onion Router) was used	—	—
is-whitelisted	boolean	If an IP is spotted in any of AbuseIPDB's whitelists	—	—

ai-chat-prompt

Object describing an AI prompt such as ChatGPT.

ai-chat-prompt 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	Multiple
act-as	text	Act as a specific person. ['Security Analysts', 'Incident Responder', 'IT Expert', 'Cyber Security Specialists', 'Technical Writer']	—	—
comment	text	Comment associated to the AI chat prompt.	—	—
model	text	AI chatbot model used for the prompt. ['GPT 3.5', 'GPT 4.0', 'GPT 3.0', 'DALL-E', 'Whisper', 'Embeddings', 'Moderation', 'Codex', 'BioGPT', 'LLaMA', 'GPT4ALL', 'Bing AI', 'Google Bard AI']	✔	✔
prompt	text	Prompt text used for a specific AI chat.	✔	✔
result	text	Result ['Unknown', 'Harmless', 'Correct', 'Dangerous', 'Incorrect']	✔	✔
role	text	Role as defined in OpenAI or similar API. ['system', 'user', 'assistant']	—	—

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	Multiple
duplicate	text	Duplicate of the existing leaks.	–	✔
duplicate_number	counter	Number of known duplicates.	✔	–
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.	✔	–
origin	text	The link where the leak is (or was) accessible at first-seen.	–	–
original-date	datetime	When the information available in the leak was created. It's usually before the first-seen.	✔	–
raw-data	attachment	Raw data as received by the AIL sensor compressed and encoded in Base64.	✔	–
sensor	text	The AIL sensor uuid where the leak was processed and analysed.	✔	–

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
text	text	A description of the leak which could include the potential victim(s) or description of the leak.	✔	—

ais

Automatic Identification System (AIS) is an automatic tracking system that uses transceivers on ships.

ais 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	Multiple
ETA	datetime	Estimated time of arrival at destination	✔	—
IMO-number	text	IMO ship identification number: a seven digit number that remains unchanged upon transfer of the ship's registration to another country	—	—
MMSI	text	Vessel Maritime Maritime Mobile Service Identity (MMSI): a unique nine digit identification number.	—	—
call-sign	text	International radio call-sign, up to 7 characters.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
course-over-ground	float	The course of the vessel, relative to true north to 0.1 degree	✔	—
destination	text	Destination of the vessel in max 20 characters	✔	—
dimension-a	float	Distance in meters from Forward Perpendicular (FP)	—	—
dimension-b	float	Distance in meters from After Perpendicular (AP)	—	—
dimension-c	float	Distance in meters inboard from port side	—	—
dimension-d	float	Distance in meters inboard from starboard side	—	—
draught	float	Draught of ship. 0.1-25.5 meters	—	—
first-seen	datetime	When the location was seen for the first time.	✔	—
last-seen	datetime	When the location was seen for the last time.	✔	—
latitude	float	The latitude is the decimal value of the latitude in the World Geodetic System 84 (WGS84) reference.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
longitude	float	The longitude is the decimal value of the longitude in the World Geodetic System 84 (WGS84) reference	✔	—
name	text	20 characters to represent the name of the vessel	—	—
navigational-status	float	1. at anchor, 2. under command, 3. Restricted Manoeuvrability, etc.	✔	—
rate-of-turn	text	right or left, from 0 to 720 degrees per minute	✔	—
speed-over-ground	float	0.1 knot resolution from 0 to 102 knots	✔	—
true-heading	float	The true heading of the vessel. 0 to 359 degrees	✔	—
true-heading-at-own-position	float	The true heading at own position of the vessel. 0 to 359 degrees	✔	—
type-of-ship	text	Type of ship/cargo	✔	—

ais-info

Automated Indicator Sharing (AIS) Information Source Markings.

ais-info 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	Multiple
administrative-area	text	AIS Administrative Area represented using ISO-3166-2.	➖	➖
country	text	AIS Country represented using ISO-3166-1_alpha-2.	➖	➖
industry	text	AIS IndustryType. ['Chemical Sector', 'Commercial Facilities Sector', 'Communications Sector', 'Critical Manufacturing Sector', 'Dams Sector', 'Defense Industrial Base Sector', 'Emergency Services Sector', 'Energy Sector', 'Financial Services Sector', 'Food and Agriculture Sector', 'Government Facilities Sector', 'Healthcare and Public Health Sector', 'Information Technology Sector', 'Nuclear Reactors, Materials, and Waste Sector', 'Transportation Systems Sector', 'Water and Wastewater Systems Sector', 'Other']	➖	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
organisation	text	AIS Organisation Name.	—	—

android-app

Indicators related to an Android app.

android-app 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	Multiple
appid	text	Application ID	—	✔
certificate	sha1	Android certificate (SHA1)	—	✔
certificate-sha256	sha256	Android certificate (SHA256)	—	✔
domain	domain	Domain used by the app	—	✔
name	text	Generic name of the application	—	—
sha256	sha256	SHA256 of the APK.	—	✔

android-permission

A set of android permissions - one or more permission(s) which can be linked to other objects (e.g. malware, app).

android-permission 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	Multiple
comment	comment	Comment about the set of android permission(s)	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
permission	text	Android permission ['ACCESS_CHECKIN_PROPERTIES', 'ACCESS_COARSE_LOCATION', 'ACCESS_FINE_LOCATION', 'ACCESS_LOCATION_EXTRA_COMMANDS', 'ACCESS_NETWORK_STATE', 'ACCESS_NOTIFICATION_POLICY', 'ACCESS_WIFI_STATE', 'ACCOUNT_MANAGER', 'ADD_VOICEMAIL', 'ANSWER_PHONE_CALLS', 'BATTERY_STATS', 'BIND_ACCESSIBILITY_SERVICE', 'BIND_APPWIDGET', 'BIND_AUTOFILL_SERVICE', 'BIND_CARRIER_MESSAGING_SERVICE', 'BIND_CHOOSER_TARGET_SERVICE', 'BIND_CONDITION_PROVIDER_SERVICE', 'BIND_DEVICE_ADMIN', 'BIND_DREAM_SERVICE', 'BIND_INCALL_SERVICE', 'BIND_INPUT_METHOD', 'BIND_MIDI_DEVICE_SERVICE',	━	✔

annotation

An annotation object allowing analysts to add annotations, comments, executive summary to a MISP event, objects or attributes.

annotation 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	Multiple
attachment	attachment	An attachment to support the annotation	—	✔
creation-date	datetime	Initial creation of the annotation	—	—
format	text	Format of the annotation ['text', 'markdown', 'asciidoctor', 'MultiMarkdown', 'GFM', 'pandoc', 'Fountain', 'CommonWork', 'kramdown-rfc2629', 'rfc7328', 'Extra']	✔	—
modification-date	datetime	Last update of the annotation	—	—
ref	link	Reference(s) to the annotation	—	✔
text	text	Raw text of the annotation	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
type	text	Type of the annotation ['Annotation', 'Executive Summary', 'Introduction', 'Conclusion', 'Disclaimer', 'Keywords', 'Acknowledgement', 'Other', 'Copyright', 'Authors', 'Logo', 'Full Report']	✔	—

anonymisation

Anonymisation object describing an anonymisation technique used to encode MISP attribute values. Reference: https://www.caida.org/tools/taxonomy/anonymization.xml.

anonymisation 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	Multiple
description	text	Description of the anonymisation technique or tool used	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
encryption-function	text	Encryption function or algorithm used to anonymise the attribute ['aes128', 'aes-128-cbc', 'aes-128-cfb', 'aes-128-cfb1', 'aes-128-cfb8', 'aes-128-ctr', 'aes-128-ecb', 'aes-128-ofb', 'aes192', 'aes-192-cbc', 'aes-192-cfb', 'aes-192-cfb1', 'aes-192-cfb8', 'aes-192-ctr', 'aes-192-ecb', 'aes-192-ofb', 'aes-256-cfb', 'aes-256-cfb1', 'aes-256-cfb8', 'aes-256-ctr', 'aes-256-ecb', 'aes-256-ofb', 'bf', 'bf-cbc', 'bf-cfb', 'bf-ecb', 'bf-ofb', 'blowfish', 'camellia128', 'camellia-128-cbc', 'camellia-128-cfb', 'camellia-128-cfb1', 'camellia-128-cfb8', 'camellia-128-ctr', 'camellia-128-ecb', 'camellia-128-ofb', 'camellia192', 'camellia-192-cbc', 'camellia-192-cfb', 'camellia-192-cfb1', 'camellia-192-cfb8', 'camellia-192-ctr', 'camellia-192-ecb', 'camellia-192-ofb', 'camellia256', 'camellia-256-cbc', 'camellia-256-cfb', 'camellia-256-cfb1', 'camellia-	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
iv	text	Initialisation vector for the encryption function used to anonymise the attribute	✔	—
key	text	Key (such as a PSK in a keyed-hash-function) used to anonymise the attribute	✔	—
keyed-hash-function	text	Keyed-hash function used to anonymise the attribute ['hmac-sha1', 'hmac-md5', 'hmac-sha256', 'hmac-sha384', 'hmac-sha512']	✔	—
level-of-knowledge	text	Level of knowledge of the organisation who created this object ['Only the anonymised data is known', 'Deanonymised data is known']	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
method	text	Anonymisation (or pseudo-anonymisation) method(s) used ["hiding - Attribute is replaced with a constant value (typically 0) of the same size. Sometimes called 'black marker'.", 'hash - A hash function maps each attribute to a new (not necessarily unique) attribute.', 'permutation - Maps each original value to a unique new value.', "prefix-preserving - Any two values that had the same n-bit prefix before anonymisation will still have the same n-bit prefix as each other after anonymization. (Would be more accurately called 'prefix-relationship-preserving', because the actual prefix values are not preserved.) ", 'shift - Adds a fixed offset to each value/attribute.', 'enumeration - Map each original value to a new	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
regexp	text	Regular expression to perfom the anonymisation (reversible or not)	✔	—

apivoid-email-verification

Apivoid email verification API result. Reference: https://www.apivoid.com/api/email-verify/.

apivoid-email-verification 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	Multiple
china_free_email	boolean	True if email is a free China email, i.e 163.com.	✔	—
comment	text	Field for comments or correlating text	✔	—
dirty_words_domain	boolean	True if domain contains dirty/bad words.	✔	—
dirty_words_username	boolean	True if username contains dirty/bad words.	✔	—
disposable	boolean	True if email is disposable, i.e yopmail.com.	✔	—
dmarc_configured	boolean	True if domain has DMARC records configured.	✔	—
dmarc_enforced	boolean	True if domain is configured for DMARC and set to an enforcement policy.	✔	—
domain	domain	Email domain.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
domain_popular	boolean	True if domain is a known popular domain.	✔	—
educational_domain	boolean	True if domain is an educational domain, i.e .edu	✔	—
email	email	The email address that was queried.	—	—
free_email	boolean	True if email is a free email, i.e gmail.com.	✔	—
government_domain	boolean	True if domain is a government domain, i.e .gov	✔	—
has_a_records	boolean	True if domain has A records configured.	✔	—
has_mx_records	boolean	True if domain has MX records configured.	✔	—
has_spf_records	boolean	True if domain has SPF records configured.	✔	—
is_spoofable	boolean	True if domain does not have SPF records or if ~all is not configured.	✔	—
police_domain	boolean	True if domain is a police domain (such as **polizei**, **police**, etc).	✔	—
risky_tld	boolean	True if domain TLD is risky, i.e .top or .pro.	✔	—
role_address	boolean	True if email is a role address, i.e admin@website.com	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
russian_free_email	boolean	True if email is a free Russian email, i.e mail.ru.	✔	—
score	float	A number between 0 (bad) and 100 (good).	✔	—
should_block	boolean	True if the score is bad (⇐ 70) and thus it should be blocked.	✔	—
suspicious_domain	boolean	True if domain is suspicious, i.e known spam or parked.	✔	—
suspicious_email	boolean	True if email is considered suspicious.	✔	—
suspicious_username	boolean	True if username is suspicious, i.e only numbers.	✔	—
username	text	Username part of the email address (email prefix)	✔	—
valid_format	boolean	True if email has a valid format.	✔	—
valid_tld	boolean	True if domain TLD is valid, i.e .com or .co.uk	✔	—

artifact

The Artifact object permits capturing an array of bytes (8-bits), as a base64-encoded string, or linking to a file-like payload. From STIX 2.1 (6.1).

artifact 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	Multiple
decryption_key	text	Specifies the decryption key for the encrypted binary data (either via payload_bin or url). For example, this may be useful in cases of sharing malware samples, which are often encoded in an encrypted archive.	–	–
encryption_algorithm	text	If the artifact is encrypted, specifies the type of encryption algorithm the binary data (either via payload_bin or url) is encoded in.	–	–
md5	md5	[Insecure] MD5 hash (128 bits)	–	–

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
mime_type	mime-type	Whenever feasible, this value SHOULD be one of the values defined in the Template column in the IANA media type registry [Media Types]. Maintaining a comprehensive universal catalog of all extant file types is obviously not possible. When specifying a MIME Type not included in the IANA registry, implementers should use their best judgement so as to facilitate interoperability.	✔	—
payload_bin	attachment	Specifies the binary data contained in the artifact as a base64-encoded string.	—	—
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	—	—
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	—	—
sha3-256	sha3-256	Secure Hash Algorithm 3 (256 bits)	—	—
sha3-512	sha3-512	Secure Hash Algorithm 3 (512 bits)	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	—	—
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	—	—
tlsh	tlsh	Fuzzy hash by Trend Micro: Locality Sensitive Hash	—	—
url	url	The value of this property MUST be a valid URL that resolves to the unencoded content. When present, at least one hash value MUST be present too.	—	—

asn

Autonomous system object describing an autonomous system which can include one or more network operators managing 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	Multiple
asn	AS	Autonomous System Number	—	—
country	text	Country code of the main location of the autonomous system	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
description	text	Description of the autonomous system	–	–
export	text	The outbound routing policy of the AS in RFC 2622 – Routing Policy Specification Language (RPSL) format	–	✔
first-seen	datetime	First time the ASN was seen	✔	–
import	text	The inbound IPv4 routing policy of the AS in RFC 2622 – Routing Policy Specification Language (RPSL) format	–	✔
last-seen	datetime	Last time the ASN was seen	✔	–
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	–	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
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	➖	✔
subnet-announced	ip-src	Subnet announced	➖	✔

attack-pattern

Attack pattern describing a common attack pattern enumeration and classification.

attack-pattern 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	Multiple
id	text	CAPEC ID.	✔	➖
name	text	Name of the attack pattern.	➖	➖
prerequisites	text	Prerequisites for the attack pattern to succeed.	➖	➖
references	link	External references	➖	✔
related-weakness	weakness	Weakness related to the attack pattern.	➖	✔
solutions	text	Solutions for the attack pattern to be countered.	➖	➖
summary	text	Summary description of the attack pattern.	➖	➖

attack-step

An object defining a singular attack-step. Especially useful for red/purple teaming, but can also be used for actual attacks.

attack-step 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	Multiple
command-line	text	Command line used to execute attack step, if any.	—	✔
description	text	Description of the attack step	—	—
detections	text	Detections by the victim's monitoring capabilities.	—	—
dst-domain	domain	Domain destination of the attack step, if any.	✔	—
dst-ip	ip-dst	IP destination of the attack step, if any.	✔	✔
dst-misc	text	Other type of destination of the attack step, if any. This can be e.g. localhost.	—	✔
expected-response	text	Response or detection expected (in case of purple teaming)	—	—
key-step	boolean	Was this attack step object a key step within the context of the incident/event? ['True', 'False']	—	—
source-domain	domain	Domain source of the attack step, if any.	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
source-ip	ip-src	IP source of the attack step, if any.	—	✔
source-misc	text	Other type of source of the attack step, if any. This can be e.g. rotating ip from cloud providers such as AWS, or localhost.	—	✔
succesful	boolean	Was this attack step succesful? ['True', 'False']	—	—

attacker-infra

Attacker Infrastructure.

> attacker-infra 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	Multiple
architecture	text	The CPU architecture of the beacon. Either x86 or x64	✔	✔
asn	AS	ASN where the IP resides	—	—
beacon_host	text	C2 of the beacon IP/hostname. (often matches the host that was scanned)	✔	✔
beacon_http_get	text	Path that the beacon uses for the GET method	✔	✔
beacon_http_post	text	Path that the beacon uses for the POST method	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
beacon_type	text	Protocol that the beacon speaks. Usually HTTP	✔	✔
binary_md5	md5	MD5 of the PE binary	✔	✔
binary_sha1	sha1	SHA1 of the PE binary	✔	✔
binary_sha256	sha256	SHA256 of the PE binary	✔	✔
city	text	City location of the IP in question	✔	—
config_md5	md5	MD5 of the config file	✔	✔
config_sha1	sha1	SHA1 of the config file	✔	✔
config_sha256	sha256	SHA256 of the config file	✔	✔
content_length	text	The length of the response body in octets	✔	✔
content_type	text	The MIME type of the body of the request	✔	✔
encoded_data	text	Base64 encoded config file	✔	✔
encoded_length	text	Length of the base64 decoded raw config	✔	✔
geo	text	Country location of the IP	✔	—
hostname	text	Reverse DNS name of the device in question	—	—
hostname_source	text	Source of the hostname field contents	✔	✔
http	text	HTTP version in used in response, e.g HTTP/1.1	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
http_code	text	HTTP Response code: e.g., 200, 401, 404	✔	✔
http_url	text	URL used to illicit the server response	✔	✔
ip	ip-src	IP of the of the URL	—	✔
license_id	text	The license number	✔	✔
naics	text	North American Industry Classification System Code	✔	✔
port	text	Port that the response came from	✔	—
protocol	text	Protocol the response came in on	✔	—
region	text	State / Province / Administrative region where the device in question resides	✔	—
sector	text	Sector of the device in question	✔	✔
severity	text	Severity of the event	✔	—
tag	text	Attribute tags	—	✔
timestamp	datetime	Time that the IP was probed in UTC+0	✔	—

authentication-failure-report

Authentication Failure Report.

authentication-failure-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	Multiple
ip-dst	ip-dst	Destination IP.	—	—
ip-src	ip-src	IP address originating the authentication failure.	—	—
total	counter	the number of authentication failures reported.	✔	—
type	text	the type of authentication failure. ['ssh']	✔	—
username	text	the username used.	✔	—

authenticode-signerinfo

Authenticode Signer Info.

authenticode-signerinfo 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	Multiple
content-type	text	Content type	—	—
digest-base64	text	Signature created by the signing certificate's private key	✔	—
digest_algorithm	text	Algorithm used to hash the file.	✔	—
encryption_algorithm	text	Algorithm used to encrypt the digest	✔	—
issuer	text	Issuer of the certificate	✔	—
program-name	text	Program name	—	—
serial-number	text	Serial number of the certificate	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
signature_algorithm	text	Signature algorithm ['SHA1_WITH_RSA_ENCRYPTION', 'SHA256_WITH_RSA_ENCRYPTION']	✔	—
text	text	Free text description of the signer info	—	—
url	url	Url	—	✔
version	text	Version of the certificate	✔	—

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	Multiple
datetime	datetime	Datetime	✔	—
signature	text	Name of detection signature	—	—
software	text	Name of antivirus software	✔	—
text	text	Free text value to attach to the file	✔	—

availability-impact

Availability Impact object as described in STIX 2.1 Incident object extension.

> availability-impact 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	Multiple
availability_impact	text	The availability impact. ['Not Specified', 'None', 'Minimal', 'Significant', 'Denial', 'Loss of Control']	✔	—
criticality	text	Criticality of the impact ['Not Specified', 'False Positive', 'Low', 'Moderate', 'High', 'Extreme']	✔	—
description	text	Additional details about the impact.	—	—
end_time	datetime	The date and time the impact was last recorded.	—	—
end_time_fidelity	text	Level of fidelity that the `end_time` is recorded in. ['day', 'hour', 'minute', 'month', 'second', 'year']	✔	—
recoverability	text	Recoverability of this particular impact with respect to feasibility and required time and resources. ['extended', 'not-applicable', 'not-recoverable', 'regular', 'supplemented']	✔	—
start_time	datetime	The date and time the impact was first recorded.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
start_time_fidelity	text	Level of fidelity that the `start_time` is recorded in. ['day', 'hour', 'minute', 'month', 'second', 'year']	✔	—

bank-account

An object describing bank account information based on account description from goAML 4.0.

> bank-account 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	Multiple
aba-rtn	aba-rtn	ABA routing transit number	—	—
account	bank-account-nr	Account number	—	—
account-name	text	A field to freely describe the bank account details.	—	—
balance	text	The balance of the account after the suspicious transaction was processed.	✔	—
beneficiary	text	Final beneficiary of the bank account.	✔	—
beneficiary-comment	text	Comment about the final beneficiary.	✔	—
branch	text	Branch code or name	✔	—
client-number	text	Client number as seen by the bank.	—	—
closed	datetime	When the account was closed.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
comments	text	Comments about the bank account.	✔	—
currency-code	text	Currency of the account. ['USD', 'EUR']	✔	—
date-balance	datetime	When the balance was reported.	✔	—
iban	iban	IBAN of the bank account.	—	—
institution-code	text	Institution code of the bank.	✔	—
institution-name	text	Name of the bank or financial organisation.	✔	—
non-banking-institution	boolean	A flag to define if this account belong to a non-banking organisation. If set to true, it's a non-banking organisation. ['True', 'False']	✔	—
opened	datetime	When the account was opened.	✔	—
personal-account-type	text	Account type. ['A - Business', 'B - Personal Current', 'C - Savings', 'D - Trust Account', 'E - Trading Account', 'O - Other']	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
report-code	text	Report code of the bank account. ['CTR Cash Transaction Report', 'STR Suspicious Transaction Report', 'EFT Electronic Funds Transfer', 'IFT International Funds Transfer', 'TFR Terror Financing Report', 'BCR Border Cash Report', 'UTR Unusual Transaction Report', 'AIF Additional Information File – Can be used for example to get full disclosure of transactions of an account for a period of time without reporting it as a CTR.', 'IRI Incoming Request for Information – International', 'ORI Outgoing Request for Information – International', 'IRD Incoming Request for Information – Domestic', 'ORD Outgoing Request for Information – Domestic']	✔	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
status-code	text	Account status at the time of the transaction processed. ['A - Active', 'B - Inactive', 'C - Dormant']	✔	—
swift	bic	SWIFT or BIC as defined in ISO 9362.	✔	—
text	text	A description of the bank account.	✔	—

bgp-hijack

Object encapsulating BGP Hijack description as specified, for example, by bgpstream.com.

bgp-hijack 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	Multiple
country	text	Country code of the main location of the attacking autonomous system	—	—
description	text	BGP Hijack details	—	—
detected-asn	AS	Detected Autonomous System Number	—	—
end	datetime	Last time the Prefix hijack was seen	✔	—
expected-asn	AS	Expected Autonomous System Number	—	—
start	datetime	First time the Prefix hijack was seen	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
subnet-announced	ip-src	Subnet announced	➖	✔

bgp-ranking

BGP Ranking object describing the ranking of an ASN for a given day, along with its position, 1 being the most malicious ASN of the day, with the highest ranking. This object is meant to have a relationship with the corresponding ASN object and represents its ranking for a specific date.

bgp-ranking 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	Multiple
address-family	text	The IP address family concerned by the ranking. ['v4', 'v6']	✔	➖
date	datetime	Date fo the ranking.	✔	➖
position	float	Position of the ASN for a given day.	✔	➖
ranking	float	Ranking of the Autonomous System number.	✔	➖

blog

Blog post like Medium or WordPress.

blog 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	Multiple
archive	link	Archive of the original document (Internet Archive, Archive.is, etc).	➖	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
creation-date	datetime	Initial creation of the blog post.	➖	➖
embedded-link	url	Site linked by the blog post.	➖	✔
embedded-safe-link	link	Safe site linked by the blog post.	➖	✔
link	link	Original link into the blog post (Supposed harmless).	➖	➖
modification-date	datetime	Last update of the blog post.	➖	➖
post	text	Raw post.	➖	➖
removal-date	datetime	When the blog post was removed.	➖	➖
title	text	Title of blog post.	➖	➖
type	text	Type of blog post. ['Medium', 'WordPress', 'Blogger', 'Tumbler', 'LiveJournal', 'Forum', 'Other']	✔	➖
url	url	Original URL location of the blog post (potentially malicious).	➖	➖
username	text	Username who posted the blog post.	➖	➖
username-quoted	text	Username who are quoted into the blog post.	➖	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
verified-username	text	Is the username account verified by the operator of the blog platform. ['Verified', 'Unverified', 'Unknown']	✔	—

boleto

A common form of payment used in Brazil.

boleto 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	Multiple
beneficiary	text	Final beneficiary of the boleto.	—	—
beneficiary-bank-account	bank-account-nr	Recipient bank account number	—	—
beneficiary-bank-agency	bank-account-nr	Recipient bank agency number	—	—
boleto-number	text	Boleto code numbers	—	—
creation-date	datetime	Date the boleto was created	✔	—
febraban-code	text	Financial institution code in Brazil that created the boleto.	✔	—
generator-financial-institution	text	Name of the bank or financial organisation that created the boleto.	✔	—
payment-due-date	datetime	Boleto payment date	✔	—
payment-status	text	Inform if boleto was as paid or not ['Not Paid', 'Paid']	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
payment-value	float	The payment boleto value in Brazilian Reais	✔	—
requester	text	Organisation, service or affiliated person that requested creation of the boleto.	—	—

btc-transaction

An object to describe a Bitcoin transaction. Best to be used with bitcoin-wallet.

btc-transaction 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	Multiple
btc-address	btc	A Bitcoin transactional address	✔	—
time	datetime	Date and time of transaction	✔	—
transaction-number	text	A Bitcoin transaction number in a sequence of transactions	✔	✔
value_BTC	float	Value in BTC at date/time displayed in field 'time'	✔	—
value_EUR	float	Value in EUR with conversion rate as of date/time displayed in field 'time'	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
value_USD	float	Value in USD with conversion rate as of date/time displayed in field 'time'	✔	—

btc-wallet

An object to describe a Bitcoin wallet. Best to be used with btc-transaction object.

btc-wallet 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	Multiple
BTC_received	float	Value of received BTC	✔	—
BTC_sent	float	Value of sent BTC	✔	—
balance_BTC	float	Value in BTC at date/time displayed in field 'time'	✔	—
time	datetime	Date and time of lookup/conversion	✔	—
wallet-address	btc	A Bitcoin wallet address	—	—

c2-list

List of C2-servers with common ground, e.g. extracted from a blog post or ransomware analysis.

c2-list 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	Multiple
c2-ip	ip-src	IP of C2 server with unknown port	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
c2-ipport	ip-src	port	IP:Port of C2 server	➖
✔	report-url	link	URL of source of information, e.g. blog post, ransomware analysis	✔
✔	threat	text	threat actor or malware	➖

cap-alert

Common Alerting Protocol Version (CAP) alert object.

cap-alert 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	Multiple
addresses	text	The group listing of intended recipients of the alert message. (1) Required when <scope> is “Private”, optional when <scope> is “Public” or “Restricted”. (2) Each recipient SHALL be identified by an identifier or an address. (3) Multiple space-delimited addresses MAY be included. Addresses including whitespace MUST be enclosed in double-quotes.	✔	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
code	text	The code denoting the special handling of the alert message.	✔	—
identifier	text	The identifier of the alert message in a number or string uniquely identifying this message, assigned by the sender.	✔	—
incident	text	The group listing naming the referent incident(s) of the alert message. (1) Used to collate multiple messages referring to different aspects of the same incident. (2) If multiple incident identifiers are referenced, they SHALL be separated by whitespace. Incident names including whitespace SHALL be surrounded by double-quotes.	✔	—
msgType	text	The code denoting the nature of the alert message. ['Alert', 'Update', 'Cancel', 'Ack', 'Error']	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
note	text	The text describing the purpose or significance of the alert message.	✔	—
references	text	The group listing identifying earlier message(s) referenced by the alert message. (1) The extended message identifier(s) (in the form sender,identifier,sent) of an earlier CAP message or messages referenced by this one. (2) If multiple messages are referenced, they SHALL be separated by whitespace.	✔	—
restriction	text	The text describing the rule for limiting distribution of the restricted alert message.	✔	—
scope	text	The code denoting the intended distribution of the alert message. ['Public', 'Restricted', 'Private']	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
sender	text	The identifier of the sender of the alert message which identifies the originator of this alert. Guaranteed by assigner to be unique globally; e.g., may be based on an Internet domain name.	✔	—
sent	datetime	The time and date of the origination of the alert message.	✔	—
source	text	The text identifying the source of the alert message. The particular source of this alert; e.g., an operator or a specific device.	✔	—
status	text	The code denoting the appropriate handling of the alert message. ['Actual', 'Exercise', 'System', 'Test', 'Draft']	—	—

cap-info

Common Alerting Protocol Version (CAP) info object.

cap-info 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	Multiple
audience	text	The text describing the intended audience of the alert message.	✔	—
category	text	The code denoting the category of the subject event of the alert message. ['Geo', 'Met', 'Safety', 'Security', 'Rescue', 'Fire', 'Health', 'Env', 'Transport', 'Infra', 'CBRNE', 'Other']	✔	—
certainty	text	The code denoting the certainty of the subject event of the alert message. For backward compatibility with CAP 1.0, the deprecated value of “Very Likely” SHOULD be treated as equivalent to “Likely”. ['Likely', 'Possible', 'Unlikely', 'Unknown']	✔	—
contact	text	The text describing the contact for follow-up and confirmation of the alert message.	✔	—
description	text	The text describing the subject event of the alert message.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
effective	datetime	The effective time of the information of the alert message.	✔	—
event	text	The text denoting the type of the subject event of the alert message.	✔	—
eventCode	text	A system-specific code identifying the event type of the alert message.	✔	—
expires	datetime	The expiry time of the information of the alert message.	✔	—
headline	text	The text headline of the alert message.	✔	—
instruction	text	The text describing the recommended action to be taken by recipients of the alert message.	✔	—
language	text	The code denoting the language of the info sub-element of the alert message.	✔	—
onset	datetime	The expected time of the beginning of the subject event of the alert message.	✔	—
parameter	text	A system-specific additional parameter associated with the alert message.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
responseType	text	The code denoting the type of action recommended for the target audience. ['Shelter', 'Evacuate', 'Prepare', 'Execute', 'Avoid', 'Monitor', 'Assess', 'AllClear', 'None']	✔	—
senderName	text	The text naming the originator of the alert message.	✔	—
severity	text	The code denoting the severity of the subject event of the alert message. ['Extreme', 'Severe', 'Moderate', 'Minor', 'Unknown']	✔	—
urgency	text	The code denoting the urgency of the subject event of the alert message. ['Immediate', 'Expected', 'Future', 'Past', 'Unknown']	✔	—
web	link	The identifier of the hyperlink associating additional information with the alert message.	✔	—

cap-resource

Common Alerting Protocol Version (CAP) resource object.

cap-resource 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	Multiple
derefUri	attachment	The base-64 encoded data content of the resource file.	✔	—
digest	sha1	The code representing the digital digest (“hash”) computed from the resource file (OPTIONAL).	—	—
mimeType	mime-type	The identifier of the MIME content type and sub-type describing the resource file.	✔	—
resourceDesc	text	The text describing the type and content of the resource file.	✔	—
size	text	The integer indicating the size of the resource file.	✔	—
uri	link	The identifier of the hyperlink for the resource file.	—	—

cert-pl-phishing

cert.pl phishing object template representing an url along with some metadata as such phash, html-structure or partial-hash.

cert-pl-phishing 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	Multiple
favicon-mmh3	text	Favicon of the phishing url in Murmurhash3 format (base64).	—	—
html-structure	text	HTML tags defining the structure of the HTML page.	✔	—
phash-dct-base64	text	pHash (DCT hash) - as described in https://github.com/thorn-oss/perception.	—	—
truncated-hash-html-structure	text	Truncated hash value of the html-structure.	—	—
url	url	Full URL of the phishing object.	—	—

cloth

Describes clothes a natural person wears.

cloth 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	Multiple
bottom-accessories	text	Cloth and accessories on the bottom part of the body ['trousers', 'skirt', 'underpants / panties', 'shorts', 'boxer shorts', 'body stocking', 'sock', 'shoe', 'boot', 'sandal', 'slipper', 'sneaker', 'hiking boot', 'high tops']	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
cloth-color	text	Cloth's colors ['black', 'white', 'red', 'green', 'blue', 'cyan', 'orange', 'violet', 'pink', 'yellow', 'brown', 'grey']	–	✔
cloth-picture	attachment	Cloth's pictures	–	✔
description	text	Cloth's Description of a natural person	–	–
head-accessories	text	Cloth and accessories on the head ['hat', 'cap', 'bonnet', 'glasses', 'bandeau']	–	✔
top-accessories	text	Cloth and accessories on the top part of the body ['jacket', 'coat', 'dress', 'shirt', 'top', 'pullover', 'sweatshirt', 'suit', 'tie', 'bow tie', "lady's suit", 'waistcoat', 'cardigan', 'undershirt', 't-shirt', 'bra', 'scarf', 'glove']	–	✔

coin-address

An address used in a cryptocurrency.

coin-address 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	Multiple
address	btc	Bitcoin address used as a payment destination in a cryptocurrency	—	—
address-crypto	text	Generic cryptocurrency address if the format is not a standard BTC or XMR address	—	—
address-xmr	xmr	Monero address used as a payment destination in a cryptocurrency	—	—
current-balance	float	Current balance of address	✔	—
first-seen	datetime	First time this payment destination address has been seen	✔	—
last-seen	datetime	Last time this payment destination address has been seen	✔	—
last-updated	datetime	Last time the balances and totals have been updated	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
symbol	text	The (uppercase) symbol of the cryptocurrency used. Symbol should be from https://coinmarketcap.com/all/views/all/ ['BTC', 'ETH', 'BCH', 'XRP', 'MIOTA', 'DASH', 'BTG', 'LTC', 'ADA', 'XMR', 'ETC', 'NEO', 'NEM', 'EOS', 'XLM', 'BCC', 'LSK', 'OMG', 'QTUM', 'ZEC', 'USDT', 'HSR', 'STRAT', 'WAVES', 'PPT', 'ETN']	✔	—
text	text	Free text value	✔	—
total-received	float	Total balance received	✔	—
total-sent	float	Total balance sent	✔	—
total-transactions	text	Total transactions performed	✔	—

command

Command functionalities related to specific commands executed by a program, whether it is malicious or not. Command-line are attached to this object for the related commands.

command 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	Multiple
description	text	Description of the command functionalities	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
location	text	Location of the command functionality ['Bundled', 'Module', 'Libraries', 'Unknown']	✔	—
trigger	text	How the commands are triggered ['Local', 'Network', 'Unknown']	✔	—

command-line

Command line and options related to a specific command executed by a program, whether it is malicious or not.

command-line 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	Multiple
command_line	text	command code line	—	✔
description	text	description of the command	—	—
software	text	type of shell (bash/sh,powershell,cmd.exe) ['Shell', 'Bash', 'zsh', 'Powershell', 'cmd.exe']	—	—

concordia-mtmf-intrusion-set

Intrusion Set - Phase Description.

concordia-mtmf-intrusion-set 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	Multiple
AttackName	text	Name of the Attack	—	—
CMTMF_ATCKID	integer	Identifier of the Attack	—	—
FeedbackLoop	integer	Feedback Loop Sequence	—	—
PhName	text	Name of the Phase (Tactic)	✔	—
PhSequence	integer	Phase Sequence	✔	—
description	text	Description of the phase	✔	—

confidentiality-impact

Confidentiality Impact object as described in STIX 2.1 Incident object extension.

confidentiality-impact 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	Multiple
criticality	text	Criticality of the impact ['Not Specified', 'False Positive', 'Low', 'Moderate', 'High', 'Extreme']	✔	—
description	text	Additional details about the impact.	—	—
end_time	datetime	The date and time the impact was last recorded.	—	—
end_time_fidelity	text	Level of fidelity that the `end_time` is recorded in. ['day', 'hour', 'minute', 'month', 'second', 'year']	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
information_type	text	Type of information that had its confidentiality compromised. ['classified-material', 'communication', 'credentials-admin', 'credentials-user', 'financial', 'leval', 'payment', 'phi', 'pii', 'proprietary']	✔	—
loss_type	text	The type of loss that occurred to the relevant information. ['confirmed-loss', 'contained', 'exploited-loss', 'none', 'suspected-loss']	✔	—
record_count	counter	The number of records of this type that were compromised.	✔	—
record_size	size-in-bytes	The amount of data that was compromised in bytes.	✔	—
recoverability	text	Recoverability of this particular impact with respect to feasibility and required time and resources. ['extended', 'not-applicable', 'not-recoverable', 'regular', 'supplemented']	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
start_time	datetime	The date and time the impact was first recorded.	—	—
start_time_fidelity	text	Level of fidelity that the `start_time` is recorded in. ['day', 'hour', 'minute', 'month', 'second', 'year']	✔	—

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	Multiple
cookie	cookie	Full cookie	—	—
cookie-name	text	Name of the cookie (if splitted)	—	—
cookie-value	text	Value of the cookie (if splitted)	—	—
expires	datetime	Expiration date/time of the cookie	✔	—
http-only	boolean	True if send only through HTTP ['True', 'False']	✔	—
path	text	Path defined in the cookie	✔	—
secure	boolean	True if cookie is sent over TLS ['True', 'False']	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
text	text	A description of the cookie.	✔	—
type	text	Type of cookie and how it's used in this specific object. ['Session management', 'Personalization', 'Tracking', 'Exfiltration', 'Malicious Payload', 'Beaconing']	—	—

cortex

Cortex object describing a complete Cortex analysis. Observables would be attribute with a relationship from this object.

cortex 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	Multiple
full	text	Cortex report object (full report) in JSON	✔	—
name	text	Cortex analyser/worker name	✔	—
server-name	text	Name of the cortex server	✔	—
start-date	datetime	When the Cortex analyser was started	✔	—
success	boolean	Result of the cortex job ['True', 'False']	✔	—
summary	text	Cortex summary object (summary) in JSON	—	—

cortex-taxonomy

Cortex object describing a Cortex Taxonomy (or mini report).

cortex-taxonomy 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	Multiple
cortex_url	link	URL to the Cortex job	✔	—
level	text	Cortex Taxonomy Level ['info', 'safe', 'suspicious', 'malicious']	✔	—
namespace	text	Cortex Taxonomy Namespace	✔	—
predicate	text	Cortex Taxonomy Predicate	✔	—
value	text	Cortex Taxonomy Value	✔	—

course-of-action

An object describing a specific measure taken to prevent or respond to an attack.

course-of-action 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	Multiple
cost	text	The estimated cost of applying the course of action. ['High', 'Medium', 'Low', 'None', 'Unknown']	✔	—
description	text	A description of the course of action.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
efficacy	text	The estimated efficacy of applying the course of action. ['High', 'Medium', 'Low', 'None', 'Unknown']	✔	—
impact	text	The estimated impact of applying the course of action. ['High', 'Medium', 'Low', 'None', 'Unknown']	✔	—
name	text	The name used to identify the course of action.	✔	—
objective	text	The objective of the course of action.	✔	—
stage	text	The stage of the threat management lifecycle that the course of action is applicable to. ['Remedy', 'Response', 'Further Analysis Required']	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
type	text	The type of the course of action. ['Perimeter Blocking', 'Internal Blocking', 'Redirection', 'Redirection (Honey Pot)', 'Hardening', 'Patching', 'Eradication', 'Rebuilding', 'Training', 'Monitoring', 'Physical Access Restrictions', 'Logical Access Restrictions', 'Public Disclosure', 'Diplomatic Actions', 'Policy Actions', 'Other']	✔	—

covid19-csse-daily-report

CSSE COVID-19 Daily report.

covid19-csse-daily-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	Multiple
active	counter	the number of active cases.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
confirmed	counter	the number of confirmed cases. For Hubei Province: from Feb 13 (GMT +8), we report both clinically diagnosed and lab-confirmed cases. For lab-confirmed cases only (Before Feb 17), please refer to https://github.com/CSSEGISandData/COVID-19/tree/master/who_covid_19_situation_reports.	✔	—
country-region	text	country/region name conforming to WHO (will be updated).	✔	—
county	integer	US County (US Only)	✔	—
death	counter	the number of deaths.	✔	—
fips	integer	Federal Information Processing Standard county code (US Only)	✔	—
latitude	float	Approximate latitude of the entry	✔	—
longitude	float	Approximate longitude of the entry	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
province-state	text	province name; US/Canada/Australia/ - city name, state/province name; Others - name of the event (e.g., "Diamond Princess" cruise ship); other countries - blank.	✔	—
recovered	counter	the number of recovered cases.	✔	—
update	datetime	Time of the last update that day (UTC)	✔	—

covid19-dxy-live-city

COVID 19 from dxy.cn - Aggregation by city.

covid19-dxy-live-city 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	Multiple
city	text	Name of the Chinese city, in Chinese.	✔	—
current-confirmed	counter	Current number of confirmed cases	✔	—
total-confirmed	counter	Total number of confirmed cases.	✔	—
total-cured	counter	Total number of cured cases.	✔	—
total-death	counter	Total number of deaths.	✔	—
update	datetime	Approximate time of the update (~hour)	✔	—

covid19-dxy-live-province

COVID 19 from dxy.cn - Aggregation by province.

covid19-dxy-live-province 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	Multiple
comment	text	Comment, in chinese	✔	—
current-confirmed	counter	Current number of confirmed cases	✔	—
province	text	Name of the Chinese province, in Chinese.	✔	—
total-confirmed	counter	Total number of confirmed cases.	✔	—
total-cured	counter	Total number of cured cases.	✔	—
total-death	counter	Total number of deaths.	✔	—
update	datetime	Approximate time of the update (~hour)	✔	—

cowrie

Cowrie honeypot object template.

cowrie 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	Multiple
compCS	text	SSH compression algorithm supported in the session	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
dst_ip	ip-dst	Destination IP address of the session	✔	—
dst_port	port	Destination port of the session	✔	—
encCS	text	SSH symmetric encryption algorithm supported in the session	✔	✔
eventid	text	Eventid of the session in the cowrie honeypot	✔	—
hassh	hassh-md5	HASSH of the client SSH session following Salesforce algorithm	—	—
input	text	Input of the session	—	—
isError	text	isError	✔	—
keyAlgs	text	SSH public-key algorithm supported in the session	✔	✔
macCS	text	SSH MAC supported in the sesssion	✔	✔
message	text	Message of the cowrie honeypot	✔	—
password	text	Password	—	✔
protocol	text	Protocol used in the cowrie honeypot	✔	—
sensor	text	Cowrie sensor name	✔	—
session	text	Session id	—	—
src_ip	ip-src	Source IP address of the session	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
src_port	port	Source port of the session	✔	—
system	text	System origin in cowrie honeypot	✔	—
timestamp	datetime	When the event happened	✔	—
username	text	Username related to the password(s)	—	—

cpe-asset

An asset which can be defined by a CPE. This can be a generic asset. CPE is a structured naming scheme for information technology systems, software, and packages.

cpe-asset 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	Multiple
cpe	cpe	CPE—the well-formed CPE name(WFN). WFNs can be used to describe a set of products or to identify an individual product.	—	—
description	text	Complementary description of the asset	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
edition	text	The edition attribute is considered deprecated in this specification, and it SHOULD be assigned the logical value ANY except where required for backward compatibility with version 2.2 of the CPE specification.This attribute is referred to as the “legacyedition”attribute.If this attribute is used,values for this attribute SHOULD capture edition-related terms applied by the vendor to the product. Values for this attribute SHOULD be selected from an attribute-specific valid-values list, which MAYbe defined by other specifications that utilize this specification. Any character string meeting the requirements for WFNs (cf. 5.3.2) MAY be specified as the value of the attribute.	✔	–

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
language	text	Values for thisattribute SHALL be valid language tags as defined by [RFC5646], and SHOULD be used to define the language supported in the user interface of the product being described.Although any valid language tag MAY be used, only tags containing language and region codesSHOULD be used.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
other	text	Values for this attribute SHOULD capture any other general descriptive or identifying information which is vendor- or product-specific and which does not logically fit in any other attribute value. Values SHOULD NOT be used for storing instance-specific data (e.g., globally-unique identifiers or Internet Protocol addresses).Values for this attribute SHOULD be selected from a valid-values list that is refined over time; this list MAYbe defined by other specifications that utilize this specification. Any character string meeting the requirements for WFNs (cf. 5.3.2) MAYbe specified as the value of the attribute.	✔	—
part	text	Part - application, operating systems or hardware devices ['a', 'o', 'h']	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
product	text	Values for this attribute SHOULD describe or identify the most common and recognizable title or name of the product. Values for this attribute SHOULD be selected from an attribute-specific valid-values list, which MAYbe defined by other specifications that utilize this specification. Any character string meeting the requirements for WFNs(cf. 5.3.2) MAY be specified as the value of the attribute.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
sw_edition	text	Values for this attribute SHOULD characterize how the product is tailored to a particular market or class of end users. Values for this attribute SHOULD be selected from an attribute-specific valid-values list, which MAYbe defined by other specifications that utilize this specification. Any character string meeting the requirements for WFNs(cf. 5.3.2) MAYbe specified as the value of the attribute.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
target_hw	text	Values for this attribute SHOULD characterize the instruction set architecture (e.g., x86) on which the product being described or identified by the WFN operates. Bytecode-intermediate languages, such as Java bytecode for the Java Virtual Machine or Microsoft Common Intermediate Language for the Common Language Runtime virtual machine, SHALL be considered instruction set architectures. Values for this attribute SHOULD be selected from an attribute-specific valid-values list, which MAYbe defined by other specifications that utilize this specification. Any character string meeting the requirements for WFNs(cf. 5.3.2) MAYbe specified as the value of the attribute.	✔	–

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
target_sw	text	Values for this attribute SHOULDi characterize the software computing environment within which the product operates.Values for this attribute SHOULD be selected from an attribute-specific valid-values list, which MAYbe defined by other specifications that utilize this specification. Any character string meeting the requirements for WFNs(cf. 5.3.2) MAYbe specified as the value of the attribute.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
update	text	Values for this attribute SHOULD be vendor-specific alphanumeric strings characterizing the particular update, service pack, or point release of the product.Values for this attribute SHOULD be selected from an attribute-specific valid-values list, which MAYbe defined by other specifications that utilize this specification. Any character string meeting the requirements for WFNs (cf. 5.3.2) MAYbe specified as the value of the attribute.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
vendor	text	Values for this attribute SHOULD describe or identify the person or organization that manufactured or created the product. Values for this attribute SHOULD be selected from an attribute-specific valid-values list, which MAYbe defined by other specifications that utilize this specification. Any character string meeting the requirements for WFNs (cf. 5.3.2) MAY be specified as the value of the attribute	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
version	text	Values for this attribute SHOULD be vendor-specific alphanumeric strings characterizing the particular release version of the product.Version information SHOULD be copied directly (with escaping of printable non-alphanumeric characters as required) from discoverable data and SHOULD NOTbe truncated or otherwise modified. Any character string meeting the requirements for WFNs (cf. 5.3.2) MAYbe specified as the value of the attribute.	✔	—

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

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	Multiple
bank_name	text	Name of the bank which have issued 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.	—	—
comment	comment	A description of the card.	—	—
expiration	datetime	Maximum date of validity	—	—
iin	text	International Issuer Number (First eight digits of the credit card number	—	—
issued	datetime	Initial date of validity or issued date.	—	—
name	text	Name of the card owner.	—	—
version	text	Version of the card.	—	—

crowdsec-ip-context

CrowdSec Threat Intelligence - IP CTI search.

crowdsec-ip-context 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	Multiple
as-name	text	Autonomous system name	✔	✔
as-num	AS	Autonomous system number	✔	✔
attack-details	text	Triggered scenarios	✔	➖
background-noise	float	High background noise scores highlight untargeted, mild threat mass-attacks	✔	➖
behaviors	text	Attack categories	✔	✔
city	text	City of origin	✔	➖
classifications	text	Classification category of the IP address	✔	✔
country	text	Country of origin	✔	➖
country-code	text	Country Code	✔	➖
cves	text	CVEs exploited by the observed IP	✔	✔
dst-port	port	Destination port	✔	✔
false-positives	text	False positive category of the IP address	✔	✔
ip	ip-src	IP Address	➖	➖
ip-range	ip-src	destination IP address	➖	➖
ip-range-score	float	destination IP address	✔	➖
latitude	float	Latitude of origin	✔	➖
longitude	float	Longitude of origin	✔	➖
mitre-techniques	text	MITRE ATT&CK techniques used by the observed IP	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
reputation	text	Real-time, actionable IP reputation score derived from trusted reports and consensus-validated data in CrowdSec CTI	✔	—
reverse-dns	hostname	Reverse DNS name	—	—
scores	text	Scores	✔	—
target-countries	text	Target countries (top 10)	✔	—
trust	float	Trust level	✔	—

crowdstrike-report

An Object Template to encode an Crowdstrike detection report.

crowdstrike-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	Multiple
command	text	Commandline triggering the detection	✔	✔
file-hash	sha256	Unique file hash	—	—
filename	filename	Filename on disk	✔	✔
fullpath	text	Complete path of the filename including the filename	✔	✔
ip	ip-src	Source IP address	—	—
parent-command	text	Commandline of the parent process	✔	✔
process-name	text	Name of the process trigerring the detection	—	✔

crypto-material

Cryptographic materials such as public or/and private keys.

crypto-material 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	Multiple
Gx	text	Curve Parameter - Gx in decimal	✔	—
Gy	text	Curve Parameter - Gy in decimal	✔	—
b	text	Curve Parameter - B in decimal	✔	—
curve-length	text	Length of the Curve in bits	✔	—
e	text	RSA public exponent	—	—
ecdsa-type	text	Curve type of the ECDSA cryptographic materials ['Anomalous', 'M-221', 'E-222', 'NIST P-224', 'Curve1174', 'Curve25519', 'BN(2,254)', 'brainpoolP256t1', 'ANSSI FRP256v1', 'NIST P-256', 'secp256k1', 'E-382', 'M-383', 'Curve383187', 'brainpoolP384t1', 'NIST P-384', 'Curve41417', 'Ed448-Goldilocks', 'M-511', 'E-521']	✔	—
g	text	Curve Parameter - G in decimal	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
generic-symmetric-key	text	Generic symmetric key (please precise the type)	➖	➖
modulus	text	Modulus Parameter - in hexadecimal - no 0x, no :	➖	➖
n	text	Curve Parameter - N in decimal	✔	➖
origin	text	Origin of the cryptographic materials ['mathematical-attack', 'exhaustive-search', 'bruteforce-attack', 'malware-extraction', 'memory-interception', 'network-interception', 'leak', 'unknown']	✔	➖
p	text	Prime Parameter - P in decimal	➖	➖
private	text	Private part of the cryptographic materials in PEM format	➖	➖
public	text	Public part of the cryptographic materials in PEM format	➖	➖
q	text	Prime Parameter - Q in decimal	➖	➖
rsa-modulus-size	text	RSA modulus size in bits	✔	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
text	text	A description of the cryptographic materials.	✔	—
type	text	Type of crytographic materials ['RSA', 'DSA', 'ECDSA', 'RC4', 'XOR', 'unknown']	✔	—
x	text	Curve Parameter - X in decimal	✔	—
y	text	Curve Parameter - Y in decimal	✔	—

cryptocurrency-transaction

An object to describe a cryptocurrency transaction.

cryptocurrency-transaction 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	Multiple
address	btc	A cryptocurrency transactional address	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
symbol	text	The (uppercase) symbol of the cryptocurrency used. Symbol should be from https://coinmarketcap.com/all/views/all/ ['BTC', 'ETH', 'BCH', 'XRP', 'MIOTA', 'DASH', 'BTG', 'LTC', 'ADA', 'XMR', 'ETC', 'NEO', 'NEM', 'EOS', 'XLM', 'BCC', 'LSK', 'OMG', 'QTUM', 'ZEC', 'USDT', 'HSR', 'STRAT', 'WAVES', 'PPT', 'ETN']	✔	—
time	datetime	Date and time of transaction	✔	—
transaction-number	text	A transaction number in a sequence of transactions	—	✔
value	float	Value in cryptocurrency at date/time displayed in field 'time'	✔	—
value_EUR	float	Value in EUR with conversion rate as of date/time displayed in field 'time'	✔	—
value_USD	float	Value in USD with conversion rate as of date/time displayed in field 'time'	✔	—

cs-beacon-config

Cobalt Strike Beacon Config.

cs-beacon-config 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	Multiple
architecture	text	Hardware architecture of the sample	✔	—
asn	AS	Originating ASN for the CS Beacon Config	✔	—
beacon-host	ip-dst	Beacon host IP	—	—
beacon-type	text	Beacon type used	✔	—
binary-md5	md5	MD5 of the binary delivered	—	—
binary-sha1	sha1	SHA1 of the binary delivered	—	—
binary-sha256	sha256	SHA256 of the binary delivered	—	—
c2	url	The C2 sample communicates with	—	✔
city	text	City location of the CS Beacon Config in question	✔	—
config-md5	md5	MD5 of the configuration	—	—
config-sha1	sha1	SHA1 of the configuration	—	—
config-sha256	sha256	SHA256 of the configuration	—	—
content-length	size-in-bytes	Content length of the payload	✔	—
content-type	text	Content/type received	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
encoded-data	attachment	Encoded payload data in Base64 as file attachment	➖	➖
encoded-length	size-in-bytes	Length of the encoded data	✔	➖
geo	text	Country location of the CS Beacon Config	✔	➖
http	text	HTTP protocol used	✔	➖
http-code	integer	HTTP return code	✔	➖
http-url	text	HTTP url path of the beacon	➖	➖
ip	ip-dst	IP of the C2	➖	✔
jar-md5	md5	MD5 of adversary cobaltstrike.jar file	➖	➖
license-id	text	License ID of the Colbalt Strike	➖	➖
md5	md5	MD5 of sample containing the Cobalt Strike shellcode	➖	➖
naics	text	North American Industry Classification System Code (NAICS)	✔	✔
sector	text	Sector of for the CS Beacon Config in question	✔	✔
sha1	sha1	SHA1 of sample containing the Cobalt Strike shellcode	➖	➖
sha256	sha256	SHA256 of sample containing the Cobalt Strike shellcode	➖	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
vt-sha256	sha256	SHA256 of sample uploaded to VirusTotal	—	—
watermark	text	The watermark of sample	—	—

ctf-challenge

Capture-the-flag challenge object as defined by Rectifyq.

> ctf-challenge 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	Multiple
attachment	attachment	Any relevant supporting files or resources that are attached to the challenge	✔	✔
category	text	The type of challenge (e.g., web, binary, forensics) ['Web', 'Reverse Engineering', 'Binary Exploitation', 'Forensics', 'Networking', 'Cryptography', 'OSINT', 'Misc']	✔	✔
description	text	A brief explanation of the challenge	✔	—
flag	text	Submitted and accepted CTF Challenge's flag	✔	—
hints	text	Clues to help solve the challenge	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
max_attempts	counter	Maximum tries allowed	✔	—
points	float	The rewarded points for completing the challenge	✔	—
solves	counter	Number of people who solved the challenge	✔	—
title	text	The name of the challenge	✔	—

cytomic-orion-file

Cytomic Orion File Detection.

cytomic-orion-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	Multiple
classification	text	File classification - number	—	—
classificationName	text	File classification	—	—
fileName	filename	Original filename	—	—
fileSize	size-in-bytes	Size of the file	—	—
first-seen	datetime	First seen timestamp of the file	—	—
last-seen	datetime	Last seen timestamp of the file	—	—

cytomic-orion-machine

Cytomic Orion File at Machine Detection.

cytomic-orion-machine 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	Multiple
clientCreationDateUTC	datetime	Client creation date UTC	—	—
clientId	text	Client id	—	—
clientName	target-org	Client name	—	—
creationDate	datetime	Client creation date	—	—
first-seen	datetime	First seen on machine	—	—
last-seen	datetime	Last seen on machine	—	—
lastSeenUtc	datetime	Client last seen UTC	—	—
machineMuid	text	Machine UID	—	—
machineName	target-machine	Machine name	—	—
machinePath	text	Path of observable	—	—

dark-pattern-item

An Item whose User Interface implements a dark pattern.

dark-pattern-item 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	Multiple
comment	text	textual comment about the item	✔	—
gain	text	What is the implementer is gaining by deceiving the user ['registration', 'personal data', 'money', 'contacts', 'audience']	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
implementer	text	Who is the vendor / holder of the item	✔	—
location	text	Location where to find the item	✔	✔
screenshot	attachment	A screencapture or a screengrab of the item at work	✔	—
time	datetime	Date and time when first-seen	✔	—
user	text	who are the user of the item	✔	—

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 or using the type field.

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	Multiple
backscatter-threshold	integer	The minimum amount of backscatter received in 5 minutes / day. This field is only used when the capture origin is indirect network capture such as backscatter.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
capture-origin	text	Origin of the (D)DoS evidences ['Direct network capture', 'Logs', 'Indirect network capture (e.g. backscatter)', 'Unknown']	✔	—
domain-dst	domain	Destination domain (victim)	—	—
dst-port	port	Destination port of the attack	—	✔
first-seen	datetime	Beginning of the attack	✔	—
ip-dst	ip-dst	Destination IP (victim)	—	—
ip-src	ip-src	IP address originating the attack	—	✔
last-seen	datetime	End of the attack	✔	—
protocol	text	Protocol used for the attack ['TCP', 'UDP', 'ICMP', 'IP']	✔	—
src-port	port	Port originating the attack	—	✔
text	text	Description of the DDoS	✔	—
total-bps	integer	Bits per second (maximum rate of bits per second measured)	✔	—
total-bytes-sent	size-in-bytes	Total number of bytes sent by the sources mentioned	✔	—
total-packets-sent	counter	Total number of packets sent by the source mentioned	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
total-pps	integer	Packets per second (maximum rate of packets per second measured)	✔	—
type	text	Type(s) or Technique(s) of Denial of Service ['amplification-attack', 'reflected-spoofed-attack', 'slow-read-attack', 'flooding-attack', 'post-attack', 'chargen-amplification', 'dns', 'dns-amplification', 'ip-fragmentation', 'ip-private', 'icmp', 'memcached-amplification', 'ms-sql-rs-amplification', 'ntp-amplification', 'snmp-amplification', 'ssdp-amplification', 'tcp-null', 'tcp-rst', 'tcp-syn', 'udp']	✔	✔

ddos-claim

DDoS-claim object describes a current claim of DDoS activity.

ddos-claim 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	Multiple
claim-validity	text	Validity of the claim. Valid means, a trusted entity having the technical capabilities to perform analysis confirmed the detection of DDoS activities. ['Unknown', 'Valid', 'Invalid']	✔	—
proof	text	The claim in text format.	✔	✔
proof-screenshot	attachment	Screenshot of the claim.	—	✔
reference	link	Reference to the DDoS claim.	✔	✔
target	text	Target of the DDoS claim.	✔	—

ddos-config

DDoS-claim object describes a current claim of DDoS activity.

ddos-config 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	Multiple
body	text	Payload used for the DDos	✔	✔
ddos-tool	text		✔	—
headers	text	Headers used in the DDoS requests	✔	✔
host	hostname	Hostname used as target of the DDoS attack	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
ip	ip-dst	IP address used as target of the DDoS attack	✔	✔
method	text	Method of DDoS attack used ['ack', 'GET', 'method', 'PING', 'POST', 'syn', 'SYN', 'syn_ack', 'udp_flood']	✔	—
path	text	URL path used for the DDoS attack (excluded hostname)	✔	✔
port	port	Port used for attack (when the type and method requires it)	✔	—
request-id	text	request id	✔	—
target-id	text	target id	✔	—
type	text	Type of network protocol used for the DDoS attack ['http', 'http2', 'http3', 'nginx_loris', 'tcp', 'type', 'udp']	✔	—
use-ssl	text	TLS/SSL used for the attack ['true', 'false']	✔	—

device

An object to define a device.

device 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	Multiple
MAC-address	mac-address	Device MAC address	➖	➖
OS	text	OS of the device	✔	✔
alias	text	Alias of the Device	➖	✔
analysis-date	datetime	Date of device analysis	➖	➖
attachment	attachment	An attachment	➖	✔
description	text	Description of the Device	✔	➖
device-type	text	Type of the device ['PC', 'Mobile', 'Laptop', 'HID', 'TV', 'IoT', 'Hardware', 'Other']	✔	➖
dns-name	text	Device DNS Name	➖	✔
hits	counter	Number of hits for the device	✔	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
infection_type	text	Type of infection if the device is in Infected status ['android_spams', 'android.bakdoor.prizmes', 'android.bankbot', 'android.banker.anubis', 'android.bankspy', 'android.cliaid', 'android.darksilent', 'android.fakeav', 'android.fakebank', 'android.fakedoc', 'android.fakeinst', 'android.fakemart', 'android.faketoken', 'android.fobus', 'android.fungram', 'android.geost', 'android.gopl', 'android.hiddad', 'android.hqwar', 'android.hummer', 'android.infosteal', 'android.iop', 'android.lockdroid', 'android.milipnot', 'android.nitmo', 'android.opfake', 'android.premiumtext', 'android.provar', 'android.pwstealer', 'android.rootnik', 'android.skyfin', 'android.smsbot', 'android.smssilence', 'android.smsspy', 'android.smsspy.b	✔	━

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
ip-address	ip-src	Device IP address	—	✔
name	text	Name of the Device	—	—
status	text	Status of the device ['Infected', 'Exposed', 'Unknown', 'Clean']	✔	—
version	text	Version of the device/ OS	✔	—

diameter-attack

Attack as seen on the diameter signaling protocol supporting LTE networks.

diameter-attack 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	Multiple
ApplicationId	text	Application-ID is used to identify for which Diameter application the message is applicable. Application-ID is a decimal representation.	—	—
CmdCode	text	A decimal representation of the diameter Command Code.	✔	—
Destination-Host	text	Destination-Host.	—	✔
Destination-Realm	text	Destination-Realm.	—	✔
IdrFlags	text	IDR-Flags.	✔	—
Origin-Host	text	Origin-Host.	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
Origin-Host-CountryISO2	text	Origin-Host Country ISO2	—	✔
Origin-Host-OperatorName	text	Origin-Host Operator Name	—	✔
Origin-Host-TADIG	text	Origin-Host Operator TADIG	—	✔
Origin-Realm	text	Origin-Realm.	—	✔
Origin-Realm-CountryISO2	text	Origin-Realm Country ISO2	—	✔
Origin-Realm-OperatorName	text	Origin-Realm Operator Name	—	✔
Origin-Realm-TADIG	text	Origin-Realm Operator TADIG	—	✔
SessionId	text	Session-ID.	—	—
Username	text	Username (in this case, usually the IMSI).	—	✔
category	text	Category. ['Cat0', 'Cat1', 'Cat2', 'Cat3', 'CatSMS']	✔	—
first-seen	datetime	When the attack has been seen for the first time.	✔	—
text	text	A description of the attack seen.	✔	—

diamond-event

A diamond model event object consisting of the four diamond features advesary, infrastructure, capability and victim, several meta-features and ioc attributes.

diamond-event 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	Multiple
Advesary	text	The advesary who attacks the victim	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
Capability	text	The capability used to attack the victim	—	—
Description	text	Further context to the event	—	—
Direction	text	The network-based direction of the event ['Victim-to-Infrastructure', 'Infrastructure-to-Victim', 'Infrastructure-to-Infrastructure', 'Adversary-to-Infrastructure', 'Infrastructure-to-Adversary', 'Bidirectional', 'Unknown']	—	—
EventID	integer	Id of the event	—	—
Infrastructure	text	The infrastructure used in the attack	—	—
Methodology	text	Mitre-Attack mapping of the event	—	—
Phase	text	The event mapped to a phase of the killchain ['Reconnaissance', 'Weaponization', 'Delivery', 'Exploitation', 'Installation', 'C2', 'Action on Objectives']	—	—
Resources	text	The resources the attacker needed for the event to succeed	—	—
Result	text	The result of the event	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
Timestamp	datetime	Timestamp when the event happened	—	—
Victim	text	The attacked victim	—	—
ioc	text	Generic IOC	—	✔
textfield	text	Generic textfield	—	✔

directory

Directory object describing a directory with meta-information.

directory 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	Multiple
access-time	datetime	The last time the directory was accessed	—	—
creation-time	datetime	Creation time of the directory	—	—
modification-time	datetime	Modification time of the directory	—	—
path	text	Path of the directory, complete or partial	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
path-encoding	text	Encoding format of the directory ['Adobe-Standard-Encoding', 'Adobe-Symbol-Encoding', 'Amiga-1251', 'ANSI_X3.110-1983', 'ASMO_449', 'Big5', 'Big5-HKSCS', 'BOCU-1', 'BRF', 'BS_4730', 'BS_viewdata', 'CESU-8', 'CP50220', 'CP51932', 'CSA_Z243.4-1985-1', 'CSA_Z243.4-1985-2', 'CSA_Z243.4-1985-gr', 'CSN_369103', 'DEC-MCS', 'DIN_66003', 'dk-us', 'DS_2089', 'EBCDIC-AT-DE', 'EBCDIC-AT-DE-A', 'EBCDIC-CA-FR', 'EBCDIC-DK-NO', 'EBCDIC-DK-NO-A', 'EBCDIC-ES', 'EBCDIC-ES-A', 'EBCDIC-ES-S', 'EBCDIC-FI-SE', 'EBCDIC-FI-SE-A', 'EBCDIC-FR', 'EBCDIC-IT', 'EBCDIC-PT', 'EBCDIC-UK', 'EBCDIC-US', 'ECMA-cyrillic', 'ES', 'ES2', 'EUC-KR', 'Extended_UNIX_Code_Fixed_Width_for_Japanese', 'Extended_UNIX_Code_Packed_Format_for_Japanese',	✔	━

dkim

DomainKeys Identified Mail - DKIM.

dkim 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	Multiple
d	domain	DKIM domain used for the selector record	—	—
dkim	dkim	DomainKeys Identified Mail - DKIM full DNS TXT record	—	—
h	text	DKIM hash type ['sha1', 'md5']	✔	—
k	text	DKIM key type ['rsa']	✔	—
n	text	DKIM administrator note	✔	—
public-key	text	DKIM public key	—	—
s	text	DKIM service record	✔	—
t	text	DKIM domain testing ['y', 's']	✔	—
version	text	DKIM version ['DKIM1']	✔	—

dns-record

A set of DNS records observed for a specific domain.

dns-record 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	Multiple
a-record	ip-dst	IPv4 address associated with A record	—	✔
aaaa-record	ip-dst	IPv6 address associated with AAAA record	—	✔
cname-record	domain	Domain associated with CNAME record	—	✔
mx-record	domain	Domain associated with MX record	—	✔
ns-record	domain	Domain associated with NS record	—	✔
ptr-record	domain	Domain associated with PTR record	—	✔
queried-domain	domain	Domain name	—	—
soa-record	domain	Domain associated with SOA record	—	✔
spf-record	ip-dst	IP addresses associated with SPF record	—	✔
srv-record	domain	Domain associated with SRV record	—	✔
text	text	A description of the records	—	—
txt-record	text	Content associated with TXT record	—	✔

url

dom-hash object to describe similar structure of HTML pages.

> 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	Multiple
dom-hash	dom-hash	dom-hash value of the url(s)	—	—
ref	link	Reference link for the complete analysis of this dom-hash	—	✔
url	url	Full URL of the dom-hashed HTML structure	—	✔

domain-crawled

A domain crawled over time.

domain-crawled 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	Multiple
domain	domain	Domain name	—	—
text	text	A description of the tuple	✔	—
url	url	domain url	—	✔

domain-ip

A domain/hostname 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	Multiple
domain	domain	Domain name	—	✔
first-seen	datetime	First time the tuple has been seen	✔	—
hostname	hostname	Hostname related to the IP	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
ip	ip-dst	IP Address	—	✔
last-seen	datetime	Last time the tuple has been seen	✔	—
port	port	Associated TCP port with the domain	—	✔
registration-date	datetime	Registration date of domain	—	—
text	text	A description of the tuple	✔	—

edr-report

An Object Template to encode an EDR detection report.

edr-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	Multiple
additional-file	attachment	Additional file involved in detection	✔	✔
command	attachment	JSON file containing the output of a command ran at report generation	✔	✔
comment	text	Any valuable comment about the report	✔	—
drivers	attachment	JSON file containing metadata about drivers loaded on the system	✔	—
endpoint-id	text	Unique identifier of the endpoint concerned by the report	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
event	attachment	Raw EDR event which triggered reporting	✔	—
executable	attachment	Executable file involved in detection	✔	✔
hostname	text	Endpoint hostname	—	—
id	text	Report unique identifier	—	—
ip	ip-src	Endpoint IP address	✔	—
modules	attachment	JSON file containing metadata about modules loaded on the system	✔	—
processes	attachment	JSON file containing metadata about running processes at the time of detection	✔	—
product	text	EDR product name	✔	—

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	Multiple
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',	✔	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
entrypoint-address	text	Address of the entry point	✔	—
number-sections	counter	Number of sections	✔	—
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']	✔	—
text	text	Free text value to attach to the ELF	✔	—
type	text	Type of ELF ['CORE', 'DYNAMIC', 'EXECUTABLE', 'HIPROC', 'LOPROC', 'NONE', 'RELOCATABLE']	✔	—

elf-section

Object describing a section of an Executable and Linkable Format.

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

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
entropy	float	Entropy of the whole section	✔	—
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']	✔	✔
md5	md5	[Insecure] MD5 hash (128 bits)	—	—
name	text	Name of the section	✔	—
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	—	—
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	—	—
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	—	—
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	—	—
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	—	—
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	—	—
size-in-bytes	size-in-bytes	Size of the section, in bytes	✔	—
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	—	—
text	text	Free text value to attach to the section	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
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']	✔	—

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	Multiple
attachment	email-attachment	Attachment	➖	✔
bcc	email-dst	Blind carbon copy	✔	✔
bcc-display-name	email-dst-display-name	Display name of the blind carbon copy	➖	✔
cc	email-dst	Carbon copy	✔	✔
cc-display-name	email-dst-display-name	Display name of the carbon copy	➖	✔
email-body	email-body	Body of the email	✔	✔
email-body-attachment	attachment	Body of the email as an attachment	✔	➖
eml	attachment	Full EML	✔	➖
from	email-src	Sender email address	➖	✔
from-display-name	email-src-display-name	Display name of the sender	➖	✔
from-domain	domain	Sender domain address (when only the source domain is known)	➖	✔
header	email-header	Full headers	✔	✔
ip-src	ip-src	Source IP address of the email sender	➖	✔
message-id	email-message-id	Message ID	✔	➖
mime-boundary	email-mime-boundary	MIME Boundary	✔	➖
msg	attachment	Full MSG	✔	➖
received-header-hostname	hostname	Extracted hostname from parsed headers	➖	✔
received-header-ip	ip-src	Extracted IP address from parsed headers	➖	✔
reply-to	email-reply-to	Email address the reply will be sent to	➖	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
reply-to-display-name	email-dst-display-name	Display name of the email address the reply will be sent to	—	✔
return-path	email-src	Message return path	—	—
screenshot	attachment	Screenshot of email	✔	—
send-date	datetime	Date the email has been sent	✔	—
subject	email-subject	Subject	—	✔
thread-index	email-thread-index	Identifies a particular conversation thread	✔	—
to	email-dst	Destination email address	✔	✔
to-display-name	email-dst-display-name	Display name of the receiver	—	✔
user-agent	text	User Agent of the sender	✔	—
x-mailer	email-x-mailer	X-Mailer generally tells the program that was used to draft and send the original email	✔	—

employee

An employee and related data points.

> employee 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	Multiple
business-unit	target-org	the organizational business unit associated with the employee	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
email-address	target-email	Employee Email Address	—	—
employee-type	text	type of employee ['Mid-Level Manager', 'Senior Manager', 'Non-Manager', 'Supervisor', 'First-Line Manager', 'Director']	✔	—
first-name	first-name	Employee's first name	✔	—
full-name	full-name	Employee's full name	✔	—
last-name	last-name	Employee's last name	✔	—
primary-asset	target-machine	Asset tag of the primary asset assigned to employee	—	—
text	text	A description of the person or identity.	✔	—
userid	target-user	EMployee user identification	✔	—

error-message

An error message which can be related to the processing of data such as import, export scripts from the original MISP instance.

error-message 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	Multiple
message	text	Content of the error message.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
source	text	Source of the error message. ['misp-stix', 'lief', 'other']	✔	—

event

Event object as described in STIX 2.1 Incident object extension.

> event 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	Multiple
description	text	Description of the event.	—	—
end_time	datetime	The date and time the event was last recorded.	—	—
end_time_fidelity	text	Level of fidelity that the `end_time` is recorded in. ['day', 'hour', 'minute', 'month', 'second', 'year']	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
event_type	text	Type of event. ['aggregation-information-phishing-schemes', 'benign', 'blocked', 'brute-force-attempt', 'c&c-server-hosting', 'compromised-system', 'confirmed', 'connection-malware-port', 'connection-malware-system', 'content-forbidden-by-law', 'control-system-bypass', 'copyrighted-content', 'data-exfiltration', 'deferred', 'deletion-information', 'denial-of-service', 'destruction', 'dictionary-attack-attempt', 'discarded', 'disruption-data-transmission', 'dissemination-malware-email', 'dissemination-phishing-emails', 'dns-cache-poisoning', 'dns-local-resolver-hijacking', 'dns-spoofing-registered', 'dns-rebinding', 'dns-server-compromise', 'dns-spoofing-	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
goal	text	The assumed objective of the event.	—	—
name	text	Name of the event.	—	—
start_time	datetime	The date and time the event was first recorded.	—	—
start_time_fidelity	text	Level of fidelity that the `start_time` is recorded in. ['day', 'hour', 'minute', 'month', 'second', 'year']	✔	—
status	text	Current status of the event. ['not-occurred', 'ongoing', 'occurred', 'pending', 'undetermined']	✔	—

exploit

Exploit object describes a program in binary or source code form used to abuse one or more vulnerabilities.

> exploit 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	Multiple
0day-today-id	text	Reference to the 0day.today referencing this exploit.	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
accessibility	text	Accessibility of the exploit. ['Unknown', 'Public', 'Limited', 'Paid']	✔	—
comment	text	Comment associated to the exploit.	—	—
credit	text	Credit(s) for the exploit (such as author, distributor or original source).	—	✔
cve-id	vulnerability	Reference to the CVE value targeted by the exploit.	—	✔
description	text	Description of the exploit.	—	—
exploit	text	Free text of the exploit.	—	—
exploit-as-attachment	attachment	Attachment of the exploit.	—	—
exploitdb-id	text	Reference to the ExploitDB referencing this exploit.	—	✔
filename	filename	Filename used for the exploit.	✔	✔
level	text	Level of the exploit. ['Unknown', 'Proof-of-Concept', 'Functional', 'Production-ready']	✔	—
reference	link	Reference to the exploit.	✔	✔
software	text	Software impacted	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
title	text	Title of the exploit.	—	—

exploit-poc

Exploit-poc object describing a proof of concept or exploit of a vulnerability. This object has often a relationship with a vulnerability object.

exploit-poc 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	Multiple
author	text	Author of the exploit - proof of concept	✔	✔
description	text	Description of the exploit - proof of concept	—	—
poc	attachment	Proof of Concept or exploit (as a script, binary or described process)	✔	✔
references	link	External references	—	✔
vulnerable_configuration	text	The vulnerable configuration described in CPE format where the exploit/proof of concept is valid	—	✔

external-impact

External Impact object as described in STIX 2.1 Incident object extension.

external-impact 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	Multiple
criticality	text	Criticality of the impact ['Not Specified', 'False Positive', 'Low', 'Moderate', 'High', 'Extreme']	✔	—
description	text	Additional details about the impact.	—	—
end_time	datetime	The date and time the impact was last recorded.	—	—
end_time_fidelity	text	Level of fidelity that the `end_time` is recorded in. ['day', 'hour', 'minute', 'month', 'second', 'year']	✔	—
impact_type	text	Type of impact. ['economic', 'emergency-services', 'foreign-relations', 'national-secuirty', 'public-confidence', 'public-health', 'public-safety']	✔	—
recoverability	text	Recoverability of this particular impact with respect to feasibility and required time and resources. ['extended', 'not-applicable', 'not-recoverable', 'regular', 'supplemented']	✔	—
start_time	datetime	The date and time the impact was first recorded.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
start_time_fidelity	text	Level of fidelity that the `start_time` is recorded in. ['day', 'hour', 'minute', 'month', 'second', 'year']	✔	—

facebook-account

Facebook account.

facebook-account 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	Multiple
account-id	text	Account id.	—	—
account-name	text	Account name.	—	—
archive	link	Archive of the account (Internet Archive, Archive.is, etc).	✔	✔
attachment	attachment	A screen capture or exported list of contacts etc.	—	✔
description	text	A description of the user.	—	—
link	link	Original link to the page (supposed harmless).	—	—
url	url	Original URL location of the page (potentially malicious).	—	—
user-avatar	attachment	A user profile picture or avatar.	—	✔

facebook-group

Public or private facebook group.

facebook-group 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	Multiple
administrator	text	A user account who is an owner or admin of the group.	—	✔
archive	link	Archive of the original group (Internet Archive, Archive.is, etc).	✔	✔
attachment	attachment	A screen capture or exported list of contacts, group members, etc.	—	✔
creator	text	The user account that created the group.	—	—
description	text	A description of the group, channel or community.	—	—
embedded-link	url	Link embedded in the group description (potentially malicious).	—	✔
embedded-safe-link	link	Link embedded in the group description (supposed safe).	—	✔
group-alias	text	Aliases or previous names of group.	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
group-name	text	The name of the group, channel or community.	➖	➖
group-type	text	Facebook group type, e.g. general, buy and sell etc.	➖	➖
hashtag	text	Hashtag used to identify or promote the group.	➖	✔
id	text	Unique identified of the group.	➖	➖
link	link	Original link to the group (supposed harmless).	➖	➖
privacy	text	Group privacy: public, closed, secret. ['Public', 'Closed', 'Secret']	➖	➖
url	url	Original URL location of the group (potentially malicious).	➖	➖

facebook-page

Facebook page.

facebook-page 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	Multiple
archive	link	Archive of the original page (Internet Archive, Archive.is, etc).	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
attachment	attachment	A screen capture or exported list of contacts, page members, etc.	➖	✔
contact-detail	url	Contact url listed on about page.	➖	✔
creator	text	The user account that created the page.	➖	➖
description	text	A description of the page.	➖	➖
embedded-link	url	Link embedded in the page description (potentially malicious).	➖	✔
embedded-safe-link	link	Link embedded in the page description (supposed safe).	➖	✔
event	text	Event announcement on page.	➖	✔
hashtag	text	Hashtag used to identify or promote the page.	➖	✔
link	link	Original link to the page (supposed harmless).	➖	➖
page-alias	text	Aliases or previous names of page.	➖	✔
page-id	text	Page id (without the @).	➖	➖
page-name	text	The name of the page.	➖	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
page-type	text	Facebook page type, e.g. community, product etc.	—	—
related-page-id	text	id of a page listed as related to this one (without the @).	—	✔
related-page-name	text	name of a page listed as related to this one.	—	✔
team-member	text	A user account who is a member of the page.	—	✔
url	url	Original URL location of the page (potentially malicious).	—	—

facebook-post

Post on a Facebook wall.

facebook-post 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	Multiple
archive	link	Archive of the original document (Internet Archive, Archive.is, etc).	—	✔
attachment	attachment	The facebook post file or screen capture.	—	✔
embedded-link	url	Link in the facebook post	—	✔
embedded-safe-link	link	Safe link in the facebook post	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
hashtag	text	Hashtag embedded in the facebook post	➖	✔
in-reply-to-display-name	text	The user display name of the facebook this post shares.	➖	✔
in-reply-to-status-id	text	The facebook ID of the post that this post shares.	➖	✔
in-reply-to-user-id	text	The user ID of the facebook this post shares.	➖	✔
language	text	The language of the post.	✔	✔
link	link	Original link to the facebook post (supposed harmless).	➖	✔
post	text	Raw text of the post.	➖	➖
post-id	text	The facebook post id.	➖	➖
post-location	text	id of the group, page or wall the post was posted to.	➖	➖
removal-date	datetime	When the facebook post was removed.	➖	➖
url	url	Original URL of the facebook post, e.g. link shortener (potentially malicious).	➖	✔
user-id	text	Id of the account who posted.	➖	➖
user-name	text	Display name of the account who posted.	➖	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
username	text	Username who posted the facebook post	—	—
username-quoted	text	Username who is quoted in the facebook post.	—	✔

facebook-reaction

Reaction to facebook posts.

facebook-reaction 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	Multiple
link	link	Link to the user account which did the reaction.	—	—
name	text	The name of A user account which did the reaction.	—	—
type	text	Type of reaction. ['like', 'love', 'sad', 'haha', 'wow', 'care']	✔	—

facial-composite

An object which describes a facial composite.

facial-composite 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	Multiple
facial-composite	attachment	Facial composite image.	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
technique	text	Construction technique of the facial composite. ['E-FIT', 'PROfit', 'Sketch', 'Photofit', 'EvoFIT', 'PortraitPad']	✔	—
text	text	A description of the facial composite.	✔	—

fail2ban

Fail2ban event.

fail2ban 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	Multiple
attack-type	text	Type of the attack	✔	—
banned-ip	ip-src	IP Address banned by fail2ban	—	—
failures	counter	Amount of failures that lead to the ban.	✔	—
logfile	attachment	Full logfile related to the attack.	✔	—
logline	text	Example log line that caused the ban.	✔	—
processing-timestamp	datetime	Timestamp of the report	✔	—
sensor	text	Identifier of the sensor	✔	—
victim	text	Identifier of the victim	✔	—

favicon

A favicon, also known as a shortcut icon, website icon, tab icon, URL icon, or bookmark icon, is a file containing one or more small icons, associated with a particular website or web page. The object template can include the murmur3 hash of the favicon to facilitate correlation.

favicon 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	Multiple
favicon	attachment	The raw favicon file.	—	—
favicon-mmh3	favicon-mmh3	favicon-mmh3 is the murmur3 hash of a favicon as used in Shodan.	—	—
link	link	The original link where the favicon was seen.	—	✔

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	Multiple
access-time	datetime	The last time the file was accessed	—	—
attachment	attachment	A non-malicious file.	—	—
authentihash	authentihash	Authenticode executable signature hash	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
certificate	x509-fingerprint-sha1	Certificate value if the binary is signed with another authentication scheme than authenticode	➖	➖
compilation-timestamp	datetime	Compilation timestamp	➖	➖
creation-time	datetime	Creation time of the file	➖	➖
dom-hash	dom-hash	Dom-hash of the file	➖	➖
entropy	float	Entropy of the whole file	✔	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
file-encoding	text	Encoding format of the file ['Adobe-Standard-Encoding', 'Adobe-Symbol-Encoding', 'Amiga-1251', 'ANSI_X3.110-1983', 'ASMO_449', 'Big5', 'Big5-HKSCS', 'BOCU-1', 'BRF', 'BS_4730', 'BS_viewdata', 'CESU-8', 'CP50220', 'CP51932', 'CSA_Z243.4-1985-1', 'CSA_Z243.4-1985-2', 'CSA_Z243.4-1985-gr', 'CSN_369103', 'DEC-MCS', 'DIN_66003', 'dk-us', 'DS_2089', 'EBCDIC-AT-DE', 'EBCDIC-AT-DE-A', 'EBCDIC-CA-FR', 'EBCDIC-DK-NO', 'EBCDIC-DK-NO-A', 'EBCDIC-ES', 'EBCDIC-ES-A', 'EBCDIC-ES-S', 'EBCDIC-FI-SE', 'EBCDIC-FI-SE-A', 'EBCDIC-FR', 'EBCDIC-IT', 'EBCDIC-PT', 'EBCDIC-UK', 'EBCDIC-US', 'ECMA-cyrillic', 'ES', 'ES2', 'EUC-KR', 'Extended_UNIX_Code_Fixed_Width_for_Japanese', 'Extended_UNIX_Code_Packed_Format_for_Japanese',	✔	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
filename	filename	Filename on disk	✔	✔
fullpath	text	Complete path of the filename including the filename	—	✔
imphash	imphash	Hash (md5) calculated from the PE import table	—	—
malware-sample	malware-sample	The file itself (binary)	—	—
md5	md5	[Insecure] MD5 hash (128 bits)	—	—
mimetype	mime-type	Mime type	✔	—
modification-time	datetime	Last time the file was modified	—	—
path	text	Path of the filename complete or partial	✔	✔
pattern-in-file	pattern-in-file	Pattern that can be found in the file	—	✔
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	—	—
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	—	—
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	—	—
sha3-224	sha3-224	Secure Hash Algorithm 3 (224 bits)	—	—
sha3-256	sha3-256	Secure Hash Algorithm 3 (256 bits)	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
sha3-384	sha3-384	Secure Hash Algorithm 3 (384 bits)	—	—
sha3-512	sha3-512	Secure Hash Algorithm 3 (512 bits)	—	—
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	—	—
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	—	—
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	—	—
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	—	—
size-in-bytes	size-in-bytes	Size of the file, in bytes	✔	—
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	—	—
state	text	State of the file ['Malicious', 'Harmless', 'Signed', 'Revoked', 'Expired', 'Trusted']	✔	✔
telfhash	telfhash	telfhash - Symbol hash for ELF files.	—	—
text	text	Free text value to attach to the file	✔	✔
tlsh	tlsh	Fuzzy hash by Trend Micro: Locality Sensitive Hash	—	—
vhash	vhash	vhash by VirusTotal	—	—

flowintel-cm-case

A case as defined by flowintel-cm.

flowintel-cm-case 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	Multiple
case-owner-org-name	text	Name of the organisation that created the case.	✔	—
case-owner-org-uuid	text	UUID of the organisation that created the case.	✔	—
case-uuid	text	UUID of the case	✔	—
creation-date	datetime	Creation date of the case	✔	—
deadline	datetime	Deadline of the case	✔	—
description	text	A description of the case	✔	—
finish-date	datetime	Finish date of the case	✔	—
notes	text	Notes of the case	✔	—
origin-url	url	Origin of the case	✔	—
recurring-type	text	Recurring type ['once', 'weekly', 'daily', 'monthly']	✔	—
status	text	Status of the case ['created', 'ongoing', 'recurring', 'unavailable', 'rejected', 'finished']	✔	—
title	text	Title of the case	✔	—

flowintel-cm-task

A task as defined by flowintel-cm.

flowintel-cm-task 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	Multiple
case-uuid	text	UUID of the parent case	✔	—
creation-date	datetime	Creation date of the task	✔	—
deadline	datetime	Deadline of the task	✔	—
description	text	A description of the task	✔	—
file	attachment	File	✔	✔
finish-date	datetime	Finish date of the task	✔	—
origin-url	url	Origin of the task	✔	—
status	text	Status of the task ['created', 'ongoing', 'recurring', 'unavailable', 'rejected', 'finished']	✔	—
task-uuid	text	UUID of the task	✔	—
title	text	Title of the task	✔	—
url	url	An url to an external tool	✔	—

flowintel-cm-task-note

A task's note as defined by flowintel-cm.

flowintel-cm-task-note 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	Multiple
note	text	Notes of the task	✔	✔
note-uuid	text	UUID of the note	✔	—
origin-url	url	Origin of the task	✔	—
task-uuid	text	UUID of the parent task	✔	—

forensic-case

An object template to describe a digital forensic case.

forensic-case 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	Multiple
additional-comments	text	Comments.	✔	—
analysis-start-date	datetime	Date when the analysis began.	✔	—
case-name	text	Name to address the case.	—	—
case-number	text	Any unique number assigned to the case for unique identification.	—	—
name-of-the-analyst	text	Name(s) of the analyst assigned to the case.	✔	✔
references	link	External references	—	✔

forensic-evidence

An object template to describe a digital forensic evidence.

forensic-evidence 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	Multiple
acquisition-method	text	Method used for acquisition of the evidence. ['Live acquisition', 'Dead/Offline acquisition', 'Physical collection', 'Logical collection', 'File system extraction', 'Chip-off', 'Other']	✔	➖
acquisition-tools	text	Tools used for acquisition of the evidence. ['dd', 'dc3dd', 'dcfldd', 'EnCase', 'FTK Imager', 'FDAS', 'TrueBack', 'Guymager', 'IXimager', 'Other']	✔	✔
additional-comments	text	Comments.	✔	➖
case-number	text	A unique number assigned to the case for unique identification.	➖	➖
evidence-number	text	A unique number assigned to the evidence for unique identification.	➖	➖
name	text	Name of the evidence acquired.	➖	➖
references	link	External references	➖	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
type	text	Evidence type. ['Computer', 'Network', 'Mobile Device', 'Multimedia', 'Cloud', 'IoT', 'Other']	✔	✔

forged-document

Object describing a forged document.

forged-document 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	Multiple
archive	link	Archive of the original document (Internet Archive, Archive.is, etc).	—	✔
attachment	attachment	The forged document file.	—	—
document-name	text	Title of the document.	—	—
document-text	text	Raw text of document	—	—
document-type	text	The type of document (not the file type). ['email', 'letterhead', 'speech', 'literature', 'blog', 'microblog', 'photo', 'audio', 'invoice', 'receipt', 'other']	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
first-seen	datetime	When the document has been accessible or seen for the first time.	✔	—
last-seen	datetime	When the document has been accessible or seen for the last time.	✔	—
link	link	Original link into the document (Supposed harmless)	—	—
objective	text	Objective of the forged document. ['Disinformation', 'Advertising', 'Parody', 'Other']	✔	✔
purpose-of-document	text	What the document is used for. ['Identification', 'Travel', 'Health', 'Legal', 'Financial', 'Government', 'Military', 'Media', 'Communication', 'Other']	✔	✔
url	url	Original URL location of the document (potentially malicious)	—	—

ftm-Airplane

An airplane, helicopter or other flying vehicle.

ftm-Airplane 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	Multiple
address	text	Address	—	✔
alephUrl	url	Aleph URL	—	✔
alias	text	Other name	—	✔
amount	float	Amount	✔	✔
amountEur	float	Amount in EUR	✔	✔
amountUsd	float	Amount in USD	✔	✔
buildDate	text	Build Date	—	✔
country	text	Country	—	✔
currency	text	Currency	✔	✔
description	text	Description	✔	✔
icaoCode	text	ICAO aircraft type designator	✔	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	—	✔
keywords	text	Keywords	✔	✔
manufacturer	text	Manufacturer	✔	✔
model	text	Model	✔	✔
modifiedAt	text	Modified on	—	✔
name	text	Name	—	✔
notes	text	Notes	✔	✔
previousName	text	Previous name	—	✔
program	text	Program	✔	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
registrationDate	text	Registration Date	—	✔
registrationNumber	text	Registration Number	—	✔
retrievedAt	text	Retrieved on	—	✔
serialNumber	text	Serial Number	—	✔
sourceUrl	url	Source link	—	✔
summary	text	Summary	✔	✔
topics	text	Topics	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
type	text	Type	✔	✔
weakAlias	text	Weak alias	✔	✔
wikidataId	text	Wikidata ID	—	✔
wikipediaUrl	url	Wikipedia Article	—	✔

ftm-Assessment

Assessment with meta-data.

ftm-Assessment 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	Multiple
address	text	Address	—	✔
alephUrl	url	Aleph URL	—	✔
alias	text	Other name	—	✔
assessmentId	text	Assessment ID	✔	✔
country	text	Country	—	✔
description	text	Description	✔	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	—	✔
keywords	text	Keywords	✔	✔
modifiedAt	text	Modified on	—	✔
name	text	Name	—	✔
notes	text	Notes	✔	✔
previousName	text	Previous name	—	✔
program	text	Program	✔	✔
publishDate	text	Date of publishing	—	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
retrievedAt	text	Retrieved on	—	✔
sourceUrl	url	Source link	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
summary	text	Summary	✔	✔
topics	text	Topics	—	✔
weakAlias	text	Weak alias	✔	✔
wikidataId	text	Wikidata ID	—	✔
wikipediaUrl	url	Wikipedia Article	—	✔

ftm-Asset

A piece of property which can be owned and assigned a monetary value.

ftm-Asset 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	Multiple
address	text	Address	—	✔
alephUrl	url	Aleph URL	—	✔
alias	text	Other name	—	✔
amount	float	Amount	✔	✔
amountEur	float	Amount in EUR	✔	✔
amountUsd	float	Amount in USD	✔	✔
country	text	Country	—	✔
currency	text	Currency	✔	✔
description	text	Description	✔	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	—	✔
keywords	text	Keywords	✔	✔
modifiedAt	text	Modified on	—	✔
name	text	Name	—	✔
notes	text	Notes	✔	✔
previousName	text	Previous name	—	✔
program	text	Program	✔	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
retrievedAt	text	Retrieved on	—	✔
sourceUrl	url	Source link	—	✔
summary	text	Summary	✔	✔
topics	text	Topics	—	✔
weakAlias	text	Weak alias	✔	✔
wikidataId	text	Wikidata ID	—	✔
wikipediaUrl	url	Wikipedia Article	—	✔

ftm-Associate

Non-family association between two people.

ftm-Associate 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	Multiple
alephUrl	url	Aleph URL	—	✔
date	text	Date	—	✔
description	text	Description	✔	✔
endDate	text	End date	—	✔
indexText	text	Index text	✔	✔
modifiedAt	text	Modified on	—	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
recordId	text	Record ID	✔	✔
relationship	text	Nature of the association	✔	✔
retrievedAt	text	Retrieved on	—	✔
sourceUrl	url	Source URL	—	✔
startDate	text	Start date	—	✔
summary	text	Summary	✔	✔

ftm-Audio

Audio with meta-data.

ftm-Audio 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	Multiple
address	text	Address	–	✔
alephUrl	url	Aleph URL	–	✔
alias	text	Other name	–	✔
author	text	The original author, not the uploader	✔	✔
authoredAt	text	Authored on	–	✔
companiesMentioned	text	Detected companies	–	✔
contentHash	sha1	SHA1 hash of the data	–	✔
country	text	Country	–	✔
crawler	text	The crawler used to acquire this file	✔	✔
date	text	If not otherwise specified	–	✔
description	text	Description	✔	✔
detectedCountry	text	Detected country	–	✔
detectedLanguage	text	Detected language	✔	✔
duration	float	Duration of the audio in ms	✔	✔
emailMentioned	email-src	Detected e-mail addresses	–	✔
encoding	text	File encoding	✔	✔
extension	text	File extension	✔	✔
fileName	text	File name	✔	✔
fileSize	float	File size	✔	✔
generator	text	The program used to generate this file	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
ibanMentioned	iban	Detected IBANs	—	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	—	✔
ipMentioned	ip-src	Detected IP addresses	—	✔
keywords	text	Keywords	✔	✔
language	text	Language	✔	✔
locationMentioned	text	Detected locations	—	✔
messageId	text	Message ID of a document; unique in most cases	✔	✔
mimeType	mime-type	MIME type	✔	✔
modifiedAt	text	Modified on	—	✔
name	text	Name	—	✔
namesMentioned	text	Detected names	—	✔
notes	text	Notes	✔	✔
peopleMentioned	text	Detected people	—	✔
phoneMentioned	phone-number	Detected phones	—	✔
previousName	text	Previous name	—	✔
processingError	text	Processing error	✔	✔
processingStatus	text	Processing status	✔	✔
program	text	Program	✔	✔
publishedAt	text	Published on	—	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
retrievedAt	text	Retrieved on	—	✔
samplingRate	float	Sampling rate of the audio in Hz	✔	✔
sourceUrl	url	Source link	—	✔
summary	text	Summary	✔	✔
title	text	Title	✔	✔
topics	text	Topics	—	✔
weakAlias	text	Weak alias	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
wikidataId	text	Wikidata ID	—	✔
wikipediaUrl	url	Wikipedia Article	—	✔

ftm-BankAccount

An account held at a bank and controlled by an owner. This may also be used to describe more complex arrangements like correspondent bank settlement accounts.

ftm-BankAccount 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	Multiple
accountNumber	text	Account Number	—	✔
accountType	text	Account Type	✔	✔
address	text	Address	—	✔
alephUrl	url	Aleph URL	—	✔
alias	text	Other name	—	✔
amount	float	Amount	✔	✔
amountEur	float	Amount in EUR	✔	✔
amountUsd	float	Amount in USD	✔	✔
balance	float	Balance	✔	✔
bankAddress	text	Bank Address	✔	✔
bankName	text	Bank Name	✔	✔
bic	text	Bank Identifier Code	✔	✔
country	text	Country	—	✔
currency	text	Currency	✔	✔
description	text	Description	✔	✔
iban	iban	IBAN	—	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	—	✔
keywords	text	Keywords	✔	✔
modifiedAt	text	Modified on	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
name	text	Name	—	✔
notes	text	Notes	✔	✔
previousName	text	Previous name	—	✔
program	text	Program	✔	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
retrievedAt	text	Retrieved on	—	✔
sourceUrl	url	Source link	—	✔
summary	text	Summary	✔	✔
topics	text	Topics	—	✔
weakAlias	text	Weak alias	✔	✔
wikidataId	text	Wikidata ID	—	✔
wikipediaUrl	url	Wikipedia Article	—	✔

ftm-Call

Phone call object template including the call and all associated meta-data.

ftm-Call 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	Multiple
alephUrl	url	Aleph URL	—	✔
callerNumber	phone-number	Caller's Number	—	✔
date	text	Date	—	✔
description	text	Description	✔	✔
duration	float	Call Duration in seconds	✔	✔
endDate	text	End date	—	✔
indexText	text	Index text	✔	✔
modifiedAt	text	Modified on	—	✔
publisher	text	Publishing source	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
publisherUrl	url	Publishing source URL	—	✔
receiverNumber	phone-number	Receiver's Number	—	✔
recordId	text	Record ID	✔	✔
retrievedAt	text	Retrieved on	—	✔
sourceUrl	url	Source URL	—	✔
startDate	text	Start date	—	✔
summary	text	Summary	✔	✔

ftm-Company

A legal entity representing an association of people, whether natural, legal or a mixture of both, with a specific objective.

ftm-Company 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	Multiple
address	text	Address	—	✔
alephUrl	url	Aleph URL	—	✔
alias	text	Other name	—	✔
amount	float	Amount	✔	✔
amountEur	float	Amount in EUR	✔	✔
amountUsd	float	Amount in USD	✔	✔
bikCode	text	Russian bank account code	✔	✔
bvdId	text	Bureau van Dijk ID	—	✔
caemCode	text	(RO) What kind of activity a legal entity is allowed to develop	✔	✔
capital	text	Capital	✔	✔
cikCode	text	US SEC Central Index Key	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
classification	text	Classification	✔	✔
coatoCode	text	COATO / SOATO / OKATO	—	✔
country	text	Country	—	✔
currency	text	Currency	✔	✔
description	text	Description	✔	✔
dissolutionDate	text	The date the legal entity was dissolved, if applicable	—	✔
dunsCode	text	Dun & Bradstreet identifier	—	✔
email	email-src	Email address	—	✔
fnsCode	text	(RU, ФНС) Federal Tax Service related info	—	✔
fssCode	text	(RU, ФСС) Social Security	✔	✔
ibcRuc	text	ibcRUC	—	✔
icijId	text	ID according to International Consortium for Investigative Journalists	✔	✔
idNumber	text	ID number of any applicable ID	—	✔
incorporationDate	text	The date the legal entity was incorporated	—	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	—	✔
innCode	text	Russian company ID	—	✔
ipoCode	text	IPO	—	✔
irsCode	text	US tax ID	—	✔
jibCode	text	Yugoslavia company ID	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
jurisdiction	text	Jurisdiction	➖	✔
keywords	text	Keywords	✔	✔
kppCode	text	(RU, КПП) in addition to INN for orgs; reason for registration at FNS	➖	✔
legalForm	text	Legal form	✔	✔
mainCountry	text	Primary country of this entity	➖	✔
mbsCode	text	MBS	➖	✔
modifiedAt	text	Modified on	➖	✔
name	text	Name	➖	✔
notes	text	Notes	✔	✔
ogrnCode	text	Major State Registration Number	➖	✔
okopfCode	text	(RU, ОКОПФ) What kind of business entity	✔	✔
okpoCode	text	Russian industry classifier	➖	✔
oksmCode	text	Russian (ОКСМ) countries classifer	✔	✔
okvedCode	text	(RU, ОКВЭД) Economical activity classifier. OKVED2 is the same but newer	✔	✔
opencorporatesUrl	url	OpenCorporates URL	➖	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
pfrNumber	text	(RU, ПФР) Pension Fund Registration number. AAA-BBB-CCCCCC, where AAA is organisation region, BBB is district, CCCCCC number at a specific branch	➖	✔
phone	phone-number	Phone number	➖	✔
previousName	text	Previous name	➖	✔
program	text	Program	✔	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	➖	✔
registrationNumber	text	Registration number	➖	✔
retrievedAt	text	Retrieved on	➖	✔
sector	text	Sector	✔	✔
sourceUrl	url	Source link	➖	✔
status	text	Status	✔	✔
summary	text	Summary	✔	✔
swiftBic	text	Bank identifier code	➖	✔
taxNumber	text	Tax identification number	➖	✔
taxStatus	text	Tax status	✔	✔
topics	text	Topics	➖	✔
vatCode	text	(EU) VAT number	➖	✔
voenCode	text	Azerbaijan taxpayer ID	➖	✔
weakAlias	text	Weak alias	✔	✔
website	url	Website address	➖	✔
wikidataId	text	Wikidata ID	➖	✔
wikipediaUrl	url	Wikipedia Article	➖	✔

ftm-Contract

An contract or contract lot issued by an authority. Multiple lots may be awarded to different suppliers (see ContractAward). .

ftm-Contract 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	Multiple
address	text	Address	–	✔
alephUrl	url	Aleph URL	–	✔
alias	text	Other name	–	✔
amount	float	Amount	✔	✔
amountEur	float	Amount in EUR	✔	✔
amountUsd	float	Amount in USD	✔	✔
cancelled	text	Cancelled?	✔	✔
classification	text	Classification	✔	✔
contractDate	text	Contract date	–	✔
country	text	Country	–	✔
criteria	text	Contract award criteria	✔	✔
currency	text	Currency	✔	✔
description	text	Description	✔	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	–	✔
keywords	text	Keywords	✔	✔
language	text	Language	✔	✔
method	text	Procurement method	✔	✔
modifiedAt	text	Modified on	–	✔
name	text	Contract name	✔	✔
notes	text	Notes	✔	✔
noticeId	text	Contract Award Notice ID	✔	✔
numberAwards	text	Number of awards	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
previousName	text	Previous name	✖	✔
procedure	text	Contract procedure	✔	✔
procedureNumber	text	Procedure number	✔	✔
program	text	Program	✔	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	✖	✔
retrievedAt	text	Retrieved on	✖	✔
sourceUrl	url	Source link	✖	✔
status	text	Procurement status	✔	✔
summary	text	Summary	✔	✔
title	text	Contract title	✔	✔
topics	text	Topics	✖	✔
type	text	Type of contract. Potentially W (Works), U (Supplies), S (Services).	✔	✔
weakAlias	text	Weak alias	✔	✔
wikidataId	text	Wikidata ID	✖	✔
wikipediaUrl	url	Wikipedia Article	✖	✔

ftm-ContractAward

A contract or contract lot as awarded to a supplier.

ftm-ContractAward 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	Multiple
alephUrl	url	Aleph URL	✖	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
amended	text	Was this award amended, modified or updated by a subsequent document?	✔	✔
amount	float	Amount	✔	✔
amountEur	float	Amount in EUR	✔	✔
amountUsd	float	Amount in USD	✔	✔
cpvCode	text	Contract Procurement Vocabulary (what type of goods/services, EU)	✔	✔
currency	text	Currency	✔	✔
date	text	Date	➖	✔
decisionReason	text	Decision reason	✔	✔
description	text	Description	✔	✔
documentNumber	text	Document number	✔	✔
documentType	text	Document type	✔	✔
endDate	text	End date	➖	✔
indexText	text	Index text	✔	✔
lotNumber	text	Lot number	✔	✔
modifiedAt	text	Modified on	➖	✔
nutsCode	text	Nomencalture of Territorial Units for Statistics (NUTS)	✔	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	➖	✔
recordId	text	Record ID	✔	✔
retrievedAt	text	Retrieved on	➖	✔
role	text	Role	✔	✔
sourceUrl	url	Source URL	➖	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
startDate	text	Start date	—	✔
status	text	Status	✔	✔
summary	text	Summary	✔	✔

ftm-CourtCase

Court case.

ftm-CourtCase 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	Multiple
address	text	Address	—	✔
alephUrl	url	Aleph URL	—	✔
alias	text	Other name	—	✔
caseNumber	text	Case number	—	✔
category	text	Category	✔	✔
closeDate	text	Close date	—	✔
country	text	Country	—	✔
court	text	Court	✔	✔
description	text	Description	✔	✔
fileDate	text	File date	—	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	—	✔
keywords	text	Keywords	✔	✔
modifiedAt	text	Modified on	—	✔
name	text	Name	—	✔
notes	text	Notes	✔	✔
previousName	text	Previous name	—	✔
program	text	Program	✔	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
retrievedAt	text	Retrieved on	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
sourceUrl	url	Source link	—	✔
status	text	Status	✔	✔
summary	text	Summary	✔	✔
topics	text	Topics	—	✔
type	text	Type	✔	✔
weakAlias	text	Weak alias	✔	✔
wikidataId	text	Wikidata ID	—	✔
wikipediaUrl	url	Wikipedia Article	—	✔

ftm-CourtCaseParty

Court Case Party.

ftm-CourtCaseParty 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	Multiple
alephUrl	url	Aleph URL	—	✔
date	text	Date	—	✔
description	text	Description	✔	✔
endDate	text	End date	—	✔
indexText	text	Index text	✔	✔
modifiedAt	text	Modified on	—	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
recordId	text	Record ID	✔	✔
retrievedAt	text	Retrieved on	—	✔
role	text	Role	✔	✔
sourceUrl	url	Source URL	—	✔
startDate	text	Start date	—	✔
status	text	Status	✔	✔
summary	text	Summary	✔	✔

ftm-Debt

A monetary debt between two parties.

ftm-Debt 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	Multiple
alephUrl	url	Aleph URL	—	✔
amount	float	Amount	✔	✔
amountEur	float	Amount in EUR	✔	✔
amountUsd	float	Amount in USD	✔	✔
currency	text	Currency	✔	✔
date	text	Date	—	✔
description	text	Description	✔	✔
endDate	text	End date	—	✔
indexText	text	Index text	✔	✔
modifiedAt	text	Modified on	—	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
recordId	text	Record ID	✔	✔
retrievedAt	text	Retrieved on	—	✔
sourceUrl	url	Source URL	—	✔
startDate	text	Start date	—	✔
summary	text	Summary	✔	✔

ftm-Directorship

Directorship.

ftm-Directorship 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	Multiple
alephUrl	url	Aleph URL	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
date	text	Date	–	✔
description	text	Description	✔	✔
endDate	text	End date	–	✔
indexText	text	Index text	✔	✔
modifiedAt	text	Modified on	–	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	–	✔
recordId	text	Record ID	✔	✔
retrievedAt	text	Retrieved on	–	✔
role	text	Role	✔	✔
secretary	text	Secretary	✔	✔
sourceUrl	url	Source URL	–	✔
startDate	text	Start date	–	✔
status	text	Status	✔	✔
summary	text	Summary	✔	✔

ftm-Document

Document.

ftm-Document 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	Multiple
address	text	Address	–	✔
alephUrl	url	Aleph URL	–	✔
alias	text	Other name	–	✔
author	text	The original author, not the uploader	✔	✔
authoredAt	text	Authored on	–	✔
companiesMentioned	text	Detected companies	–	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
contentHash	sha1	SHA1 hash of the data	—	✔
country	text	Country	—	✔
crawler	text	The crawler used to acquire this file	✔	✔
date	text	If not otherwise specified	—	✔
description	text	Description	✔	✔
detectedCountry	text	Detected country	—	✔
detectedLanguage	text	Detected language	✔	✔
emailMentioned	email-src	Detected e-mail addresses	—	✔
encoding	text	File encoding	✔	✔
extension	text	File extension	✔	✔
fileName	text	File name	✔	✔
fileSize	float	File size	✔	✔
generator	text	The program used to generate this file	✔	✔
ibanMentioned	iban	Detected IBANs	—	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	—	✔
ipMentioned	ip-src	Detected IP addresses	—	✔
keywords	text	Keywords	✔	✔
language	text	Language	✔	✔
locationMentioned	text	Detected locations	—	✔
messageId	text	Message ID of a document; unique in most cases	✔	✔
mimeType	mime-type	MIME type	✔	✔
modifiedAt	text	Modified on	—	✔
name	text	Name	—	✔
namesMentioned	text	Detected names	—	✔
notes	text	Notes	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
peopleMentioned	text	Detected people	—	✔
phoneMentioned	phone-number	Detected phones	—	✔
previousName	text	Previous name	—	✔
processingError	text	Processing error	✔	✔
processingStatus	text	Processing status	✔	✔
program	text	Program	✔	✔
publishedAt	text	Published on	—	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
retrievedAt	text	Retrieved on	—	✔
sourceUrl	url	Source link	—	✔
summary	text	Summary	✔	✔
title	text	Title	✔	✔
topics	text	Topics	—	✔
weakAlias	text	Weak alias	✔	✔
wikidataId	text	Wikidata ID	—	✔
wikipediaUrl	url	Wikipedia Article	—	✔

ftm-Documentation

Documentation.

ftm-Documentation 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	Multiple
alephUrl	url	Aleph URL	—	✔
date	text	Date	—	✔
description	text	Description	✔	✔
endDate	text	End date	—	✔
indexText	text	Index text	✔	✔
modifiedAt	text	Modified on	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
recordId	text	Record ID	✔	✔
retrievedAt	text	Retrieved on	—	✔
role	text	Role	✔	✔
sourceUrl	url	Source URL	—	✔
startDate	text	Start date	—	✔
status	text	Status	✔	✔
summary	text	Summary	✔	✔

ftm-EconomicActivity

A foreign economic activity.

ftm-EconomicActivity 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	Multiple
alephUrl	url	Aleph URL	—	✔
ccdNumber	text	Customs Cargo Declaration Number	—	✔
ccdValue	text	Declaration Value	✔	✔
customsAmount	text	Customs Value of goods	✔	✔
customsProcedure	text	Customs Procedure — type of customs clearance	✔	✔
date	text	Date	—	✔
departureCountry	text	Country out of which the goods are transported	—	✔
description	text	Description	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
destinationCountry	text	Final destination for the goods	➖	✔
directionOfTransportation	text	Direction of transportation (import/export)	✔	✔
dollarExchRate	text	USD Exchange Rate for the activity	✔	✔
endDate	text	End date	➖	✔
goodsDescription	text	Description of goods	✔	✔
indexText	text	Index text	✔	✔
invoiceAmount	text	Invoice Value of goods	✔	✔
modifiedAt	text	Modified on	➖	✔
originCountry	text	Country of origin of goods	➖	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	➖	✔
recordId	text	Record ID	✔	✔
retrievedAt	text	Retrieved on	➖	✔
sourceUrl	url	Source URL	➖	✔
startDate	text	Start date	➖	✔
summary	text	Summary	✔	✔
tradingCountry	text	Trading Country of the company which transports the goods via Russian border	➖	✔
vedCode	text	(Код ТН ВЭД) Foreign Economic Activity Commodity Code	➖	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
vedCodeDescription	text	(Описание кода ТН ВЭД) Foreign Economic Activity Commodity Code description	✔	✔

ftm-Email

Email.

ftm-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	Multiple
address	text	Address	—	✔
alephUrl	url	Aleph URL	—	✔
alias	text	Other name	—	✔
author	text	The original author, not the uploader	✔	✔
authoredAt	text	Authored on	—	✔
bcc	text	Blind carbon copy	✔	✔
bodyHtml	text	HTML	✔	✔
bodyText	text	Text	✔	✔
cc	text	Carbon copy	✔	✔
companiesMentioned	text	Detected companies	—	✔
contentHash	sha1	SHA1 hash of the data	—	✔
country	text	Country	—	✔
crawler	text	The crawler used to acquire this file	✔	✔
date	text	If not otherwise specified	—	✔
description	text	Description	✔	✔
detectedCountry	text	Detected country	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
detectedLanguage	text	Detected language	✔	✔
emailMentioned	email-src	Detected e-mail addresses	—	✔
encoding	text	File encoding	✔	✔
extension	text	File extension	✔	✔
fileName	text	File name	✔	✔
fileSize	float	File size	✔	✔
from	text	From	✔	✔
generator	text	The program used to generate this file	✔	✔
headers	text	Raw headers	✔	✔
ibanMentioned	iban	Detected IBANs	—	✔
inReplyTo	text	Message ID of the preceding email in the thread	✔	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	—	✔
ipMentioned	ip-src	Detected IP addresses	—	✔
keywords	text	Keywords	✔	✔
language	text	Language	✔	✔
locationMentioned	text	Detected locations	—	✔
messageId	text	Message ID of a document; unique in most cases	✔	✔
mimeType	mime-type	MIME type	✔	✔
modifiedAt	text	Modified on	—	✔
name	text	Name	—	✔
namesMentioned	text	Detected names	—	✔
notes	text	Notes	✔	✔
peopleMentioned	text	Detected people	—	✔
phoneMentioned	phone-number	Detected phones	—	✔
previousName	text	Previous name	—	✔
processingError	text	Processing error	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
processingStatus	text	Processing status	✔	✔
program	text	Program	✔	✔
publishedAt	text	Published on	—	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
retrievedAt	text	Retrieved on	—	✔
sender	text	Sender	✔	✔
sourceUrl	url	Source link	—	✔
subject	text	Subject	✔	✔
summary	text	Summary	✔	✔
threadTopic	text	Thread topic	✔	✔
title	text	Title	✔	✔
to	text	To	✔	✔
topics	text	Topics	—	✔
weakAlias	text	Weak alias	✔	✔
wikidataId	text	Wikidata ID	—	✔
wikipediaUrl	url	Wikipedia Article	—	✔

ftm-Event

Event.

ftm-Event 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	Multiple
address	text	Address	—	✔
alephUrl	url	Aleph URL	—	✔
alias	text	Other name	—	✔
companiesMentioned	text	Detected companies	—	✔
country	text	Country	—	✔
date	text	Date	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
description	text	Description	✔	✔
detectedCountry	text	Detected country	—	✔
detectedLanguage	text	Detected language	✔	✔
emailMentioned	email-src	Detected e-mail addresses	—	✔
endDate	text	End date	—	✔
ibanMentioned	iban	Detected IBANs	—	✔
important	text	Important	✔	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	—	✔
ipMentioned	ip-src	Detected IP addresses	—	✔
keywords	text	Keywords	✔	✔
location	text	Location	—	✔
locationMentioned	text	Detected locations	—	✔
modifiedAt	text	Modified on	—	✔
name	text	Name	—	✔
namesMentioned	text	Detected names	—	✔
notes	text	Notes	✔	✔
peopleMentioned	text	Detected people	—	✔
phoneMentioned	phone-number	Detected phones	—	✔
previousName	text	Previous name	—	✔
program	text	Program	✔	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
recordId	text	Record ID	✔	✔
retrievedAt	text	Retrieved on	—	✔
sourceUrl	url	Source link	—	✔
startDate	text	Start date	—	✔
summary	text	Summary	✔	✔
topics	text	Topics	—	✔
weakAlias	text	Weak alias	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
wikidataId	text	Wikidata ID	✖	✔
wikipediaUrl	url	Wikipedia Article	✖	✔

ftm-Family

Family relationship between two people.

ftm-Family 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	Multiple
alephUrl	url	Aleph URL	✖	✔
date	text	Date	✖	✔
description	text	Description	✔	✔
endDate	text	End date	✖	✔
indexText	text	Index text	✔	✔
modifiedAt	text	Modified on	✖	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	✖	✔
recordId	text	Record ID	✔	✔
relationship	text	Nature of the relationship, from the person's perspective eg. 'mother', where 'relative' is mother of 'person'.	✔	✔
retrievedAt	text	Retrieved on	✖	✔
sourceUrl	url	Source URL	✖	✔
startDate	text	Start date	✖	✔
summary	text	Summary	✔	✔

ftm-Folder

Folder.

ftm-Folder 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	Multiple
address	text	Address	–	✔
alephUrl	url	Aleph URL	–	✔
alias	text	Other name	–	✔
author	text	The original author, not the uploader	✔	✔
authoredAt	text	Authored on	–	✔
companiesMentioned	text	Detected companies	–	✔
contentHash	sha1	SHA1 hash of the data	–	✔
country	text	Country	–	✔
crawler	text	The crawler used to acquire this file	✔	✔
date	text	If not otherwise specified	–	✔
description	text	Description	✔	✔
detectedCountry	text	Detected country	–	✔
detectedLanguage	text	Detected language	✔	✔
emailMentioned	email-src	Detected e-mail addresses	–	✔
encoding	text	File encoding	✔	✔
extension	text	File extension	✔	✔
fileName	text	File name	✔	✔
fileSize	float	File size	✔	✔
generator	text	The program used to generate this file	✔	✔
ibanMentioned	iban	Detected IBANs	–	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	–	✔
ipMentioned	ip-src	Detected IP addresses	–	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
keywords	text	Keywords	✔	✔
language	text	Language	✔	✔
locationMentioned	text	Detected locations	—	✔
messageId	text	Message ID of a document; unique in most cases	✔	✔
mimeType	mime-type	MIME type	✔	✔
modifiedAt	text	Modified on	—	✔
name	text	Name	—	✔
namesMentioned	text	Detected names	—	✔
notes	text	Notes	✔	✔
peopleMentioned	text	Detected people	—	✔
phoneMentioned	phone-number	Detected phones	—	✔
previousName	text	Previous name	—	✔
processingError	text	Processing error	✔	✔
processingStatus	text	Processing status	✔	✔
program	text	Program	✔	✔
publishedAt	text	Published on	—	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
retrievedAt	text	Retrieved on	—	✔
sourceUrl	url	Source link	—	✔
summary	text	Summary	✔	✔
title	text	Title	✔	✔
topics	text	Topics	—	✔
weakAlias	text	Weak alias	✔	✔
wikidataId	text	Wikidata ID	—	✔
wikipediaUrl	url	Wikipedia Article	—	✔

ftm-HyperText

HyperText.

ftm-HyperText 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	Multiple
address	text	Address	—	✔
alephUrl	url	Aleph URL	—	✔
alias	text	Other name	—	✔
author	text	The original author, not the uploader	✔	✔
authoredAt	text	Authored on	—	✔
bodyHtml	text	HTML	✔	✔
bodyText	text	Text	✔	✔
companiesMentioned	text	Detected companies	—	✔
contentHash	sha1	SHA1 hash of the data	—	✔
country	text	Country	—	✔
crawler	text	The crawler used to acquire this file	✔	✔
date	text	If not otherwise specified	—	✔
description	text	Description	✔	✔
detectedCountry	text	Detected country	—	✔
detectedLanguage	text	Detected language	✔	✔
emailMentioned	email-src	Detected e-mail addresses	—	✔
encoding	text	File encoding	✔	✔
extension	text	File extension	✔	✔
fileName	text	File name	✔	✔
fileSize	float	File size	✔	✔
generator	text	The program used to generate this file	✔	✔
ibanMentioned	iban	Detected IBANs	—	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
ipMentioned	ip-src	Detected IP addresses	—	✔
keywords	text	Keywords	✔	✔
language	text	Language	✔	✔
locationMentioned	text	Detected locations	—	✔
messageId	text	Message ID of a document; unique in most cases	✔	✔
mimeType	mime-type	MIME type	✔	✔
modifiedAt	text	Modified on	—	✔
name	text	Name	—	✔
namesMentioned	text	Detected names	—	✔
notes	text	Notes	✔	✔
peopleMentioned	text	Detected people	—	✔
phoneMentioned	phone-number	Detected phones	—	✔
previousName	text	Previous name	—	✔
processingError	text	Processing error	✔	✔
processingStatus	text	Processing status	✔	✔
program	text	Program	✔	✔
publishedAt	text	Published on	—	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
retrievedAt	text	Retrieved on	—	✔
sourceUrl	url	Source link	—	✔
summary	text	Summary	✔	✔
title	text	Title	✔	✔
topics	text	Topics	—	✔
weakAlias	text	Weak alias	✔	✔
wikidataId	text	Wikidata ID	—	✔
wikipediaUrl	url	Wikipedia Article	—	✔

ftm-Image

Image.

ftm-Image 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	Multiple
address	text	Address	—	✔
alephUrl	url	Aleph URL	—	✔
alias	text	Other name	—	✔
author	text	The original author, not the uploader	✔	✔
authoredAt	text	Authored on	—	✔
bodyText	text	Text	✔	✔
companiesMentioned	text	Detected companies	—	✔
contentHash	sha1	SHA1 hash of the data	—	✔
country	text	Country	—	✔
crawler	text	The crawler used to acquire this file	✔	✔
date	text	If not otherwise specified	—	✔
description	text	Description	✔	✔
detectedCountry	text	Detected country	—	✔
detectedLanguage	text	Detected language	✔	✔
emailMentioned	email-src	Detected e-mail addresses	—	✔
encoding	text	File encoding	✔	✔
extension	text	File extension	✔	✔
fileName	text	File name	✔	✔
fileSize	float	File size	✔	✔
generator	text	The program used to generate this file	✔	✔
ibanMentioned	iban	Detected IBANs	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	—	✔
ipMentioned	ip-src	Detected IP addresses	—	✔
keywords	text	Keywords	✔	✔
language	text	Language	✔	✔
locationMentioned	text	Detected locations	—	✔
messageId	text	Message ID of a document; unique in most cases	✔	✔
mimeType	mime-type	MIME type	✔	✔
modifiedAt	text	Modified on	—	✔
name	text	Name	—	✔
namesMentioned	text	Detected names	—	✔
notes	text	Notes	✔	✔
peopleMentioned	text	Detected people	—	✔
phoneMentioned	phone-number	Detected phones	—	✔
previousName	text	Previous name	—	✔
processingError	text	Processing error	✔	✔
processingStatus	text	Processing status	✔	✔
program	text	Program	✔	✔
publishedAt	text	Published on	—	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
retrievedAt	text	Retrieved on	—	✔
sourceUrl	url	Source link	—	✔
summary	text	Summary	✔	✔
title	text	Title	✔	✔
topics	text	Topics	—	✔
weakAlias	text	Weak alias	✔	✔
wikidataId	text	Wikidata ID	—	✔
wikipediaUrl	url	Wikipedia Article	—	✔

ftm-Land

Land.

ftm-Land 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	Multiple
address	text	Address	—	✔
alephUrl	url	Aleph URL	—	✔
alias	text	Other name	—	✔
amount	float	Amount	✔	✔
amountEur	float	Amount in EUR	✔	✔
amountUsd	float	Amount in USD	✔	✔
area	float	Area	✔	✔
cadastralCode	text	Cadastral code	—	✔
censusBlock	text	Census block	✔	✔
country	text	Country	—	✔
createDate	text	Record date	—	✔
currency	text	Currency	✔	✔
description	text	Description	✔	✔
encumbrance	text	An encumbrance is a right to, interest in, or legal liability on real property that does not prohibit passing title to the property but that diminishes its value.	✔	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	—	✔
keywords	text	Keywords	✔	✔
landType	text	Land type	✔	✔
latitude	float	Latitude	✔	✔
longitude	float	Longitude	✔	✔
modifiedAt	text	Modified on	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
name	text	Name	➖	✔
notes	text	Notes	✔	✔
previousName	text	Previous name	➖	✔
program	text	Program	✔	✔
propertyType	text	Property type	✔	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	➖	✔
registrationNumber	text	Registration number	➖	✔
retrievedAt	text	Retrieved on	➖	✔
sourceUrl	url	Source link	➖	✔
summary	text	Summary	✔	✔
tenure	text	Tenure	✔	✔
titleNumber	text	Title number	➖	✔
topics	text	Topics	➖	✔
weakAlias	text	Weak alias	✔	✔
wikidataId	text	Wikidata ID	➖	✔
wikipediaUrl	url	Wikipedia Article	➖	✔

ftm-LegalEntity

A legal entity may be a person or a company.

ftm-LegalEntity 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	Multiple
address	text	Address	➖	✔
alephUrl	url	Aleph URL	➖	✔
alias	text	Other name	➖	✔
bvdId	text	Bureau van Dijk ID	➖	✔
classification	text	Classification	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
country	text	Country	➖	✔
description	text	Description	✔	✔
dissolutionDate	text	The date the legal entity was dissolved, if applicable	➖	✔
dunsCode	text	Dun & Bradstreet identifier	➖	✔
email	email-src	Email address	➖	✔
icijId	text	ID according to International Consortium for Investigative Journalists	✔	✔
idNumber	text	ID number of any applicable ID	➖	✔
incorporationDate	text	The date the legal entity was incorporated	➖	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	➖	✔
innCode	text	Russian company ID	➖	✔
jurisdiction	text	Country or region in which this entity operates	➖	✔
keywords	text	Keywords	✔	✔
legalForm	text	Legal form	✔	✔
mainCountry	text	Primary country of this entity	➖	✔
modifiedAt	text	Modified on	➖	✔
name	text	Name	➖	✔
notes	text	Notes	✔	✔
okpoCode	text	Russian industry classifier	➖	✔
opencorporatesUrl	url	OpenCorporates URL	➖	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
phone	phone-number	Phone number	—	✔
previousName	text	Previous name	—	✔
program	text	Program	✔	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
registrationNumber	text	Company registration number	—	✔
retrievedAt	text	Retrieved on	—	✔
sector	text	Sector	✔	✔
sourceUrl	url	Source link	—	✔
status	text	Status	✔	✔
summary	text	Summary	✔	✔
swiftBic	text	Bank identifier code	—	✔
taxNumber	text	Tax identification number	—	✔
taxStatus	text	Tax status	✔	✔
topics	text	Topics	—	✔
vatCode	text	(EU) VAT number	—	✔
weakAlias	text	Weak alias	✔	✔
website	url	Website address	—	✔
wikidataId	text	Wikidata ID	—	✔
wikipediaUrl	url	Wikipedia Article	—	✔

ftm-License

A grant of land, rights or property. A type of Contract.

ftm-License 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	Multiple
address	text	Address	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
alephUrl	url	Aleph URL	—	✔
alias	text	Other name	—	✔
amount	float	Amount	✔	✔
amountEur	float	Amount in EUR	✔	✔
amountUsd	float	Amount in USD	✔	✔
area	text	Area	✔	✔
cancelled	text	Cancelled?	✔	✔
classification	text	Classification	✔	✔
commodities	text	Commodities	✔	✔
contractDate	text	Contract date	—	✔
country	text	Country	—	✔
criteria	text	Contract award criteria	✔	✔
currency	text	Currency	✔	✔
description	text	Description	✔	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	—	✔
keywords	text	Keywords	✔	✔
language	text	Language	✔	✔
method	text	Procurement method	✔	✔
modifiedAt	text	Modified on	—	✔
name	text	Contract name	✔	✔
notes	text	Notes	✔	✔
noticeId	text	Contract Award Notice ID	✔	✔
numberAwards	text	Number of awards	✔	✔
previousName	text	Previous name	—	✔
procedure	text	Contract procedure	✔	✔
procedureNumber	text	Procedure number	✔	✔
program	text	Program	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
retrievedAt	text	Retrieved on	—	✔
reviewDate	text	License review date	✔	✔
sourceUrl	url	Source link	—	✔
status	text	Procurement status	✔	✔
summary	text	Summary	✔	✔
title	text	Contract title	✔	✔
topics	text	Topics	—	✔
type	text	Type of contract. Potentially W (Works), U (Supplies), S (Services).	✔	✔
weakAlias	text	Weak alias	✔	✔
wikidataId	text	Wikidata ID	—	✔
wikipediaUrl	url	Wikipedia Article	—	✔

ftm-Membership

Membership.

ftm-Membership 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	Multiple
alephUrl	url	Aleph URL	—	✔
date	text	Date	—	✔
description	text	Description	✔	✔
endDate	text	End date	—	✔
indexText	text	Index text	✔	✔
modifiedAt	text	Modified on	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
recordId	text	Record ID	✔	✔
retrievedAt	text	Retrieved on	—	✔
role	text	Role	✔	✔
sourceUrl	url	Source URL	—	✔
startDate	text	Start date	—	✔
status	text	Status	✔	✔
summary	text	Summary	✔	✔

ftm-Message

Message.

ftm-Message 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	Multiple
address	text	Address	—	✔
alephUrl	url	Aleph URL	—	✔
alias	text	Other name	—	✔
author	text	The original author, not the uploader	✔	✔
authoredAt	text	Authored on	—	✔
bodyHtml	text	HTML	✔	✔
bodyText	text	Text	✔	✔
companiesMentioned	text	Detected companies	—	✔
contentHash	sha1	SHA1 hash of the data	—	✔
country	text	Country	—	✔
crawler	text	The crawler used to acquire this file	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
date	text	If not otherwise specified	—	✔
description	text	Description	✔	✔
detectedCountry	text	Detected country	—	✔
detectedLanguage	text	Detected language	✔	✔
emailMentioned	email-src	Detected e-mail addresses	—	✔
encoding	text	File encoding	✔	✔
endDate	text	End date	—	✔
extension	text	File extension	✔	✔
fileName	text	File name	✔	✔
fileSize	float	File size	✔	✔
generator	text	The program used to generate this file	✔	✔
ibanMentioned	iban	Detected IBANs	—	✔
inReplyTo	text	Message ID of the preceding message in the thread	✔	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	—	✔
ipMentioned	ip-src	Detected IP addresses	—	✔
keywords	text	Keywords	✔	✔
language	text	Language	✔	✔
locationMentioned	text	Detected locations	—	✔
messageId	text	Message ID of a document; unique in most cases	✔	✔
metadata	text	Metadata	✔	✔
mimeType	mime-type	MIME type	✔	✔
modifiedAt	text	Modified on	—	✔
name	text	Name	—	✔
namesMentioned	text	Detected names	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
notes	text	Notes	✔	✔
peopleMentioned	text	Detected people	—	✔
phoneMentioned	phone-number	Detected phones	—	✔
previousName	text	Previous name	—	✔
processingError	text	Processing error	✔	✔
processingStatus	text	Processing status	✔	✔
program	text	Program	✔	✔
publishedAt	text	Published on	—	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
recordId	text	Record ID	✔	✔
retrievedAt	text	Retrieved on	—	✔
sourceUrl	url	Source link	—	✔
startDate	text	Start date	—	✔
subject	text	Subject	✔	✔
summary	text	Summary	✔	✔
threadTopic	text	Thread topic	✔	✔
title	text	Title	✔	✔
topics	text	Topics	—	✔
weakAlias	text	Weak alias	✔	✔
wikidataId	text	Wikidata ID	—	✔
wikipediaUrl	url	Wikipedia Article	—	✔

ftm-Organization

Organization.

ftm-Organization 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	Multiple
address	text	Address	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
alephUrl	url	Aleph URL	—	✔
alias	text	Other name	—	✔
bvdId	text	Bureau van Dijk ID	—	✔
classification	text	Classification	✔	✔
country	text	Country	—	✔
description	text	Description	✔	✔
dissolutionDate	text	The date the legal entity was dissolved, if applicable	—	✔
dunsCode	text	Dun & Bradstreet identifier	—	✔
email	email-src	Email address	—	✔
icijId	text	ID according to International Consortium for Investigative Journalists	✔	✔
idNumber	text	ID number of any applicable ID	—	✔
incorporationDate	text	The date the legal entity was incorporated	—	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	—	✔
innCode	text	Russian company ID	—	✔
jurisdiction	text	Country or region in which this entity operates	—	✔
keywords	text	Keywords	✔	✔
legalForm	text	Legal form	✔	✔
mainCountry	text	Primary country of this entity	—	✔
modifiedAt	text	Modified on	—	✔
name	text	Name	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
notes	text	Notes	✔	✔
okpoCode	text	Russian industry classifier	—	✔
opencorporatesUrl	url	OpenCorporates URL	—	✔
phone	phone-number	Phone number	—	✔
previousName	text	Previous name	—	✔
program	text	Program	✔	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
registrationNumber	text	Company registration number	—	✔
retrievedAt	text	Retrieved on	—	✔
sector	text	Sector	✔	✔
sourceUrl	url	Source link	—	✔
status	text	Status	✔	✔
summary	text	Summary	✔	✔
swiftBic	text	Bank identifier code	—	✔
taxNumber	text	Tax identification number	—	✔
taxStatus	text	Tax status	✔	✔
topics	text	Topics	—	✔
vatCode	text	(EU) VAT number	—	✔
weakAlias	text	Weak alias	✔	✔
website	url	Website address	—	✔
wikidataId	text	Wikidata ID	—	✔
wikipediaUrl	url	Wikipedia Article	—	✔

ftm-Ownership

Ownership.

ftm-Ownership 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	Multiple
alephUrl	url	Aleph URL	—	✔
date	text	Date	—	✔
description	text	Description	✔	✔
endDate	text	End date	—	✔
indexText	text	Index text	✔	✔
legalBasis	text	Legal basis	✔	✔
modifiedAt	text	Modified on	—	✔
ownershipType	text	Type of ownership	✔	✔
percentage	text	Percentage held	✔	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
recordId	text	Record ID	✔	✔
retrievedAt	text	Retrieved on	—	✔
role	text	Role	✔	✔
sharesCount	text	Number of shares	✔	✔
sharesCurrency	text	Currency of shares	✔	✔
sharesType	text	Type of shares	✔	✔
sharesValue	text	Value of shares	✔	✔
sourceUrl	url	Source URL	—	✔
startDate	text	Start date	—	✔
status	text	Status	✔	✔
summary	text	Summary	✔	✔

ftm-Package

Package.

ftm-Package 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	Multiple
address	text	Address	➖	✔
alephUrl	url	Aleph URL	➖	✔
alias	text	Other name	➖	✔
author	text	The original author, not the uploader	✔	✔
authoredAt	text	Authored on	➖	✔
companiesMentioned	text	Detected companies	➖	✔
contentHash	sha1	SHA1 hash of the data	➖	✔
country	text	Country	➖	✔
crawler	text	The crawler used to acquire this file	✔	✔
date	text	If not otherwise specified	➖	✔
description	text	Description	✔	✔
detectedCountry	text	Detected country	➖	✔
detectedLanguage	text	Detected language	✔	✔
emailMentioned	email-src	Detected e-mail addresses	➖	✔
encoding	text	File encoding	✔	✔
extension	text	File extension	✔	✔
fileName	text	File name	✔	✔
fileSize	float	File size	✔	✔
generator	text	The program used to generate this file	✔	✔
ibanMentioned	iban	Detected IBANs	➖	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	➖	✔
ipMentioned	ip-src	Detected IP addresses	➖	✔
keywords	text	Keywords	✔	✔
language	text	Language	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
locationMentioned	text	Detected locations	–	✔
messageId	text	Message ID of a document; unique in most cases	✔	✔
mimeType	mime-type	MIME type	✔	✔
modifiedAt	text	Modified on	–	✔
name	text	Name	–	✔
namesMentioned	text	Detected names	–	✔
notes	text	Notes	✔	✔
peopleMentioned	text	Detected people	–	✔
phoneMentioned	phone-number	Detected phones	–	✔
previousName	text	Previous name	–	✔
processingError	text	Processing error	✔	✔
processingStatus	text	Processing status	✔	✔
program	text	Program	✔	✔
publishedAt	text	Published on	–	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	–	✔
retrievedAt	text	Retrieved on	–	✔
sourceUrl	url	Source link	–	✔
summary	text	Summary	✔	✔
title	text	Title	✔	✔
topics	text	Topics	–	✔
weakAlias	text	Weak alias	✔	✔
wikidataId	text	Wikidata ID	–	✔
wikipediaUrl	url	Wikipedia Article	–	✔

ftm-Page

Page.

ftm-Page 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	Multiple
bodyText	text	Text	✔	✔
detectedLanguage	text	Auto-detected language	✔	✔
index	float	Index	✔	✔
indexText	text	Index text	✔	✔

ftm-Pages

Pages.

ftm-Pages 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	Multiple
address	text	Address	–	✔
alephUrl	url	Aleph URL	–	✔
alias	text	Other name	–	✔
author	text	The original author, not the uploader	✔	✔
authoredAt	text	Authored on	–	✔
companiesMentioned	text	Detected companies	–	✔
contentHash	sha1	SHA1 hash of the data	–	✔
country	text	Country	–	✔
crawler	text	The crawler used to acquire this file	✔	✔
date	text	If not otherwise specified	–	✔
description	text	Description	✔	✔
detectedCountry	text	Detected country	–	✔
detectedLanguage	text	Detected language	✔	✔
emailMentioned	email-src	Detected e-mail addresses	–	✔
encoding	text	File encoding	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
extension	text	File extension	✔	✔
fileName	text	File name	✔	✔
fileSize	float	File size	✔	✔
generator	text	The program used to generate this file	✔	✔
ibanMentioned	iban	Detected IBANs	—	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	—	✔
ipMentioned	ip-src	Detected IP addresses	—	✔
keywords	text	Keywords	✔	✔
language	text	Language	✔	✔
locationMentioned	text	Detected locations	—	✔
messageId	text	Message ID of a document; unique in most cases	✔	✔
mimeType	mime-type	MIME type	✔	✔
modifiedAt	text	Modified on	—	✔
name	text	Name	—	✔
namesMentioned	text	Detected names	—	✔
notes	text	Notes	✔	✔
pdfHash	sha1	PDF alternative version checksum	—	✔
peopleMentioned	text	Detected people	—	✔
phoneMentioned	phone-number	Detected phones	—	✔
previousName	text	Previous name	—	✔
processingError	text	Processing error	✔	✔
processingStatus	text	Processing status	✔	✔
program	text	Program	✔	✔
publishedAt	text	Published on	—	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
retrievedAt	text	Retrieved on	—	✔
sourceUrl	url	Source link	—	✔
summary	text	Summary	✔	✔
title	text	Title	✔	✔
topics	text	Topics	—	✔
weakAlias	text	Weak alias	✔	✔
wikidataId	text	Wikidata ID	—	✔
wikipediaUrl	url	Wikipedia Article	—	✔

ftm-Passport

Passport.

ftm-Passport 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	Multiple
alephUrl	url	Aleph URL	—	✔
authority	text	Authority	✔	✔
birthDate	text	Date of birth	—	✔
birthPlace	text	Place of birth	✔	✔
country	text	Country	—	✔
date	text	Date	—	✔
description	text	Description	✔	✔
endDate	text	End date	—	✔
gender	text	Gender	✔	✔
givenName	text	Given name	✔	✔
indexText	text	Index text	✔	✔
modifiedAt	text	Modified on	—	✔
passportNumber	text	Passport number	—	✔
personalNumber	text	Personal number	—	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
recordId	text	Record ID	✔	✔
retrievedAt	text	Retrieved on	—	✔
sourceUrl	url	Source URL	—	✔
startDate	text	Start date	—	✔
summary	text	Summary	✔	✔
surname	text	Surname	✔	✔
type	text	Document type	✔	✔

ftm-Payment

A monetary payment between two parties.

ftm-Payment 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	Multiple
alephUrl	url	Aleph URL	—	✔
amount	float	Amount	✔	✔
amountEur	float	Amount in EUR	✔	✔
amountUsd	float	Amount in USD	✔	✔
currency	text	Currency	✔	✔
date	text	Date	—	✔
description	text	Description	✔	✔
endDate	text	End date	—	✔
indexText	text	Index text	✔	✔
modifiedAt	text	Modified on	—	✔
programme	text	Programme name, funding code, category identifier, etc.	✔	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
purpose	text	Payment purpose	✔	✔
recordId	text	Record ID	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
retrievedAt	text	Retrieved on	—	✔
sequenceNumber	text	Sequence number	✔	✔
sourceUrl	url	Source URL	—	✔
startDate	text	Start date	—	✔
summary	text	Summary	✔	✔
transactionNumber	text	Transaction number	✔	✔

ftm-Person

An individual.

ftm-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	Multiple
address	text	Address	—	✔
alephUrl	url	Aleph URL	—	✔
alias	text	Other name	—	✔
birthDate	text	Birth date	—	✔
birthPlace	text	Place of birth	✔	✔
bvdId	text	Bureau van Dijk ID	—	✔
classification	text	Classification	✔	✔
country	text	Country	—	✔
deathDate	text	Death date	—	✔
description	text	Description	✔	✔
dissolutionDate	text	The date the legal entity was dissolved, if applicable	—	✔
dunsCode	text	Dun & Bradstreet identifier	—	✔
email	email-src	Email address	—	✔
fatherName	text	Patronymic	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
firstName	text	First name	✔	✔
gender	text	Gender	✔	✔
icijId	text	ID according to International Consortium for Investigative Journalists	✔	✔
idNumber	text	ID number of any applicable ID	—	✔
incorporationDate	text	The date the legal entity was incorporated	—	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	—	✔
innCode	text	Russian company ID	—	✔
jurisdiction	text	Country or region in which this entity operates	—	✔
keywords	text	Keywords	✔	✔
lastName	text	Last name	✔	✔
legalForm	text	Legal form	✔	✔
mainCountry	text	Primary country of this entity	—	✔
middleName	text	Middle name	✔	✔
modifiedAt	text	Modified on	—	✔
motherName	text	Matronymic	✔	✔
name	text	Name	—	✔
nationality	text	Nationality	—	✔
notes	text	Notes	✔	✔
okpoCode	text	Russian industry classifier	—	✔
opencorporatesUrl	url	OpenCorporates URL	—	✔
passportNumber	text	Passport	—	✔
phone	phone-number	Phone number	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
position	text	Position	✔	✔
previousName	text	Previous name	—	✔
program	text	Program	✔	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
registrationNumber	text	Company registration number	—	✔
retrievedAt	text	Retrieved on	—	✔
secondName	text	Second name	✔	✔
sector	text	Sector	✔	✔
sourceUrl	url	Source link	—	✔
status	text	Status	✔	✔
summary	text	Summary	✔	✔
swiftBic	text	Bank identifier code	—	✔
taxNumber	text	Tax identification number	—	✔
taxStatus	text	Tax status	✔	✔
title	text	Title	✔	✔
topics	text	Topics	—	✔
vatCode	text	(EU) VAT number	—	✔
weakAlias	text	Weak alias	✔	✔
website	url	Website address	—	✔
wikidataId	text	Wikidata ID	—	✔
wikipediaUrl	url	Wikipedia Article	—	✔

ftm-PlainText

Plaintext.

ftm-PlainText 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	Multiple
address	text	Address	–	✔
alephUrl	url	Aleph URL	–	✔
alias	text	Other name	–	✔
author	text	The original author, not the uploader	✔	✔
authoredAt	text	Authored on	–	✔
bodyText	text	Text	✔	✔
companiesMentioned	text	Detected companies	–	✔
contentHash	sha1	SHA1 hash of the data	–	✔
country	text	Country	–	✔
crawler	text	The crawler used to acquire this file	✔	✔
date	text	If not otherwise specified	–	✔
description	text	Description	✔	✔
detectedCountry	text	Detected country	–	✔
detectedLanguage	text	Detected language	✔	✔
emailMentioned	email-src	Detected e-mail addresses	–	✔
encoding	text	File encoding	✔	✔
extension	text	File extension	✔	✔
fileName	text	File name	✔	✔
fileSize	float	File size	✔	✔
generator	text	The program used to generate this file	✔	✔
ibanMentioned	iban	Detected IBANs	–	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	–	✔
ipMentioned	ip-src	Detected IP addresses	–	✔
keywords	text	Keywords	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
language	text	Language	✔	✔
locationMentioned	text	Detected locations	—	✔
messageId	text	Message ID of a document; unique in most cases	✔	✔
mimeType	mime-type	MIME type	✔	✔
modifiedAt	text	Modified on	—	✔
name	text	Name	—	✔
namesMentioned	text	Detected names	—	✔
notes	text	Notes	✔	✔
peopleMentioned	text	Detected people	—	✔
phoneMentioned	phone-number	Detected phones	—	✔
previousName	text	Previous name	—	✔
processingError	text	Processing error	✔	✔
processingStatus	text	Processing status	✔	✔
program	text	Program	✔	✔
publishedAt	text	Published on	—	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
retrievedAt	text	Retrieved on	—	✔
sourceUrl	url	Source link	—	✔
summary	text	Summary	✔	✔
title	text	Title	✔	✔
topics	text	Topics	—	✔
weakAlias	text	Weak alias	✔	✔
wikidataId	text	Wikidata ID	—	✔
wikipediaUrl	url	Wikipedia Article	—	✔

ftm-PublicBody

A public body, such as a ministry, department or state company.

ftm-PublicBody 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	Multiple
address	text	Address	➖	✔
alephUrl	url	Aleph URL	➖	✔
alias	text	Other name	➖	✔
bvdId	text	Bureau van Dijk ID	➖	✔
classification	text	Classification	✔	✔
country	text	Country	➖	✔
description	text	Description	✔	✔
dissolutionDate	text	The date the legal entity was dissolved, if applicable	➖	✔
dunsCode	text	Dun & Bradstreet identifier	➖	✔
email	email-src	Email address	➖	✔
icijId	text	ID according to International Consortium for Investigative Journalists	✔	✔
idNumber	text	ID number of any applicable ID	➖	✔
incorporationDate	text	The date the legal entity was incorporated	➖	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	➖	✔
innCode	text	Russian company ID	➖	✔
jurisdiction	text	Country or region in which this entity operates	➖	✔
keywords	text	Keywords	✔	✔
legalForm	text	Legal form	✔	✔
mainCountry	text	Primary country of this entity	➖	✔
modifiedAt	text	Modified on	➖	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
name	text	Name	➖	✔
notes	text	Notes	✔	✔
okpoCode	text	Russian industry classifier	➖	✔
opencorporatesUrl	url	OpenCorporates URL	➖	✔
phone	phone-number	Phone number	➖	✔
previousName	text	Previous name	➖	✔
program	text	Program	✔	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	➖	✔
registrationNumber	text	Company registration number	➖	✔
retrievedAt	text	Retrieved on	➖	✔
sector	text	Sector	✔	✔
sourceUrl	url	Source link	➖	✔
status	text	Status	✔	✔
summary	text	Summary	✔	✔
swiftBic	text	Bank identifier code	➖	✔
taxNumber	text	Tax identification number	➖	✔
taxStatus	text	Tax status	✔	✔
topics	text	Topics	➖	✔
vatCode	text	(EU) VAT number	➖	✔
weakAlias	text	Weak alias	✔	✔
website	url	Website address	➖	✔
wikidataId	text	Wikidata ID	➖	✔
wikipediaUrl	url	Wikipedia Article	➖	✔

ftm-RealEstate

A piece of land or property.

ftm-RealEstate 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	Multiple
address	text	Address	–	✔
alephUrl	url	Aleph URL	–	✔
alias	text	Other name	–	✔
amount	float	Amount	✔	✔
amountEur	float	Amount in EUR	✔	✔
amountUsd	float	Amount in USD	✔	✔
area	float	Area	✔	✔
cadastralCode	text	Cadastral code	–	✔
censusBlock	text	Census block	✔	✔
country	text	Country	–	✔
createDate	text	Record date	–	✔
currency	text	Currency	✔	✔
description	text	Description	✔	✔
encumbrance	text	An encumbrance is a right to, interest in, or legal liability on real property that does not prohibit passing title to the property but that diminishes its value.	✔	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	–	✔
keywords	text	Keywords	✔	✔
landType	text	Land type	✔	✔
latitude	float	Latitude	✔	✔
longitude	float	Longitude	✔	✔
modifiedAt	text	Modified on	–	✔
name	text	Name	–	✔
notes	text	Notes	✔	✔
previousName	text	Previous name	–	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
program	text	Program	✔	✔
propertyType	text	Property type	✔	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
registrationNumber	text	Registration number	—	✔
retrievedAt	text	Retrieved on	—	✔
sourceUrl	url	Source link	—	✔
summary	text	Summary	✔	✔
tenure	text	Tenure	✔	✔
titleNumber	text	Title number	—	✔
topics	text	Topics	—	✔
weakAlias	text	Weak alias	✔	✔
wikidataId	text	Wikidata ID	—	✔
wikipediaUrl	url	Wikipedia Article	—	✔

ftm-Representation

A mediatory, intermediary, middleman, or broker acting on behalf of a legal entity.

ftm-Representation 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	Multiple
alephUrl	url	Aleph URL	—	✔
date	text	Date	—	✔
description	text	Description	✔	✔
endDate	text	End date	—	✔
indexText	text	Index text	✔	✔
modifiedAt	text	Modified on	—	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
recordId	text	Record ID	✔	✔
retrievedAt	text	Retrieved on	—	✔
role	text	Role	✔	✔
sourceUrl	url	Source URL	—	✔
startDate	text	Start date	—	✔
status	text	Status	✔	✔
summary	text	Summary	✔	✔

ftm-Row

Row.

ftm-Row 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	Multiple
cells	text	Cells	✔	✔
index	float	Index	✔	✔
indexText	text	Index text	✔	✔

ftm-Sanction

A sanction designation.

ftm-Sanction 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	Multiple
alephUrl	url	Aleph URL	—	✔
authority	text	Authority	✔	✔
country	text	Country	—	✔
date	text	Date	—	✔
description	text	Description	✔	✔
duration	text	Duration	✔	✔
endDate	text	End date	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
indexText	text	Index text	✔	✔
modifiedAt	text	Modified on	—	✔
program	text	Program	✔	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
reason	text	Reason	✔	✔
recordId	text	Record ID	✔	✔
retrievedAt	text	Retrieved on	—	✔
sourceUrl	url	Source URL	—	✔
startDate	text	Start date	—	✔
status	text	Status	✔	✔
summary	text	Summary	✔	✔

ftm-Succession

Two entities that legally succeed each other.

ftm-Succession 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	Multiple
alephUrl	url	Aleph URL	—	✔
date	text	Date	—	✔
description	text	Description	✔	✔
endDate	text	End date	—	✔
indexText	text	Index text	✔	✔
modifiedAt	text	Modified on	—	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
recordId	text	Record ID	✔	✔
retrievedAt	text	Retrieved on	—	✔
role	text	Role	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
sourceUrl	url	Source URL	—	✔
startDate	text	Start date	—	✔
status	text	Status	✔	✔
summary	text	Summary	✔	✔

ftm-Table

Table.

ftm-Table 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	Multiple
address	text	Address	—	✔
alephUrl	url	Aleph URL	—	✔
alias	text	Other name	—	✔
author	text	The original author, not the uploader	✔	✔
authoredAt	text	Authored on	—	✔
columns	text	Column headings	✔	✔
companiesMentioned	text	Detected companies	—	✔
contentHash	sha1	SHA1 hash of the data	—	✔
country	text	Country	—	✔
crawler	text	The crawler used to acquire this file	✔	✔
csvHash	sha1	CSV alternative version checksum	—	✔
date	text	If not otherwise specified	—	✔
description	text	Description	✔	✔
detectedCountry	text	Detected country	—	✔
detectedLanguage	text	Detected language	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
emailMentioned	email-src	Detected e-mail addresses	—	✔
encoding	text	File encoding	✔	✔
extension	text	File extension	✔	✔
fileName	text	File name	✔	✔
fileSize	float	File size	✔	✔
generator	text	The program used to generate this file	✔	✔
ibanMentioned	iban	Detected IBANs	—	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	—	✔
ipMentioned	ip-src	Detected IP addresses	—	✔
keywords	text	Keywords	✔	✔
language	text	Language	✔	✔
locationMentioned	text	Detected locations	—	✔
messageId	text	Message ID of a document; unique in most cases	✔	✔
mimeType	mime-type	MIME type	✔	✔
modifiedAt	text	Modified on	—	✔
name	text	Name	—	✔
namesMentioned	text	Detected names	—	✔
notes	text	Notes	✔	✔
peopleMentioned	text	Detected people	—	✔
phoneMentioned	phone-number	Detected phones	—	✔
previousName	text	Previous name	—	✔
processingError	text	Processing error	✔	✔
processingStatus	text	Processing status	✔	✔
program	text	Program	✔	✔
publishedAt	text	Published on	—	✔
publisher	text	Publishing source	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
publisherUrl	url	Publishing source URL	—	✔
retrievedAt	text	Retrieved on	—	✔
rowCount	float	Number of rows	✔	✔
sourceUrl	url	Source link	—	✔
summary	text	Summary	✔	✔
title	text	Title	✔	✔
topics	text	Topics	—	✔
weakAlias	text	Weak alias	✔	✔
wikidataId	text	Wikidata ID	—	✔
wikipediaUrl	url	Wikipedia Article	—	✔

ftm-TaxRoll

A tax declaration of an individual.

ftm-TaxRoll 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	Multiple
alephUrl	url	Aleph URL	—	✔
birthDate	text	Date of birth	—	✔
country	text	Country	—	✔
date	text	Date	—	✔
description	text	Description	✔	✔
endDate	text	End date	—	✔
givenName	text	Given name	✔	✔
income	text	Registered income	✔	✔
indexText	text	Index text	✔	✔
modifiedAt	text	Modified on	—	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
recordId	text	Record ID	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
retrievedAt	text	Retrieved on	—	✔
sourceUrl	url	Source URL	—	✔
startDate	text	Start date	—	✔
summary	text	Summary	✔	✔
surname	text	Surname	✔	✔
taxPaid	text	Amount of tax paid	✔	✔
wealth	text	Registered wealth	✔	✔

ftm-UnknownLink

Unknown Link.

ftm-UnknownLink 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	Multiple
alephUrl	url	Aleph URL	—	✔
date	text	Date	—	✔
description	text	Description	✔	✔
endDate	text	End date	—	✔
indexText	text	Index text	✔	✔
modifiedAt	text	Modified on	—	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
recordId	text	Record ID	✔	✔
retrievedAt	text	Retrieved on	—	✔
role	text	Role	✔	✔
sourceUrl	url	Source URL	—	✔
startDate	text	Start date	—	✔
status	text	Status	✔	✔
summary	text	Summary	✔	✔

ftm-UserAccount

User Account.

ftm-UserAccount 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	Multiple
address	text	Address	–	✔
alephUrl	url	Aleph URL	–	✔
alias	text	Other name	–	✔
country	text	Country	–	✔
description	text	Description	✔	✔
email	email-src	E-mail	–	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	–	✔
keywords	text	Keywords	✔	✔
modifiedAt	text	Modified on	–	✔
name	text	Name	–	✔
notes	text	Notes	✔	✔
number	phone-number	Phone Number	–	✔
password	text	Password	✔	✔
previousName	text	Previous name	–	✔
program	text	Program	✔	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	–	✔
retrievedAt	text	Retrieved on	–	✔
service	text	Service	✔	✔
sourceUrl	url	Source link	–	✔
summary	text	Summary	✔	✔
topics	text	Topics	–	✔
username	text	Username	✔	✔
weakAlias	text	Weak alias	✔	✔
wikidataId	text	Wikidata ID	–	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
wikipediaUrl	url	Wikipedia Article	➖	✔

ftm-Vehicle

Vehicle.

ftm-Vehicle 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	Multiple
address	text	Address	➖	✔
alephUrl	url	Aleph URL	➖	✔
alias	text	Other name	➖	✔
amount	float	Amount	✔	✔
amountEur	float	Amount in EUR	✔	✔
amountUsd	float	Amount in USD	✔	✔
buildDate	text	Build Date	➖	✔
country	text	Country	➖	✔
currency	text	Currency	✔	✔
description	text	Description	✔	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	➖	✔
keywords	text	Keywords	✔	✔
model	text	Model	✔	✔
modifiedAt	text	Modified on	➖	✔
name	text	Name	➖	✔
notes	text	Notes	✔	✔
previousName	text	Previous name	➖	✔
program	text	Program	✔	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	➖	✔
registrationDate	text	Registration Date	➖	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
registrationNumber	text	Registration Number	—	✔
retrievedAt	text	Retrieved on	—	✔
sourceUrl	url	Source link	—	✔
summary	text	Summary	✔	✔
topics	text	Topics	—	✔
type	text	Type	✔	✔
weakAlias	text	Weak alias	✔	✔
wikidataId	text	Wikidata ID	—	✔
wikipediaUrl	url	Wikipedia Article	—	✔

ftm-Vessel

A boat or ship.

ftm-Vessel 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	Multiple
address	text	Address	—	✔
alephUrl	url	Aleph URL	—	✔
alias	text	Other name	—	✔
amount	float	Amount	✔	✔
amountEur	float	Amount in EUR	✔	✔
amountUsd	float	Amount in USD	✔	✔
buildDate	text	Build Date	—	✔
callSign	text	Call Sign	—	✔
country	text	Country	—	✔
crsNumber	text	CRS Number	—	✔
currency	text	Currency	✔	✔
description	text	Description	✔	✔
flag	text	Flag	—	✔
grossRegisteredTonnage	float	Gross Registered Tonnage	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
imoNumber	text	IMO Number	➖	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	➖	✔
keywords	text	Keywords	✔	✔
mmsi	text	MMSI	➖	✔
model	text	Model	✔	✔
modifiedAt	text	Modified on	➖	✔
name	text	Name	➖	✔
nameChangeDate	text	Date of Name Change	➖	✔
navigationArea	text	Navigation Area	✔	✔
notes	text	Notes	✔	✔
pastFlags	text	Past Flags	✔	✔
pastNames	text	Past Names	➖	✔
pastTypes	text	Past Types	✔	✔
previousName	text	Previous name	➖	✔
program	text	Program	✔	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	➖	✔
registrationDate	text	Registration Date	➖	✔
registrationNumber	text	Registration Number	➖	✔
registrationPort	text	Port of Registration	✔	✔
retrievedAt	text	Retrieved on	➖	✔
sourceUrl	url	Source link	➖	✔
summary	text	Summary	✔	✔
tonnage	text	Tonnage	✔	✔
topics	text	Topics	➖	✔
type	text	Type	✔	✔
weakAlias	text	Weak alias	✔	✔
wikidataId	text	Wikidata ID	➖	✔
wikipediaUrl	url	Wikipedia Article	➖	✔

ftm-Video

Video.

ftm-Video 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	Multiple
address	text	Address	–	✔
alephUrl	url	Aleph URL	–	✔
alias	text	Other name	–	✔
author	text	The original author, not the uploader	✔	✔
authoredAt	text	Authored on	–	✔
companiesMentioned	text	Detected companies	–	✔
contentHash	sha1	SHA1 hash of the data	–	✔
country	text	Country	–	✔
crawler	text	The crawler used to acquire this file	✔	✔
date	text	If not otherwise specified	–	✔
description	text	Description	✔	✔
detectedCountry	text	Detected country	–	✔
detectedLanguage	text	Detected language	✔	✔
duration	float	Duration of the video in ms	✔	✔
emailMentioned	email-src	Detected e-mail addresses	–	✔
encoding	text	File encoding	✔	✔
extension	text	File extension	✔	✔
fileName	text	File name	✔	✔
fileSize	float	File size	✔	✔
generator	text	The program used to generate this file	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
ibanMentioned	iban	Detected IBANs	—	✔
indexText	text	Index text	✔	✔
indexUpdatedAt	text	Index updated at	—	✔
ipMentioned	ip-src	Detected IP addresses	—	✔
keywords	text	Keywords	✔	✔
language	text	Language	✔	✔
locationMentioned	text	Detected locations	—	✔
messageId	text	Message ID of a document; unique in most cases	✔	✔
mimeType	mime-type	MIME type	✔	✔
modifiedAt	text	Modified on	—	✔
name	text	Name	—	✔
namesMentioned	text	Detected names	—	✔
notes	text	Notes	✔	✔
peopleMentioned	text	Detected people	—	✔
phoneMentioned	phone-number	Detected phones	—	✔
previousName	text	Previous name	—	✔
processingError	text	Processing error	✔	✔
processingStatus	text	Processing status	✔	✔
program	text	Program	✔	✔
publishedAt	text	Published on	—	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
retrievedAt	text	Retrieved on	—	✔
sourceUrl	url	Source link	—	✔
summary	text	Summary	✔	✔
title	text	Title	✔	✔
topics	text	Topics	—	✔
weakAlias	text	Weak alias	✔	✔
wikidataId	text	Wikidata ID	—	✔
wikipediaUrl	url	Wikipedia Article	—	✔

ftm-Workbook

Workbook.

ftm-Workbook 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	Multiple
address	text	Address	–	✔
alephUrl	url	Aleph URL	–	✔
alias	text	Other name	–	✔
author	text	The original author, not the uploader	✔	✔
authoredAt	text	Authored on	–	✔
companiesMentioned	text	Detected companies	–	✔
contentHash	sha1	SHA1 hash of the data	–	✔
country	text	Country	–	✔
crawler	text	The crawler used to acquire this file	✔	✔
date	text	If not otherwise specified	–	✔
description	text	Description	✔	✔
detectedCountry	text	Detected country	–	✔
detectedLanguage	text	Detected language	✔	✔
emailMentioned	email-src	Detected e-mail addresses	–	✔
encoding	text	File encoding	✔	✔
extension	text	File extension	✔	✔
fileName	text	File name	✔	✔
fileSize	float	File size	✔	✔
generator	text	The program used to generate this file	✔	✔
ibanMentioned	iban	Detected IBANs	–	✔
indexText	text	Index text	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
indexUpdatedAt	text	Index updated at	—	✔
ipMentioned	ip-src	Detected IP addresses	—	✔
keywords	text	Keywords	✔	✔
language	text	Language	✔	✔
locationMentioned	text	Detected locations	—	✔
messageId	text	Message ID of a document; unique in most cases	✔	✔
mimeType	mime-type	MIME type	✔	✔
modifiedAt	text	Modified on	—	✔
name	text	Name	—	✔
namesMentioned	text	Detected names	—	✔
notes	text	Notes	✔	✔
peopleMentioned	text	Detected people	—	✔
phoneMentioned	phone-number	Detected phones	—	✔
previousName	text	Previous name	—	✔
processingError	text	Processing error	✔	✔
processingStatus	text	Processing status	✔	✔
program	text	Program	✔	✔
publishedAt	text	Published on	—	✔
publisher	text	Publishing source	✔	✔
publisherUrl	url	Publishing source URL	—	✔
retrievedAt	text	Retrieved on	—	✔
sourceUrl	url	Source link	—	✔
summary	text	Summary	✔	✔
title	text	Title	✔	✔
topics	text	Topics	—	✔
weakAlias	text	Weak alias	✔	✔
wikidataId	text	Wikidata ID	—	✔
wikipediaUrl	url	Wikipedia Article	—	✔

game-cheat

Describes a game cheat or a cheatware.

game-cheat 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	Multiple
affected-game	text	Name of the game that is targeted by the cheatware.	—	—
cheat-name	text	Known name of the game cheat, if given.	✔	—
cheat-screenshot	attachment	Screenshot of the cheat at work.	—	—
cheat-type	text	Select a type of cheat. ['Aimbot', 'Artificial lag', 'Auto farmer', 'DDoS', 'Disconnecting', 'Exploit', 'Fly', 'Force field', 'Full brightness', 'Ghosting', 'God mode', 'Invicibility', 'Macros', 'No clip', 'No fog', 'RapidFire', 'Scripting', 'Show Hitboxes', 'Wallhack', 'Others']	—	✔
cheat-version	text	Any information about the cheatware version.	✔	—
compilation-date	datetime	Compilation date of the game cheat, if known.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
creator	threat-actor	Individual and/or Group and/or Organization that created the cheat.	➖	➖
ig-cheat-behaviour	comment	Describe the in-game behaviour of the cheat (e.g. You selected 'Aim Bot', here you can add details like 'Activate by pressing F7, Deactivate by pressing F8. Not detected be Easy Anti-Cheat.')	✔	➖
implementation	text	How cheatware is implemented ['Game code modification', 'In-memory data manipulation', 'System software modification', 'Packet interception and manipulation']	✔	➖
implementation-details	text	Additionnal informations about the implementation of the cheatware. (e.g. Requires to swap a dll file.)	✔	➖
operating-system	text	Operating system required and its version.	✔	✔
pricing	text	Cheatware price, 0 if free.	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
webpage	url	Place where the cheat is promoted. Website, Forum, Download page, ...	—	—

Generalizing Persuasion Framework

By placing their work within the GP Framework, scholars will help the field resolve inconsistencies, identify and address open questions, and ensure collective progress. The GP Framework is not meant to compete with other theories (such as the ELM) but rather to fill in two gaps. First, it allows one to consider how individual persuasion studies connect to one another and why studies may arrive at contradictory conclusions. Second, it highlights the sources of variations that should be studied. (James N. Druckman).

Generalizing Persuasion Framework is a MISP object available in JSON format at https://github.com/MISP/misp-objects/blob/main/objects/generalizing persuasion framework/definition.json[**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	Multiple
actors_receiver	text	Assessments across weighted dimensions. Effort, motivation, prior attitudes	✔	✔
actors_speaker_motivation	text	Motivations in crafting messages	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
actors_speaker_type	text	Types (e.g., elites, media, opinion leaders, friends/family). ['Politician', 'Government Official', 'Law Enforcement', 'Media', 'Religious Leader', 'CEO/Executive', 'Community Leader', 'Teacher/Professor', 'Coache/Mentor', 'Expert in a specific field', 'Celebrity', 'Athlete', 'Social Media Personality', 'Trendsetter', 'Salesperson', 'Marketeer', 'Friend/Family', 'Lobbyist', 'Advocacy Group', 'Professional Association', 'Leaked document', 'Whistle-blower', 'Online forum', 'Algorithm']	✔	✔
outcomes_attitude	text	General evaluation of an object (where the 'object' is broadly construed).	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
outcomes_behavior	text	Does not always follow from an attitude. Depends on attitude attributes, injunctive and descriptive norms, behavioral control, and emotions.	✔	✔
outcomes_emotion	text	Can inform conscious evaluations or override them.	✔	✔
outcomes_identity	text	A dimension of evaluation. Often activated when threatened.	✔	✔
settings_competition_observers	float	Number of observers.	✔	➖
settings_competition_receivers	float	Number of receivers.	✔	➖
settings_competition_speakers	float	Number of speakers.	✔	➖
settings_culture	text	Shapes understandings of topics. Alters salience of different values.	✔	✔
settings_process	text	Threatening settings. Political (conflictual) settings versus deliberative settings	✔	✔
settings_space	text	Attitude or behavioral change in one setting may not generalize to other settings.	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
settings_time	text	Pretreatment effects—what happened prior to the persuasive message. Posttreatment duration—how long an effect lasts. Time between exposure and outcome measurement.	✔	✔
treatments_medium	text	Alters frames, processing goals, and/or effort. Interactions with other persuasion variables.	✔	✔
treatments_message_content	text	Argument strength (and inadequacy). Framing and evaluations. Matching to receivers' goals. Altering receivers' motivations (e.g., using narratives).	✔	✔
treatments_topic	text	Persons/groups, issues, institutions, products. Variation within a topic (e.g., different policy issues)	✔	✔

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	Multiple
accuracy-radius	float	The approximate accuracy radius, in kilometers, around the latitude and longitude for the geographical entity (country, subdivision, city or postal code) associated with the related object. (based on geoip2 accuracy of maxmind)	✔	—
address	text	Address.	—	—
altitude	float	The altitude is the decimal value of the altitude in the World Geodetic System 84 (WGS84) reference.	✔	—
city	text	City.	—	—
country	text	Country.	—	—
countrycode	text	Country code in ISO 3166-1 alpha-2	—	—
epsg	text	EPSG Geodetic Parameter value. This is an integer value of the EPSG.	✔	—
first-seen	datetime	When the location was seen for the first time.	✔	—
last-seen	datetime	When the location was seen for the last time.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
latitude	float	The latitude is the decimal value of the latitude in the World Geodetic System 84 (WGS84) reference.	✔	—
longitude	float	The longitude is the decimal value of the longitude in the World Geodetic System 84 (WGS84) reference	✔	—
neighborhood	text	Neighborhood.	—	—
region	text	Region.	—	—
spacial-reference	text	Default spacial or projection refence for this object. ['WGS84 EPSG:4326', 'Mercator EPSG:3857']	✔	—
text	text	A generic description of the location.	✔	—
zipcode	text	Zip Code.	—	—

git-vuln-finder

Export from git-vuln-finder.

git-vuln-finder 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	Multiple
author	text	Commit author	—	—
author-email	email-src	Commit authors email	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
authored_date	datetime	Date the commit was originally made	—	—
branches	text	Branches the commit is on	✔	✔
commit-id	git-commit-id	Commit ID where the vulnerability is fixed.	—	—
committed_date	datetime	Date the commit was modified last	—	—
cve	vulnerability	CVE associated to the vulnerability	—	—
language	text	Language of the commit (ISO 639-1 codes)	✔	✔
message	text	Commit message	✔	—
origin	text	Origin of the repository	—	—
origin-github-api	url	Full path to the commit on github	✔	—
pattern-matches	text	Pattern matching for the vulnerability	✔	✔
pattern-selected	text	Pattern used to find the vulnerability	✔	—
state	text	State of the vulnerability ['under-review', 'cve-assigned']	✔	—
stats.deletions	counter	Number of deletions in the commit	✔	—
stats.files	counter	Number of files changed in the commit	✔	—
stats.insertions	counter	Number of insertions in the commit	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
stats.lines	counter	Number of line changes in the commit	✔	—
summary	text	Commit summary	✔	—
tags	text	User defined tags	✔	✔

github-repo

GitHub repository.

> github-repo 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	Multiple
archived	text	Is the repository archived? ['True', 'False']	✔	—
created-at	datetime	Date of the repository creation	—	—
description	text	Repository description	—	—
disabled	text	Is the repository disabled? ['True', 'False']	✔	—
fork	text	Is the repository a forked repository? ['True', 'False']	✔	—
forks-count	counter	Number of forks	—	—
full-name	text	Full name of the repository. [Username/Repository name]	—	—
has-downloads	text	Have the repository been downloaded? ['True', 'False']	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
has-wiki	text	Does the repository have a wiki? ['True', 'False']	✔	—
id	text	Repository id	—	—
languages	text	Languages used in the repository	—	✔
link	link	Link to the GitHub repository.	—	✔
name	text	name of the repository. [Repository name]	—	—
open-issues	counter	Number of open issues	—	—
private	text	Is the repository private? ['True', 'False']	✔	—
pushed-at	datetime	Date of last push	—	—
topics	text	Topics linked to the repository	—	✔
updated-at	datetime	Date of the last update	—	—
username	text	Owner of the repository. [Username]	—	—

github-user

GitHub user.

> github-user 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	Multiple
avatar_url	link	Avatar URL	—	—
bio	text	Biography of the GitHub user.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
blog	text	Blog - often used as website field of the user	➖	➖
company	text	Company	➖	➖
follower	github-username	GitHub user is followed by.	➖	✔
following	github-username	Followed GitHub users by the GitHub user.	➖	✔
id	text	User id	➖	➖
link	link	Original Link to the GitHub account.	➖	✔
location	text	Location given by the GitHub user	✔	➖
node_id	text	GitHub GraphQL node_id	➖	➖
organisation	github-organisation	Organisation affiliation of the GitHub user (it can be multiple).	➖	✔
profile-image	attachment	Profile image of the GitHub user (it can be multiple).	➖	✔
public_gists	text		✔	➖
public_repos	text		✔	➖
repository	github-repository	GitHub repository under the GitHub user.	➖	✔
ssh-public-key	text	SSH public key associated to the GitHub user.	➖	✔
twitter_username	text	Associated twitter account	➖	➖
user-fullname	text	Fullname of the GitHub user.	➖	➖
username	github-username	GitHub username.	➖	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
verified	text	User verified. ['True', 'False']	✔	—

gitlab-user

GitLab user. Gitlab.com user or self-hosted GitLab instance.

gitlab-user 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	Multiple
avatar_url	link	Avatar url of the GitLab User	—	—
id	text	GitLab User id	—	—
name	text	Complete Name of the GitLab User Id	—	—
state	text	State of the GitLab User ['active', 'inactive', 'blocked']	✔	—
username	text	Username of the GitLab User	—	—
web_url	link	Profile url of the GitLab User	—	✔

google-safe-browsing

Google Safe checks a URL against Google's constantly updated list of unsafe web resources.

google-safe-browsing 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	Multiple
malicious	boolean	If the URL comes back as malicious	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
platforms	text	The platform identified (windows, linux, etc...)	—	—
threats	text	The threat type related to that URL (malware, social engineering, etc...)	—	—

google-threat-intelligence-report

Google Threat Intelligence report that provides an assessment (verdict, severity and scoring) and combined information from VirusTotal and Mandiant.

> google-threat-intelligence-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	Multiple
detection-ratio	text	Detection Ratio	✔	—
first-submission	datetime	First Submission	✔	—
last-submission	datetime	Last Submission	✔	—
permalink	link	Permalink Reference	✔	—
severity	text	GTI Severity	✔	—
threat-score	integer	GTI Threat Score	✔	—
verdict	text	GTI Verdict	✔	—

greynoise-ip

GreyNoise IP Information.

> greynoise-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	Multiple
actor	text	GreyNoise Actor	✔	—
classification	text	GreyNoise Classification	✔	—
first-seen	datetime	First Seen	✔	—
ip-src	ip-src	Source IP address of the network connection.	—	—
last-seen	datetime	Last Seen	✔	—
link	link	GreyNoise Visualizer Link	✔	—
noise	text	GreyNoise Internet Scanning Flag	✔	—
provider	text	GreyNoise Service Provider	✔	—
riot	text	GreyNoise Common Business Service Flag	✔	—
trust-level	text	GreyNoise RIOT Trust Level	✔	—

gtp-attack

GTP attack object as attack as seen on the GTP signaling protocol supporting GPRS/LTE networks.

gtp-attack 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	Multiple
GtpImei	text	GTP IMEI (International Mobile Equipment Identity).	—	—
GtpImsi	text	GTP IMSI (International mobile subscriber identity).	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
GtpInterface	text	GTP interface. ['S5', 'S11', 'S10', 'S8', 'Gn', 'Gp']	✔	✔
GtpMessageType	text	GTP defines a set of messages between two associated GSNs or an SGSN and an RNC. Message type is described as a decimal value.	✔	—
GtpMsisdn	text	GTP MSISDN.	—	—
GtpServingNetwork	text	GTP Serving Network.	✔	—
GtpVersion	text	GTP version ['0', '1', '2']	✔	—
PortDest	text	Destination port.	✔	—
PortSrc	port	Source port.	✔	—
first-seen	datetime	When the attack has been seen for the first time.	✔	—
ipDest	ip-dst	IP destination address.	—	—
ipSrc	ip-src	IP source address.	—	—
text	text	A description of the GTP attack.	✔	—

hashlookup

hashlookup object as described on hashlookup services from circl.lu - https://www.circl.lu/services/hashlookup.

hashlookup 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	Multiple
FileName	filename	Complete path of the filename including the filename	✔	—
FileSize	size-in-bytes	Size of the file, in bytes	✔	—
KnownMalicious	text	Source of the hashlookup record if it's a known malicious file	✔	—
MD5	md5	MD5 hash (128 bits) in hex representation	—	—
PackageArch	text	Package architecture	✔	—
PackageDescription	text	Package description and information	✔	—
PackageMaintainer	text	Package Maintainer(s)	—	—
PackageName	text	Package Name	✔	—
PackageRelease	text	Package Release	✔	—
PackageVersion	text	Package Version	✔	—
SHA-1	sha1	Secure Hash Algorithm 1 (160 bits) in hex representation	—	—
SHA-256	sha256	Secure Hash Algorithm 2 (256 bits) in hex representation	—	—
SSDEEP	ssdeep	SSDEEP - Fuzzy hashing	—	—
TLSH	tlsh	TLSH - Trend Micro Locality Sensitive Hash	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
source	text	Source of the hashlookup record	✔	—

hhhash

An object describing a HHHash object with the hash value along with the crawling parameters. For more information: https://www.foo.be/2023/07/HTTP-Headers-Hashing_HHHash.

hhhash 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	Multiple
comment	comment	A description of the HHHash object.	—	—
hhhash	text	HHHash hash in format hhh:version:hash_value	—	—
hhhash-headers	text	HHHash value before being hash in the format each header is separated by a :.	—	—
hhhash-query-headers	text	Set of headers used for the query in the format where each header is separated by a : .	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
hhhash-tool	text	HHHash crawling infrastructure or tool used to produce the HHHash value. ['python-hhhash', 'c-hhhash', 'go-hhhash', 'r-hhhash', 'lacus', 'Common Crawl', 'other']	✔	—

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	Multiple
basicauth-password	text	HTTP Basic Authentication Password	—	—
basicauth-user	text	HTTP Basic Authentication Username	—	—
content-type	other	The MIME type of the body of the request	—	—
cookie	text	An HTTP cookie previously sent by the server with Set-Cookie	—	✔
header	text	An HTTP header sent during HTTP request	—	✔
host	hostname	The domain name of the server	—	—
ip-dst	ip-dst	The IP address of the server	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
ip-src	ip-src	The IP address of the client	—	—
method	http-method	HTTP Method invoked (one of GET, POST, PUT, HEAD, DELETE, OPTIONS, CONNECT)	✔	—
proxy-password	text	HTTP Proxy Password	—	—
proxy-user	text	HTTP Proxy Username	—	—
referer	other	This is the address of the previous web page from which a link to the currently requested page was followed	—	—
text	text	HTTP Request comment	✔	—
uri	uri	Request URI	—	—
url	url	Full HTTP Request URL	—	—
user-agent	user-agent	The user agent string of the user agent	—	—

identity

Identities can represent actual individuals, organizations, or groups (e.g., ACME, Inc.) as well as classes of individuals, organizations, systems or groups (e.g., the finance sector). The Identity SDO can capture basic identifying information, contact information, and the sectors that the Identity belongs to. Identity is used in STIX to represent, among other things, targets of attacks, information sources, object creators, and threat actor identities. (ref. STIX 2.1 - 4.5).

identity 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	Multiple
contact_information	text	The contact information (e-mail, phone number, etc.) for this Identity. No format for this information is currently defined by this specification.	➖	➖
description	text	A description that provides more details and context about the Identity, potentially including its purpose and its key characteristics.	✔	➖
identity_class	text	The type of entity that this Identity describes, e.g., an individual or organization. ['individual', 'group', 'system', 'organization', 'class', 'unknown']	➖	➖
name	text	The name of this Identity. When referring to a specific entity (e.g., an individual or organization), this property SHOULD contain the canonical name of the specific entity.	➖	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
roles	text	The list of roles that this Identity performs (e.g., CEO, Domain Administrators, Doctors, Hospital, or Retailer).	➖	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
sectors	text	Description of the organization ['agriculture', 'aerospace', 'automotive', 'chemical', 'commercial', 'communication', 'construction', 'defense', 'education', 'energy', 'entertainment', 'financial-services', 'government', 'government emergency-services', 'government government-local', 'government-national', 'government-public-services', 'government-regional', 'healthcare', 'hospitality-leasure', 'infrastructure', 'infrastructure dams', 'infrastructure nuclear', 'infrastructure water', 'insurance', 'manufacturing', 'mining', 'non-profit', 'pharmaceuticals', 'retail', 'technology', 'telecommunication', 'transportation', 'utilities']	–	✔

ilr-impact

Institut Luxembourgeois de Regulation - Impact.

ilr-impact 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	Multiple
duree	text	Duree de l'incident en hh : mm	✔	—
nombre-utilisateurs-touches	text	Nombre d'utilisateurs touches par l'incident	✔	—
pourcentage-utilisateurs-touches	text	Pourcentage d'utilisateurs du service touches par l'incident	✔	—
service	text	Service impacte par l'incident ['Telephonie fixe', 'Acces Internet fixe', 'Telephonie mobile', 'Acces Internet mobile']	✔	✔

ilr-notification-incident

Institut Luxembourgeois de Regulation - Notification d'incident.

ilr-notification-incident 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	Multiple
actions-corrective	text	Actions correctives a long terme	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
actions-posterieur	text	Actions posterieures de l'incident pour minimiser le risque	✔	—
autres-informations	text	Autres informations concernant la nature de l'incident notamment la liste des actifs affectes et les causes subsequentes eventuelles, declenches par la cause initiale	✔	—
cause-initiale-incident	text	Cause initiale de l'incident ['Erreur humaine', "Defaut systeme 'hardware', 'software', 'procedures'", 'Attaque malveillante', 'Defaut d'une partie tierce ou externe', 'Catastrophe naturelle']	✔	—
date-incident	datetime	Date/heure de la detection de l'incident:	✔	—
date-pre-notification	text	Date de la pre-notification	✔	—
delimitation-geographique	text	Delimitation geographique ['Nationale', 'Regionale']	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
description-incident	text	Description generale de l'incident	✔	—
description-probleme-services-urgence	text	Description du probleme sur les services d'urgences impactes	✔	—
details-service	text	Details relatifs au service concerne et a l'impact de l'incident	✔	—
email-contact-incident	text	Email de la personne de contact en rapport avec l'incident	✔	—
impact-servicesw-urgence	text	Services d'urgences impactes ? ['Oui', 'Non']	✔	—
interconnections-affectees	text	Interconnections nationales et/ou internationales affectees	✔	—
nom-contact-incident	text	Nom de la personne de contact en rapport avec l'incident	✔	—
nom-entreprise	text	Nom de l'entreprise notifiee	✔	—
remarques	text	Remarque(s), notamment les experiences gagnees et les leçons tirees de l'incident	✔	—
telephone-contact-incident	text	Telephone de la personne de contact en rapport avec l'incident	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
traitement-incident	text	Traitement de l'incident et actions effectuees en ordre chronologique	✔	—
zone-impactee	text	zones/communes/villes impactees	✔	✔

image

Object describing an image file.

image 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	Multiple
archive	link	Archive of the image (Internet Archive, Archive.is, etc).	—	✔
attachment	attachment	The image file.	—	—
filename	filename	The image filename.	—	—
image-text	text	Raw text of image	—	—
link	link	Original link into the image (Supposed harmless)	—	—
url	url	Original URL location of the image (potentially malicious)	—	—
username	text	Username who posted the image.	—	—

impersonation

Represent an impersonating account.

impersonation 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	Multiple
account-name	text	Name of the impersonating account	—	—
account-url	url	url of the impersonating account	—	—
impersonated-account-name	text	Name of the impersonated account	—	—
impersonated-account-url	link	url of the impersonated account	—	—
objective	text	Objective of the impersonation ['Information stealing', 'Disinformation', 'Distrusting', 'Advertising', 'Parody', 'Other']	✔	✔
real-name	text	Real name of the impersonated person or entity	—	—
type	text	Type of the account ['Person', 'Association', 'Enterprise', 'Other']	✔	—
type-of-account	text	Type of the impersonated account ['Twitter', 'Facebook', 'LinkedIn', 'Reddit', 'Google+', 'Instagram', 'Forum', 'Other']	✔	—

imsi-catcher

IMSI Catcher entry object based on the open source IMSI cather.

imsi-catcher 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	Multiple
brand	text	Brand associated with the IMSI registration.	✔	—
cellid	text	CellID	✔	—
country	text	Country where the IMSI is registered.	✔	—
first-seen	datetime	When the IMSI has been accessible or seen for the first time.	✔	—
imsi	text	A usually unique International Mobile Subscriber Identity (IMSI) is allocated to each mobile subscriber in the GSM/UMTS/EPS system. IMSI can also refer to International Mobile Station Identity in the ITU nomenclature.	—	—
lac	text	LAC - Location Area Code	✔	—
mcc	text	MCC - Mobile Country Code	✔	—
mnc	text	MNC - Mobile Network Code	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
operator	text	Operator associated with the IMSI registration.	✔	—
seq	integer	A sequence number for the collection	✔	—
text	text	A description of the IMSI record.	✔	—
tmsi-1	text	Temporary Mobile Subscriber Identities (TMSI) to visiting mobile subscribers can be allocated.	—	—
tmsi-2	text	Temporary Mobile Subscriber Identities (TMSI) to visiting mobile subscribers can be allocated.	—	—

incident

Incident object template as described in STIX 2.1 Incident object and its core extension.

incident 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	Multiple
criticality	text	Criticality of the incident ['Not Specified', 'False Positive', 'Low', 'Moderate', 'High', 'Extreme']	✔	—
description	text	Description of the incident.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
detection_method	text	Methods used to detect the activity. ['automated-tool', 'human-review', 'message-from-attacker', 'system-outage', 'user-reporting']	✔	✔
determination	text	Determination on the outcome of the incident. ['blocked', 'successful-attempt', 'failed-attempt', 'false-positive', 'low-value', 'suspected']	✔	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
incident_type	text	Type of incident ['aggregation-information-phishing-schemes', 'benign', 'blocked', 'brute-force-attempt', 'c&c-server-hosting', 'compromised-system', 'confirmed', 'connection-malware-port', 'connection-malware-system', 'content-forbidden-by-law', 'control-system-bypass', 'copyrighted-content', 'data-exfiltration', 'deferred', 'deletion-information', 'denial-of-service', 'destruction', 'dictionary-attack-attempt', 'discarded', 'disruption-data-transmission', 'dissemination-malware-email', 'dissemination-phishing-emails', 'dns-cache-poisoning', 'dns-local-resolver-hijacking', 'dns-spoofing-registered', 'dns-rebinding', 'dns-server-compromise', 'dns-spoofing-	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
investigation_status	text	Current status of the incident investigation. ['closed', 'new', 'open']	✔	—
name	text	Name of the incident.	—	—
recoverability	text	Recoverability of the incident, with respect to feasibility and required time and resources. ['extended', 'not-applicable', 'not-recoverable', 'regular', 'supplemented']	✔	—
score	text	Incident score, with a name, an optional description and the numeric score value.	—	✔

infrastructure

The Infrastructure object represents a type of TTP and describes any systems, software services and any associated physical or virtual resources intended to support some purpose (e.g., C2 servers used as part of an attack, device or server that are part of defense, database servers targeted by an attack, etc.). While elements of an attack can be represented by other objects, the Infrastructure object represents a named group of related data that constitutes the infrastructure. STIX 2.1 - 4.8.

infrastructure 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	Multiple
alias	text	Alternative names used to identify this Infrastructure.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
description	text	A description that provides more details and context about the Infrastructure, potentially including its purpose, how it is being used, how it relates to other intelligence activities captured in related objects, and its key characteristics.	➖	➖
infrastructure_type	text	The type of infrastructure being described. The values for this property SHOULD come from the infrastructure-type-ov open vocabulary. ['amplification', 'anonymization', 'botnet', 'command-and-control', 'exfiltration', 'hosting-malware', 'hosting-target-lists', 'phishing', 'reconnaissance', 'staging', 'unknown']	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
kill_chain_phases	text	The list of Kill Chain Phases for which this Infrastructure is used. ['(1) Reconnaissance', '(2) Weaponization', '(3) Deliver', '(4) Exploitation', '(5) Installation', '(6) Command and Control', '(7) Actions on objectives']	✔	—
name	text	A name or characterizing text used to identify the Infrastructure.	—	—

instagram-account

Instagram account.

instagram-account 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	Multiple
account-id	text	Account id.	—	—
account-name	text	Account name.	—	—
archive	link	Archive of the account (Internet Archive, Archive.is, etc).	✔	✔
attachment	attachment	A screen capture or exported list of contacts etc.	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
description	text	A description of the user.	—	—
is-verified	boolean	If the user is verified.	—	—
link	link	Original link to the page (supposed harmless).	—	—
url	url	Original URL location of the page (potentially malicious).	—	—
user-avatar	attachment	A user profile picture or avatar.	—	✔

instant-message

Instant Message (IM) object template describing one or more IM message.

> instant-message 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	Multiple
app-used	text	The IM application used to send the message. ['WhatsApp', 'Google Hangouts', 'Facebook Messenger', 'Telegram', 'Signal', 'WeChat', 'BlackBerry Messenger', 'TeamSpeak', 'TorChat', 'Tox', 'RetroShare', 'Slack', 'Wire', 'Threema', 'Discord', 'Mumble', 'Jabber', 'Twitter', 'Mattermost']	✔	➖
archive	link	Archive of the original message (Internet Archive, Archive.is, etc).	➖	✔
attachment	attachment	The message file or screen capture.	➖	✔
body	text	Message body of the IM.	➖	➖
from-name	text	Name of the person that sent the message.	➖	✔
from-number	phone-number	Phone number used to send the message.	➖	✔
from-user	text	User account that sent the message.	➖	✔
link	link	Original link into the message (Supposed harmless).	➖	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
received-date	datetime	Received date of the message.	✔	—
sent-date	datetime	Initial sent date of the message.	✔	—
subject	text	Subject of the message if any.	—	—
to-name	text	Name of the person that received the message.	—	✔
to-number	phone-number	Phone number receiving the message.	—	✔
to-user	text	User account that received the message.	—	✔
url	url	Original URL location of the message (potentially malicious).	—	—

instant-message-group

Instant Message (IM) group object template describing a public or private IM group, channel or conversation.

instant-message-group 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	Multiple
app-used	text	The IM application used to send the message. ['WhatsApp', 'Google Hangouts', 'Facebook Messenger', 'Telegram', 'Signal', 'WeChat', 'BlackBerry Messenger', 'TeamSpeak', 'TorChat', 'Tox', 'RetroShare', 'Slack']	✔	✔
archive	link	Archive of the original group (Internet Archive, Archive.is, etc).	—	✔
attachment	attachment	A screen capture or exported list of contacts, group members, etc.	—	✔
group-alias	text	Aliases of group, channel or community.	—	✔
group-name	text	The name of the group, channel or community.	—	—
link	link	Original link into the group (Supposed harmless).	—	—
person-name	text	A person who is a member of the group.	—	✔
url	url	Original URL location of the group (potentially malicious).	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
username	text	A user account who is a member of the group.	➖	✔

integrity-impact

Integrity Impact object as described in STIX 2.1 Incident object extension.

integrity-impact 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	Multiple
alteration	text		✔	➖
criticality	text	Criticality of the impact ['Not Specified', 'False Positive', 'Low', 'Moderate', 'High', 'Extreme']	✔	➖
description	text	Additional details about the impact.	➖	➖
end_time	datetime	The date and time the impact was last recorded.	➖	➖
end_time_fidelity	text	Level of fidelity that the `end_time` is recorded in. ['day', 'hour', 'minute', 'month', 'second', 'year']	✔	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
information_type	text	Type of information that had its confidentiality compromised. ['classified-material', 'communication', 'credentials-admin', 'credentials-user', 'financial', 'leval', 'payment', 'phi', 'pii', 'proprietary']	✔	—
record_count	counter	The number of records of this type that were compromised.	✔	—
record_size	size-in-bytes	The amount of data that was compromised in bytes.	✔	—
recoverability	text	Recoverability of this particular impact with respect to feasibility and required time and resources. ['extended', 'not-applicable', 'not-recoverable', 'regular', 'supplemented']	✔	—
start_time	datetime	The date and time the impact was first recorded.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
start_time_fidelity	text	Level of fidelity that the `start_time` is recorded in. ['day', 'hour', 'minute', 'month', 'second', 'year']	✔	—

intel471-vulnerability-intelligence

Intel 471 vulnerability intelligence object.

> intel471-vulnerability-intelligence 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	Multiple
activity-location-open-source	boolean	The vulnerability is being discussed in open source. ['True', 'False']	✔	—
activity-location-private	boolean	The vulnerability is being discussed in private/direct communications. ['True', 'False']	✔	—
activity-location-underground	boolean	The vulnerability is being discussed in the underground. ['True', 'False']	✔	—
countermeasures	text	Summary of countermeasures to protect against the vulnerability.	✔	—
cve-id	text	The vulnerability's CVE ID.	—	—
cvss-score-v2	float	CVSS score (version 2).	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
cvss-score-v3	float	CVSS score (version 3).	✔	—
detection	text	Detection signatures/definitions exist for the vulnerability.	✔	—
exploit-status-available	boolean	Exploit code for the vulnerability is available. ['True', 'False']	✔	—
exploit-status-not-observed	boolean	Exploit code or usage has not been observed for the vulnerability. ['True', 'False']	✔	—
exploit-status-productized	boolean	There is a module for the vulnerability in commercial exploit kits or network security tools. ['True', 'False']	✔	—
exploit-status-weaponized	boolean	The vulnerability has been used in an attack or has been included in an exploit kit. ['True', 'False']	✔	—
interest-level-disclosed-publicly	boolean	The vulnerability has been disclosed publicly. ['True', 'False']	✔	—
interest-level-exploit-sought	boolean	An exploit for the vulnerability is being sought. ['True', 'False']	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
interest-level-researched-publicly	boolean	The vulnerability has been researched or documented publicly. ['True', 'False']	✔	—
modified	datetime	Last modification date.	✔	—
patch-status	text	Availability of a patch for the vulnerability.	✔	—
product-name	text	Product name.	✔	—
proof-of-concept	text	Proof of concept code or demonstration exists.	✔	—
published	datetime	Initial publication date.	✔	—
references	link	External references.	—	✔
risk-level	text	Risk level of the vulnerability.	✔	—
summary	text	Summary of the vulnerability.	✔	—
underground-activity-status	text	Indicates if underground activity has been observed for the vulnerability.	✔	—
underground-activity-summary	text	Description of underground activity related to the vulnerability.	✔	—
vendor-name	text	Vendor name.	✔	—
vulnerability-status	text	The status of vulnerability.	✔	—
vulnerability-type	text	The type of vulnerability.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
vulnerable-configuration	text	Vulnerable configuration in CPE format.	➖	✔

intelmq_event

IntelMQ Event.

intelmq_event 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	Multiple
classification.identifier	text	The lowercase identifier defines the actual software or service (e.g. 'heartbleed' or 'ntp_version') or standardized malware name (e.g. 'zeus'). Note that you MAY overwrite this field during processing for your individual setup. This field is not standardized across IntelMQ setups/users.	➖	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
classification.taxonomy	text	We recognize the need for the CSIRT teams to apply a static (incident) taxonomy to abuse data. With this goal in mind the type IOC will serve as a basis for this activity. Each value of the dynamic type mapping translates to a an element in the static taxonomy. The European CSIRT teams for example have decided to apply the eCSIRT.net incident classification. The value of the taxonomy key is thus a derivative of the dynamic type above. For more information about check [ENISA taxonomies](http://www.enisa.europa.eu/activities/cert/support/incident-management/browsable/incident-handling-process/incident-taxonomy/existing-taxonomies).	–	–

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
classification.type	text	The abuse type IOC is one of the most crucial pieces of information for any given abuse event. The main idea of dynamic typing is to keep our ontology flexible, since we need to evolve with the evolving threatscape of abuse data. In contrast with the static taxonomy below, the dynamic typing is used to perform business decisions in the abuse handling pipeline. Furthermore, the value data set should be kept as minimal as possible to avoid 'type explosion', which in turn dilutes the business value of the dynamic typing. In general, we normally have two types of abuse type IOC: ones referring to a compromised resource or ones referring to pieces of the criminal infrastructure, such as a command and control servers for example.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
comment	text	Free text commentary about the abuse event inserted by an analyst.	—	—
destination.abuse_contact	text	Abuse contact for destination address. A comma separated list.	—	—
destination.account	text	An account name or email address, which has been identified to relate to the destination of an abuse event.	—	—
destination.allocated	datetime	Allocation date corresponding to BGP prefix.	—	—
destination.as_name	text	The autonomous system name to which the connection headed.	—	—
destination.asn	AS	The autonomous system number to which the connection headed.	—	—
destination.domain_suffix	text	The suffix of the domain from the public suffix list.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
destination.fqdn	domain	A DNS name related to the host from which the connection originated. DNS allows even binary data in DNS, so we have to allow everything. A final point is stripped, string is converted to lower case characters.	–	–
destination.geolocation.cc	text	Country-Code according to ISO3166-1 alpha-2 for the destination IP.	–	–
destination.geolocation.city	text	Some geolocation services refer to city-level geolocation.	–	–
destination.geolocation.country	text	The country name derived from the ISO3166 country code (assigned to cc field).	–	–
destination.geolocation.latitude	float	Latitude coordinates derived from a geolocation service, such as MaxMind geoip db.	–	–
destination.geolocation.longitude	float	Longitude coordinates derived from a geolocation service, such as MaxMind geoip db.	–	–

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
destination.geolocation.region	text	Some geolocation services refer to region-level geolocation.	—	—
destination.geolocation.state	text	Some geolocation services refer to state-level geolocation.	—	—
destination.ip	ip-dst	The IP which is the target of the observed connections.	—	—
destination.local_hostname	hostname	Some sources report a internal hostname within a NAT related to the name configured for a compromized system	—	—
destination.local_ip	ip-dst	Some sources report a internal (NATed) IP address related a compromized system. N.B. RFC1918 IPs are OK here.	—	—
destination.network	ip-dst	CIDR for an autonomous system. Also known as BGP prefix. If multiple values are possible, select the most specific.	—	—
destination.port	port	The port to which the connection headed.	—	—
destination.registry	text	The IP registry a given ip address is allocated by.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
destination.reverse_dns	text	Reverse DNS name acquired through a reverse DNS query on an IP address. N.B. Record types other than PTR records may also appear in the reverse DNS tree. Furthermore, unfortunately, there is no rule prohibiting people from writing anything in a PTR record. Even JavaScript will work. A final point is stripped, string is converted to lower case characters.	—	—
destination.tor_node	boolean	If the destination IP was a known tor node. ['True', 'False']	—	—
destination.url	url	A URL denotes on IOC, which refers to a malicious resource, whose interpretation is defined by the abuse type. A URL with the abuse type phishing refers to a phishing resource.	—	—
destination.urlpath	text	The path portion of an HTTP or related network request.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
event_description.target	text	Some sources denominate the target (organization) of a an attack.	–	–
event_description.text	text	A free-form textual description of an abuse event.	–	–
event_description.url	url	A description URL is a link to a further description of the the abuse event in question.	–	–

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
event_hash	text	Computed event hash with specific keys and values that identify a unique event. At present, the hash should default to using the SHA1 function. Please note that for an event hash to be able to match more than one event (deduplication) the receiver of an event should calculate it based on a minimal set of keys and values present in the event. Using for example the observation time in the calculation will most likely render the checksum useless for deduplication purposes.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
extra	text	All anecdotal information, which cannot be parsed into the data harmonization elements. E.g. os.name, os.version, etc. **Note**: this is only intended for mapping any fields which can not map naturally into the data harmonization. It is not intended for extending the data harmonization with your own fields.	—	—
feed.accuracy	float	A float between 0 and 100 that represents how accurate the data in the feed is	—	—
feed.code	text	Code name for the feed, e.g. DFGS, HSDAG etc.	—	—
feed.documentation	text	A URL or hint where to find the documentation of this feed.	—	—
feed.name	text	Name for the feed, usually found in collector bot configuration.	—	—
feed.provider	text	Name for the provider of the feed, usually found in collector bot configuration.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
feed.url	url	The URL of a given abuse feed, where applicable	—	—
malware.hash.md5	md5	A string depicting an MD5 checksum for a file, be it a malware sample for example.	—	—
malware.hash.sha1	sha1	A string depicting a SHA1 checksum for a file, be it a malware sample for example.	—	—
malware.hash.sha256	sha256	A string depicting a SHA256 checksum for a file, be it a malware sample for example.	—	—
malware.name	text	The malware name in lower case.	—	—
malware.version	text	A version string for an identified artifact generation, e.g. a crime-ware kit.	—	—
misp.attribute_uuid	text	MISP - Malware Information Sharing Platform & Threat Sharing UUID of an attribute.	—	—
misp.event_uuid	text	MISP - Malware Information Sharing Platform & Threat Sharing UUID.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
output	text	Event data converted into foreign format, intended to be exported by output plugin.	—	—
protocol.application	text	e.g. vnc, ssh, sip, irc, http or smtp.	—	—
protocol.transport	text	e.g. tcp, udp, icmp.	—	—
raw	text	The original line of the event from encoded in base64.	—	—
rtir_id	integer	Request Tracker Incident Response ticket id.	—	—
screenshot_url	url	Some source may report URLs related to a an image generated of a resource without any metadata. Or an URL pointing to resource, which has been rendered into a webshot, e.g. a PNG image and the relevant metadata related to its retrieval/generation.	—	—
source.abuse_contact	text	Abuse contact for source address. A comma separated list.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
source.account	text	An account name or email address, which has been identified to relate to the source of an abuse event.	–	–
source.allocated	datetime	Allocation date corresponding to BGP prefix.	–	–
source.as_name	text	The autonomous system name from which the connection originated.	–	–
source.asn	AS	The autonomous system number from which originated the connection.	–	–
source.domain_suffix	text	The suffix of the domain from the public suffix list.	–	–
source.fqdn	domain	A DNS name related to the host from which the connection originated. DNS allows even binary data in DNS, so we have to allow everything. A final point is stripped, string is converted to lower case characters.	–	–
source.geolocation.cc	text	Country-Code according to ISO3166-1 alpha-2 for the source IP.	–	–

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
source.geolocation.city	text	Some geolocation services refer to city-level geolocation.	–	–
source.geolocation.country	text	The country name derived from the ISO3166 country code (assigned to cc field).	–	–
source.geolocation.cymru_cc	text	The country code denoted for the ip by the Team Cymru asn to ip mapping service.	–	–
source.geolocation.geoip_cc	text	MaxMind Country Code (ISO3166-1 alpha-2).	–	–
source.geolocation.latitude	float	Latitude coordinates derived from a geolocation service, such as MaxMind geoip db.	–	–
source.geolocation.longitude	float	Longitude coordinates derived from a geolocation service, such as MaxMind geoip db.	–	–
source.geolocation.region	text	Some geolocation services refer to region-level geolocation.	–	–
source.geolocation.state	text	Some geolocation services refer to state-level geolocation.	–	–
source.ip	ip-src	The ip observed to initiate the connection	–	–

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
source.local_hostname	hostname	Some sources report a internal hostname within a NAT related to the name configured for a compromised system	—	—
source.local_ip	ip-src	Some sources report a internal (NATed) IP address related a compromised system. N.B. RFC1918 IPs are OK here.	—	—
source.network	ip-src	CIDR for an autonomous system. Also known as BGP prefix. If multiple values are possible, select the most specific.	—	—
source.port	port	The port from which the connection originated.	—	—
source.registry	text	The IP registry a given ip address is allocated by.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
source.reverse_dns	text	Reverse DNS name acquired through a reverse DNS query on an IP address. N.B. Record types other than PTR records may also appear in the reverse DNS tree. Furthermore, unfortunately, there is no rule prohibiting people from writing anything in a PTR record. Even JavaScript will work. A final point is stripped, string is converted to lower case characters.	—	—
source.tor_node	boolean	If the source IP was a known tor node. ['True', 'False']	—	—
source.url	url	A URL denotes an IOC, which refers to a malicious resource, whose interpretation is defined by the abuse type. A URL with the abuse type phishing refers to a phishing resource.	—	—
source.urlpath	text	The path portion of an HTTP or related network request.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
status	text	Status of the malicious resource (phishing, dropzone, etc), e.g. online, offline.	—	—
time.observation	datetime	The time the collector of the local instance processed (observed) the event.	✔	—
time.source	datetime	The time of occurence of the event as reported the feed (source).	✔	—
tlp	text	Traffic Light Protocol level of the event.	—	—

intelmq_report

IntelMQ Report.

intelmq_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	Multiple
extra	text	All anecdotal information of the report, which cannot be parsed into the data harmonization elements. E.g. subject of mails, etc. This is data is not automatically propagated to the events.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
feed.accuracy	float	A float between 0 and 100 that represents how accurate the data in the feed is	—	—
feed.code	text	Code name for the feed, e.g. DFGS, HSDAG etc.	—	—
feed.documentation	text	A URL or hint where to find the documentation of this feed.	—	—
feed.name	text	Name for the feed, usually found in collector bot configuration.	—	—
feed.provider	text	Name for the provider of the feed, usually found in collector bot configuration.	—	—
feed.url	url	The URL of a given abuse feed, where applicable	—	—
raw	text	The original raw and unparsed data encoded in base64.	—	—
rtir_id	integer	Request Tracker Incident Response ticket id.	—	—
time.observation	datetime	The time the collector of the local instance processed (observed) the event.	✔	—

internal-reference

Internal reference.

internal-reference 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	Multiple
comment	comment	Comment associated to the identifier.	—	—
identifier	text	Identifier of the reference. Should be unique in your system.	—	—
link	link	Link associated to the identifier.	—	—
type	text	Type of internal reference.	—	—

interpol-notice

An object which describes a Interpol notice.

interpol-notice 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	Multiple
alias	text	Alias name or known as.	—	✔
charges	text	Charges published as provided by requesting entity	✔	✔
colour-of-eyes	text	Description of a person's colour of eyes.	✔	—
colour-of-hair	text	Description of a person's colour of hair.	✔	—
date-of-birth	date-of-birth	Date of birth of a natural person (in YYYY-MM-DD format).	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
date-of-disappearance	text	Date of disappearance of a missing person.	➖	➖
distinguishing-marks-and-characteristics	text	Distinguishing marks and characteristics of a person.	✔	➖
father-s-family-name-&-forename	text	Father’s family name & forename.	➖	➖
forename	first-name	First name of a natural person.	✔	➖
height	text	Height of a person.	✔	➖
language-spoken	text	Languages spoken by a person.	✔	✔
mother-s-family-name-&-forename	text	Mother’s family name & forename.	➖	➖
nationality	nationality	The nationality of a natural person.	✔	✔
notice-color	text	The color/type of the notice ['Red', 'Yellow', 'Blue', 'Black', 'Green', 'Orange', 'Purple']	➖	➖
place-of-birth	place-of-birth	Place of birth of a natural person.	✔	➖
place-of-disappearance	text	Place of birth of a natural person.	➖	➖
portrait	attachment	Portrait of the person.	➖	✔
present-family-name	last-name	Last name of a natural person.	➖	➖
sex	gender	The gender of a natural person. ['Male', 'Female', 'Other', 'Prefer not to say']	✔	➖
weight	text	weight of a person.	✔	➖

intrusion-set

A object template describing an Intrusion Set as defined in STIX 2.1. An Intrusion Set is a grouped set of adversarial behaviors and resources with common properties that is believed to be orchestrated by a single organization. An Intrusion Set may capture multiple Campaigns or other activities that are all tied together by shared attributes indicating a commonly known or unknown Threat Actor. New activity can be attributed to an Intrusion Set even if the Threat Actors behind the attack are not known. Threat Actors can move from supporting one Intrusion Set to supporting another, or they may support multiple Intrusion Sets. Where a Campaign is a set of attacks over a period of time against a specific set of targets to achieve some objective, an Intrusion Set is the entire attack package and may be used over a very long period of time in multiple Campaigns to achieve potentially multiple purposes. While sometimes an Intrusion Set is not active, or changes focus, it is usually difficult to know if it has truly disappeared or ended. Analysts may have varying level of fidelity on attributing an Intrusion Set back to Threat Actors and may be able to only attribute it back to a nation state or perhaps back to an organization within that nation state.

intrusion-set 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	Multiple
aliases	text	Alternative names used to identify this Intrusion Set.	—	✔
description	text	A description that provides more details and context about the Intrusion Set, potentially including its purpose and its key characteristics.	—	—
first_seen	datetime	The time that the intrusion set was first seen.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
goals	text	The high-level goals of this Intrusion Set, namely, what are they trying to do. For example, they may be motivated by personal gain, but their goal is to steal credit card numbers. To do this, they may execute specific Campaigns that have detailed objectives like compromising point of sale systems at a large retailer. Another example: to gain information about latest merger and IPO information from ACME Bank.	✔	✔
last_seen	datetime	The time that the intrusion set was last seen.	—	—
name	text	A name used to identify this Intrusion Set.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
primary-motivation	text	The primary reason, motivation, or purpose behind this Intrusion Set. The motivation is why the Intrusion Set wishes to achieve the goal (what they are trying to achieve). For example, an Intrusion Set with a goal to disrupt the finance sector in a country might be motivated by ideological hatred of capitalism. ['accidental - A non-hostile actor whose benevolent or harmless intent inadvertently causes harm. For example, a well-meaning and dedicated employee who through distraction or poor training unintentionally causes harm to his or her organization.', "coercion - Being forced to act on someone else's behalf. Adversaries who are motivated by coercion are often forced through intimidation or blackmail to act illegally for	✔	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
resource_level	text	This property specifies the organizational level at which this Intrusion Set typically works, which in turn determines the resources available to this Intrusion Set for use in an attack. ['individual - Resources limited to the average individual; Threat Actor acts independently.', 'club - Members interact on a social and volunteer basis, often with little personal interest in the specific target. An example might be a core group of unrelated activists who regularly exchange tips on a particular blog. Group persists long term.', "contest - A short-lived and perhaps anonymous interaction that concludes when the participants have achieved a single goal. For example, people who break into systems just for thrills or prestige may hold a contest	✔	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
secondary-motivation	text	The secondary reasons, motivations, or purposes behind this Intrusion Set. These motivations can exist as an equal or near-equal cause to the primary motivation. However, it does not replace or necessarily magnify the primary motivation, but it might indicate additional context. The position in the list has no significance. ['accidental - A non-hostile actor whose benevolent or harmless intent inadvertently causes harm. For example, a well-meaning and dedicated employee who through distraction or poor training unintentionally causes harm to his or her organization.', "coercion - Being forced to act on someone else's behalf. Adversaries who are motivated by coercion are often forced through	✔	—

iot-device

An IoT device.

iot-device 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	Multiple
architecture	text	architecture of the IoT device ['ARC', 'ARM', 'M68000', 'MicroBlaze', 'MIPS', 'NSD32', 'Nios II', 'PowerPC', 'RISC-V', 'Sandbox', 'SH', 'x86', 'Xtensa']	—	—
boot-log	attachment	Boot log of the IoT device	—	✔
fcc-id	text	FCC-ID of the IoT device	—	✔
jtag-interface	text	JTAG interface of the IoT device ['Yes', 'No', 'Unknown', 'Disabled']	✔	—
model	text	Model of the IoT device	—	✔
picture-device	attachment	Picture of the IoT device	—	✔
picture-pcb	attachment	Picture of the IoT device PCB	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
platform	text	Platform of of the IoT device ['mach-aspeed', 'mach-at91', 'mach-bcm283x', 'mach-bcmstb', 'mach-cortina', 'mach-davinci', 'mach-exynos', 'mach-highbank', 'mach-imx', 'mach-integrator', 'mach-k3', 'mach-keystone', 'mach-kirkwood', 'mach-mediatek', 'mach-meson', 'mach-mvebu', 'mach-omap2', 'mach-orion5x', 'mach-owl', 'mach-qemu', 'mach-rmobile', 'mach-rockchip', 'mach-s5pc1xx', 'mach-snapdragon', 'mach-socfpga', 'mach-sti', 'mach-stm32', 'mach-stm32mp', 'mach-sunxi', 'mach-tegra', 'mach-u8500', 'mach-uniphier', 'mach-versal', 'mach-versatile', 'mach-zynq', 'mach-zynqmp', 'mach-zynqmp-r5', 'mcf5227x', 'mcf523x', 'mcf52x2', 'mcf530x', 'mcf532x', 'mcf5445x', 'mcf547x_8x', 'mach-ath79',	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
reference	link	Reference of the IoT device	—	✔
serial-interface	text	Serial interface of the IoT device ['Yes', 'No', 'Unknown', 'Disabled']	✔	—
spi-interface	text	SPI interface of the IoT device ['Yes', 'No', 'Unknown', 'Disabled']	✔	—
vendor	text	Vendor of the IoT device	—	—

iot-firmware

A firmware for an IoT device.

iot-firmware 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	Multiple
binwalk-entropy-graph	attachment	Entropy graph of the firmware	✔	—
binwalk-output	attachment	Binwalk output of the firmware image	—	—
boot-log	attachment	Boot log of the IoT device for this firmware	—	✔
filename	text	Filename of the firmware	—	—
firmware	attachment	Firmware of the IoT device	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
format	text	Format of the firmware ['raw', 'Intel hex', 'Motorola S-Record', 'Unknown']	—	—
md5	md5	[Insecure] MD5 hash (128 bits)	—	—
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	—	—
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	—	—
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	—	—
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	—	—
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	—	—
size-in-bytes	size-in-bytes	Size of the file, in bytes	✔	—
version	text	Version of the firmware	—	✔

ip-api-address

IP Address information. Useful if you are pulling your ip information from ip-api.com.

ip-api-address 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	Multiple
ISP	text	ISP.	✔	—
asn	AS	Autonomous System Number	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
city	text	City.	✔	—
country	text	Country name	✔	—
country-code	text	Country code	✔	—
first-seen	datetime	First time the ASN was seen	✔	—
ip-src	ip-src	Source IP address of the network connection.	—	—
last-seen	datetime	Last time the ASN was seen	✔	—
latitude	float	The latitude is the decimal value of the latitude in the World Geodetic System 84 (WGS84) reference.	✔	—
longitude	float	The longitude is the decimal value of the longitude in the World Geodetic System 84 (WGS84) reference	✔	—
organization	text	organization	✔	—
region	text	Region. example: California.	✔	—
region-code	text	Region code. example: CA	✔	—
state	text	State.	✔	—
zipcode	text	Zip Code.	✔	—

ip-port

An IP address (or domain or hostname) 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	Multiple
AS	AS	Autonomous system	✔	✔
country-code	text	Country Code	✔	—
domain	domain	Domain	—	✔
dst-port	port	Destination port	✔	✔
first-seen	datetime	First time the tuple has been seen	✔	—
hostname	hostname	Hostname	—	✔
ip	ip-dst	IP Address	—	✔
ip-dst	ip-dst	destination IP address	—	✔
ip-src	ip-src	source IP address	—	✔
last-seen	datetime	Last time the tuple has been seen	✔	—
protocol	text	Protocol	✔	—
src-port	port	Source port	✔	✔
text	text	Description of the tuple	✔	—

irc

An IRC object to describe an IRC server and the associated channels.

irc 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	Multiple
channel	text	IRC channel associated to the IRC server	—	✔
dst-port	port	Destination port to reach the IRC server	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
first-seen	datetime	First time the IRC server with the associated channels has been seen	✔	—
hostname	hostname	Hostname of the IRC server	—	✔
ip	ip-dst	IP address of the IRC server	—	✔
last-seen	datetime	Last time the IRC server with the associated channels has been seen	✔	—
nickname	text	IRC nickname used to connect to the associated IRC server and channels	—	✔
text	text	Description of the IRC server	✔	—

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	Multiple
description	text	Type of detected software ie software, malware	—	—
first-seen	datetime	First seen of the SSL/TLS handshake	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
ip-dst	ip-dst	Destination IP address	—	—
ip-src	ip-src	Source IP Address	—	—
ja3-fingerprint-md5	ja3-fingerprint-md5	Hash identifying source	—	—
last-seen	datetime	Last seen of the SSL/TLS handshake	✔	—

ja3s

JA3S is JA3 for the Server side of the SSL/TLS communication and fingerprints how servers respond to particular clients. JA3S fingerprints are composed of Server Hello packet; SSL Version, Cipher, SSLExtensions. https://github.com/salesforce/ja3.

ja3s 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	Multiple
description	text	Type of detected software ie software, malware, c&c	—	—
domain	domain	Destination domain	—	—
first-seen	datetime	First seen of the SSL/TLS handshake	✔	—
hostname	hostname	Destination hostname	—	—
ip-dst	ip-dst	Destination IP address	—	—
ip-src	ip-src	Source IP Address	—	—
ja3-fingerprint-md5	ja3-fingerprint-md5	Hash identifying client	—	—
ja3s-fingerprint-md5	ja3-fingerprint-md5	Hash identifying server	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
last-seen	datetime	Last seen of the SSL/TLS handshake	✔	—

ja4-plus

JA4 is a technique for creating network fingerprints that are easy to produce and can be easily shared for threat intelligence. https://github.com/FoxIO-LLC/ja4/blob/main/technical_details/README.md.

ja4-plus 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	Multiple
description	text	Description of the JA4+ fingerprint including scope, collection or specific notes which could help an analyst to reproduce the calculation.	—	—
ip-src	ip-src	IP address related to this JA4+ fingerprint.	—	✔
ja4-fingerprint	text	A JA4+ fingerprint as defined by the JA4+ standard in textual format.	—	—
ja4-type	text	One of the JA4+ type expressed as short name. ['JA4', 'JA4S', 'JA4H', 'JA4L', 'JA4X', 'JA4SSH', 'JA4T', 'JA4TS', 'JA4TScan']	—	—

jarm

Jarm object to describe an TLS/SSL implementation used for malicious or legitimate use-case.

jarm 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	Multiple
jarm	jarm-fingerprint	JARM Hash of this implementation	—	—
reference	link	Reference to the tool matching this fingerprint	✔	—
scope	text	Scope of the tool ['Malicious - C2', 'Malicious - Client', 'Malicious - Unknown', 'Legitimate', 'Undefined']	✔	—
tls-implementation	text	SSL/TLS implementation matching this object	✔	—
tool	text	Tool having this jarm fingerprint	✔	—

keybase-account

Information related to a keybase account, from API Users Object.

keybase-account 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	Multiple
bio	text	Bio of the keybase user	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
cryptocurrency_addresses	btc	Associated cryptocurrency address with the keybase user	—	✔
emails	text	Emails associated with the keybase user	—	✔
full_name	text	Full name	—	—
id	text	Keybase user identifier	—	—
location	text	Location	—	—
private_keys	text	OpenPGP private keys associated with the keybase user	—	✔
public_keys	text	OpenPGP public keys associated with the keybase user	—	✔
username	text	Keybase username	—	—

language-content

The Language Content object represents text content for objects represented in languages other than that of the original object. Language content may be a translation of the original object by a third-party, a first-source translation by the original publisher, or additional official language content provided at the time of creation. STIX 2.1 ref 7.1.

language-content 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	Multiple
content	text	The contents property contains the actual Language Content (translation).	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
language	text	RFC 5646 language codes for which language content is being provided. ['af', 'af-ZA', 'ar', 'ar-AE', 'ar-BH', 'ar-DZ', 'ar-EG', 'ar-IQ', 'ar-JO', 'ar-KW', 'ar-LB', 'ar-LY', 'ar-MA', 'ar-OM', 'ar-QA', 'ar-SA', 'ar-SY', 'ar-TN', 'ar-YE', 'az', 'az-AZ', 'az-Cyrl-AZ', 'be', 'be-BY', 'bg', 'bg-BG', 'bs-BA', 'ca', 'ca-ES', 'cs', 'cs-CZ', 'cy', 'cy-GB', 'da', 'da-DK', 'de', 'de-AT', 'de-CH', 'de-DE', 'de-LI', 'de-LU', 'dv', 'dv-MV', 'el', 'el-GR', 'en', 'en-AU', 'en-BZ', 'en-CA', 'en-CB', 'en-GB', 'en-IE', 'en-JM', 'en-NZ', 'en-PH', 'en-TT', 'en-US', 'en-ZA', 'en-ZW', 'eo', 'es', 'es-AR', 'es-BO', 'es-CL', 'es-CO', 'es-CR', 'es-DO', 'es-EC', 'es-ES', 'es-GT', 'es-HN', 'es-MX', 'es-NI', 'es-PA', 'es-PE', 'es-PR', 'es-PY', 'es-SV', 'es-UY', 'es-VE', 'et', 'et-EE', 'eu', 'eu-ES', 'fa', 'fa-IR', 'fi', 'fi-FI', 'fo', 'fo-FO', 'fr', 'fr-BE', 'fr-CA', 'fr-CH', 'fr-FR', 'fr-LU', 'fr-MC', 'gl', 'gl-ES', 'gu', 'gu-IN', 'he', 'he-IL', 'hi', 'hi-IN', 'hr', 'hr-BA',	✔	—

leaked-document

Object describing a leaked document.

leaked-document 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	Multiple
archive	link	Archive of the original document (Internet Archive, Archive.is, etc).	—	✔
attachment	attachment	The leaked document file.	—	—
document-name	text	Title of the document.	—	—
document-text	text	Raw text of document	—	—
document-type	text	The type of document (not the file type). ['email', 'letterhead', 'speech', 'literature', 'photo', 'audio', 'invoice', 'receipt', 'other']	✔	✔
first-seen	datetime	When the document has been accessible or seen for the first time.	✔	—
last-seen	datetime	When the document has been accessible or seen for the last time.	✔	—
link	link	Original link into the document (Supposed harmless)	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
objective	text	Reason for leaking the document. ['Disinformation', 'Influence', 'Whistleblowing', 'Extortion', 'Other']	✔	✔
origin	text	Original source of leaked document.	—	—
purpose-of-document	text	What the document is used for. ['Identification', 'Travel', 'Health', 'Legal', 'Financial', 'Government', 'Military', 'Media', 'Communication', 'Other']	✔	✔
url	url	Original URL location of the document (potentially malicious)	—	—

legal-entity

An object to describe a legal entity.

legal-entity 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	Multiple
business	text	Business area of the entity.	—	—
commercial-name	text	Commercial name of the entity.	—	—
legal-form	text	Legal form of the entity.	—	—
logo	attachment	Logo of the entity.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
name	text	Name of the entity.	—	—
phone-number	phone-number	Phone number of the entity.	—	—
registration-number	text	Registration number of the entity in the relevant authority.	—	—
text	text	A description of the entity.	✔	—
website	link	Website of the entity.	—	—

lnk

LNK object describing a Windows LNK binary file (aka Windows shortcut).

lnk 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	Multiple
birth-droid-file-identifier	text	Birth droid volume identifier (UUIDv1 where MAC can be extracted)	—	—
birth-droid-volume-identifier	text	Droid volume identifier	—	—
droid-file-identifier	text	Droid file identifier (UUIDv1 where MAC can be extracted)	—	—
droid-volume-identifier	text	Droid volume identifier	—	—
entropy	float	Entropy of the whole file	✔	—
filename	filename	Filename on disk	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
fullpath	text	Complete path of the LNK filename including the filename	➖	✔
lnk-access-time	datetime	Access time of the LNK	✔	➖
lnk-command-line-arguments	text	LNK command line arguments	✔	➖
lnk-creation-time	datetime	Creation time of the LNK	✔	➖
lnk-description	text	LNK description	✔	➖
lnk-drive-serial-number	text	Drive serial number	➖	➖
lnk-drive-type	text	Drive type	✔	➖
lnk-file-attribute-flags	text	File attribute flags	✔	➖
lnk-file-size	size-in-bytes	Size of the target file, in bytes	✔	➖
lnk-hot-key-value	text	Hot Key value	✔	➖
lnk-icon-index	text	Icon index	✔	➖
lnk-local-path	text	Local path	✔	➖
lnk-mft-object	text	LinkTargetIDList MFT entry. Name:MFTID	SeqID	BTimestamp
➖	✔	lnk-modification-time	datetime	Modification time of the LNK
✔	➖	lnk-propertystore-sid	text	SID reference in ExtraData.PropertyStore
➖	➖	lnk-relative-path	text	Relative path
✔	➖	lnk-show-window-value	text	Show Window value
✔	➖	lnk-volume-label	text	Volume label
✔	➖	lnk-working-directory	text	LNK working path
✔	➖	machine-identifier	text	Machine identifier

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
—	—	malware-sample	malware-sample	The LNK file itself (binary)
—	—	md5	md5	[Insecure] MD5 hash (128 bits)
—	—	path	text	Path of the LNK filename complete or partial
✔	✔	pattern-in-file	pattern-in-file	Pattern that can be found in the file
—	✔	sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)
—	—	sha224	sha224	Secure Hash Algorithm 2 (224 bits)
—	—	sha256	sha256	Secure Hash Algorithm 2 (256 bits)
—	—	sha384	sha384	Secure Hash Algorithm 2 (384 bits)
—	—	sha512	sha512	Secure Hash Algorithm 2 (512 bits)
—	—	sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)
—	—	sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)
—	—	size-in-bytes	size-in-bytes	Size of the LNK file, in bytes
✔	—	ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
—	—	state	text	State of the LNK file ['Malicious', 'Harmless', 'Trusted']
✔	✔	text	text	Free text value to attach to the file
✔	✔	tlsh	tlsh	Fuzzy hash by Trend Micro: Locality Sensitive Hash

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	Multiple
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	✔	—
type	text	Type of Mach-O ['BUNDLE', 'CORE', 'DSYM', 'DYLIB', 'DYLIB_STUB', 'DYLINKER', 'EXECUTE', 'FVMLIB', 'KEXT_BUNDLE', 'OBJECT', 'PRELOAD']	—	—

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

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
text	text	Free text value to attach to the section	✔	—

mactime-timeline-analysis

Mactime template, used in forensic investigations to describe the timeline of a file activity.

> mactime-timeline-analysis 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	Multiple
activityType	text	Determines the type of activity conducted on the file at a given time ['Accessed', 'Created', 'Changed', 'Modified', 'Other']	✔	—
datetime	datetime	Date and time when the operation was conducted on the file	✔	—
file	attachment	Mactime output file	✔	—
file-path	text	Location of the file on the disc	—	—
filePermissions	text	Describes permissions assigned the file	✔	—
file_size	size-in-bytes	Determines the file size in bytes	✔	—

malware

Malware is a type of TTP that represents malicious code.

malware 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	Multiple
alias	text	Alternative name used to identify this malware or malware family.	—	✔
architecture_execution_env	text	The processor architecture that the malware instance or family is executable on. ['alpha', 'arm', 'ia-64', 'mips', 'powerpc', 'sparc', 'x86', 'x86-64']	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
capability	text	Any of the capabilities identified for the malware instance or family. ['accesses-remote-machines', 'anti-debugging', 'anti-disassembly', 'anti-emulation', 'anti-memory-forensics', 'anti-sandbox', 'anti-vm', 'captures-input-peripherals', 'captures-output-peripherals', 'captures-system-state-data', 'cleans-traces-of-infection', 'commits-fraud', 'communicates-with-c2', 'compromises-data-availability', 'compromises-data-integrity', 'compromises-system-availability', 'controls-local-machine', 'degrades-security-software', 'degrades-system-updates', 'determines-c2-server', 'emails-spam', 'escalates-privileges', 'evades-av', 'exfiltrates-data', 'fingerprints-host', 'hides-artifacts', 'hides-executing-code', 'infects-	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
description	text	A description that provides more details and context about the malware instance or family, potentially including its purpose and its key characteristics.	➖	➖
first_seen	datetime	The time that the malware instance or family was first seen.	➖	➖
implementation_language	text	The programming language used to implement the malware instance or family. ['applescript', 'bash', 'c', 'c++', 'c#', 'go', 'java', 'javascript', 'lua', 'objective-c', 'perl', 'php', 'powershell', 'python', 'ruby', 'scala', 'swift', 'typescript', 'visual-basic', 'x86-32', 'x86-64']	✔	✔
is_family	boolean	Defines whether the object represents a malware family or a malware instance.	✔	➖
last_seen	datetime	The time that the malware family or malware instance was last seen.	➖	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
malware_type	text	A set of categorizations for the malware being described. ['adware', 'backdoor', 'bot', 'bootkit', 'ddos', 'downloader', 'dropper', 'exploit-kit', 'keylogger', 'ransomware', 'remote-access-trojan', 'resource-exploitation', 'rogue-security-software', 'rootkit', 'screen-capture', 'spyware', 'trojan', 'unknown', 'virus', 'webshell', 'wiper', 'worm']	✔	✔
name	text	A name used to identify the malware instance or family. For a malware family the name MUST be defined. If a name for a malware instance is not available, the SHA-256 hash value or sample's filename MAY be used instead.	—	—

malware-analysis

Malware Analysis captures the metadata and results of a particular static or dynamic analysis performed on a malware instance or family.

malware-analysis 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	Multiple
analysis_definition_version	text	The version of the analysis definitions used by the analysis tool.	✔	—
analysis_engine_version	text	The version of the analysis engine or product that was used to perform the analysis.	✔	—
configuration_version	text	The named configuration of additional product configuration parameters for this analysis run.	✔	—
end_time	datetime	The date and time that the malware analysis ended.	—	—
module	text	The specific analysis module that was used and configured in the product during this analysis run.	—	✔
product	text	The name of the analysis engine or product that was used.	—	—
result	text	The classification result as determined by the scanner or tool analysis process. ['benign', 'malicious', 'suspicious', 'unknown']	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
result_name	text	The classification result or name assigned to the malware instance by the scanner tool.	—	—
start_time	datetime	The date and time that the malware analysis was initiated.	—	—
submitted_time	datetime	The date and time that the malware was first submitted for scanning or analysis.	—	—
version	text	The version of the analysis product that was used to perform the analysis.	✔	—

malware-config

Malware configuration recovered or extracted from a malicious binary.

malware-config 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	Multiple
config	text	Raw (decrypted, decoded) text of the malware configuration.	—	—
description	text	Description of the malware configuration	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
encrypted	text	Encrypted or encoded text of the malware configuration in base64.	—	—
file-config	attachment	File configuration as an attachment	—	—
first-seen	datetime	When the malware configuration has been seen for the first time.	✔	—
format	text	Original format of the malware configuration. ['JSON', 'yaml', 'INI', 'other']	✔	—
last-seen	datetime	When the malware configuration has been seen for the last time.	✔	—
password	text	Password or encryption key used to encrypt the malware configuration.	—	—

meme-image

Object describing a meme (image).

meme-image 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	Multiple
5Ds-of-propaganda	text	5 D's of propaganda are tactics of rebuttal used to defend against criticism and adversarial narratives. ['dismiss', 'distort', 'distract', 'dismay', 'divide']	✔	✔
a/b-test	boolean	A flag to define if this meme is part of an a/b test. If set to true, it is part of an a/b test set. ['True', 'False']	✔	➖
archive	link	Archive of the original document (Internet Archive, Archive.is, etc).	➖	✔
attachment	attachment	The image file.	➖	➖
crosspost	link	Safe site where the meme has been posted.	➖	✔
crosspost-unsafe	url	Unsafe site where the meme has been posted.	➖	✔
document-text	text	Raw text of meme	➖	➖
first-seen	datetime	When the meme has been accessible or seen for the first time.	✔	➖
last-seen	datetime	When the meme has been accessible or seen for the last time.	✔	➖
link	link	Original link into the meme (Supposed harmless)	➖	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
meme-reference	link	A link to know-your-meme or similar reference material.	—	—
objective	text	Objective of the meme. ['Disinformation', 'Advertising', 'Parody', 'Other']	✔	✔
url	url	Original URL location of the meme (potentially malicious)	—	—
username	text	Username who posted the meme.	—	—

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	Multiple
archive	link	Archive of the original document (Internet Archive, Archive.is, etc).	—	✔
attachment	attachment	The microblog post file or screen capture.	—	✔
creation-date	datetime	Initial creation of the microblog post	—	—
display-name	text	Display name of the account who posted the microblog.	—	—
embedded-link	url	Link into the microblog post	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
embedded-safe-link	link	Safe link into the microblog post	➖	✔
hashtag	text	Hashtag embedded in the microblog post	➖	✔
in-reply-to-display-name	text	The user display name of the microblog this post replies to.	➖	✔
in-reply-to-status-id	text	The microblog ID of the microblog this post replies to.	➖	✔
in-reply-to-user-id	text	The user ID of the microblog this post replies to.	➖	✔
language	text	The language of the post.	➖	✔
link	link	Original link to the microblog post (supposed harmless).	➖	✔
modification-date	datetime	Last update of the microblog post	➖	➖
post	text	Raw text of the post.	➖	➖
removal-date	datetime	When the microblog post was removed.	➖	➖
state	text	State of the microblog post ['Informative', 'Malicious', 'Misinformation', 'Disinformation', 'Unknown']	✔	➖
title	text	Title of the post.	➖	➖
twitter-id	twitter-id	The microblog post id.	➖	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
type	text	Type of the microblog post ['Twitter', 'Facebook', 'LinkedIn', 'Reddit', 'Google+', 'Instagram', 'Forum', 'Other']	✔	—
url	url	Original URL of the microblog post (potentially malicious).	—	✔
username	text	Username who posted the microblog post (without the @ prefix)	—	—
username-quoted	text	Username who are quoted in the microblog post.	—	✔
verified-username	text	Is the username account verified by the operator of the microblog platform ['Verified', 'Unverified', 'Unknown']	✔	—

monetary-impact

Monetary Impact object as described in STIX 2.1 Incident object extension.

monetary-impact 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	Multiple
conversion_rate	float	Conversion rate between currency and currency_actual (if needed).	✔	—
conversion_time	datetime	Timestamp when the conversion rate was queried.	—	—
criticality	text	Criticality of the impact ['Not Specified', 'False Positive', 'Low', 'Moderate', 'High', 'Extreme']	✔	—
currency	text	Currency used to describe the max and min amount of the impact.	✔	—
currency_actual	text	Currency that the impact actually used.	✔	—
description	text	Additional details about the impact.	—	—
end_time	datetime	The date and time the impact was last recorded.	—	—
end_time_fidelity	text	Level of fidelity that the `end_time` is recorded in. ['day', 'hour', 'minute', 'month', 'second', 'year']	✔	—
max_amount	float	Maximum damage estimate.	✔	—
min_amount	float	Minimum damage estimate.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
recoverability	text	Recoverability of this particular impact with respect to feasibility and required time and resources. ['extended', 'not-applicable', 'not-recoverable', 'regular', 'supplemented']	✔	—
start_time	datetime	The date and time the impact was first recorded.	—	—
start_time_fidelity	text	Level of fidelity that the `start_time` is recorded in. ['day', 'hour', 'minute', 'month', 'second', 'year']	✔	—
variety	text	Variety of the moneraty impact. ['asset-and-fraud', 'brand-damage', 'business-disruption', 'competitive-advantage', 'legal-and-regulatory', 'operating-costs', 'ransom-demand', 'ransom-payment', 'response-and-recovery', 'uncategorized']	✔	—

mutex

Object to describe mutual exclusion locks (mutex) as seen in memory or computer program.

mutex 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	Multiple
description	text	Description	—	—
name	text	name of the mutex	—	—
operating-system	text	Operating system where the mutex has been seen ['Windows', 'Unix']	—	—

narrative

Object describing a narrative.

narrative 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	Multiple
5Ds-of-propaganda	text	5 D's of propaganda are tactics of rebuttal used to defend against criticism and adversarial narratives. ['dismiss', 'distort', 'distract', 'dismay', 'divide']	✔	✔
archive	link	Archive of the original narrative source (Internet Archive, Archive.is, etc).	✔	✔
attachment	attachment	Documents related to the narrative.	—	—
external-references	link	Link to external references.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
link	link	Original link to the narrative source (Supposed harmless)	—	—
narrative-disproof	text	Disproof or evidence against the narrative.	✔	—
narrative-summary	text	A summary of the narrative.	—	—
objective	text	Objective of the narrative. ['Disinformation', 'Advertising', 'Parody', 'Other']	✔	✔
url	url	Original link to the narrative source (Supposed malicious)	—	—

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	Multiple
byte-count	size-in-bytes	Bytes counted in this flow	✔	—
community-id	community-id	Community id of the represented flow	—	—
direction	text	Direction of this flow ['Ingress', 'Egress']	✔	—
dst-as	AS	Destination AS number for this flow	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
dst-port	port	Destination port of the netflow	—	—
first-packet-seen	datetime	First packet seen in this flow	✔	—
flow-count	counter	Flows counted in this flow	✔	—
icmp-type	text	ICMP type of the flow (if the traffic is ICMP)	✔	—
ip-dst	ip-dst	IP address destination of the netflow	—	—
ip-protocol-number	integer	IP protocol number of this flow	✔	—
ip-src	ip-src	IP address source of the netflow	—	—
ip_version	integer	IP version of this flow	✔	—
last-packet-seen	datetime	Last packet seen in this flow	✔	—
packet-count	counter	Packets counted in this flow	✔	—
protocol	text	Protocol used for this flow ['TCP', 'UDP', 'ICMP', 'IP']	✔	—
src-as	AS	Source AS number for this flow	—	—
src-port	port	Source port of the netflow	—	—
tcp-flags	text	TCP flags of the flow	✔	—

network-connection

A local or remote network connection.

network-connection 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	Multiple
community-id	community-id	Flow description as a community ID hash value	—	—
count	counter	Number of similar network connections seen	—	—
dst-bytes-count	size-in-bytes	Number of bytes sent from the source to the destination.	✔	—
dst-packets-count	counter	Number of packets sent from the source to the destination.	✔	—
dst-port	port	Destination port of the nework connection.	—	—
first-packet-seen	datetime	Datetime of the first packet seen.	✔	—
hostname-dst	hostname	Destination hostname of the network connection.	—	—
hostname-src	hostname	Source hostname of the network connection.	—	—
ip-dst	ip-dst	Destination IP address of the nework connection.	—	—
ip-src	ip-src	Source IP address of the nework connection.	—	—
last-packet-seen	datetime	Datetime of the last packet seen.	✔	—
layer3-protocol	text	Layer 3 protocol of the network connection. ['IP', 'ICMP', 'ARP']	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
layer4-protocol	text	Layer 4 protocol of the network connection. ['TCP', 'UDP']	✔	—
layer7-protocol	text	Layer 7 protocol of the network connection. ['HTTP', 'HTTPS', 'FTP']	✔	✔
mac-dst	mac-address	Destination MAC address of the network connection.	—	—
mac-src	mac-address	Source MAC address of the network connection.	—	—
src-bytes-count	size-in-bytes	Number of bytes sent from the destination to the source.	✔	—
src-packets-count	counter	Number of packets sent from the destination to the source.	✔	—
src-port	port	Source port of the nework connection.	—	—

network-profile

Elements that can be used to profile, pivot or identify a network infrastructure, including domains, ip and urls.

network-profile 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	Multiple
asn	AS	ASN where the content is hosted	—	—
certificate-common-name	text	Certificate common name	—	—
certificate-country	text	Certificate country name	—	—
certificate-creation-date	datetime	Certificate date it was created	—	—
certificate-expiry-date	datetime	Certificate date it will expire	—	—
certificate-issuer	text	Certificate Issuer	—	—
certificate-organization	text	Certificate organization	—	—
certificate-organization-locality	text	Certificate locality	—	—
certificate-organization-state	text	Certificate state or provincy name	—	—
certificate-organization-unit	text	Certificate organization unit	—	—
dns-server	hostname	DNS server	—	✔
domain	domain	Domain of the whois entry	—	✔
evidences	attachment	Screenshot of the network resources.	✔	✔
google-analytics-id	text	Google analytics IDS	—	—
hosting-provider	text	The hosting provider/ISP where the resources are.	—	—
ip-address	ip-src	IP address of the whois entry	—	✔
jarm	jarm-fingerprint	JARM Footprint string	—	—
port	port	Port number	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
query_string	text	Query (after path, preceded by '?')	➖	✔
resource_path	text	Path (between hostname:port and query)	➖	✔
service-abuse	text	Service abused by threat actors as part of their infrastructure. ['OneDrive', 'Google Drive', 'Dropbox', 'Microsoft', 'Google', 'DuckDNS', 'Cloudflare', 'AWS', 'Yandex']	➖	✔
subdomain	text	Subdomain	✔	➖
text	text	Full whois entry	✔	➖
threat-actor-infrastructure-pattern	text	Patterns found on threat actor infrastructure that can correlate with other analysis.	➖	✔
threat-actor-infrastructure-value	text	Unique valeu found on threat actor infrastructure identified through an investigation.	➖	✔
tld	text	Top-Level Domain	✔	➖
url	url	Full URL	➖	➖
whois-creation-date	datetime	Initial creation of the whois entry	✔	➖
whois-expiration-date	datetime	Expiration of the whois entry	✔	➖
whois-registrant-email	whois-registrant-email	Registrant email address	➖	➖
whois-registrant-name	whois-registrant-name	Registrant name	➖	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
whois-registrant-org	whois-registrant-org	Registrant organisation	–	–
whois-registrant-phone	whois-registrant-phone	Registrant phone number	–	–
whois-registrar	whois-registrar	Registrar of the whois entry	–	–

network-socket

Network socket object describes a local or remote network connections based on the socket data structure.

network-socket 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	Multiple
address-family	text	Address family who specifies the address family type (AF_*) of the socket connection. ['AF_UNSPEC', 'AF_LOCAL', 'AF_UNIX', 'AF_FILE', 'AF_INET', 'AF_AX25', 'AF_IPX', 'AF_APPLETALK', 'AF_NETROM', 'AF_BRIDGE', 'AF_ATMPVC', 'AF_X25', 'AF_INET6', 'AF_ROSE', 'AF_DECnet', 'AF_NETBEUI', 'AF_SECURITY', 'AF_KEY', 'AF_NETLINK', 'AF_ROUTE', 'AF_PACKET', 'AF_ASH', 'AF_ECONET', 'AF_ATMSVC', 'AF_RDS', 'AF_SNA', 'AF_IRDA', 'AF_PPPOX', 'AF_WANPIPE', 'AF_LLC', 'AF_IB', 'AF_MPLS', 'AF_CAN', 'AF_TIPC', 'AF_BLUETOOTH', 'AF_IUCV', 'AF_RXRPC', 'AF_ISDN', 'AF_PHONET', 'AF_IEEE802154', 'AF_CAIF', 'AF_ALG', 'AF_NFC', 'AF_VSOCK',	–	–

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
domain-family	text	Domain family who specifies the communication domain (PF_*) of the socket connection. ['PF_UNSPEC', 'PF_LOCAL', 'PF_UNIX', 'PF_FILE', 'PF_INET', 'PF_AX25', 'PF_IPX', 'PF_APPLETALK', 'PF_NETROM', 'PF_BRIDGE', 'PF_ATMPVC', 'PF_X25', 'PF_INET6', 'PF_ROSE', 'PF_DECnet', 'PF_NETBEUI', 'PF_SECURITY', 'PF_KEY', 'PF_NETLINK', 'PF_ROUTE', 'PF_PACKET', 'PF_ASH', 'PF_ECONET', 'PF_ATMSVC', 'PF_RDS', 'PF_SNA', 'PF_IRDA', 'PF_PPPOX', 'PF_WANPIPE', 'PF_LLC', 'PF_IB', 'PF_MPLS', 'PF_CAN', 'PF_TIPC', 'PF_BLUETOOTH', 'PF_IUCV', 'PF_RXRPC', 'PF_ISDN', 'PF_PHONET', 'PF_IEEE802154', 'PF_CAIF', 'PF_ALG', 'PF_NFC',	–	–

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
dst-bytes-count	size-in-bytes	Number of bytes sent from the source to the destination.	✔	—
dst-packets-count	counter	Number of packets sent from the source to the destination.	✔	—
dst-port	port	Destination port of the network socket connection.	—	—
filename	filename	Socket using filename	—	—
first-packet-seen	datetime	Datetime of the first packet seen.	✔	—
hostname-dst	hostname	Destination hostname of the network socket connection.	—	—
hostname-src	hostname	Source (local) hostname of the network socket connection.	—	—
ip-dst	ip-dst	Destination IP address of the network socket connection.	—	—
ip-src	ip-src	Source (local) IP address of the network socket connection.	—	—
last-packet-seen	datetime	Datetime of the last packet seen.	✔	—
mac-dst	mac-address	Destination MAC address as it is included in the packets sent	—	—
mac-src	mac-address	Source (local) MAC address as it is included in the packets sent	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
option	text	Option on the socket connection.	—	✔
protocol	text	Protocol used by the network socket. ['TCP', 'UDP', 'ICMP', 'IP']	—	✔
socket-type	text	Type of the socket. ['SOCK_STREAM', 'SOCK_DGRAM', 'SOCK_RAW', 'SOCK_RDM', 'SOCK_SEQPACKET']	—	—
src-bytes-count	size-in-bytes	Number of bytes sent from the destination to the source.	✔	—
src-packets-count	counter	Number of packets sent from the destination to the source.	✔	—
src-port	port	Source (local) port of the network socket connection.	—	—
state	text	State of the socket connection. ['blocking', 'listening']	—	✔

network-traffic

Generic network traffic that originates from a source and is addressed to a destination.

network-traffic 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	Multiple
dst_bytes_count	size-in-bytes	Number of bytes sent from the destination to the source	➖	➖
dst_hostname	hostname	Destination hostname of the network traffic	➖	➖
dst_ip	ip-dst	Destination IP address of the network traffic	➖	➖
dst_mac	mac-address	Destination MAC address of the network traffic	➖	➖
dst_packets	counter	Number of packets sent from the destination to the source	➖	➖
dst_port	port	Destination port of the nework connection	➖	➖
end_time	datetime	Time the network traffic ended	➖	➖
is_active	boolean	Indicates whether the network traffic is still ongoing. Must be False if the end_time attribute is present	➖	➖
protocol	text	Protocol observed in the network traffic	➖	✔
src_bytes_count	size-in-bytes	Number of bytes sent from the source to the destination	➖	➖
src_hostname	hostname	Destination hostname of the network traffic	➖	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
src_ip	ip-dst	Source IP address of the network traffic	—	—
src_mac	mac-address	Source MAC address of the network traffic	—	—
src_packets	counter	Number of packets sent from the source to the destination	—	—
src_port	port	Source port of the nework connection	—	—
start_time	datetime	Time the network traffic started	—	—

news-agency

News agencies compile news and disseminate news in bulk.

news-agency 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	Multiple
address	text	Postal address of the news agency.	—	✔
alias	text	Alias of the news agency.	✔	✔
archive	link	Archive of the original document (Internet Archive, Archive.is, etc).	—	✔
attachment	attachment	The news file, screen capture, audio, etc.	—	✔
e-mail	email-src	Email address of the organization.	—	✔
fax-number	phone-number	Fax number of the news agency.	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
link	link	Original link to the news agency (Supposed harmless).	—	✔
name	text	Name of the news agency.	✔	—
phone-number	phone-number	Phone number of the news agency.	—	✔
url	url	Original URL location of the news agency (potentially malicious).	—	✔

news-media

News media are forms of mass media delivering news to the general public.

news-media 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	Multiple
address	text	Postal address of the news source.	—	✔
alias	text	Alias of the news source.	✔	✔
archive	link	Archive of the news (Internet Archive, Archive.is, etc).	—	✔
attachment	attachment	The news file, screen capture, audio, etc.	—	✔
content	text	Raw content of the news.	—	—
e-mail	email-src	Email address of the news source.	—	✔
embedded-link	url	Site linked by the blog post.	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
embedded-safe-link	link	Safe site linked by the blog post.	➖	✔
fax-number	phone-number	Fax number of the news source.	➖	✔
link	link	Original link to news (Supposed harmless).	➖	✔
phone-number	phone-number	Phone number of the news source.	➖	✔
source	text	Name of the news source.	✔	➖
sub-type	text	Format of the news post (business daily, local news, metasite, etc). ['Business Daily', 'Local News', 'State News', 'National News', 'Metasite', 'Political Commentary', 'Clipper', 'Pressure Group', 'Staging', 'Trade Site', 'Governmental Communication', 'Alert', 'Other']	✔	➖
title	text	Title of the post.	➖	➖
transcription	text	Transcribed audio/visual content.	➖	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
type	text	Type of news media (newspaper, TV, podcast, etc). ['Newspaper', 'Newspaper (Online)', 'Magazine', 'Magazine (Online)', 'TV', 'Tube', 'Radio', 'Radio (Online)', 'Podcast', 'Alternative Media', 'Governmental', 'News agency', 'Other']	✔	✔
url	url	Original URL location of news (potentially malicious).	—	✔
username	text	Username who posted the blog post.	—	—

open-data-security

An object describing an open dataset available and described under the open data security model. ref. https://github.com/CIRCL/open-data-security.

> open-data-security 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	Multiple
description	comment	an exhaustive description of the dataset including methods of collection, extraction or analysis	✔	—
frequency	text	frequency of the dataset generation which MUST be expressed in yearly, monthly, daily, hourly ['yearly', 'monthly', 'daily', 'hourly']	✔	—
human-validated	text	human-validated describes if the dataset has been manually validated ['true', 'false', 'unknown']	✔	—
license	text	license MUST be expressed in SPDX format to describe under which license the dataset is distributed	✔	—
link	link	link to open dataset	—	—
machine-validated	text	machine-validated describes if the dataset has been automatically validated ['true', 'false', 'unknown']	✔	—
producer	link	producer MUST be expressed as an URI to reference the original producer of the dataset	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
source	text	original source of the dataset	✔	✔
subtitle	text	an extended title of the dataset	✔	—
time-precision	text	time-precision MUST be expressed in years, months, days, hours, minutes or seconds to describe the precision of the time expressed ['years', 'months', 'days', 'hours', 'minutes', 'seconds']	✔	—
title	text	a comprehensive and concise title of the dataset	✔	—

opentide

Object that is a container for threat or detection data, in accordance with the OpenTIDE Framework (https://code.europa.eu/ec-digit-s2/opentide).

opentide 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	Multiple
name	text	Name of the OpenTIDE Object	—	—
opentide-object	text	YAML Content of the Opentide Object	—	—
opentide-relation	text	UUID of other OpenTIDE Objects with a relation to this Object	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
opentide-type	text	Type of the OpenTIDE Object ['tvm', 'cdm', 'mdr']	✔	—
uuid	text	UUID of the OpenTIDE Object	—	—
version	text	Version of the OpenTIDE Object ['1']	✔	—

organization

An object which describes an organization.

organization 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	Multiple
VAT	text	VAT or TAX-ID of the organization	—	✔
address	text	Postal address of the organization.	—	✔
alias	text	Alias of the organization	—	✔
contact_information	text	Generic contact information (e-mail, phone number, etc.) for this Organization, with no specific format requirement.	—	—
date-of-inception	datetime	Date of inception of the organization	—	—
description	text	Description of the organization	—	—
e-mail	email-src	Email address of the organization.	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
fax-number	phone-number	Fax number of the organization.	➖	✔
misp-uuid	text	MISP UUID of the organization	➖	✔
name	text	Name of the organization	➖	➖
phone-number	phone-number	Phone number of the organization.	➖	✔
registration-number	text	Registration number of the organization	➖	➖
role	text	The role of the organization. ['Suspect', 'Victim', 'Defendent', 'Accused', 'Culprit', 'Accomplice', 'Target', 'Source', 'Originator', 'Informant', 'Emitter', 'Impersonated']	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
sector	text	Describing the organization's sector of activity. ['agriculture', 'aerospace', 'automotive', 'chemical', 'commercial', 'communication', 'construction', 'defense', 'education', 'energy', 'entertainment', 'financial-services', 'government', 'government emergency-services', 'government government-local', 'government-national', 'government-public-services', 'government-regional', 'healthcare', 'hospitality-leasure', 'infrastructure', 'infrastructure dams', 'infrastructure nuclear', 'infrastructure water', 'insurance', 'manufacturing', 'mining', 'non-profit', 'pharmaceuticals', 'private', 'retail', 'technology', 'telecommunication', 'transportation',	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
type-of-organization	text	Type of the organization	—	—

original-imported-file

Object describing the original file used to import data in MISP.

original-imported-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	Multiple
format	text	Format of data imported. ['STIX 1.0', 'STIX 1.1', 'STIX 1.2', 'STIX 2.0', 'OpenIOC']	✔	—
imported-sample	attachment	The original imported file itself (binary).	✔	—
uri	uri	URI related to the imported file.	—	—

paloalto-threat-event

Palo Alto Threat Log Event.

paloalto-threat-event 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	Multiple
app	text	The application identified (e.g. vnc, ssh, sip, irc, http or smtp).	✔	—
direction	text	The Direction of the Event.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
dport	port	The port to which the connection headed.	✔	—
dst	ip-dst	The Destination IP which is the target of the observed connections.	—	—
dstloc	text	The Destination Location of the event.	✔	—
proto	text	The transport protocol (e.g. tcp, udp, icmp).	✔	—
sport	port	The port from which the connection originated.	✔	—
src	ip-src	The ip observed to initiate the connection	—	—
srcloc	text	The Source Location of the event.	✔	—
subtype	text	The subtype of the Log Event.	✔	—
thr_category	text	The Threat Category.	✔	—
threatid	text	The Threat ID.	✔	—
time_generated	datetime	The datetime of the event.	✔	—
type	text	The type of the Log Event	✔	—

parler-account

Parler account.

parler-account 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	Multiple
account-id	text	Numeric id of the account.	➖	➖
account-name	text	Name of the account.	➖	➖
archive	link	Archive of the original parley (Internet Archive, Archive.is, etc).	➖	✔
attachment	attachment	The parley file or screen capture.	➖	✔
badge	float	Post badge.	✔	✔
bio	text	The account bio.	➖	➖
comments	text	The number of user comments.	✔	➖
cover-photo	attachment	Comment controversy.	➖	➖
followers	text	Number of followers.	✔	➖
following	text	Number user is following.	✔	➖
human	boolean	Account 'human' bool. ['True', 'False']	✔	➖
interactions	float	Account interactions.	✔	➖
likes	text	Number user likes.	✔	➖
link	link	Original URL of the parley (supposed harmless).	➖	✔
posts	text	Number user posts.	✔	➖
profile-photo	attachment	Comment controversy.	➖	➖
score	text	User score.	✔	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
url	url	Original URL of the parley, e.g. link shortener (potentially malicious).	—	✔
verified	boolean	Account 'verified' bool. ['True', 'False']	✔	—

parler-comment

Parler comment.

parler-comment 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	Multiple
archive	link	Archive of the original parley (Internet Archive, Archive.is, etc).	—	✔
attachment	attachment	The parley file or screen capture.	—	✔
badge	float	Comment badge.	✔	—
body	text	Raw text of the post.	—	—
comment-depth	float	Comment nesting depth.	✔	—
comments	text	Comments on this object.	✔	—
controversy	float	Comment controversy.	✔	—
creator	text	Name of the account that posted this parley.	—	—
creator-id	text	ID of the account that posted this parley.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
downvotes	text	Comment downvotes.	✔	—
embedded-link	url	Link in the parley	—	✔
embedded-safe-link	link	Safe link in the parley	—	✔
hashtag	text	Hashtag embedded in the parley.	—	✔
in-reply-to-display-name	text	The user display name of the parley this post shares.	—	✔
in-reply-to-parley-id	text	The Parler ID of the parley that this post shares.	—	✔
in-reply-to-user-id	text	The user ID of the parley this post shares.	—	✔
link	link	Original link to the post (supposed harmless).	—	✔
post-id	text	Numeric id of the parley.	—	—
score	text	Comment score.	✔	—
upvotes	text	Comment upvotes.	✔	—
url	url	Original URL of the parley, e.g. link shortener (potentially malicious).	—	✔
username-quoted	text	Username who is quoted in the parley.	—	✔

parler-post

Parler post (parley).

parler-post 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	Multiple
archive	link	Archive of the original parley (Internet Archive, Archive.is, etc).	—	✔
article	boolean	Indicates if the post is an article. ['True', 'False']	✔	—
attachment	attachment	The parley file or screen capture.	—	✔
badge	float	Post badge.	✔	—
body	text	Raw text of the post.	—	—
comments	text	Number of comments on this object.	✔	—
creator	text	Name of the account that posted this parley.	—	—
creator-id	text	ID of the account that posted this parley.	—	—
depth	float	Post nesting depth.	✔	—
embedded-link	url	Link in the parley	—	✔
embedded-safe-link	link	Safe link in the parley	—	✔
hashtag	text	Hashtag embedded in the parley.	—	✔
impressions	text	Number of impressions.	✔	—
in-reply-to-display-name	text	The user display name of the parley this post shares.	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
in-reply-to-parley-id	text	The Parler ID of the parley that this post shares.	—	✔
in-reply-to-user-id	text	The user ID of the parley this post shares.	—	✔
link	link	Original link to the post (supposed harmless).	—	✔
post-id	text	Numeric id of the parley.	—	—
share-link	link	Sharable link generated by Parler (supposed harmless).	—	✔
upvotes	text	Comment upvotes.	✔	—
url	url	Original URL of the parley, e.g. link shortener (potentially malicious).	—	✔
username-quoted	text	Username who is quoted in the parley.	—	✔

passive-dns

Passive DNS records as expressed in draft-dulaunoy-dnsop-passive-dns-cof-07. See https://tools.ietf.org/id/draft-dulaunoy-dnsop-passive-dns-cof-07.html.

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	Multiple
bailiwick	domain	Best estimate of the apex of the zone where this data is authoritative	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
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.	✔	—
origin	text	Origin of the Passive DNS response. This field is represented as a Uniform Resource Identifier (URI)	✔	—
raw_rdata	text	Resource records of the queried resource, in hexadecimal. **All** rdata entries at once.	—	—
rdata	text	Resource records of the queried resource. Note that this field is added for **each** rdata entry in the rrset.	—	—
rrname	text	Resource Record name of the queried resource.	—	—
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	Multiple
sensor_id	text	Sensor information where the record was seen	✔	—
text	text	Description of the passive DNS record.	✔	—
time_first	datetime	First time that the unique tuple (rrname, rrtype, rdata) has been seen by the passive DNS	✔	—
time_first_ms	datetime	Same meaning as the field 'time_first', with the only difference, that the resolution is in milliseconds since 1st of January 1970 (UTC)	✔	—
time_last	datetime	Last time that the unique tuple (rrname, rrtype, rdata) record has been seen by the passive DNS	✔	—
time_last_ms	datetime	Same meaning as the field 'time_last', with the only difference, that the resolution is in milliseconds since 1st of January 1970 (UTC)	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
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.	✔	—

passive-dns-dnsdbflex

DNSDBFLEX object. This object is used at farsight security. Roughly based on Passive DNS records as expressed in draft-dulaunoy-dnsop-passive-dns-cof-07. See https://tools.ietf.org/id/draft-dulaunoy-dnsop-passive-dns-cof-07.html.

passive-dns-dnsdbflex 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	Multiple
rrname	text	Resource Record name of the queried resource.	—	—
rrtype	text	Resource Record type as seen by the passive DNS. ['A', 'AAAA', 'CNAME', 'PTR', 'SOA', 'TXT', 'DNAME', 'NS', 'SRV', 'RP', 'NAPTR', 'HINFO', 'A6']	✔	—

passive-ssh

Passive-ssh object as described on passive-ssh services from circl.lu - https://github.com/D4-project/

passive-ssh.

passive-ssh 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	Multiple
banner	text	SSH banner	✗	✓
base64	text	Base64 representation of the ssh-key	✓	✓
fingerprint	ssh-fingerprint	Fingerprint of the SSH key	✓	✓
first_seen	datetime	First time that the passive-ssh object has been seen by the passive SSH	✓	✗
hassh	hassh-md5	Hassh fingerprint	✗	✗
host	ip-dst	IP Address of the host(s) that exposed this SSH key	✗	✓
last_seen	datetime	Last time that the passive-ssh object has been seen by the passive SSH	✓	✗
port	port	Port of the connection	✗	✗

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	Multiple
first-seen	datetime	When the paste has been accessible or seen for the first time.	✓	✗

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
last-seen	datetime	When the paste has been accessible or seen for the last time.	✔	—
link	link	Link to the original source of the source or post (when used legitimately for OSINT source or alike).	—	—
origin	text	Original source of the paste or post. ['pastebin.com', 'pastebin.com_pro', 'pastebin.fr', 'pastie.org', 'slexy.org', 'gist.github.com', 'codepad.org', 'safebin.net', 'hastebin.com', 'ghostbin.com', 'paste.ee', '0bin.net']	✔	—
paste	text	Raw text of the paste or post	—	—
paste-file	attachment	Content of the paste in file	—	—
title	text	Title of the paste or post.	—	—
url	url	Link to the original source of the paste or post (when used maliciously).	—	—
username	text	User who posted the post.	—	—

pcap-metadata

Network packet capture metadata.

pcap-metadata 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	Multiple
capture-interface	text	Interface name where the packet capture was running.	✔	—
capture-length	text	Capture length set on the captured interface.	✔	—
first-packet-seen	datetime	When the first packet has been seen.	✔	—
last-packet-seen	datetime	When the last packet has been seen.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
protocol	text	Capture protocol (linktype name). ['PER_PACKET', 'UNKNOWN', 'ETHERNET', 'TOKEN_RING', 'SLIP', 'PPP', 'FDDI', 'FDDI_BITSWAPPED', 'RAW_IP', 'ARCNET', 'ARCNET_LINUX', 'ATM_RFC1483', 'LINUX_ATM_CLIP', 'LAPB', 'ATM_PDUS', 'ATM_PDUS_UNTRUNCATED', 'NULL', 'ASCEND', 'ISDN', 'IP_OVER_FC', 'PPP_WITH_PHDR', 'IEEE_802_11', 'IEEE_802_11_PRISM', 'IEEE_802_11_WITH_RADIO', 'IEEE_802_11_RADIOTAP', 'IEEE_802_11_AVS', 'SLL', 'FRELAY', 'FRELAY_WITH_PHDR', 'CHDLC', 'CISCO_IOS', 'LOCALTALK', 'OLD_PFLOG', 'HHDLC', 'DOCSIS', 'COSINE', 'WFLEET_HDLC', 'SDLC', 'TZSP', 'ENC', 'PFLOG', 'CHDLC_WITH_PHDR', 'BLUETOOTH_H4', 'MTP2', 'MTP3', 'IRDA', 'USER0', 'USER1', 'USER2', 'USER3', 'USER4',	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
text	text	A description of the packet capture.	✔	—

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	Multiple
authentihash	authentihash	Authenticode executable signature hash (sha256)	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
characteristics	text	The characteristics that indicate the attributes of the file ['AGGRESSIVE_WS_TRIM', 'BYTES_REVERSED_HI', 'BYTES_REVERSED_LO', 'DEBUG_STRIPPED', 'DLL', 'EXECUTABLE_IMAGE', 'LARGE_ADDRESS_AWARE', 'LINE_NUMS_STRIPPED', 'LOCAL_SYMS_STRIPPED', 'NEED_32BIT_MACHINE', 'NET_RUN_FROM_SWAP', 'RELOCS_STRIPPED', 'REMOVABLE_RUN_FROM_SWAP', 'SYSTEM', 'UP_SYSTEM_ONLY']	✔	✔
characteristics-hex	hex	The characteristics in a single hex value	✔	➖
company-name	text	CompanyName in the resources	✔	➖
compilation-timestamp	datetime	Compilation timestamp defined in the PE header	➖	➖
entrypoint-address	text	Address of the entry point	✔	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
entrypoint-section-at-position	text	Name of the section and position of the section in the PE	✔	—
file-description	text	FileDescription in the resources	✔	—
file-version	text	FileVersion in the resources	✔	—
impfuzzy	impfuzzy	Fuzzy Hash (ssdeep) calculated from the import table	—	—
imphash	imphash	Hash (md5) calculated from the import table	—	—
internal-filename	filename	InternalFilename in the resources	✔	—
lang-id	text	Lang ID in the resources	✔	—
legal-copyright	text	LegalCopyright in the resources	✔	—
machine-type	text	Type of machine ['AM33', 'AMD64', 'ARM', 'ARM64', 'ARMNT', 'EBC', 'I386', 'IA64', 'M32R', 'MIPS16', 'MIPSFPU', 'MIPSFPU16', 'POWERPC', 'POWERPCFP', 'R4000', 'SH3', 'SH3DSP', 'SH4', 'SH5', 'THUMB', 'UNKNOWN', 'WCEMIPSV2']	✔	—
machine-type-hex	hex	Type of machine in a simple hex value	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
number-of-symbols	counter	Number of entries in the symbol table	✔	—
number-sections	counter	Number of sections	✔	—
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/	—	—
pointer-to-symbol-table	hex	The file offset of the COFF symbol table.	✔	—
product-name	text	ProductName in the resources	✔	—
product-version	text	ProductVersion in the resources	✔	—
richpe	md5	RichPE metadata hash	—	✔
size-of-optional-header	size-in-bytes	Size of the optional header and the data directories which follow this header	—	—
text	text	Free text value to attach to the PE	✔	—
type	text	Type of PE ['exe', 'dll', 'driver', 'unknown']	✔	—

pe-optional-header

Object describing a Portable Executable Optional Header.

pe-optional-header 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	Multiple
address-of-entrypoint	integer	The address of the entry point relative to the image base when the executable file is loaded into memory	✔	—
base-of-code	integer	Address relative to the imagebase where the binary's code starts	✔	—
base-of-data	integer	Address relative to the imagebase where the binary's data starts	✔	—
checksum	hex	The image file checksum	✔	—
dll-characteristics	text	Some characteristics of the underlying binary ['APPCONTAINER', 'DYNAMIC_BASE', 'FORCE_INTEGRITY', 'GUARD_CF', 'HIGH_ENTROPY_VA', 'NO_BIND', 'NO_ISOLATION', 'NO_SEH', 'NX_COMPAT', 'TERMINAL_SERVER_AWARE', 'WDM_DRIVER']	✔	✔
dll-characteristics-hex	hex	The DLL characteristics in a single hex value	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
file-alignment	size-in-bytes	The alignment factor (in bytes) that is used to align the raw data of sections in the image file	✔	—
image-base	integer	The preferred base address when mapping the binary in memory	✔	—
loader-flags	hex	According to the PE specifications, this value is reserved and should be 0	✔	—
magic	text	Magic value (PE_TYPE) that identifies a PE32 from a PE64 ['PE32', 'PE32_PLUS']	✔	—
magic-hex	hex	The magic value in a simple hex value	✔	—
major-image-version	integer	The major version number of the image	✔	—
major-linker-version	integer	The linker major version number	✔	—
major-os-version	integer	The major version number of the required operating system	✔	—
major-subsystem-version	integer	The major version number of the subsystem	✔	—
minor-image-version	integer	The minor version number of the image	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
minor-linker-version	integer	The linker minor version number	✔	—
minor-os-version	integer	The minor version number of the required operating system	✔	—
minor-subsystem-version	integer	The minor version number of the subsystem	✔	—
number-of-rva-and-size	integer	The number of DataDirectory that follow this header	✔	—
section-alignment	size-in-bytes	The alignment (in bytes) of sections when they are loaded into memory. It must be greater than or equal to file_alignment and the default is the page size for the architecture	✔	—
size-of-code	size-in-bytes	The size of the code .text section or the sum of all the sections that contain code	✔	—
size-of-headers	size-in-bytes	The combined size of an MS-DOS stub, PE header, and section headers rounded up to a multiple of file_alignment	✔	—
size-of-heap-commit	size-in-bytes	The size of the local heap space to commit	✔	—
size-of-heap-reserve	size-in-bytes	The size of the local heap space to reserve	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
size-of-image	size-in-bytes	The size (in bytes) of the image, including all headers, as the image is loaded in memory	✔	—
size-of-initialised-data	size-in-bytes	The size of the initialized data which are usually located in the .data section. If the initialized data are split across multiple sections, it is the sum of the sections	✔	—
size-of-stack-commit	size-in-bytes	The size of the stack to commit	✔	—
size-of-stack-reserve	size-in-bytes	The size of the stack to reserve	✔	—
size-of-uninitialised-data	size-in-bytes	The size of the uninitialized data which are usually located in the .bss section. If the uninitialized data are split across multiple sections, it is the sum of the sections	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
subsystem	text	Target subsystem ['EFI_APPLICATION', 'EFI_BOOT_SERVICE_DRIVER', 'EFI_ROM', 'EFI_RUNTIME_DRIVER', 'NATIVE', 'NATIVE_WINDOWS', 'OS2_CUI', 'POSIX_CUI', 'UNKNOWN', 'WINDOWS_BOOT_APPLICATION', 'WINDOWS_CE_GUI', 'WINDOWS_CUI', 'WINDOWS_GUI', 'XBOX']	✔	—
subsystem-hex	hex	The subsystem in a simple hex value	✔	—
win32-version-value	hex	Specifies the reserved win32 version value (must be zero)	✔	—

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	Multiple
characteristic	text	Characteristic of the section ['read', 'write', 'executable']	—	—
entropy	float	Entropy of the whole section	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
md5	md5	[Insecure] MD5 hash (128 bits)	➖	➖
name	text	Name of the section ['.rsrc', '.reloc', '.rdata', '.data', '.text']	✔	➖
offset	hex	Section's offset	✔	➖
sha1	sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	➖	➖
sha224	sha224	Secure Hash Algorithm 2 (224 bits)	➖	➖
sha256	sha256	Secure Hash Algorithm 2 (256 bits)	➖	➖
sha384	sha384	Secure Hash Algorithm 2 (384 bits)	➖	➖
sha512	sha512	Secure Hash Algorithm 2 (512 bits)	➖	➖
sha512/224	sha512/224	Secure Hash Algorithm 2 (224 bits)	➖	➖
sha512/256	sha512/256	Secure Hash Algorithm 2 (256 bits)	➖	➖
size-in-bytes	size-in-bytes	Size of the section, in bytes	✔	➖
ssdeep	ssdeep	Fuzzy hash using context triggered piecewise hashes (CTPH)	➖	➖
text	text	Free text value to attach to the section	✔	➖
virtual_address	hex	Section's virtual address	✔	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
virtual_size	size-in-bytes	Section's virtual size	✔	—

Deception PersNOna

Fake persona with tasks.

> Deception PersNOna is a MISP object available in JSON format at https://github.com/MISP/misp-objects/blob/main/objects/deception persnona/definition.json[**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	Multiple
actions	text	Actions by this PersNOna or engagement with adversary or relateda party.	—	✔
alias	text	Aliases or Nicknames of fake PesNOna on differenet media.	—	✔
background	text	Background of operation, PersNOna or actions, which needs to be explain to other party in case of share of this profile.	—	✔
conversations	text	Conversations with targets	—	✔
critical_tasks	text	Critical Tasks or tasks which this PersNOna has to accomplish.	—	✔
goals	text	Goals of creating of this PersNOna.	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
location	text	Location, where PersNOna is right now at home, home town, county, country etc.	✔	✔
media	text	Media where is PersNOna active ie. facebook, telegram etc.	—	✔
name	full-name	Name - full name of PersNOna.	—	✔
oppportunities	text	Opportunities for another development, introducing another PersNOna etc.	—	✔
photo	url	Photo of PersNOna, url where is photo uploaded or website of fake profile as LinkedIn etc.	—	—
questions	text	Questions, which have to be answered by this profile goal.	✔	✔
responsi	text	Responsibilities of PersNOna, who this PersNOna communicates with, what should discuss and how far.	—	✔

person

An object 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	Multiple
address	text	Postal address of the person.	—	✔
alias	text	Alias name or known as.	—	✔
birth-certificate-number	text	Birth Certificate Number	—	—
date-of-birth	date-of-birth	Date of birth of a natural person (in YYYY-MM-DD format).	—	—
dni	text	Spanish National ID	—	✔
e-mail	email-src	Email address of the person.	—	✔
fax-number	phone-number	Fax number of the person.	—	✔
first-name	first-name	First name of a natural person.	✔	—
full-name	full-name	Full name of a natural person usually composed of first-name, middle-name and last-name.	—	—
function	text	Function of the natural person such as analyst, cyber operator, lawyer.	✔	—
gender	gender	The gender of a natural person. ['Male', 'Female', 'Other', 'Prefer not to say', 'Unknown']	✔	—
handle	text	Handle used by the user in application.	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
identity-card-number	identity-card-number	The identity card number of a natural person.	➖	➖
instant-messaging-used	text	The IM application used by this person. ['WhatsApp', 'Google Hangouts', 'Facebook Messenger', 'Telegram', 'Signal', 'WeChat', 'BlackBerry Messenger', 'TeamSpeak', 'TorChat', 'Tox', 'RetroShare', 'Slack', 'Wire', 'Threema', 'Discord', 'Mumble', 'Jabber', 'Twitter']	✔	✔
ip-src	ip-src	Source IP address used by this person.	➖	✔
last-name	last-name	Last name of a natural person.	➖	➖
middle-name	middle-name	Middle name of a natural person.	➖	➖
mothers-name	text	Mother name, father, second name or other names following country's regulation.	➖	➖
nationality	nationality	The nationality of a natural person.	✔	✔
nic-hdl	text	NIC Handle (Network Information Centre handle) of the person.	➖	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
nie	text	Foreign National ID (Spain)	➖	✔
nif	text	Tax ID Number (Spain)	➖	✔
occupation	text	Work or occupation of the person or identity.	✔	➖
ofac-identification-number	text	ofac-identification Number	➖	➖
passport-country	passport-country	The country in which the passport was issued.	✔	➖
passport-creation	datetime	The creation date of the passport.	✔	➖
passport-expiration	passport-expiration	The expiration date of the passport.	✔	➖
passport-number	passport-number	The passport number of a natural person.	➖	➖
phone-number	phone-number	Phone number of the person.	➖	✔
place-of-birth	place-of-birth	Place of birth of a natural person.	✔	➖
portrait	attachment	Portrait of the person.	➖	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
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.	➖	➖
role	text	The role of a person. ['Suspect', 'Victim', 'Defendent', 'Accused', 'Culprit', 'Accomplice', 'Witness', 'Target', 'Source', 'Originator', 'Informant', 'Emitter', 'Impersonated']	✔	✔
social-security-number	text	Social security number.	➖	➖
text	text	A description of the person or identity.	✔	➖
title	text	Title of the natural person such as Dr. or equivalent.	✔	➖

personification

An object which describes a person or an identity.

personification 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	Multiple
age-range	float	Age range that the person appears to be	—	—
beard	text	Description of the characteristics of someones beard. ['Beardless', 'Stubble Short', 'Stuble Medium', 'Stuble Long', 'Full Beard', 'French Fork', 'Ducktail', 'Goatee', 'Imperial', 'Van Dyke', 'Anchor', 'Balbo', 'Mutton Chops', 'Verdi', 'Garibaldi', 'Dutch', 'Winter Beard', 'Mustache', 'Unknown']	—	✔
birthmark	text	Position(s) of birthmarks. ['Head', 'Arms', 'Back', 'Torso', 'Legs', 'Foot', 'Backside', 'Unknown']	—	✔
body-type	text	Body type of a person. ['Slim', 'Tone', 'Muscular', 'Stocky', 'Large', 'Unknown']	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
color-of-eyes	text	Description of a person’s colour of eyes. ['Amber', 'Blue', 'Brown', 'Gray', 'Green', 'Hazel', 'Red', 'Unknown']	➖	✔
hair-characteristics	text	Description of the characteristics of someones hairs. ['Straight', 'Wavy', 'Curly', 'Coily', 'Unknown']	➖	✔
hair-color	text	Description of a person’s colour of hair. ['Black', 'Brown', 'Auburn', 'Red', 'Blond', 'Gray', 'White', 'Blue', 'Pink', 'Green', 'Violet', 'Unknown']	➖	✔
haircut	text	Description of the characteristics of someones hairs. ['Crew Cut', 'Shaved', 'Bald', 'Long', 'Spiky', 'Dreadlocks', 'Cornrow', 'Bob', 'Layered', 'Flat-top', 'Chignon', 'Bun', 'French Twist', 'Medium', 'Braid', 'Pigtails', 'Ponytail', 'Unknown']	➖	✔
height	float	Height of a person in cm.	➖	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
other-facial-features	text	Description of other facial features such as nose, cheeks, lips etc...	➖	✔
portrait	attachment	Portrait of the person.	➖	✔
shape-of-eyes	text	Description of a person's eye shape. ['Monolids', 'Hooded', 'Upturned', 'Downturned', 'Round', 'Almond', 'Unknown']	➖	✔
shoe-size	float	Shoe size of a person. ['US', 'UK', 'EU', 'Asia', 'CM', 'Inches']	➖	✔
skin-charateristics	text	Traits or features of a person's skin ['Normal', 'Irritated', 'Dry', 'Oily', 'Scaly', 'Red spots', 'Skin moles']	➖	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
skin-complexion	text	Skin tone and complexion of a person. Type I: Extremely fair skin, always burns, never tans. Type II: Fair skin, always burns, sometimes tans.Dry: Medium skin, sometimes burns, always tans.Type IV: Olive skin, rarely burns, always tans. Type V: Moderately pigmented brown skin, never burns, always tans. Type VI: Markedly pigmented black skin, never burns, always tans. ['Type I', 'Type II', 'Type III', 'Type IV', 'Type V', 'Type VI', 'Unknown']	—	✔
weight	float	Weight of a person in Kg.	—	✔

pgp-meta

Metadata extracted from a PGP keyblock, message or signature.

pgp-meta 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	Multiple
key-id	text	Key ID in hexadecimal	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
user-id-email	text	User ID packet, email address of the key holder (UTF-8 text)	—	✔
user-id-name	text	User ID packet, name of the key holder	—	✔

phishing

Phishing template to describe a phishing website and its analysis.

phishing 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	Multiple
hostname	hostname	host of the phishing website	—	✔
internal-reference	text	Internal reference such as ticket ID	—	—
ip	ip-dst	IP address of the phishing website	—	✔
online	text	If the phishing is online and operational, by default is yes ['Yes', 'No']	✔	—
phishtank-detail-url	link	Phishtank detail URL to the reported phishing	—	—
phishtank-id	text	Phishtank ID of the reported phishing	—	—
screenshot	attachment	Screenshot of phishing site	✔	✔
submission-time	datetime	When the phishing was submitted and/or reported	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
takedown-request	datetime	When the phishing was requested to be taken down	✔	—
takedown-request-to	text	Destination email address for take-down request	✔	✔
takedown-time	datetime	When the phishing was taken down	✔	—
target	text	Targeted organisation by the phishing	—	✔
url	url	Original URL of the phishing website	—	—
url-redirect	url	Redirect URL of the phishing website	—	✔
verification-time	datetime	When the phishing was verified	✔	—
verified	text	The phishing has been verified by the team handling the phishing ['No', 'Yes']	✔	—

phishing-kit

Object to describe a phishing-kit.

phishing-kit 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	Multiple
date-found	datetime	Date when the phishing kit was found	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
email-type	text	Type of the Email	✔	—
internal-reference	text	Internal reference such as ticket ID	—	—
kit-mailer	text	Mailer Kit Used	✔	✔
kit-name	text	Name of the Phishing Kit	—	—
kit-url	url	URL of Phishing Kit	—	—
online	text	If the phishing kit is online and operational, by default is yes ['Yes', 'No']	✔	—
phishing-domain	url	Domain used for Phishing	—	✔
reference-link	link	Link where the Phishing Kit was observed	—	✔
target	text	What was targeted using this phishing kit	—	✔
threat-actor	text	Identified threat actor	—	✔
threat-actor-email	email-src	Email of the Threat Actor	—	✔

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	Multiple
brand	text	Brand of the phone.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
first-seen	datetime	When the phone has been accessible or seen for the first time.	✔	—
gummei	text	Globally Unique MME Identifier (GUMMEI) is composed from MCC, MNC and MME Identifier (MMEI).	—	—
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.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
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.	✔	➖
model	text	Model of the phone.	✔	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
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.	—	—
serial-number	text	Serial Number.	—	—
text	text	A description of the phone.	✔	—
tmsi	text	Temporary Mobile Subscriber Identities (TMSI) to visiting mobile subscribers can be allocated.	—	—

phone-number

Phone number based on the E.164 international public telecommunication numbering plan.

phone-number 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	Multiple
country-code	text	Country code in text format (e.g., US)	✔	—
country-code-numeric	text	Country code as per the E.164 numbering plan (e.g., +1)	✔	—
national-destination-code	text	National destination code as per the E.164 numbering plan (e.g., 415)	✔	—
phone-number	phone-number	Phone number in E.164 format (e.g., +14155552671)	—	—
subscriber-number	text	Subscriber number as per the E.164 numbering plan (e.g., 5552671)	✔	—
text	text	Description or additional information about the phone number.	✔	—

physical-impact

Physical Impact object as described in STIX 2.1 Incident object extension.

> physical-impact 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	Multiple
asset_type	text	The type or property or system that was affected by this impact. ['building-doors', 'building-windows', 'buildings', 'computers-mobile', 'computers-personal', 'computers-server', 'environment', 'ics-actuator', 'ics-engineering-workstation', 'ics-historian', 'ics-hmi', 'ics-other', 'ics-plc', 'ics-safety-system', 'ics-sensor', 'inventory', 'network-device', 'private-infrastructure', 'public-infrastructure', 'security-containers', 'vehicles']	✔	—
criticality	text	Criticality of the impact ['Not Specified', 'False Positive', 'Low', 'Moderate', 'High', 'Extreme']	✔	—
description	text	Additional details about the impact.	—	—
end_time	datetime	The date and time the impact was last recorded.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
end_time_fidelity	text	Level of fidelity that the `end_time` is recorded in. ['day', 'hour', 'minute', 'month', 'second', 'year']	✔	—
impact_type	text	Type of physical impact. ['damaged-functional', 'damaged-nonfunctional', 'destruction', 'none', 'unknown']	✔	—
recoverability	text	Recoverability of this particular impact with respect to feasibility and required time and resources. ['extended', 'not-applicable', 'not-recoverable', 'regular', 'supplemented']	✔	—
start_time	datetime	The date and time the impact was first recorded.	—	—
start_time_fidelity	text	Level of fidelity that the `start_time` is recorded in. ['day', 'hour', 'minute', 'month', 'second', 'year']	✔	—

postal-address

A postal address.

postal-address 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	Multiple
apartment	text	Apartment / suite number	✔	—
city	text	City or town name	✔	—
country	text	Country	✔	—
description	text	Description of the address	✔	—
number	text	House number	✔	—
postal-code	text	ZIP / postal code	✔	—
province	text	Province	✔	—
state	text	State	✔	—
street	text	Street name	—	—

probabilistic-data-structure

Probabilistic data structure object describe a space-efficient data structure such as Bloom filter or similar structure.

probabilistic-data-structure 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	Multiple
link	link	Source of the probabilistic data structure.	✔	—
probability	float	The false positive rate of the probabilistic data structure. ['0.1', '0.01', '0.001', '0.0001']	✔	—
total-bits	integer	The number of bits used by this probabilistic data structure.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
total-capacity	integer	The total capacity of the total set represented in this probabilistic data structure.	✔	—
type	text	Type of the probabilistic data structure. ['Bloom filter', 'Ribbon filter', 'Cuckoo filter', 'Quotient filter', 'Xor filter', 'Taffy filter', 'HyperLogLog filter', 'Count–min sketch filter']	✔	—
updatable	boolean	Is the probabilistic data structure updatable? ['False', 'True']	✔	—
used-capacity	integer	The used capacity (and cardinality) of the set represented in this probabilistic data structure.	✔	—
vendor-implementation-ref	link	Details about the implementation of the probabilistic data structure.	✔	—

process

Object describing a system process.

> process 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	Multiple
args	text	Arguments of the process	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
child-pid	text	Process ID of the child(ren) process	✔	✔
command-line	text	Command line of the process	—	—
creation-time	datetime	Local date/time at which the process was created	✔	—
current-directory	text	Current working directory of the process	✔	—
environment-variables	text	Environment variables associated to the process	✔	—
fake-process-name	boolean	Is the process spawned under a false name. ['1', '0']	✔	—
guid	text	The globally unique identifier of the assigned by the vendor product	—	—
hidden	boolean	Specifies whether the process is hidden ['True', 'False']	✔	—
image	filename	Path of process image	—	—
integrity-level	text	Integrity level of the process ['system', 'high', 'medium', 'low', 'untrusted']	✔	—
name	text	Name of the process	—	—
parent-command-line	text	Command line of the parent process	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
parent-guid	text	The globally unique idenifier of the parent process assigned by the vendor product	➖	➖
parent-image	filename	Path of parent process image	➖	➖
parent-pid	text	Process ID of the parent process	✔	➖
parent-process-name	text	Process name of the parent	➖	➖
parent-process-path	text	Parent process path of the parent	➖	➖
pgid	text	Identifier of the group of processes the process belong to	✔	➖
pid	text	Process ID of the process	✔	➖
port	port	Port(s) owned by the process	✔	✔
process-state	process-state	State of process. ['D', 'R', 'S', 'T', 't', 'W', 'X', 'Z', '<', 'N', 'L', 's', 'l', '+']	✔	➖
start-time	datetime	Local date/time at which the process was started	✔	➖
user-creator	text	User who created of the process	✔	➖
user-process	text	User who is running the process at the time of the analysis	✔	➖

publication

An object to describe a book, journal, or academic publication.

publication 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	Multiple
DOI	text	DOI System is used to identify digital resources.	—	✔
ISBN	text	International Standard Book Number.	—	✔
academic-institution	text	Academic institution associated with the publisher or authors.	—	✔
archive	link	Archive of the original document (Internet Archive, Archive.is, etc).	—	✔
attachment	attachment	The publication file or screen capture.	—	✔
author	text	Author of the publication.	—	✔
content	text	Content of the publication.	—	—
contributor	text	Contributors include editors, compilers, and translators.	—	✔
description	text	A description of the publication.	✔	—
edition	text	Edition of the publication.	✔	—
embedded-link	url	Link contained in the publication (possibly malicious).	—	✔
embedded-safe-link	link	Link contained in the publication (assumed safe).	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
link	link	Original link to the publication (supposed harmless).	—	✔
publisher	text	Publisher of the document.	—	—
series	text	Series of the publication.	✔	—
title	text	Content of the publication.	—	—
url	url	Original link to the publication (possibly malicious).	—	✔
volume	text	Volume of the publication.	✔	—
website	link	Website of the publisher.	✔	—
year	text	Year of publication.	✔	—

python-etvx-event-log

Event log object template to share information of the activities conducted on a system. .

> python-etvx-event-log 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	Multiple
Computer	text	Computer name on which the event occurred	✔	—
Correlation-ID	text	Unique activity identity which relates the event to a process.	—	—
Event-data	text	Event data description.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
Keywords	text	Tags used for the event for the purpose of filtering or searching. ['Network', 'Security', 'Resource not found', 'other']	—	—
Operational-code	text	The opcode (numeric value or name) associated with the activity carried out by the event.	✔	—
Processor-ID	text	ID of the processor that processed the event.	✔	—
Relative-Correlation-ID	text	Related activity ID which identity similar activities which occurred as a part of the event.	✔	—
Session-ID	text	Terminal server session ID.	✔	—
Thread-ID	text	Thread id that generated the event.	✔	—
User	text	Name or the User ID the event is associated with.	✔	—
comment	text	Additional comments.	✔	—
event-channel	text	Channel through which the event occurred ['Application', 'System', 'Security', 'Setup', 'other']	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
event-date-time	datetime	Date and time when the event was logged.	✔	—
event-id	text	A unique number which identifies the event.	✔	—
event-type	text	Event-type assigned to the event ['Admin', 'Operational', 'Audit', 'Analytic', 'Debug', 'other']	✔	—
kernel-time	datetime	Execution time of the kernel mode instruction.	✔	—
level	text	Determines the event severity. ['Information', 'Warning', 'Error', 'Critical', 'Success Audit', 'Failure Audit']	—	—
log	text	Log file where the event was recorded.	✔	—
name	text	Name of the event.	✔	—
source	text	The source of the event log - application/software that logged the event.	—	—
task-category	text	Activity by the event publisher	✔	—
user-time	datetime	Date and time when the user instruction was executed.	✔	—

query

An object describing a query, along with its format.

query 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	Multiple
author	text	Author of the query	✔	—
comment	comment	A description of the query rule.	—	—
format	text	Format of the query. ['event query language (eql)', 'keyword query language (kql)', 'Kusto Query Language', 'Query DSL', 'Query (Elastic Search)', 'Search Processing Language - SPL (Splunk)', 'Sigma', 'Lucene query', 'Google search query', 'Ariel Query Language (qradar)', 'Grep', 'Devo LINQ']	✔	—
query	text	Query rule in the format specified in the format field.	—	—
query-rule-name	text	Query rule name.	—	—

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	Multiple
callback-average	integer	Average size of a callback	✔	—
callback-largest	integer	Largest callback	✔	—
callbacks	counter	Amount of callbacks (functions started as thread)	✔	—
create-thread	counter	Amount of calls to CreateThread	✔	—
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	✔	—
gml	attachment	Graph export in G>raph Modelling Language format	✔	—
local-references	counter	Amount of API calls inside a code section	✔	—
memory-allocations	counter	Amount of memory allocations	✔	—
miss-api	counter	Amount of API call reference that does not resolve to a function offset	✔	—
not-referenced-strings	counter	Amount of not referenced strings	✔	—
r2-commit-version	text	Radare2 commit ID used to generate this object	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
ratio-api	float	Ratio: amount of API calls per kilobyte of code section	✔	—
ratio-functions	float	Ratio: amount of functions per kilobyte of code section	✔	—
ratio-string	float	Ratio: amount of referenced strings per kilobyte of code section	✔	—
referenced-strings	counter	Amount of referenced strings	✔	—
refsglobalvar	counter	Amount of API calls outside of code section (glob var, dynamic API)	✔	—
shortest-path-to-create-thread	integer	Shortest path to the first time the binary calls CreateThread	✔	—
text	text	Description of the r2graphity object	✔	—
total-api	counter	Total amount of API calls	✔	—
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)	✔	—

ransom-negotiation

An object to describe ransom negotiations, as seen in ransomware incidents.

ransom-negotiation 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	Multiple
Remarks	text	Remarks	✔	—
annual_revenue_EUR	float	Annual revenue of the targeted organisation in EUR	✔	—
chatsite	url	Chatsite where the negotiations take place	✔	—
chatsite_id_private	text	Second, private, chat ID given by actor	✔	—
chatsite_id_public	text	Initial chat ID given by actor	✔	—
currency	text	The currency of the initial demand. Often USD or BTC.	✔	—
data_leaked	boolean	Was data leaked in this incident? ['True', 'False']	✔	—
data_stolen	boolean	Was data exfiltrated in this incident? ['True', 'False']	✔	—
discount	float	Discount after negotiations	✔	—
email_address	text	Contact address, if any	—	—
final_ransom	float	Final ransom amount after negotiations, in the currency as displayed in field 'currency'	✔	—
initial_ransom	float	Initial ransom demand in the currency as displayed in field 'currency'	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
negotiations_screenshot	attachment	Screenshot of the negotiations	✔	✔
negotiations_transcript	text	Transcript of the negotiations	✔	—
pay_for_deletion	boolean	Does the target need/want to pay for data deletion ['True', 'False']	✔	—
pay_for_encryptor	boolean	Does the target need/want to pay for the decryptor ['True', 'False']	✔	—
percentage_of_revenue	float	Percentage of the annual revenue that the ransom demand amounts to	✔	—
time	datetime	Date and time of transaction	✔	—
url_leaksite	url	URL of the leaksite	—	—
value_EUR	float	Value in EUR of the final ransom amount, with conversion rate as of date/time displayed in field 'time'	✔	—
wallet-address	btc	A cryptocoin wallet address	—	—

ransomware-group-post

Ransomware group post as monitored by ransomlook.io or others.

ransomware-group-post 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	Multiple
actor-geo-stats-30d	text	Count of how many other victims were publicly leaked by the same ransomware actor in the country of the victim during the past 30 days	✔	—
actor-total-stats-30d	text	Count of how many other victims were publicly leaked by the same ransomware actor worldwide during the past 30 days	✔	—
date	datetime	Last update of the post as seen on the ransomware group blog. Different than the first/last seen from the crawling.	✔	—
date-published	datetime	Initial published date of the post on the ransomware group blog.	✔	—
description	text	Raw post.	—	—
entity-name	text	Entity name of the victim referenced in the post of the ransomware group.	—	—
geo	text	Geographic (main) location of the victim referenced in the post of the ransomware group.	✔	—
leak-site-url	link	Link to the post.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
link	link	Original URL location of the post.	—	—
ransomware-group	text	Ransomware group where the post is mentioned.	✔	—
sector	text	Sector (main) of the victim referenced in the post of the ransomware group.	✔	—
severity	text	Severity of the post mentioned. ['critical', 'high', 'medium', 'low', 'info']	✔	—
title	text	Title of blog post.	—	—
website	link	Website of the victim referenced in the post of the ransomware group.	—	—

reddit-account

Reddit account.

reddit-account 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	Multiple
account-avatar	attachment	A screen capture or exported account avatar.	—	✔
account-avatar-url	url	A user profile picture or avatar.	—	✔
account-id	text	Account id.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
account-name	text	Account name (do not include u/).	—	—
archive	link	Archive of the account (Internet Archive, Archive.is, etc).	✔	✔
attachment	attachment	A screen capture or exported list of contacts etc.	—	✔
description	text	A description of the user.	✔	—
link	link	Original link to the account page (supposed harmless).	—	—
moderator-of	text	Subreddits of which this account is a moderator (exclude the r/).	—	✔
trophies	text	Trophies listed in the account Trophy Case.	—	✔
url	url	Original URL location of the page (potentially malicious).	—	—

reddit-comment

A Reddit post comment.

reddit-comment 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	Multiple
archive	link	Archive of the original comment (Internet Archive, Archive.is, etc).	✔	✔
attachment	attachment	A screen capture or exported file from the comment.	—	✔
author	text	The user account that created the post (do not include u/).	—	—
body	text	The raw text of the comment.	—	—
description	text	A description of the comment.	✔	—
embedded-link	url	Link embedded in the subreddit description (potentially malicious).	—	✔
embedded-safe-link	link	Link embedded in the subreddit description (supposed safe).	—	✔
hashtag	text	Hashtag used to identify or promote the comment.	—	✔
link	link	Original link to the comment (supposed harmless).	—	—
subreddit-name	text	The name of the subreddit where it was posted (exclude the r/).	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
url	url	Original URL location of the comment (potentially malicious).	—	—
username-quoted	text	Username who are quoted in the comment (do not include u/).	—	✔

reddit-post

A Reddit post.

reddit-post 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	Multiple
archive	link	Archive of the original Reddit post (Internet Archive, Archive.is, etc).	✔	✔
attachment	attachment	A screen capture or exported file from the Reddit post.	—	✔
author	text	The user account that created the post (do not include u/).	—	—
description	text	A description of the post.	✔	—
edited	text	Has the post been edited? ['True', 'False']	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
embedded-link	url	Link embedded in the subreddit description (potentially malicious).	–	✔
embedded-safe-link	link	Link embedded in the subreddit description (supposed safe).	–	✔
hashtag	text	Hashtag used to identify or promote the Reddit post.	–	✔
link	link	Original link to the Reddit post (supposed harmless).	–	–
post-content	text	The raw text of the Reddit post.	–	–
post-title	text	The title of the Reddit post.	–	–
subreddit-name	text	The name of the subreddit where it was posted (exclude the r/).	–	✔
thumbnail	attachment	Screen capture or exported post thumbnail.	–	–
thumbnail-url	url	Link to post thumbnail.	–	–
url	url	Original URL location of the Reddit post (potentially malicious).	–	–
username-quoted	text	Username who are quoted in the Reddit post (do not include u/).	–	✔

reddit-subreddit

Public or private subreddit.

reddit-subreddit 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	Multiple
active-user-count	text	Number of active accounts in the subreddit.	✔	—
archive	link	Archive of the original subreddit (Internet Archive, Archive.is, etc).	✔	✔
attachment	attachment	A screen capture or exported list of contacts, subreddit members, etc.	—	✔
banner-background-image	attachment	A screen capture or exported subreddit header.	—	✔
banner-background-url	url	A link to the subreddit header.	—	✔
creator	text	The user account that created the subreddit (do not include u/).	—	—
description	text	A description of the subreddit.	—	—
display-name	text	The name of the subreddit (exclude the r/).	—	—
embedded-link	url	Link embedded in the subreddit description (potentially malicious).	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
embedded-safe-link	link	Link embedded in the subreddit description (supposed safe).	➖	✔
hashtag	text	Hashtag used to identify or promote the subreddit.	➖	✔
header-title	text	A title of the subreddit.	➖	✔
icon-img	attachment	A screen capture or exported subreddit community icon.	➖	✔
icon-img-url	url	A link to the subreddit community icon.	➖	✔
link	link	Original link to the subreddit (supposed harmless).	➖	➖
moderator	text	A user account who is a moderator of the subreddit (do not include u/).	➖	✔
privacy	text	Subreddit privacy. ['Public', 'Private']	➖	➖
rules	text	Raw text of the rules of the subreddit.	➖	✔
submit-text	text	The submission form raw text when posting to the subreddit.	➖	➖
subreddit-alias	text	Aliases or previous names of subreddit.	➖	✔
subreddit-type	text	Subreddit type, e.g. general, buy and sell etc.	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
url	url	Original URL location of the subreddit (potentially malicious).	—	—

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	Multiple
comment	comment	A description of the regular expression.	—	—
regexp	text	regexp	—	—
regexp-type	text	Type of the regular expression syntax. ['PCRE', 'PCRE2', 'POSIX BRE', 'POSIX ERE', 'FCRE (Farsight Compatible Regular Expressions)']	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
type	text	Specify which type corresponds to this regex. ['hostname', 'domain', 'email-src', 'email-dst', 'email-subject', 'url', 'user-agent', 'regkey', 'cookie', 'uri', 'filename', 'windows-service-name', 'windows-scheduled-task']	✔	—

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	Multiple
data	text	Data stored in the registry key	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
data-type	text	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	text	Hive used to store the registry key (file on disk)	✔	—
key	regkey	Full key path	—	—
last-modified	datetime	Last time the registry key has been modified	—	—
name	text	Name of the registry key	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
root-keys	text	Root key of the Windows registry (extracted from the key) ['HKCC', 'HKCR', 'HKCU', 'HKDD', 'HKEY_CLASSES_ROOT', 'HKEY_CURRENT_CONFIG', 'HKEY_CURRENT_USER', 'HKEY_DYN_DATA', 'HKEY_LOCAL_MACHINE', 'HKEY_PERFORMANCE_DATA', 'HKEY_USERS', 'HKLM', 'HKPD', 'HKU']	✔	—

registry-key-value

Registry key value object describing a Windows registry key value, with its data, data type and name values. To be used when a registry key has multiple values.

registry-key-value 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	Multiple
data	text	Data stored in the registry key value	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
data-type	text	Registry key 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']	✔	—
name	text	Name of the registry key value	—	—

regripper-NTUser

Regripper Object template designed to present user specific configuration details extracted from the NTUSER.dat hive.

regripper-NTUser 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	Multiple
applications-installed	text	List of applications installed.	—	✔
applications-run	text	List of applications set to run on the system.	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
comments	text	Additional information related to the user profile	✔	—
external-devices	text	List of external devices connected to the system by the user.	—	✔
key	text	Registry key where the information is retrieved from.	—	—
key-last-write-time	datetime	Date and time when the key was last updated.	✔	—
logon-user-name	text	Name assigned to the user profile.	—	—
mount-points	text	Details of the mount points created on the system.	✔	✔
network-connected-to	text	List of networks the user connected the system to.	—	✔
nukeOnDelete	boolean	Determines if the Recycle bin option has been disabled. ['True', 'False']	✔	—
recent-files-accessed	text	List of recent files accessed by the user.	—	✔
recent-folders-accessed	text	List of recent folders accessed by the user.	—	✔
typed-urls	text	Urls typed by the user in internet explorer	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
user-init	text	Applications or processes set to run when the user logs onto the windows system.	—	✔

regripper-sam-hive-single-user

Regripper Object template designed to present user profile details extracted from the SAM hive.

regripper-sam-hive-single-user 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	Multiple
comments	text	Full name assigned to the user profile.	✔	—
full-user-name	text	Full name assigned to the user profile.	—	—
key	text	Registry key where the information is retrieved from.	—	—
key-last-write-time	datetime	Date and time when the key was last updated.	✔	—
last-login-time	datetime	Date and time when the user last logged onto the system.	✔	—
login-count	counter	Number of times the user logged-in onto the system.	✔	—
pwd-fail-date	datetime	Date and time when a password last failed for this user profile.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
pwd-reset-time	datetime	Date and time when the password was last reset.	✔	—
user-name	text	User name assigned to the user profile.	—	—

regripper-sam-hive-user-group

Regripper Object template designed to present group profile details extracted from the SAM hive.

regripper-sam-hive-user-group 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	Multiple
full-name	text	Full name assigned to the profile.	—	—
group-comment	text	Any group comment added.	✔	—
group-name	text	Name assigned to the profile.	—	—
group-users	text	Users belonging to the group	—	✔
key	text	Registry key where the information is retrieved from.	—	—
key-last-write-time	datetime	Date and time when the key was last updated.	✔	—
last-write-date-time	datetime	Date and time when the group key was updated.	✔	—

regripper-software-hive-BHO

Regripper Object template designed to gather information of the browser helper objects installed on the system.

regripper-software-hive-BHO 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	Multiple
BHO-key-last-write-time	datetime	Date and time when the BHO key was last updated.	✔	—
BHO-name	text	Name of the browser helper object.	—	—
class	text	Class to which the BHO belongs to.	✔	—
comments	text	Additional comments.	✔	—
key	text	Software hive key where the information is retrieved from.	—	—
last-write-time	datetime	Date and time when the key was last updated.	✔	—
module	text	DLL module the BHO belongs to.	✔	—
references	link	References to the BHO.	—	✔

regripper-software-hive-appInit-DLLS

Regripper Object template designed to gather information of the DLL files installed on the system.

regripper-software-hive-appInit-DLLS 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	Multiple
DLL-last-write-time	datetime	Date and time when the DLL file was last updated.	✔	—
DLL-name	text	Name of the DLL file.	—	—
DLL-path	text	Path where the DLL file is stored.	—	—
comments	text	Additional comments.	✔	—
key	text	Software hive key where the information is retrieved from.	—	—
last-write-time	datetime	Date and time when the key was last updated.	✔	—
references	link	References to the DLL file.	—	✔

regripper-software-hive-application-paths

Regripper Object template designed to gather information of the application paths.

regripper-software-hive-application-paths 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	Multiple
comments	text	Additional comments.	✔	—
executable-file-name	text	Name of the executable file.	—	✔
key	text	Software hive key where the information is retrieved from.	—	—
last-write-time	datetime	Date and time when the key was last updated.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
path	text	Path of the executable file.	➖	✔
references	link	References to the application installed.	➖	✔

regripper-software-hive-applications-installed

Regripper Object template designed to gather information of the applications installed on the system.

regripper-software-hive-applications-installed 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	Multiple
app-last-write-time	datetime	Date and time when the application key was last updated.	✔	➖
app-name	text	Name of the application.	➖	➖
comments	text	Additional comments.	✔	➖
key	text	Software hive key where the information is retrieved from.	➖	➖
key-path	text	Path of the key.	➖	➖
last-write-time	datetime	Date and time when the key was last updated.	✔	➖
references	link	References to the application installed.	➖	✔
version	text	Version of the application.	➖	➖

regripper-software-hive-command-shell

Regripper Object template designed to gather information of the shell commands executed on the system.

regripper-software-hive-command-shell 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	Multiple
command	text	Command executed.	—	—
comments	text	Additional comments.	✔	—
key	text	Software hive key where the information is retrieved from.	—	—
last-write-time	datetime	Date and time when the key was last updated.	✔	—
shell	text	Type of shell used to execute the command. ['exe', 'cmd', 'bat', 'hta', 'pif', 'Other']	✔	—
shell-path	text	Path of the shell.	—	—

regripper-software-hive-software-run

Regripper Object template designed to gather information of the applications set to run on the system.

regripper-software-hive-software-run 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	Multiple
application-name	text	Name of the application run.	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
application-path	text	Path where the application is installed.	➖	✔
comments	text	Additional comments.	✔	➖
key	text	Software hive key where the information is retrieved from. ['Run', 'RunOnce', 'Runservices', 'Terminal', 'Other']	✔	➖
key-path	text	Path of the key.	✔	➖
last-write-time	datetime	Date and time when the key was last updated.	✔	➖
references	link	References to the applications.	➖	✔

regripper-software-hive-userprofile-winlogon

Regripper Object template designed to gather user profile information when the user logs onto the system, gathered from the software hive.

regripper-software-hive-userprofile-winlogon 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	Multiple
AutoAdminLogon	boolean	Flag value to determine if autologon is enabled for a user without entering the password. ['True', 'False']	✔	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
AutoRestartShell	boolean	Value of the flag set to auto restart the shell if it crashes or shuts down automatically. ['True', 'False']	✔	—
CachedLogonCount	counter	Number of times the user has logged into the system.	✔	—
Comments	text	Additional comments.	✔	—
DefaultUserName	text	user-name of the default user.	✔	—
DisableCAD	boolean	Flag to determine if user login is enabled by pressing Ctrl+ALT+Delete. ['True', 'False']	✔	—
Legal-notice-caption	text	Message title set to display when the user logs-in.	✔	✔
Legal-notice-text	text	Message set to display when the user logs-in.	✔	✔
PasswordExpiryWarining	counter	Number of times the password expiry warning appeared.	✔	—
PowerdownAfterShutDown	boolean	Flag value- if the system is set to power down after it is shutdown. ['True', 'False']	✔	—
PreCreateKnownFolders	text	create known folders key	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
ReportBootOk	boolean	Flag to check if the reboot was successful. ['True', 'False']	✔	—
SID	text	Security identifier assigned to the user profile.	✔	—
Shell	text	Shell set to run when the user logs onto the system.	✔	✔
ShutdownFlags	counter	Number of times shutdown is initiated from a process when the user is logged-in.	✔	—
ShutdownWithoutLogon	boolean	Value of the flag set to enable shutdown without requiring a user to login. ['True', 'False']	✔	—
UserInit	text	Applications and files set to run when the user logs onto the system (User logon activity).	—	✔
WinStationsDisabled	boolean	Flag value set to enable/disable logons to the system. ['True', 'False']	✔	—
user-profile-key-last-write-time	datetime	Date and time when the key was last updated.	✔	—
user-profile-key-path	text	key where the user-profile information is retrieved from.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
user-profile-last-write-time	datetime	Date and time when the user profile was last updated.	✔	—
user-profile-path	text	Path of the user profile on the system	✔	—
winlogon-key-last-write-time	datetime	Date and time when the winlogon key was last updated.	✔	—
winlogon-key-path	text	winlogon key referred in order to retrieve default user information	✔	—

regripper-software-hive-windows-general-info

Regripper Object template designed to gather general windows information extracted from the software-hive.

regripper-software-hive-windows-general-info 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	Multiple
BuildGUID	text	Build ID.	—	—
BuildLab	text	Windows BuildLab string.	—	—
BuildLabEx	text	Windows BuildLabEx string.	—	—
CSDVersion	text	Version of the service pack installed.	—	—
CurrentBuild	text	Build number of the windows OS.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
CurrentBuildType	text	Current build type of the OS.	➖	➖
CurrentVersion	text	Current version of windows	✔	➖
EditionID	text	Windows edition.	➖	➖
InstallDate	datetime	Date when windows was installed.	✔	➖
InstallationType	text	Type of windows installation.	✔	➖
PathName	text	Path to the root directory.	✔	➖
ProductID	text	ID of the product version.	➖	➖
ProductName	text	Name of the windows version.	➖	➖
RegisteredOrganization	text	Name of the registered organization.	➖	➖
RegisteredOwner	text	Name of the registered owner.	➖	➖
SoftwareType	text	Software type of windows. ['System', 'Application', 'other']	✔	➖
SystemRoot	text	Root directory.	✔	➖
comment	comment	Additional comments.	✔	➖
last-write-time	datetime	Date and time when the key was last updated.	✔	➖
win-cv-path	text	key where the windows information is retrieved from	➖	➖

regripper-system-hive-firewall-configuration

Regripper Object template designed to present firewall configuration information extracted from the system-hive.

regripper-system-hive-firewall-configuration 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	Multiple
comment	text	Additional comments.	✔	—
disable-notification	boolean	Boolean flag to determine if firewall notifications are enabled. ['True', 'False']	✔	—
enbled-firewall	boolean	Boolean flag to determine if the firewall is enabled. ['True', 'False']	✔	—
last-write-time	datetime	Date and time when the firewall profile policy was last updated.	✔	—
profile	text	Firewall Profile type ['Domain Profile', 'Standard Profile', 'Network Profile', 'Public Profile', 'Private Profile', 'other']	✔	—

regripper-system-hive-general-configuration

Regripper Object template designed to present general system properties extracted from the system-hive.

regripper-system-hive-general-configuration 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	Multiple
comment	text	Additional comments.	✔	—
computer-name	text	name of the computer under analysis	—	—
fDenyTSConnections:	boolean	Specifies whether remote connections are enabled or disabled on the system. ['True', 'False']	✔	—
last-write-time	datetime	Date and time when the key was last updated.	✔	—
shutdown-time	datetime	Date and time when the system was shutdown.	✔	—
timezone-bias	text	Offset in minutes from UTC. Offset added to the local time to get a UTC value.	✔	—
timezone-daylight-bias	text	value in minutes to be added to the value of timezone-bias to generate the bias used during daylight time.	✔	—
timezone-daylight-date	datetime	Daylight date - daylight saving months	✔	—
timezone-daylight-name	text	Timezone name used during daylight saving months.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
timezone-last-write-time	datetime	Date and time when the timezone key was last updated.	✔	—
timezone-standard-bias	text	value in minutes to be added to the value of timezone-bias to generate the bias used during standard time.	✔	—
timezone-standard-date	datetime	Standard date - non daylight saving months	✔	—
timezone-standard-name	text	Timezone standard name used during non-daylight saving months.	✔	—

regripper-system-hive-network-information

Regripper object template designed to gather network information from the system-hive.

regripper-system-hive-network-information 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	Multiple
DHCP-IP-address	ip-dst	DHCP service - IP address	—	—
DHCP-domain	text	Name of the DHCP domain service	—	—
DHCP-name-server	ip-dst	DHCP Name server - IP address.	—	—
DHCP-server	ip-dst	DHCP server - IP address.	—	—
DHCP-subnet-mask	ip-dst	DHCP subnet mask - IP address.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
TCPIP-key	text	TCPIP key	➖	➖
TCPIP-key-last-write-time	datetime	Datetime when the key was last updated.	✔	➖
additional-comments	text	Comments.	✔	➖
interface-GUID	text	GUID value assigned to the interface.	✔	➖
interface-IPcheckingEnabled	boolean		✔	➖
interface-MediaSubType	text	➖	✔	➖
interface-PnpInstanceID	text	Plug and Play instance ID assigned to the interface.	✔	➖
interface-last-write-time	datetime	Last date and time when the interface key was updated.	✔	➖
interface-name	text	Name of the interface.	➖	➖
network-key	text	Registry key assigned to the network	➖	➖
network-key-last-write-time	datetime	Date and time when the network key was last updated.	✔	➖
network-key-path	text	Path of the key where the information is retrieved from.	✔	➖

regripper-system-hive-services-drivers

Regripper Object template designed to gather information regarding the services/drivers from the system-hive.

regripper-system-hive-services-drivers 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	Multiple
comment	text	Additional comments.	✔	—
display	text	Display name/information of the service or the driver.	—	—
group	text	Group to which the system/driver belong to. ['Base', 'Boot Bus Extender', 'Boot File System', 'Cryptography', 'Extended base', 'Event Log', 'Filter', 'FSFilter Bottom', 'FSFilter Infrastructure', 'File System', 'FSFilter Virtualization', 'Keyboard Port', 'Network', 'NDIS', 'Parallel arbitrator', 'Pointer Port', 'PnP Filter', 'ProfSvc_Group', 'PNP_TDI', 'SCSI Miniport', 'SCSI CDROM Class', 'System Bus Extender', 'Video Save', 'other']	✔	—
image-path	text	Path of the service/drive	—	—
last-write-time	datetime	Date and time when the key was last updated.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
name	text	name of the key	—	—
start	text	When the service/driver starts or executes. ['Boot start', 'System start', 'Auto start', 'Manual', 'Disabled']	✔	—
type	text	Service/driver type. ['Kernel driver', 'File system driver', 'Own process', 'Share process', 'Interactive', 'Other']	✔	—

report

Report object to describe a report along with its metadata.

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	Multiple
case-number	text	Case number	—	—
link	link	Link to the report mentioned	—	✔
report-file	attachment	Attachment(s) that is related to the report	—	✔
summary	text	Free text summary of the report	—	✔
title	text	Title of the report	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
type	text	Type of report ['Alert', 'Artwork', 'Attachment', 'Audio', 'Bill', 'Blog', 'Book', 'Case', 'Conference', 'Dictionary', 'Document', 'Email', 'Encyclopedia', 'Film', 'Forum', 'Hearing', 'Incident', 'Instant', 'Interview', 'Journal', 'Letter', 'Magazine', 'Manuscript', 'Map', 'Newspaper', 'Note', 'Online', 'Operation', 'Patent', 'Podcast', 'Presentation', 'Press', 'Radio', 'Report', 'Software', 'Statute', 'Thesis', 'TV', 'Video', 'Webpage']	✔	—

research-scanner

Information related to known scanning activity (e.g. from research projects).

research-scanner 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	Multiple
asn	AS	Autonomous System Number related to project	✔	—
contact_email	email-dst	Project contact information	✔	✔
contact_phone	phone-number	Phone number related to project	✔	✔
domain	domain	Domain related to project	—	✔
project	text	Description of scanning project	✔	—
project_url	link	URL related to project	✔	✔
scanning_host	hostname	Scanning host used by project	—	✔
scanning_ip	ip-src	IP address used by project	—	✔
scheduled_end	datetime	Scheduled end of scanning activity	✔	✔
scheduled_start	datetime	Scheduled start of scanning activity	✔	✔

risk-assessment-report

Risk assessment report object which includes the assessment report from a risk assessment platform such as MONARC.

risk-assessment-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	Multiple
case-number	text	Case number	—	—
link	link	Link to the report mentioned	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
report-file	attachment	Attachment(s) that is related to the report in human readable format (PDF)	—	✔
summary	text	Free text summary of the risk assessment report	—	✔
type	text	Source of the risk assessment report ['MONARC', 'Serima']	✔	—

rmm

An object describing a RMM agent.

rmm 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	Multiple
api-key	text	Authentication or API key used by the RMM agent	—	✔
comment	comment	A description of the RMM.	—	—
guid	text	GUID or reference of the RMM agent or deployment ID.	—	✔
hostname	hostname	hostname of the control server for the RMM agent.	—	—
name	text	Name of the RMM agent.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
rmm-type	text	Type of the RMM agent described. ['AnyDesk', 'Atera', 'ASG', 'BeAnywhere', 'Domotz', 'DWservice', 'Fixme.it', 'Fleetdeck.io', 'GetScreen', 'Itarian', 'Level.io', 'Logmein', 'ManageEngine', 'MeshCentral', 'N-Able', 'Pulseway', 'RattyRat', 'Rport', 'Rsocx', 'RustDesk', 'RustScan', 'ScreenConnect', 'Splashtop', 'SSH', 'Tactical RMM', 'Teamviewer', 'TightVNC', 'TrendMicro', 'Sorillus', 'Xeox', 'ZeroTier']	✔	—
url	url	url of the control server for the RMM agent.	—	—

rogue-dns

Rogue DNS as defined by CERT.br.

rogue-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	Multiple
hijacked-domain	hostname	Domain/hostname hijacked by the the rogue DNS	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
phishing-ip	ip-dst	Resource records returns by the rogue DNS	—	—
rogue-dns	ip-dst	IP address of the rogue DNS	—	—
status	text	How many authoritative DNS answers were received at the Passive DNS Server's collectors with exactly the given set of values as answers. ['ROGUE DNS', 'Unknown']	✔	—
timestamp	datetime	Last time that the rogue DNS value was seen.	✔	—

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	Multiple
classification	text	Classification of the RTIR ticket	—	✔
constituency	text	Constituency of the RTIR ticket	—	—
ip	ip-dst	IPs automatically extracted from the RTIR ticket	—	✔
queue	text	Queue of the RTIR ticket ['incident', 'investigations', 'blocks', 'incident reports']	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
status	text	Status of the RTIR ticket ['new', 'open', 'stalled', 'resolved', 'rejected', 'deleted']	✔	—
subject	text	Subject of the RTIR ticket	—	—
ticket-number	text	ticket-number of the RTIR ticket	—	—

sandbox-report

Sandbox report.

sandbox-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	Multiple
on-premise-sandbox	text	The on-premise sandbox used ['cuckoo', 'symantec-cas-on-premise', 'bluecoat-maa', 'trendmicro-deep-discovery-analyzer', 'fireeye-ax', 'vmray', 'joe-sandbox-on-premise']	✔	—
permalink	link	Permalink reference	—	—
raw-report	text	Raw report from sandbox	✔	—
results	text	Freetext result values	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
saas-sandbox	text	A non-on-premise sandbox, also results are not publicly available ['forticloud-sandbox', 'joe-sandbox-cloud', 'symantec-cas-cloud']	✔	—
sandbox-file	attachment	File related to sandbox run	✔	✔
sandbox-type	text	The type of sandbox used ['on-premise', 'web', 'saas']	✔	—
score	text	Score	✔	—
web-sandbox	text	A web sandbox where results are publicly available via an URL ['malwr', 'hybrid-analysis']	✔	—

sb-signature

Sandbox detection signature.

sb-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	Multiple
datetime	datetime	Datetime	✔	—
signature	text	Name of detection signature - set the description of the detection signature as a comment	—	✔
software	text	Name of Sandbox software	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
text	text	Additional signature description	✔	—

scan-result

Scan result object to add meta-data and the output of the scan result by itself.

scan-result 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	Multiple
description	text	Description of the scanning performed in this scan-result	✔	—
scan-end	datetime	End of scanning activity	✔	✔
scan-result	attachment	The scan-result as a file (in machine-readable or human-readable format). The file is always consider non-malicious.	—	—
scan-result-format	text	Format used for the scan-result. ['free-text output', 'XML', 'JSON', 'CSV', 'HTML', 'PDF', 'Unknown']	—	—
scan-result-query	text	Query or parameters provided to scan-result-tool to generate the scan-result.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
scan-result-tool	text	Tool used which generated the scan-result. ['AWS Prowler Scan', 'AWS Scout2 Scan', 'AWS Security Finding Format (ASFF) Scan', 'AWS Security Hub Scan', 'Acunetix Scan', 'Acunetix360 Scan', 'Anchore Engine Scan', 'Anchore Enterprise Policy Check', 'Anchore Grype', 'AnchoreCTL Policies Report', 'AnchoreCTL Vuln Report', 'AppSpider Scan', 'Aqua Scan', 'Arachni Scan', 'AuditJS Scan', 'Azure Security Center Recommendations Scan', 'Bandit Scan', 'BinaryEdge', 'BlackDuck API', 'Blackduck Component Risk', 'Blackduck Hub Scan', 'Brakeman Scan', 'BugCrowd Scan', 'Bugcrowd API Import', 'Bundler-Audit Scan', 'Burp Enterprise Scan', 'Burp GraphQL API', 'Burp REST API', 'Burp Scan', 'CargoAudit Scan',	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
scan-start	datetime	Start of scanning activity	✔	✔
scan-type	text	Type of scanning in the scan-result. ['Network', 'System', 'Unknown']	✔	✔

scheduled-event

Event object template describing a gathering of individuals in meatspace.

scheduled-event 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	Multiple
address	text	Postal address of the event.	—	✔
administrator	text	A user account who is an owner or admin of the event.	—	✔
archive	link	Archive of the original event (Internet Archive, Archive.is, etc).	—	✔
attachment	attachment	A screen capture or other attachment relevant to the event.	—	✔
e-mail	email-src	Email address of the event contact.	—	✔
embedded-link	url	Link embedded in the event description (potentially malicious).	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
embedded-safe-link	link	Link embedded in the event description (supposed safe).	➖	✔
event-alias	text	Aliases of event.	➖	✔
event-listing	text	Social media and other platforms on which the event is advertised. ['Twitter', 'Facebook', 'Meetup', 'Eventbrite', 'Other']	✔	✔
event-name	text	The name of the event.	➖	➖
fax-number	phone-number	Fax number of the event contact.	➖	✔
hashtag	text	Hashtag used to identify or promote the event.	➖	✔
link	link	Original link into the event (supposed harmless).	➖	➖
person-name	text	A person who is going to the event.	➖	✔
phone-number	phone-number	Phone number of the event contact.	➖	✔
scheduled-date	datetime	Initial creation of the microblog post	➖	✔
url	url	Original URL location of the event (potentially malicious).	➖	➖
username	text	A user account who is going to the event.	➖	✔

scheduled-task

Windows scheduled task description.

scheduled-task 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	Multiple
Start-time	datetime	Time when the task is triggered	✔	✔
author	text	Who created the task	—	—
description	text	Description of the task	—	—
highest-privileges	boolean	Should the task run with the highest privileges	✔	—
location	text	Location (Path including filename) of the scheduled task on the computer	✔	—
name	text	Name of the scheduled task	—	—
password-stored	boolean	Should the password be stored (Only if log on is not mandatory)	✔	—
repeat	text	condition to repeat the task	✔	—
run-when-user-logged-on-only	boolean	Should the task run if the user is logged on only	✔	—
running-account	text	User account used when running the task	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
trigger	text	when should the task being triggered ['On a schedule', 'At log on', 'At startup', 'On idle', 'On an event', 'At task creation/modification', 'On connection to user session', 'On disconnect from user session', 'On workstation lock', 'On workstation unlock']	✔	✔

scrippsco2-c13-daily

Daily average C13 concentrations (ppm) derived from flask air samples.

scrippsco2-c13-daily 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	Multiple
c13-value	float	C13 value (ppm) - C13 concentrations are measured on the '08A' Calibration Scale	✔	—
flag	integer	Flag (see taxonomy for details).	✔	—
number-flask	counter	Number of flasks used in daily average.	✔	—
sample-date-excel	float	M$Excel spreadsheet date format.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
sample-date-fractional	float	Decimal year and fractional year.	✔	—
sample-datetime	datetime	Datetime the sample has been taken	✔	—

scrippsco2-c13-monthly

Monthly average C13 concentrations (ppm) derived from flask air samples.

scrippsco2-c13-monthly 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	Multiple
monthly-c13	float	Monthly C13 concentrations in micro-mol C13 per mole (ppm) reported on the 2008A SIO manometric mole fraction scale. This is the standard version of the data most often sought.	✔	—
monthly-c13-seasonal-adjustment	float	Same data after a seasonal adjustment to remove the quasi-regular seasonal cycle. The adjustment involves subtracting from the data a 4-harmonic fit with a linear gain factor.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
monthly-c13-smoothed	float	Smoothed version of the data generated from a stiff cubic spline function plus 4-harmonic functions with linear gain.	✔	—
monthly-c13-smoothed-seasonal-adjustment	float	Same smoothed version with the seasonal cycle removed.	✔	—
sample-date-excel	float	M$Excel spreadsheet date format.	✔	—
sample-date-fractional	float	Decimal year and fractional year.	✔	—
sample-datetime	datetime	The monthly values have been adjusted to 24:00 hours on the 15th of each month.	✔	—

scrippsco2-co2-daily

Daily average CO2 concentrations (ppm) derived from flask air samples.

scrippsco2-co2-daily 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	Multiple
co2-value	float	CO2 value (ppm) - CO2 concentrations are measured on the '08A' Calibration Scale	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
flag	integer	Flag (see taxonomy for details).	✔	—
number-flask	counter	Number of flasks used in daily average.	✔	—
sample-date-excel	float	M$Excel spreadsheet date format.	✔	—
sample-date-fractional	float	Decimal year and fractional year.	✔	—
sample-datetime	datetime	Datetime the sample has been taken	✔	—

scrippsco2-co2-monthly

Monthly average CO2 concentrations (ppm) derived from flask air samples.

scrippsco2-co2-monthly 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	Multiple
monthly-co2	float	Monthly CO2 concentrations in micro-mol CO2 per mole (ppm) reported on the 2008A SIO manometric mole fraction scale. This is the standard version of the data most often sought.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
monthly-co2-seasonal-adjustment	float	Same data after a seasonal adjustment to remove the quasi-regular seasonal cycle. The adjustment involves subtracting from the data a 4-harmonic fit with a linear gain factor.	✔	—
monthly-co2-smoothed	float	Smoothed version of the data generated from a stiff cubic spline function plus 4-harmonic functions with linear gain.	✔	—
monthly-co2-smoothed-seasonal-adjustment	float	Same smoothed version with the seasonal cycle removed.	✔	—
sample-date-excel	float	M$Excel spreadsheet date format.	✔	—
sample-date-fractional	float	Decimal year and fractional year.	✔	—
sample-datetime	datetime	The monthly values have been adjusted to 24:00 hours on the 15th of each month.	✔	—

scrippsco2-o18-daily

Daily average O18 concentrations (ppm) derived from flask air samples.

scrippsco2-o18-daily 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	Multiple
flag	integer	Flag (see taxonomy for details).	✔	—
number-flask	counter	Number of flasks used in daily average.	✔	—
o18-value	float	O18 value (ppm) - O18 concentrations are measured on the '08A' Calibration Scale	✔	—
sample-date-excel	float	M$Excel spreadsheet date format.	✔	—
sample-date-fractional	float	Decimal year and fractional year.	✔	—
sample-datetime	datetime	Datetime the sample has been taken	✔	—

scrippsco2-o18-monthly

Monthly average O18 concentrations (ppm) derived from flask air samples.

scrippsco2-o18-monthly 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	Multiple
monthly-o18	float	Monthly O18 concentrations in micro-mol O18 per mole (ppm) reported on the 2008A SIO manometric mole fraction scale. This is the standard version of the data most often sought.	✔	—
monthly-o18-seasonal-adjustment	float	Same data after a seasonal adjustment to remove the quasi-regular seasonal cycle. The adjustment involves subtracting from the data a 4-harmonic fit with a linear gain factor.	✔	—
monthly-o18-smoothed	float	Smoothed version of the data generated from a stiff cubic spline function plus 4-harmonic functions with linear gain.	✔	—
monthly-o18-smoothed-seasonal-adjustment	float	Same smoothed version with the seasonal cycle removed.	✔	—
sample-date-excel	float	M$Excel spreadsheet date format.	✔	—
sample-date-fractional	float	Decimal year and fractional year.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
sample-datetime	datetime	The monthly values have been adjusted to 24:00 hours on the 15th of each month.	✔	—

script

Object describing a computer program written to be run in a special run-time environment. The script or shell script can be used for malicious activities but also as support tools for threat analysts.

> script 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	Multiple
comment	text	Comment associated to the script.	—	—
filename	filename	Filename used for the script.	✔	✔
language	text	Scripting language used for the script. ['PowerShell', 'VBScript', 'Bash', 'Lua', 'JavaScript', 'AppleScript', 'AWK', 'Python', 'Perl', 'Ruby', 'Winbatch', 'AutoIt', 'PHP', 'Nim']	✔	—
script	text	Free text of the script.	—	—
script-as-attachment	attachment	Attachment of the script.	—	—
state	text	Known state of the script. ['Malicious', 'Unknown', 'Harmless', 'Trusted']	✔	✔

security-playbook

The security-playbook object provides meta-information and allows managing, storing, and sharing cybersecurity playbooks and orchestration workflows.

security-playbook 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	Multiple
description	text	An explanation, details, and more context about what this playbook does and tries to accomplish.	✔	—
labels	text	Labels for this playbook (e.g., adversary persona names, associated groups, malware family/variant/name that this playbook is related to). Another option is to use MISP tags, taxonomies, and galaxies.	✔	✔
organization-type	text	The type of organization that the playbook is intended for. This can be an industry sector. Another option is to use MISP tags, taxonomies, and galaxies.	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
playbook-abstraction	text	The playbook's level of abstraction (with regards to consumption). ['template', 'executable']	✔	—
playbook-base64	text	The entire playbook file/document encoded in base64.	—	—
playbook-creation-time	datetime	The date and time at which the playbook was originally created.	✔	—
playbook-creator	text	The entity that created the playbook. It can be a natural person or an organization. It may be represented using a unique identifier that identifies the creator.	✔	—
playbook-file	attachment	The entire playbook file/document in its native format (e.g., CACAO JSON or BPMN).	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
playbook-id	text	A value that (uniquely) identifies the playbook. If the playbook itself embeds an identifier then the playbook-id SHOULD use the same identifier (value) for correlation purposes.	–	–
playbook-impact	text	From 0 to 100, a value representing the impact the playbook has on the organization. A value of 0 means specifically undefined. Impact values range from 1, the lowest impact, to a value of 100, the highest. For example, a purely investigative playbook that is non-invasive could have a low impact value of 1. In contrast, a playbook that performs changes such as adding rules into a firewall should have a higher impact value.	✔	–

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
playbook-modification-time	datetime	The date and time at which the playbook was last modified.	✔	—
playbook-priority	text	From 0 to 100, a value representing the priority of this playbook relative to other defined playbooks. A value of 0 means specifically undefined. Priority values range from 1, the highest priority, to a value of 100, the lowest.	✔	—
playbook-severity	text	From 0 to 100, a value representing the seriousness of the conditions that this playbook addresses. A value of 0 means specifically undefined. Severity values range from 1, the lowest severity, to a value of 100, the highest.	✔	—
playbook-standard	text	The standard/format/notation the playbook conforms to (e.g., CACAO, BPMN).	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
playbook-type	text	The security-related functions the playbook supports. A playbook may account for multiple types (e.g., detection and investigation). The listed options are based on the CACAO standard and NIST SP 800-61 rev2. Another option is to use MISP tags, taxonomies, and galaxies. ['notification', 'detection', 'investigation', 'prevention', 'mitigation', 'remediation', 'analysis', 'containment', 'eradication', 'recovery', 'attack']	✔	✔
playbook-valid-from	datetime	The date and time from which the playbook is considered valid and the steps that it contains can be executed.	✔	—
playbook-valid-until	datetime	The date and time from which the playbook should no longer be considered a valid playbook to be executed.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
revoked	boolean	A boolean that identifies if the playbook is no longer valid (revoked). ['True', 'False']	✔	—

shadowserver-malware-url-report

This report identifies URLs that were observed in exploitation attempts in the last 24 hours. They are assumed to contain a malware payload or serve as C2 controllers. If a payload was successfully downloaded in the last 24 hours, it's SHA256 hash will also be published. The data is primarily sourced from honeypots (in which case they will often be IoT related), but other sources are possible. As always, you only receive information on IPs found on your network/constituency or in the case of a National CSIRT, your country. Ref: https://www.shadowserver.org/what-we-do/network-reporting/malware-url-report/.

shadowserver-malware-url-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	Multiple
application	text	Application layer protocol where occurrence of the URL was observed. Examples: http, https, ssh, telnet. ['http', 'https', 'ssh', 'telnet']	✔	—
asn	AS	ASN where the IP resides	—	—
city	text	City location of the IP in question	✔	—
geo	text	Country location of the IP	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
host	hostname	Any of the capabilities identified for the malware instance or family.	➖	✔
ip	ip-src	IP of the of the URL	➖	✔
naics	text	North American Industry Classification System Code	✔	✔
port	port	Port of the URL	➖	✔
region	text	Regional location of the IP in question	✔	➖
resource_path	text	URL resource path extracted from the url	➖	✔
sector	text	Sector of the IP in question	✔	✔
severity	text	Severity of the report ['critical', 'high', 'medium', 'low', 'info']	✔	➖
sha256	sha256	SHA256 of associated (potentially malicious) payload, if downloaded from the URL	➖	➖
source	text	Source of information, if public	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
tag	text	Array of tags associated with the URL if any. In this report typically it will be a CVE entry, for example CVE-2021-44228. This allows for better understanding of the URL context observed (ie. usage associated with a particular CVE).	✔	✔
timestamp	datetime	Timestamp of when the URL was seen (in the last 24 hours)	—	—
url	url	URL that was extracted from an observed exploitation attempt, assumed to be carrying a malware payload	—	✔

shadowserver-scan-http-proxy

This report identifies open HTTP proxy servers on multiple ports. While HTTP proxies have legitimate uses, they are also used for attacks or other forms of abuse. https://www.shadowserver.org/what-we-do/network-reporting/open-http-proxy-report/.

shadowserver-scan-http-proxy 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	Multiple
asn	AS	ASN where the IP resides	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
city	text	City location of the IP in question	✔	—
connection	text	Control options for the current connection and list of hop-by-hop request fields	✔	✔
content_length	text	The length of the response body in octets	✔	✔
content_type	text	The MIME type of the body of the request	✔	✔
geo	text	Country location of the IP	✔	—
hostname	hostname	Any of the capabilities identified for the malware instance or family.	—	✔
hostname_source	text	Hostname source	✔	✔
http	text	Hypertext Transfer Protocol Version	✔	✔
http_code	text	HTTP Response code: e.g., 200, 401, 404	✔	✔
http_date	text	The date and time that the message was sent	✔	✔
http_reason	text	The text reason to go with the HTTP Code	✔	✔
ip	ip-src	The IP address of the device in question	—	✔
naics	text	North American Industry Classification System Code	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
port	port	Port the response came from	➖	✔
protocol	text	Protocol observed in the network traffic	➖	✔
proxy_authenticate	text	The authentication method that should be used to gain access to a resource behind a proxy server	✔	✔
region	text	Regional location of the IP in question	✔	➖
sector	text	Sector of the IP in question	✔	✔
server	text	HTTP Server type	✔	✔
severity	text	Severity leve ['critical', 'high', 'medium', 'low', 'info']	✔	➖
tag	text	Array of tags associated with the URL if any. In this report typically it will be a CVE entry, for example CVE-2021-44228. This allows for better understanding of the URL context observed (ie. usage associated with a particular CVE).	✔	✔
timestamp	datetime	Time that the IP was probed in UTC+0	➖	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
transfer_encoding	text	The form of encoding used to safely transfer the entity to the user	✔	✔
via	text	General header added by proxies	✔	✔

shell-commands

Object describing a series of shell commands executed. This object can be linked with malicious files in order to describe a specific execution of shell commands.

shell-commands 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	Multiple
comment	text	Comment associated to the shell commands executed.	—	—
language	text	Scripting language used for the shell commands executed. ['PowerShell', 'VBScript', 'Bash', 'Lua', 'JavaScript', 'AppleScript', 'AWK', 'Python', 'Perl', 'Ruby', 'Winbatch', 'AutoIt', 'PHP']	✔	—
script	text	Free text of the script if available which executed the shell commands.	—	—
shell-command	text	—	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
state	text	Known state of the script. ['Malicious', 'Unknown', 'Harmless', 'Trusted']	✔	✔

shodan-report

Shodan Report for a given IP.

shodan-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	Multiple
banner	text	server banner reported	—	—
hostname	domain	Hostnames found	—	✔
ip	ip-dst	IP Address Queried	—	—
org	text	Associated Organization	—	—
port	port	Listening Port	—	—
text	text	A description of the report	—	—

short-message-service

Short Message Service (SMS) object template describing one or more SMS message. Restriction of the initial format 3GPP 23.038 GSM character set doesn't apply.

short-message-service 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	Multiple
body	text	Message body of the SMS	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
from	phone-number	Phone number used to send the SMS	—	✔
name	text	Sender name	—	—
phone-company	text	Phone company of the number used to send the SMS	—	—
received-date	datetime	Received date of the SMS	✔	—
sent-date	datetime	Initial sent date of the SMS	✔	—
smsc	phone-number	SMS Message Center	—	—
to	phone-number	Phone number receiving the SMS	—	✔
url-rfc5724	url	url representing SMS using RFC 5724 (not url contained in the SMS which should use an url object)	—	—

shortened-link

Shortened link and its redirect target.

shortened-link 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	Multiple
credential	text	Credential (username, password)	—	—
domain	domain	Full domain	—	—
first-seen	datetime	First time this shortened URL has been seen	✔	—
redirect-url	url	Redirected to URL	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
shortened-url	url	Shortened URL	—	—
text	text	Description and context of the shortened URL	—	—

sigma

An object describing a Sigma rule (or a Sigma rule name).

sigma 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	Multiple
comment	comment	A description of the Sigma rule.	—	—
context	text	Context where the Sigma rule can be applied ['all', 'disk', 'memory', 'network', 'dns']	✔	✔
reference	link	Reference/origin of the Sigma rule.	—	—
sigma	sigma	Sigma rule.	—	—
sigma-rule-name	text	Sigma rule name.	—	—

sigmf-archive

An object representing an archive containing one or multiple recordings in the Signal Metadata Format Specification (SigMF).

sigmf-archive 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	Multiple
SigMF-archive	attachment	tar archive (.sigmf)	✔	—

sigmf-expanded-recording

An object representing a single IQ/RF sample in the Signal Metadata Format Specification (SigMF).

sigmf-expanded-recording 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	Multiple
author	text	A text identifier for the author potentially including name, handle, email, and/or other ID like Amateur Call Sign.	✔	—
collection	text	The base filename of a collection with which this Recording is associated.	✔	—
data_doi	text	The registered DOI (ISO 26324) for a Recording's Dataset file.	✔	—
dataset	text	The full filename of the Dataset file this Metadata file describes.	✔	—
datatype	text	—	✔	—
description	text	A text description of the SigMF Recording.	✔	—
fft-plot	attachment	FFT plot of the signal	✔	—
geolocation_alt	text	The location of the Recording system (altitude).	✔	—
geolocation_lat	text	The location of the Recording system (latitude).	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
geolocation_long	text	The location of the Recording system (longitude).	✔	—
hw	text	A text description of the hardware used to make the Recording.	✔	—
iq-sample	attachment	Binary file of IQ samples	✔	—
license	text	A URL for the license document under which the Recording is offered.	✔	—
meta_doi	text	The registered DOI (ISO 26324) for a Recording's Metadata file.	✔	—
metadata_only	boolean	Indicates the Metadata file is intentionally distributed without the Dataset.	✔	—
num_channels	counter	Total number of interleaved channels in the Dataset file. If omitted, this defaults to one.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
offset	integer	The index number of the first sample in the Dataset. If not provided, this value defaults to zero. Typically used when a Recording is split over multiple files. All sample indices in SigMF are absolute, and so all other indices referenced in metadata for this recording SHOULD be greater than or equal to this value.	✔	—
recorder	text	The name of the software used to make this SigMF Recording.	✔	—
sample_rate	float	The sample rate of the signal in samples per second.	✔	—
sha512	sha512	The SHA512 hash of the Dataset file associated with the SigMF file.	✔	—
trailing_bytes	size-in-bytes	The number of bytes to ignore at the end of a Non-Conforming Dataset file.	✔	—
version	text	The version of the SigMF specification used to create the Metadata file.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
waterfall-plot	attachment	Waterfall plot of the signal	✔	—

sigmf-recording

An object representing a single IQ/RF sample in the Signal Metadata Format Specification (SigMF).

> sigmf-recording 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	Multiple
SigMF-data	attachment	Binary file of IQ or RF samples (.sigmf-data)	✔	—
SigMF-meta	attachment	Metadata file in SigMF format (.sigmf-meta)	✔	—

social-media-group

Social media group object template describing a public or private group or channel.

> social-media-group 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	Multiple
administrator	text	A user account who is an owner or admin of the group.	—	✔
archive	link	Archive of the original group (Internet Archive, Archive.is, etc).	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
attachment	attachment	A screen capture or exported list of contacts, group members, etc.	➖	✔
description	text	A description of the group, channel or community.	➖	➖
embedded-link	url	Link embedded in the group description (potentially malicious).	➖	✔
embedded-safe-link	link	Link embedded in the group description (supposed safe).	➖	✔
group-alias	text	Aliases of group, channel or community.	➖	✔
group-name	text	The name of the group, channel or community.	➖	➖
hashtag	text	Hashtag used to identify or promote the group.	➖	✔
link	link	Original link into the group (supposed harmless).	➖	➖
person-name	text	A person who is a member of the group.	➖	✔
platform	text	The social media platform used. ['Facebook', 'Twitter']	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
url	url	Original URL location of the group (potentially malicious).	—	—
username	text	A user account who is a member of the group.	—	✔

software

The Software object represents high-level properties associated with software, including software products. STIX 2.1 - 6.14.

software 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	Multiple
cpe	cpe	Specifies the Common Platform Enumeration (CPE) entry for the software, if available. The value for this property MUST be a CPE v2.3 entry from the official NVD CPE Dictionary [NVD] . While the CPE dictionary does not contain entries for all software, whenever it does contain an identifier for a given instance of software, this property SHOULD be present.	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
language	text	Specifies the languages supported by the software. The value of each list member MUST be a language code conformant to [RFC5646].	✔	✔
name	text	Specifies the name of the software.	—	—
swid	text	Specifies the Software Identification (SWID) Tags [SWID] entry for the software, if available. The tag attribute, tagId, a globally unique identifier, SHOULD be used as a proxy identifier of the tagged product.	—	✔
vendor	text	Specifies the name of the vendor of the software.	✔	—
version	text	Specifies the version of the software.	✔	—

spambee-report

A Spambee analysis report.

spambee-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	Multiple
feedback-requested	boolean	User has requested feedback	✔	—
feedback-sent	boolean	Feedback has been sent to user	✔	—
feedback-time	datetime	Timestamp of the feedback	✔	—
privacy	boolean	User has requested privacy	✔	—
report-status	text	Result of the Spambee analysis for the submitted email	✔	—
report-uid	text	Internal reference to the Spambee report	✔	—

spearphishing-attachment

Spearphishing Attachment.

spearphishing-attachment 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	Multiple
artifact-dropped-md5	md5	The MD5 of an additional file that was either extracted from or downloaded by the attachment.	—	✔
artifact-dropped-name	filename	Name of an additional file that was either extracted from or downloaded by the attachment.	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
artifact-dropped-sha1	sha1	The SHA1 of an additional file that was either extracted from or downloaded by the attachment.	➖	✔
artifact-dropped-sha256	sha256	The SHA256 of an additional file that was either extracted from or downloaded by the attachment.	➖	✔
attachment-md5	md5	The MD5 of the file that was attached to the e-mail itself.	➖	✔
attachment-name	filename	The name of the file that was attached to the e-mail itself.	➖	➖
attachment-sha1	sha1	The SHA1 of the file that was attached to the e-mail itself.	➖	✔
attachment-sha256	sha256	The SHA256 of the file that was attached to the e-mail itself.	➖	✔
c2-domain	domain	Command and control domain detected during analysis.	➖	✔
c2-ip	ip-dst	Command and control IP address detected during analysis.	➖	✔
c2-url	url	Command and control URL detected during analysis.	➖	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
date	text	Date and time the e-mail was sent.	✔	—
email-sender	email-src	The source address from which the e-mail was sent.	—	✔
malicious-url	url	Malicious URL that downloaded additional malware.	—	✔
research-links	link	A link to an external analysis (VirusTotal, urlscan, etc.).	—	✔
sender-ip	ip-src	The source IP from which the e-mail was sent.	—	✔
subject	email-subject	The subject line of the e-mail.	—	✔
supporting-evidence	text	Description of the spearphish e-mail.	—	—

spearphishing-link

Spearphishing Link.

spearphishing-link 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	Multiple
date	text	Date and time e-mail was sent.	✔	—
email-sender	email-src	The source address from which the e-mail was sent.	—	✔
embedded-link	url	The malicious URL in the e-mail body.	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
redirect-url	url	The redirect URL, if any, from the malicious embedded link.	➖	✔
research-links	link	A link to an external analysis (VirusTotal, urlscan, etc.).	➖	✔
sender-ip	ip-src	The source IP from which the e-mail was sent.	➖	✔
subject	email-subject	The subject line of the e-mail.	➖	✔
supporting-evidence	text	Description of the spearphish e-mail.	➖	➖

splunk

Splunk / Splunk ES object.

splunk 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	Multiple
description	comment	Description	✔	➖
drill-down	text	Drilldown	✔	✔
earliest	text	Earliest time	✔	➖
latest	text	Latest time	✔	➖
response-action	text	Response action ['notable', 'risk']	✔	✔
schedule	other	Schedule	✔	➖
search	text	Search / Correlation search	✔	✔

ss7-attack

SS7 object of an attack as seen on the SS7 signaling protocol supporting GSM/GPRS/UMTS networks.

ss7-attack 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	Multiple
Category	text	Category ['Cat0', 'Cat1', 'Cat2.1', 'Cat2.2', 'Cat3.1', 'Cat3.2', 'Cat3.3', 'CatSMS', 'CatSpoofing']	✔	✔
GtAssignee	text	GT Assignee this is the party that got the GT range assigned by their Regulator.	—	✔
GtLessee	text	GT Lessee is a third party who will use a leased global title from a GT Lessor.	—	✔
GtLessor	text	GT Lessor is a GT Assignee that has decided to lease one or more of their GTs to a third party, the GT Lessee, typically on a commercial basis.	—	✔
GtSubLessee	text	GT Sub-Lessee – this is an additional third party who has entered into an agreement with the GT Lessee to sub-lease a GT from them.	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
MapApplicationContext	text	MAP application context in OID format. ['4.0.0.1.0.1. - networkLocUp', '4.0.0.1.0.2. - locationCancel', '4.0.0.1.0.3. - roamingNbEnquiry', '4.0.0.1.0.22. - subscriberDataModificationNotification', '4.0.0.1.0.6. - callControlTransfer', '4.0.0.1.0.16. - subscriberDataMngt', '4.0.0.1.0.46. - vcsgLocationUpdate', '4.0.0.1.0.15. - interVlrInfoRetrieval', '4.0.0.1.0.18. - networkFunctionalSs', '4.0.0.1.0.39. - authenticationFailureReport', '4.0.0.1.0.44. - resourceMngt', '4.0.0.1.0.41. - shortMsgMT_VGCS_Relay', '4.0.0.1.0.5. - locInfoRetrieval', '4.0.0.1.0.32. - gprsLocationUpdate', '4.0.0.1.0.33. - gprsLocationInfoRetrieval', '4.0.0.1.0.34. - failureReport', '4.0.0.1.0.35. - gprsNotify', '4.0.0.1.0.11. - handoverControl', '4.0.0.1.0.12. - sIWFSAllocation', '4.0.0.1.0.47. - vcsgLocationCanc	✔	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
MapGmlc	text	MAP GMLC. Phone number.	—	—
MapGsmscfGT	text	MAP GSMSCF GT. Phone number.	—	—
MapImsi	text	MAP IMSI. Phone number starting with MCC/MNC.	—	✔
MapMscGT	text	MAP MSC GT. Phone number.	—	—
MapMsisdn	text	MAP MSISDN. Phone number.	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
MapOpCode	text	MAP operation codes - Decimal value between 0-99. ['updateLocation - 2', 'cancelLocation - 3', 'provideRoamingNumber - 4', 'noteSubscriberDataModified - 5', 'resumeCallHandling - 6', 'insertSubscriberData - 7', 'deleteSubscriberData - 8', 'sendParameters - 9', 'registerSS - 10', 'eraseSS - 11', 'activateSS - 12', 'deactivateSS - 13', 'interrogateSS - 14', 'authenticationFailureReport - 15', 'registerPassword - 17', 'getPassword - 18', 'processUnstructuredSS_Data - 19', 'releaseResources - 20', 'mt_ForwardSM_VGCS - 21', 'sendRoutingInfo - 22', 'updateGprsLocation - 23', 'sendRoutingInfoForGprs - 24', 'failureReport - 25', 'noteMsPresentForGprs - 26', 'performHandover - 28',	✔	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
MapSmsTP-DCS	text	MAP SMS TP-DCS.	✔	➖
MapSmsTP-OA	text	MAP SMS TP-OA. Phone number.	➖	➖
MapSmsTP-PID	text	MAP SMS TP-PID.	✔	➖
MapSmsText	text	MAP SMS Text. Important indicators in SMS text.	➖	➖
MapSmsTypeNumber	text	MAP SMS TypeNumber.	✔	➖
MapSmscGT	text	MAP SMSC. Phone number.	➖	✔
MapUssdCoding	text	MAP USSD Content.	✔	➖
MapUssdContent	text	MAP USSD Content.	➖	➖
MapVersion	text	Map version. ['1', '2', '3']	✔	➖
MapVlrGT	text	MAP VLR GT. Phone number.	➖	➖
SccpCdGT	text	Signaling Connection Control Part (SCCP) CdGT - Phone number.	➖	✔
SccpCdGT-Country	text	Country in which SCCP CDGT is registered.	➖	➖
SccpCdGT-CountryISO2	text	Code ISO 3166-1 alpha-2 from which the SCCP CDGT is allocated.	➖	➖
SccpCdGT-OperatorName	text	Operator Name under which the SCCP CDGT is registered.	➖	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
SccpCdGT-TADIG	text	TADIG under which the SCCP CDGT is registered.	➖	➖
SccpCdPC	text	Signaling Connection Control Part (SCCP) CdPC - Phone number.	➖	➖
SccpCdSSN	text	Signaling Connection Control Part (SCCP) - Decimal value between 0-255.	✔	➖
SccpCgGT	text	Signaling Connection Control Part (SCCP) CgGT - Phone number.	➖	✔
SccpCgGT-Country	text	Country in which SCCP CGGT is registered.	➖	➖
SccpCgGT-CountryISO2	text	Allocated Code ISO 3166-1 alpha-2 for the SCCP CGGT.	➖	➖
SccpCgGT-OperatorName	text	Operator Name under which the SCCP CGGT is registered.	➖	➖
SccpCgGT-TADIG	text	TADIG under which the SCCP CGGT is registered.	➖	➖
SccpCgPC	text	Signaling Connection Control Part (SCCP) CgPC - Phone number.	➖	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
SccpCgSSN	text	Signaling Connection Control Part (SCCP) - Decimal value between 0-255.	✔	—
first-seen	datetime	When the attack has been seen for the first time.	✔	—
text	text	A description of the attack seen via SS7 logging.	✔	✔

ssh-authorized-keys

An object to store ssh authorized keys file.

ssh-authorized-keys 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	Multiple
first-seen	datetime	First time the ssh authorized keys file has been seen	✔	—
full-line	text	One full-line of the authorized key file	—	✔
hostname	hostname	hostname	—	✔
ip	ip-dst	IP Address	—	✔
key	text	Public key in base64 as found in the authorized key file	—	✔
key-id	text	Key-id and option part of the public key line	—	✔
last-seen	datetime	Last time the ssh authorized keys file has been seen	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
text	text	A description of the ssh authorized keys	✔	—

stairwell

Stairwell leverages automated analysis, YARA rule libraries, shared malware feeds, privately run AV verdicts, static & dynamic analysis, malware unpacking, and variant discovery.

stairwell 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	Multiple
entropy	float	Measure of the information contained in a object as opposed to the portion of the object that is determined (or predictable)	✔	—
environment	comment	Stairwell environments that this object has been seen within	—	✔
imphash	imphash	The Mandiant import hash (imphash) of the object	—	—
magic	comment	Magic number as determined by yara rule based identification	—	—
malEval-probability	comment	Confidence that the label applies on the object	—	—
malEval-severity	comment	Severity of malware detected	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
md5	md5	The md5 hash signature of an object	—	—
mime-type	mime-type	MIME type as determined by yara rule based identification	✔	—
sha1	sha1	The sha1 hash signature of an object	—	—
sha256	sha256	The sha256 hash signature of an object	—	—
size-in-bytes	size-in-bytes	The size of the file in bytes	✔	—
stairwell-first-seen	datetime	The timestamp at which an object was first observed by Stairwell	—	—
tlsh	tlsh	The TLSH of the object	—	—
yara-rule-match	comment	Stairwell yara rule resource names which have matched on this object	—	✔

stix2-pattern

An object describing a STIX pattern. The object can be linked via a relationship to other attributes or objects to describe how it can be represented as a STIX pattern.

stix2-pattern 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	Multiple
comment	comment	A description of the stix2-pattern.	—	—
stix2-pattern	stix2-pattern	STIX 2 pattern	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
version	text	Version of STIX 2 pattern. ['stix 2.0', 'stix 2.1']	✔	—

stock

Object to describe stock market.

stock 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	Multiple
bloomberg-exchange-code	text	Bloomberg Exchange Code ['AB', 'AF', 'AO', 'AT', 'AV', 'BB', 'BC', 'BD', 'BI', 'BQ', 'BS', 'CC', 'CF', 'CG', 'CK', 'CS', 'CT', 'CV', 'CX', 'CY', 'DB', 'DC', 'DH', 'DU', 'EB', 'EC', 'FH', 'FP', 'GA', 'GB', 'GD', 'GF', 'GH', 'GI', 'GM', 'GS', 'GY', 'HB', 'HK', 'IB', 'ID', 'IJ', 'IM', 'IS', 'IT', 'IX', 'JR', 'JT', 'KK', 'KN', 'KP', 'KQ', 'LI', 'LN', 'LX', 'MC', 'MK', 'MM', 'MT', 'NA', 'NG', 'NL', 'NO', 'NS', 'NZ', 'OM', 'PE', 'PK', 'PL', 'PM', 'PO', 'PW', 'QD', 'QF', 'QT', 'RE', 'RF', 'RX', 'SE', 'SJ', 'SL', 'SM', 'SP', 'SS', 'SV', 'SY', 'TB', 'TG', 'TI', 'TQ', 'TT', 'UA', 'UF', 'UN', 'UP', 'UQ', 'UR', 'UV', 'UW', 'VH', 'VM', 'VX', 'XB', 'ZA']	✔	➖
country	text	Country	✔	➖
currency	text	Currency	✔	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
exchange	text	Exchange where the stock is traded (Google code) ['AMS', 'ASX', 'ATH', 'BAK', 'BATS', 'BDP', 'BIT', 'BME', 'BMV', 'BOM', 'BVMF', 'CAI', 'CPH', 'DFM', 'EBR', 'ELI', 'EPA', 'ETR', 'FRA', 'HEL', 'HKG', 'IRE', 'IST', 'JAK', 'JNB', 'KAR', 'KOSDAQ', 'KRX', 'KUL', 'LON', 'MCX', 'NASDAQ', 'NSE', 'NYSE', 'NYSEAMERICAN', 'NYSEARCA', 'NZE', 'OTCMKTS', 'PRG', 'PSE', 'SGX', 'SHA', 'SHE', 'STO', 'SWX', 'TLV', 'TPE', 'TSE', 'TYO', 'VIE', 'VTX', 'WSE']	✔	✔
high-price	text	Highest price seen	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
iso-mic	text	ISO MIC ['ARCX', 'BATE', 'BATS', 'BOAT', 'BVMF', 'CHIX', 'DIFX', 'DSMD', 'HSTC', 'MISX', 'MTAA', 'NEOE', 'NOTC', 'OOTC', 'ROCO', 'TOMX', 'TRQX', 'XADS', 'XAMM', 'XAMS', 'XASE', 'XASX', 'XATH', 'XBAH', 'XBER', 'XBKK', 'XBOG', 'XBOM', 'XBRU', 'XBRV', 'XBSE', 'XBUD', 'XBUE', 'XCAI', 'XCAS', 'XCNQ', 'XCOL', 'XCSE', 'XCYS', 'XDFM', 'XDHA', 'XDSE', 'XDUB', 'XDUS', 'XEQT', 'XETR', 'XFRA', 'XHAM', 'XHAN', 'XHEL', 'XHKG', 'XICE', 'XIDX', 'XIST', 'XJSE', 'XKAR', 'XKLS', 'XKOS', 'XKRX', 'XKUW', 'XLIM', 'XLIS', 'XLJU', 'XLON', 'XLUX', 'XMAD', 'XMEX', 'XMUN', 'XMUS', 'XNAI', 'XNCM', 'XNEC', 'XNGM', 'XNGS', 'XNMS', 'XNSA', 'XNSE', 'XNYS', 'XNZE', 'XOSL', 'XPAR', 'XPHS', 'XPOS', 'XPRA', 'XQTX', 'XSAU', 'XSES', 'XSGO', 'XSHE', 'XSHG', 'XSTC', 'XSTO', 'XSTU',	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
low-price	text	Lowest price seen	✔	—
symbol	text	Symbol of the stock	—	—

submarine

Submarine description.

> submarine 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	Multiple
active	counter	The number of submarines of this class in active service	—	—
armament	text	Armaments carried by the submarine	—	✔
beam	float	The beam measurement of the submarine in meters	—	—
builders	text	The organisation building this class of submarines	—	✔
cancelled	counter	The number of submarines of this class cancelled	—	—
class	text	Submarine class	—	—
complement	integer	Crew size	—	—
completed	counter	The number of submarines of this class built	—	—
displacement	integer	Displacement in tonnes	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
draught	float	The draught measurement of the submarine in meters	➖	➖
endurance	counter	Expected submerged endurance in days	➖	➖
in_service_from	integer	The year the submarine entered service	➖	➖
in_service_until	integer	The year the submarine left service	➖	➖
length	float	The length measurement of the submarine in meters	➖	➖
operator	text	The countries operating such vessels (can be multiple)	➖	✔
planned	counter	The number of submarines of this class planned to be built	➖	➖
predecessor	text	Predecessor class	➖	➖
propulsion	text	The propulsion of the submarine, add multiple if applicabe	➖	✔
retired	counter	The number of submarines of this class that has been retired	➖	➖
speed_submerged	float	Surfaced top speed in knots	➖	➖
speed_surfaced	float	Surfaced top speed in knots	➖	➖
successor	text	Successor class	➖	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
type	text	Submarine type ['Ballistic missile submarine', 'Cruise missile submarine', 'Nuclear-powered attack submarine', 'Non-nuclear attack submarine with air-independent propulsion', 'Diesel-electric attack submarine', 'Midget submarine', 'Special mission submarine']	✔	—

summariser-output

Summariser output from an AI-based or NLP summariser.

summariser-output 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	Multiple
description	text	Description of the text summarised.	✔	—
original-text	attachment	Original text before any processing.	✔	—
original-text-timestamp	datetime	Publication date of the original text (not related to the processing).	✔	—
original-url	link	URL of the original text.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
summariser-model	text	Model used for the summariser ['gpt-3.5-turbo', 'gpt-3.5-turbo-16k', 'gpt-3.5-turbo-0125 (16k)', 'gpt-4', 'gpt-4-turbo', 'gpt-4-o', 'gpt-4o-mini']	➖	✔
summariser-timestamp	datetime	Date when the summary was produced.	✔	➖
summariser-version	text	Version of the code used for the summariser.	✔	➖
summary	text	Summary of the original text by the AI-based or NLP-based summariser.	✔	➖
tcode	text	MITRE ATT&CK Technique ID extracted by the AI-based or NLP-based summariser.	✔	✔
title	text	Title of the text summarised.	✔	➖
ttp	text	TTP of the original text extracted by the AI-based or NLP-based summariser.	✔	➖

suricata

An object describing one or more Suricata rule(s) along with version and contextual information.

suricata 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	Multiple
comment	comment	A description of the Suricata rule(s).	—	—
ref	link	Reference to the Suricata rule such as origin of the rule or alike.	—	—
suricata	snort	Suricata rule.	—	✔
version	text	Version of the Suricata rule depending where the suricata rule is known to work as expected.	—	—

target-system

Description about an targeted system, this could potentially be a compromised internal system.

target-system 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	Multiple
targeted_ip_of_system	ip-src	Targeted system IP address	✔	—
targeted_machine	target-machine	Targeted system	✔	—
timestamp_seen	datetime	Registered date and time	✔	—

task

Task object as described in STIX 2.1 Incident object extension.

task 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	Multiple
description	text	Description of the task.	—	—
end_time	datetime	The date and time the event was last recorded.	—	—
end_time_fidelity	text	Level of fidelity that the `end_time` is recorded in. ['day', 'hour', 'minute', 'month', 'second', 'year']	✔	—
error	text	Details about any failure or deviation that occurred in the task.	✔	—
name	text	Name of the task.	—	—
outcome	text	Outcome of the task ['cancelled', 'failed', 'ongoing', 'pending', 'successful', 'unknown']	✔	—
priority	text	Priority or importance of the task. ['Not Specified', 'False Positive', 'Low', 'Moderate', 'High', 'Extreme']	✔	—
start_time	datetime	The date and time the event was first recorded.	—	—
start_time_fidelity	text	Level of fidelity that the `start_time` is recorded in. ['day', 'hour', 'minute', 'month', 'second', 'year']	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
task_type	text	Type of task. ['administrative', 'attribution', 'containment', 'declared', 'detected', 'eradication', 'escalated', 'exercised-control', 'external-intelligence', 'external-outreach', 'external-support', 'implemented-control', 'negotiation', 'playbook-execution', 'playbook-step-execution', 'recovery', 'reported', 'routine-updates', 'victim-notification']	✔	✔

tattoo

Describes tattoos on a natural person's body.

tattoo 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	Multiple
tattoo-body-part	text	Describe the body part where the tattoo is located. ['head', 'forehead', 'face', 'ear', 'eye', 'mouth/lips', 'neck', 'shoulder', 'chest', 'elbow', 'arm', 'forearm', 'hand', 'finger', 'thigh', 'knee', 'calf', 'heel', 'foot', 'toe']	➖	➖
tattoo-color	text	Colors of the tattoo ['black', 'white', 'red', 'green', 'blue', 'cyan', 'orange', 'violet', 'pink', 'yellow', 'brown', 'grey']	➖	✔
tattoo-description	text	Description of the tattoo,its composition.	✔	➖
tattoo-picture	attachment	Picture of the tattoo	➖	✔
tattoo-size	text	Size of the tattoo ['tiny', 'small', 'medium', 'large']	➖	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
tattoo-style	text	Style of the tattoo ['traditional', 'realism', 'watercolor', 'tribal', 'new school', 'japanese', 'blackwork', 'lettering', 'dotwork', 'abstract', 'celtic', 'geometric', 'mandala', 'minimalist', 'neo-traditional', 'portrait', 'sketch']	—	✔

telegram-account

Information related to a telegram account.

telegram-account 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	Multiple
first_name	text	First name	—	—
id	text	Telegram user identifier	—	—
last_name	text	Last name	—	—
phone	text	Phone associated with the telegram user	—	✔
username	text	Telegram username	—	—
verified	text	Verified	—	—

telegram-bot

Information related to a telegram bot.

telegram-bot 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	Multiple
chat-id	text	Telegram chat id	—	—
comment	text	Phone associated with the telegram user	✔	—
name	text	Telegram bot name	—	—
token	text	Telegram Token	—	—
username	text	Telegram bot username, must end with "bot"	—	—

temporal-event

A temporal event consists of some temporal and spacial boundaries. Spacial boundaries can be physical, virtual or hybrid.

temporal-event 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	Multiple
description	text	Free text description of the temporal event.	—	✔
link	link	Link or reference to the temporal event mentioned.	—	✔
summary	text	One line summary of the temporal event.	—	—
type	text	Type of temporal event. ['Physical Event', 'Virtual Event', 'Hybrid Event', 'Unknown']	✔	—

thaicert-group-cards

Adversary group cards inspired by ThaiCERT.

thaicert-group-cards 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	Multiple
country	text	Country of group - group location where it operates from.	—	✔
description	text	Description of group activities or TTP used for group actions.	—	—
more informations	text	List more informations by url - reports, group links etc..	—	✔
motivation	text	Motivation behind group ie. espionage, ransomware, other criminal activity, hacktivism . . .	—	✔
name	text	Names or nicknames for group.	—	✔
observed	text	What sector is this group active at? Government, telecommunicatio n etc and country of activity.	—	✔
sponsor	text	Sponsor of group ie. country, state, criminal ring, cartel etc..	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
tools used	text	What known tools are used by group.	➖	✔

threatgrid-report

ThreatGrid report.

threatgrid-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	Multiple
analysis_submitted_at	text	Submission date	➖	➖
heuristic_raw_score	text	heuristic_raw_score	✔	➖
heuristic_score	text	heuristic_score	➖	➖
id	text	ThreatGrid ID	➖	➖
iocs	text	iocs	➖	✔
original_filename	text	Original filename	➖	➖
permalink	text	permalink	➖	➖
threat_score	text	threat_score	✔	➖

timecode

Timecode object to describe a start of video sequence (e.g. CCTV evidence) and the end of the video sequence.

timecode 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	Multiple
description	text	Description of the video sequence	➖	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
end-marker-timecode	text	End marker timecode in the format hh:mm:ss;ff	—	✔
end-timecode	text	End marker timecode in the format hh:mm:ss.mms	—	✔
recording-date	datetime	Date of recording of the video sequence	—	✔
start-marker-timecode	text	Start marker timecode in the format hh:mm:ss;ff	—	✔
start-timecode	text	Start marker timecode in the format hh:mm:ss.mms	—	✔

timesketch-timeline

A timesketch timeline object based on mandatory field in timesketch to describe a log entry.

> timesketch-timeline 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	Multiple
datetime	datetime	When the log entry was seen	—	—
message	text	Informative message of the event	—	—
timestamp	text	When the log entry was seen in microseconds since Unix epoch	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
timestamp_desc	text	Text explaining what type of timestamp is it	—	—

timesketch_message

A timesketch message entry.

timesketch_message 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	Multiple
datetime	datetime	datetime of the message	✔	—
message	text	message	✔	—

timestamp

A generic timestamp object to represent time including first time and last time seen. Relationship will then define the kind of time relationship.

timestamp 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	Multiple
first-seen	datetime	First time that the linked object or attribute has been seen.	✔	—
last-seen	datetime	First time that the linked object or attribute has been seen.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
precision	text	Timestamp precision represents the precision given to first_seen and/or last_seen in this object. ['year', 'month', 'day', 'hour', 'minute', 'full']	✔	—
text	text	Description of the time object.	✔	—

tor-hiddenservice

Tor hidden service (onion service) object.

tor-hiddenservice 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	Multiple
address	onion-address	Onion address of the Tor node seen.	—	—
description	text	Tor onion service comment.	✔	—
first-seen	datetime	When the Tor hidden service was been seen for the first time.	✔	—
language	text	Language(s) detected on the onion address.	✔	✔
last-seen	datetime	When the Tor hidden service was seen for the last time.	✔	—
title	text	Known title(s) of the Tor onion address.	✔	✔

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	Multiple
address	ip-src	IP address of the Tor node seen.	—	—
description	text	Tor node description.	✔	—
document	text	Raw document from the consensus.	✔	—
fingerprint	text	router's fingerprint.	—	—
first-seen	datetime	When the Tor node designed by the IP address has been seen for the first time.	✔	—
flags	text	list of flag associated with the node.	—	—
last-seen	datetime	When the Tor node designed by the IP address has been seen for the last time.	✔	—
nickname	text	router's nickname.	—	—
published	datetime	router's publication time. This can be different from first-seen and last-seen.	✔	—
text	text	Tor node comment.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
version	text	parsed version of tor, this is None if the relay's using a new versioning scheme.	—	—
version_line	text	versioning information reported by the node.	—	—

traceability-impact

Traceability Impact object as described in STIX 2.1 Incident object extension.

traceability-impact 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	Multiple
criticality	text	Criticality of the impact ['Not Specified', 'False Positive', 'Low', 'Moderate', 'High', 'Extreme']	✔	—
description	text	Additional details about the impact.	—	—
end_time	datetime	The date and time the impact was last recorded.	—	—
end_time_fidelity	text	Level of fidelity that the `end_time` is recorded in. ['day', 'hour', 'minute', 'month', 'second', 'year']	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
recoverability	text	Recoverability of this particular impact with respect to feasibility and required time and resources. ['extended', 'not-applicable', 'not-recoverable', 'regular', 'supplemented']	✔	—
start_time	datetime	The date and time the impact was first recorded.	—	—
start_time_fidelity	text	Level of fidelity that the `start_time` is recorded in. ['day', 'hour', 'minute', 'month', 'second', 'year']	✔	—
traceability_impact	text	Impact on a system or organization's ability to perform audits or provvide non-repudiation. ['accountability-lost', 'partial-accountability', 'provable-accountability']	✔	—

tracking-id

Analytics and tracking ID such as used in Google Analytics or other analytic platform.

tracking-id 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	Multiple
description	text	Description of the tracking id.	✔	—
first-seen	datetime	First time the tracking code was seen.	✔	—
hostname	hostname	Hostname where the tracking id was found (assumed safe).	—	✔
id	text	Tracking code.	—	—
last-seen	datetime	Last time the tracking code was seen.	✔	—
tracker	text	Name of the tracker - organisation doing the tracking and/or analytics. ['Google Analytics', 'Piwik', 'Kissmetrics', 'Woopra', 'Chartbeat']	—	—
url	url	URL where the tracking id was found (potentially malicious).	—	✔

transaction

An object to describe a financial transaction.

transaction 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	Multiple
amount	text	The value of the transaction in local currency.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
authorized	text	Person who autorized the transaction.	➖	➖
date	datetime	Date and time of the transaction.	➖	➖
date-posting	datetime	Date of posting, if different from date of transaction.	➖	➖
from-country	text	Origin country of a transaction.	➖	➖
from-funds-code	text	Type of funds used to initiate a transaction. ['A Deposit', 'C Currency exchange', 'D Casino chips', 'E Bank draft', 'F Money order', 'G Traveler’s cheques', 'H Life insurance policy', 'I Real estate', 'J Securities', 'K Cash', 'O Other', 'P Cheque']	✔	➖
location	text	Location where the transaction took place.	➖	➖
teller	text	Person who conducted the transaction.	➖	➖
text	text	A description of the transaction.	✔	➖
to-country	text	Target country of a transaction.	➖	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
to-funds-code	text	Type of funds used to finalize a transaction. ['A Deposit', 'C Currency exchange', 'D Casino chips', 'E Bank draft', 'F Money order', 'G Traveler's cheques', 'H Life insurance policy', 'I Real estate', 'J Securities', 'K Cash', 'O Other', 'P Cheque']	✔	—
transaction-number	text	A unique number identifying a transaction.	—	—
transmode-code	text	How the transaction was conducted.	—	—
transmode-comment	text	Comment describing transmode-code, if needed.	—	—

translation

Used to keep a text and its translation.

translation 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	Multiple
original-language	text	Language of the original text ['Mandarin (language family)', 'Spanish', 'English', 'Hindi', 'Bengali', 'Portuguese', 'Russian', 'Japanese', 'Western Punjabi', 'Marathi', 'Telugu', 'Wu (language family)', 'Turkish', 'Korean', 'French', 'German', 'Vietnamese', 'Tamil', 'Yue (language family)', 'Urdu', 'Javanese', 'Italian', 'Egyptian Arabic', 'Gujarati', 'Iranian Persian', 'Bhojpuri', 'Min Nan (language family)', 'Hakka', 'Jinyu', 'Hausa', 'Kannada', 'Indonesian (Indonesian Malay)', 'Polish', 'Yoruba', 'Xiang Chinese (language family)', 'Malayalam', 'Odia', 'Maithili', 'Burmese', 'Eastern Punjabi', 'Sunda', 'Sudanese Arabic', 'Algerian Arabic', 'Moroccan Arabic', 'Ukrainian', 'Igbo', 'Northern Uzbek', 'Sindhi', 'North Levantine Arabic', 'Romanian', 'Tagalog', 'Dutch',	–	–

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
original-text	text	Original text	—	—
translated-text	text	Text after translation	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
translation-language	text	Language of translation ['Mandarin (language family)', 'Spanish', 'English', 'Hindi', 'Bengali', 'Portuguese', 'Russian', 'Japanese', 'Western Punjabi', 'Marathi', 'Telugu', 'Wu (language family)', 'Turkish', 'Korean', 'French', 'German', 'Vietnamese', 'Tamil', 'Yue (language family)', 'Urdu', 'Javanese', 'Italian', 'Egyptian Arabic', 'Gujarati', 'Iranian Persian', 'Bhojpuri', 'Min Nan (language family)', 'Hakka', 'Jinyu', 'Hausa', 'Kannada', 'Indonesian (Indonesian Malay)', 'Polish', 'Yoruba', 'Xiang Chinese (language family)', 'Malayalam', 'Odia', 'Maithili', 'Burmese', 'Eastern Punjabi', 'Sunda', 'Sudanese Arabic', 'Algerian Arabic', 'Moroccan Arabic', 'Ukrainian', 'Igbo', 'Northern Uzbek', 'Sindhi', 'North Levantine Arabic', 'Romanian', 'Tagalog', 'Dutch',	–	–

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
translation-service	text	translation service used for the translation ['Google Translate', 'Microsoft Translator', 'Babelfish', 'Reverso', 'Dict.cc', 'Linguee', 'unknown']	—	—
translation-type	text	type of translation ['Automated translation', 'Manual translation']	—	—

transport-ticket

A transport ticket.

transport-ticket 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	Multiple
class	text	Class of the ticket ['First', 'Second', 'Business', 'Flex', 'Economy']	✔	—
company	text	Street name	✔	—
copy	attachment	Copy of the ticket such as a photography or a FAX	—	✔
date-of-arrival	datetime	Date of arrival	✔	—
date-of-departure	datetime	Date of departure	✔	—
date-of-purchase	datetime	Date of purchase	✔	—
description	text	Description	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
destination	text	Destination	✔	—
origin	text	Origin	✔	—
ticket-number	text	Ticket Number	✔	✔
type-of-ticket	text	Type of ticket ['Purchase ticket', 'Boarding pass', 'Other']	✔	—
type-of-transport	text	Type of transport ['Plane', 'Train', 'Bus', 'Metro', 'Taxi', 'Ferry', 'Other']	✔	—

trustar_report

TruStar Report.

trustar_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	Multiple
BITCOIN_ADDRESS	btc	A bitcoin address is an identifier of 26-35 alphanumeric characters, beginning with the number 1 or 3, that represents a possible destination for a bitcoin payment.	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
CIDR_BLOCK	ip-src	CIDR (Classless Inter-Domain Routing) identifies a range of IP addresses, and was introduced as a way to allow more flexible allocation of Internet Protocol (IP) addresses than was possible with the original system of IP address classes.	➖	✔
COMMENTS	text	A space for additional comments.	➖	✔
CVE	vulnerability	The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures.	➖	✔
EMAIL_ADDRESS	email-src	An email address is a unique identifier for an email account.	➖	✔
INDICATOR_SUMMARY	text	Free text summary data related to an indicator. This should include a normalized score if one exists.	➖	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
IP	ip-dst	An Internet Protocol address (IP address) is a numerical label assigned to each device participating in a computer network that uses the Internet Protocol for communication.	➖	✔
MALWARE	malware-type	Names of software that are intended to damage or disable computers and computer systems.	➖	✔
MD5	md5	The MD5 algorithm is a widely used hash function producing a 128-bit hash value.	➖	✔
REGISTRY_KEY	regkey	The registry is a hierarchical database that contains data that is critical for the operation of Windows and the applications and services that run on Windows.	➖	✔
REPORT_LINK	link	A link to the TruSTAR report. Access may be restricted depending on user permissions.	➖	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
SHA1	sha1	SHA-1 (Secure Hash Algorithm 1) is a cryptographic hash function which takes an input and produces a 160-bit (20-byte) hash value known as a message digest - typically rendered as a hexadecimal number, 40 digits long. SHA-1 is prone to length extension attacks.	➖	✔
SHA256	sha256	SHA-256 is a member of the SHA-2 cryptographic hash functions designed by the NSA, which are the successors to SHA-1. It is represented as a 64-character hexadecimal string.	➖	✔
SOFTWARE	filename	The name of a file on a filesystem.	➖	✔
THREAT_ACTOR	threat-actor	A string identifying the threat actor.	➖	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
URL	url	A Uniform Resource Locator (URL) is a reference to a web resource that specifies its location on a computer network and a mechanism for retrieving it.	✗	✓

tsk-chats

An Object Template to gather information from evidential or interesting exchange of messages identified during a digital forensic investigation.

tsk-chats 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	Multiple
Source	text	Source of the message.(Contact details)	✓	✗
additional-comments	text	Comments.	✓	✗
app-used	text	Application used to send the message.	✓	✗
attachments	link	External references	✗	✓
datetime-received	datetime	date and time when the message was received.	✓	✓
datetime-sent	datetime	date and the time when the message was sent.	✓	✗
destination	text	Destination of the message.(Contact details)	✓	✗

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
message	text	Message exchanged.	—	—
message-type	text	the type of message extracted from the forensic-evidence. ['SMS', 'MMS', 'Instant Message (IM)', 'Voice Message']	✔	—
subject	text	Subject of the message if any.	—	—

tsk-web-bookmark

An Object Template to add evidential bookmarks identified during a digital forensic investigation.

tsk-web-bookmark 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	Multiple
URL	link	The URL saved as bookmark.	—	—
additional-comments	text	Comments.	✔	—
browser	text	Browser used to access the URL. ['IE', 'Safari', 'Chrome', 'Firefox', 'Opera mini', 'Chromium']	✔	—
datetime-bookmarked	datetime	date and time when the URL was added to favorites.	✔	—
domain-ip	ip-src	IP of the URL domain.	—	—
domain-name	text	Domain of the URL.	—	—
name	text	Book mark name.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
title	text	Title of the web page	—	—

tsk-web-cookie

An TSK-Autopsy Object Template to represent cookies identified during a forensic investigation.

tsk-web-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	Multiple
URL	link	The website URL that created the cookie.	—	—
additional-comments	text	Comments.	✔	—
browser	text	Browser on which the cookie was created. ['IE', 'Safari', 'Chrome', 'Firefox', 'Opera mini', 'Chromium']	—	—
datetime-created	datetime	date and time when the cookie was created.	✔	—
domain-ip	ip-src	IP of the domain that created the URL.	—	—
domain-name	text	Domain of the URL that created the cookie.	—	—
name	text	Name of the cookie	—	—
value	text	Value assigned to the cookie.	—	—

tsk-web-downloads

An Object Template to add web-downloads.

tsk-web-downloads 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	Multiple
additional-comments	text	Comments.	✔	—
attachment	attachment	The downloaded file itself.	✔	—
datetime-accessed	datetime	date and time when the file was downloaded.	✔	—
name	text	Name of the file downloaded.	—	—
path-downloadedTo	text	Location the file was downloaded to.	—	—
pathID	text	Id of the attribute file where the information is gathered from.	✔	—
url	url	The URL used to download the file.	—	—

tsk-web-history

An Object Template to share web history information.

tsk-web-history 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	Multiple
URL	link	The URL accessed.	—	—
additional-comments	text	Comments.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
browser	text	Browser used to access the URL. ['IE', 'Safari', 'Chrome', 'Firefox', 'Opera mini', 'Chromium']	✔	—
datetime-accessed	datetime	date and the time when the URL was accessed.	✔	—
domain-ip	ip-src	IP of the URL domain.	—	—
domain-name	text	Domain of the URL.	—	—
referrer	text	where the URL was referred from	✔	—
title	text	Title of the web page	—	—

tsk-web-search-query

An Object Template to share web search query information.

tsk-web-search-query 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	Multiple
additional-comments	text	Comments.	✔	—
browser	text	Browser used. ['IE', 'Safari', 'Chrome', 'Firefox', 'Opera mini', 'Chromium']	✔	—
datetime-searched	datetime	date and time when the search was conducted.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
domain	text	The domain of the search engine. ['Google', 'Yahoo', 'Bing', 'Alta Vista', 'MSN']	✔	—
text	text	the search word or sentence.	—	—
username	text	User name or ID associated with the search.	✔	—

twitter-account

Twitter account.

twitter-account 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	Multiple
archive	link	Archive of the account (Internet Archive, Archive.is, etc).	✔	✔
attachment	attachment	A screen capture or exported list of contacts etc.	—	✔
bio	text	Displayed biography of the user.	—	—
description	text	A description of the user.	✔	—
displayed-name	text	Displayed name.	—	—
embedded-link	url	Link embedded in the user description (potentially malicious).	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
embedded-safe-link	link	Link embedded in the user description (supposed safe).	➖	✔
followers	text	Number of followers.	✔	➖
following	text	Number of accounts this accounts is following.	✔	➖
hashtag	text	Hashtag embedded in the user description.	➖	✔
id	text	Numeric account id.	➖	➖
joined-date	datetime	When the account was created	✔	➖
likes	text	Number of likes this account has.	✔	➖
link	link	Original link to the user (supposed harmless).	➖	➖
listed	text	Number of lists the user is on.	✔	➖
location	text	User description of location.	✔	➖
media	text	Number of images and videos posted.	✔	➖
name	text	User's screen name (without the @).	➖	➖
private	text	User verified. ['True', 'False']	✔	➖
profile-banner	attachment	A screenshot or exported user avatar.	➖	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
profile-banner-url	url	A link to the user's background image.	—	—
profile-image	attachment	A screenshot or exported user avatar.	—	—
profile-image-url	url	A link to the user's avatar.	—	—
tweets	text	Number of tweets posted.	✔	—
twitter-followers	text	followers accounts of interest	—	✔
twitter-following	text	following accounts of interest	—	✔
url	url	Original URL location of the user (potentially malicious).	—	✔
verified	text	User verified. ['True', 'False']	✔	—

twitter-list

Twitter list.

twitter-list 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	Multiple
archive	link	Archive of the account (Internet Archive, Archive.is, etc).	✔	✔
attachment	attachment	A screen capture or exported list of contacts etc.	—	✔
description	text	A description of the list.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
embedded-link	url	Link embedded in the description (potentially malicious).	➖	✔
embedded-safe-link	link	Link embedded in the description (supposed safe).	➖	✔
hashtag	text	Hashtag embedded in the description.	➖	✔
id	text	Numeric list id.	➖	➖
link	link	Original link to the list (supposed harmless).	➖	➖
member-count	text	Number of accounts following this list.	✔	➖
name	text	List's screen name (without the @).	➖	➖
subscriber-count	text	Number of accounts subscribing to this list.	✔	➖
url	url	Original URL location of the list (potentially malicious).	➖	➖
user-id	text	Id of the account that manages this list.	➖	➖
user-name	text	Name of the account that manages this list (without the @).	➖	➖

twitter-post

Twitter post (tweet).

twitter-post 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	Multiple
archive	link	Archive of the original tweet (Internet Archive, Archive.is, etc).	—	✔
attachment	attachment	The tweet file or screen capture.	—	✔
created-at	datetime	Datetime of Tweet publication	—	—
embedded-link	url	Link in the tweet	—	✔
embedded-safe-link	link	Safe link in the tweet	—	✔
favorite-count	text	Number of favorites.	✔	—
geo	text	Geolocation data.	✔	—
hashtag	text	Hashtag embedded in the tweet	—	✔
in-reply-to-display-name	text	The user display name of the tweet this post shares.	—	✔
in-reply-to-status-id	text	The twitter ID of the tweet that this post shares.	—	✔
in-reply-to-user-id	text	The user ID of the tweet this post shares.	—	✔
language	text	The language of the post.	✔	✔
link	link	Original link to the post (supposed harmless).	—	✔
media	attachment	Media (Photos, videos) present in tweet	—	✔
name	text	Name of the account that posted this tweet.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
possibly-sensitive	text	Does this post contain sensitive content?	✔	—
possibly-sensitive-appealable	text	Is the sensitive content of this post appealable?	✔	—
post	text	Raw text of the post.	—	—
post-id	text	Numeric id of the tweet.	—	—
removal-date	datetime	When the tweet was removed.	✔	—
retweet-count	text	Number of retweets.	✔	—
source	text	Source of tweet (android, web etc).	✔	—
url	url	Original URL of the tweet, e.g. link shortener (potentially malicious).	—	✔
user-id	text	Id of the account that posted this tweet.	—	—
username-quoted	text	Username who is quoted in the tweet.	—	✔

typosquatting-finder

Typosquatting info.

typosquatting-finder 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	Multiple
research-domain	domain	Research domain name	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
variations-found-number	text	Number of variations for the research domain that some info is found.	✔	—
variations-number	text	Number of variations for the research domain.	✔	—

typosquatting-finder-result

Typosquatting result.

typosquatting-finder-result 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	Multiple
a-record	ip-dst	IPv4 address associated with A record	—	✔
aaaa-record	ip-dst	IPv6 address associated with AAAA record	—	✔
mx-record	domain	Domain associated with MX record	—	✔
ns-record	domain	Domain associated with NS record	—	✔
queried-domain	domain	Domain name	—	—
ratio-similarity	text	Similarity probability	✔	—
website-ressource-diff	text	Difference of website's ressources between both, research and current variations domain	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
website-similarity	text	Similarity between website of both research and current variations domain	✔	—
website-title	text	Website's title of the current queried domain	—	—

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	Multiple
credential	text	Credential (username, password)	—	—
dom-hash	dom-hash	Dom-hash of the URL	—	—
domain	domain	Full domain	—	—
domain_without_tld	text	Domain without Top-Level Domain	—	—
first-seen	datetime	First time this URL has been seen	✔	—
fragment	text	Fragment identifier is a short string of characters that refers to a resource that is subordinate to another, primary resource.	—	✔
host	hostname	Full hostname	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
ip	ip-dst	Better type when the host is an IP.	—	✔
last-seen	datetime	Last time this URL has been seen	✔	—
port	port	Port number	✔	—
query_string	text	Query (after path, preceded by '?')	—	✔
resource_path	text	Path (between hostname:port and query)	—	✔
scheme	text	Scheme ['http', 'https', 'ftp', 'gopher', 'sip']	✔	—
subdomain	text	Subdomain	✔	—
text	text	Description of the URL	—	—
tld	text	Top-Level Domain	✔	—
url	url	Full URL	—	—

user-account

User-account object, defining aspects of user identification, authentication, privileges and other relevant data points.

user-account 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	Multiple
account-type	text	Type of the account. ['facebook', 'ldap', 'nis', 'openid', 'radius', 'skype', 'tacacs', 'twitter', 'unix', 'windows-local', 'windows-domain']	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
can_escalate_privs	boolean	Specifies if the account has the ability to escalate privileges. ['True', 'False']	✔	—
created	datetime	Creation time of the account.	✔	—
description	text	A description of the user account.	✔	—
disabled	boolean	Specifies if the account is desabled. ['True', 'False']	✔	—
display-name	text	Display name of the account.	—	—
email	email	Email addresses for the account.	—	✔
expires	datetime	Expiration time of the account	✔	—
first_login	datetime	First time someone logged in to the account.	✔	—
group	text	UNIX group(s) the account is member of.	✔	✔
group-id	text	Identifier of the primary group of the account, in case of a UNIX account.	✔	—
home_dir	text	Home directory of the UNIX account.	✔	—
is_service_account	boolean	Specifies if the account is associated with a network service. ['True', 'False']	✔	—
last_login	datetime	Last time someone logged in to the account.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
link	link	Original link into the account page (Supposed harmless)	—	—
password	text	Password related to the username.	—	—
password_last_changed	datetime	Last time the password has been changed.	✔	—
privileged	boolean	Specifies if the account has privileges such as root rights. ['True', 'False']	✔	—
shell	text	UNIX command shell of the account.	✔	—
user-avatar	attachment	A user profile picture or avatar.	—	✔
user-id	text	Identifier of the account.	—	—
username	text	Username related to the password.	—	—

user-action

Represent an user action.

user-action 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	Multiple
action	text	Action performed by the user ['Click', 'Install', 'Execute', 'Plug', 'Scan', 'Unknown']	✔	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
description	text	Description of the action performed by the user	✔	—

vehicle

Vehicle object template to describe a vehicle information and registration.

vehicle 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	Multiple
date-first-registration	text	Date of first registration	—	✔
description	text	Description of the vehicle	✔	—
dyno-power	text	Dyno power output	—	✔
exterior-color	text	Exterior color of the vehicle	✔	—
gearbox	text	Gearbox	—	✔
image	attachment	Image of the vehicle.	—	✔
image-url	text	Image URL	—	✔
indicative-value	text	Indicative value	—	✔
interior-color	text	Interior color of the vehicle	✔	—
license-plate-number	text	License plate number	—	✔
make	text	Manufacturer of the vehicle	✔	—
model	text	Model of the vehicle	✔	—
state	text	State of the vehicle (stolen or recovered)	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
type	text	Type of the vehicle ['car', 'bus', 'caravan', 'bicycle', 'boat', 'taxi', 'camper van', 'motorcycle', 'truck', 'scooter', 'tractor', 'trailer', 'van']	✔	—
vin	text	Vehicle identification number (VIN)	—	—

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	Multiple
classification	text	The type of entity being targeted. ['individual', 'group', 'organization', 'class', 'unknown']	✔	—
description	text	Description of the victim	—	—
domain	domain	Domain name of the organisation targeted.	—	✔
email	target-email	The email address(es) of the user targeted.	—	✔
external	target-external	External target organisations affected by this attack.	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
ip-address	ip-dst	IP address(es) of the node targeted.	–	✔
name	target-org	The name of the department(s) or organisation(s) targeted.	–	✔
node	target-machine	Name(s) of node that was targeted.	–	✔
reference	text	External reference to the victim/case.	–	✔
regions	target-location	The list of regions or locations from the victim targeted. ISO 3166 should be used.	–	✔
roles	text	The list of roles targeted within the victim.	–	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
sectors	text	The list of sectors that the victim belong to ['academia - university', 'aerospace', 'agriculture', 'automotive', 'communications', 'construction', 'defence', 'dissident', 'education', 'energy', 'engineering', 'entertainment', 'faith-based organization', 'financial services', 'government local', 'government national', 'government public services', 'government regional', 'healthcare', 'hospitality leisure', 'information and cultural industries', 'infrastructure', 'insurance', 'international organization', 'justice', 'law enforcement', 'legal', 'manufacturing', 'mining', 'non profit', 'pharmaceuticals', 'political party', 'retail',	✖	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
user	target-user	The username(s) of the user targeted.	➖	✔

virustotal-graph

VirusTotal graph.

virustotal-graph 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	Multiple
access	text	Access to the VirusTotal graph ['Private', 'Public']	✔	➖
comment	text	Comment related to this VirusTotal graph	✔	✔
permalink	link	Permalink Reference to the VirusTotal graph	➖	➖
screenshot	attachment	Screenshot of the VirusTotal graph	✔	➖

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	Multiple
comment	text	Comment related to this hash	✔	✔
community-score	text	Community Score	✔	➖
detection-ratio	text	Detection Ratio	✔	➖

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

virustotal-submission

VirusTotal Submission.

virustotal-submission 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	Multiple
city	text	The city a file was uploaded from.	✔	—
country	text	The country a file was uploaded from.	✔	—
date	datetime	The upload date.	✔	—
filename	filename	The filename used to submit a file.	—	—
interface	text	The interface used to upload a file. ['web', 'api', 'email']	✔	—
submitter-id	text	Submitter ID, given as source_key via the VT API.	—	—

vulnerability

Vulnerability object describing a common vulnerability enumeration which can describe published, unpublished, under review or embargo vulnerability for software, equipments or hardware.

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	Multiple
created	datetime	First time when the vulnerability was discovered	✔	—
credit	text	Who reported/found the vulnerability such as an organisation, person or nickname.	✔	✔
cvss-score	float	Score of the Common Vulnerability Scoring System.	✔	—
cvss-string	text	String of the Common Vulnerability Scoring System.	✔	—
description	text	Description of the vulnerability	—	—
id	vulnerability	Vulnerability ID (generally CVE, but not necessarely). The id is not required as the object itself has an UUID and the CVE id can be update or assigned later.	—	✔
modified	datetime	Last modification date	✔	—
published	datetime	Initial publication date	✔	—
references	link	External references	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
state	text	State of the vulnerability. A vulnerability can have multiple states depending of the current actions performed. ['Published', 'Embargo', 'Reviewed', 'Vulnerability ID Assigned', 'Reported', 'Fixed', 'Encoded']	✔	✔
summary	text	Summary of the vulnerability	—	—
vulnerable-configuration	cpe	The vulnerable configuration is described in CPE format	—	✔

weakness

Weakness object describing a common weakness enumeration which can describe usable, incomplete, draft or deprecated weakness for software, equipment of hardware.

weakness 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	Multiple
description	text	Description of the weakness.	—	—
id	weakness	Weakness ID (generally CWE).	—	—
name	text	Name of the weakness.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
status	text	Status of the weakness. ['Incomplete', 'Deprecated', 'Draft', 'Usable']	✔	—
weakness-abs	text	Abstraction of the weakness. ['Class', 'Base', 'Variant']	✔	—

whois

Whois records information for a domain name or an IP address.

> 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	Multiple
comment	text	Comment of the whois entry	—	—
creation-date	datetime	Initial creation of the whois entry	✔	—
domain	domain	Domain of the whois entry	—	✔
expiration-date	datetime	Expiration of the whois entry	✔	—
ip-address	ip-src	IP address of the whois entry	—	✔
modification-date	datetime	Last update of the whois entry	✔	—
nameserver	hostname	Nameserver	✔	✔
registrant-email	whois-registrant-email	Registrant email address	—	—
registrant-name	whois-registrant-name	Registrant name	—	—
registrant-org	whois-registrant-org	Registrant organisation	—	—
registrant-phone	whois-registrant-phone	Registrant phone number	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
registrar	whois-registrar	Registrar of the whois entry	—	—
text	text	Full whois entry	✔	—

windows-service

Windows service and detailed about a service running a Windows operating system.

windows-service 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	Multiple
comment	text	Additional comments.	✔	—
display	windows-service-displayname	Display name/information of the service.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
group	text	Group to which the system/driver belong to. ['Base', 'Boot Bus Extender', 'Boot File System', 'Cryptography', 'Extended base', 'Event Log', 'Filter', 'FSFilter Bottom', 'FSFilter Infrastructure', 'File System', 'FSFilter Virtualization', 'Keyboard Port', 'Network', 'NDIS', 'Parallel arbitrator', 'Pointer Port', 'PnP Filter', 'ProfSvc_Group', 'PNP_TDI', 'SCSI Miniport', 'SCSI CDROM Class', 'System Bus Extender', 'Video Save', 'other']	✔	—
image-path	text	Path of the service/drive	—	—
name	windows-service-name	name of the service	—	—
start	text	When the service/driver starts or executes. ['Boot start', 'System start', 'Auto start', 'Manual', 'Disabled']	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
type	text	Service/driver type. ['Kernel driver', 'File system driver', 'Own process', 'Share process', 'Interactive', 'Other']	✔	—

x-header

X header generic object for SMTP, HTTP or any other protocols using X headers.

> x-header 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	Multiple
x-header-name	text	X header name is the value of the header key. The name is case sensitive.	✔	—
x-value	text	X value is the value of the specified header 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	Multiple
dns_names	hostname	Subject Alternative Name - DNS names	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
email	email-dst	Subject Alternative Name - emails	➖	✔
ip	ip-dst	Subject Alternative Name - IP	➖	✔
is_ca	boolean	CA certificate ['True', 'False']	✔	➖
issuer	text	Issuer of the certificate	✔	➖
pem	text	Raw certificate in PEM formati (Unix-like newlines)	➖	➖
pubkey-info-algorithm	text	Algorithm of the public key	✔	➖
pubkey-info-exponent	text	Exponent of the public key - in decimal	➖	➖
pubkey-info-modulus	text	Modulus of the public key - in Hexadecimal - no 0x, no :	➖	➖
pubkey-info-size	text	Length of the public key (in bits expressed in decimal: eg. 256 bits)	✔	➖
raw-base64	text	Raw certificate base64 encoded (DER format)	➖	➖
rid	text	Subject Alternative Name - RID	➖	✔
self_signed	boolean	Self-signed certificate ['True', 'False']	✔	➖
serial-number	text	Serial number of the certificate	➖	➖

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
signature_algorithm	text	Signature algorithm ['SHA1_WITH_RSA_ENCRYPTION', 'SHA256_WITH_RSA_ENCRYPTION']	✔	—
subject	text	Subject of the certificate	—	—
text	text	Free text description of the certificate	—	—
uri	uri	Subject Alternative Name - URI	—	✔
validity-not-after	datetime	Certificate invalid after that date	✔	—
validity-not-before	datetime	Certificate invalid before that date	✔	—
version	text	Version of the certificate	✔	—
x509-fingerprint-md5	x509-fingerprint-md5	[Insecure] MD5 hash (128 bits)	—	—
x509-fingerprint-sha1	x509-fingerprint-sha1	[Insecure] Secure Hash Algorithm 1 (160 bits)	—	—
x509-fingerprint-sha256	x509-fingerprint-sha256	Secure Hash Algorithm 2 (256 bits)	—	—

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

yara

An object describing a YARA rule (or a YARA rule name) along with its version.

yara 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	Multiple
comment	comment	A description of the YARA rule.	—	—
context	text	Context where the YARA rule can be applied ['all', 'disk', 'memory', 'network']	✔	—
reference	link	Reference or origin of the YARA rule.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
version	text	Version of the YARA rule depending where the yara rule is known to work as expected. ['3.7.1']	✔	—
yara	yara	YARA rule.	—	—
yara-rule-name	text	YARA rule name.	—	—

youtube-channel

A YouTube channel.

youtube-channel 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	Multiple
about	text	About page of the channel.	—	—
archive	link	Archive of the channel (Internet Archive, Archive.is, etc).	✔	✔
attachment	attachment	A screen capture or exported list of contacts etc.	—	✔
channel-avatar	attachment	A screen capture or exported channel avatar.	—	✔
channel-banner	attachment	A screen capture or exported channel header.	—	✔
channel-id	text	Channel id.	—	—
channel-name	text	Channel name.	—	—
description	text	A description of the channel.	✔	—
featured-channel	text	Featured channel names.	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
link	link	Original link to the channel page (supposed harmless).	—	—
url	url	Original URL location of the page (potentially malicious).	—	—

youtube-comment

A YouTube video comment.

youtube-comment 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	Multiple
archive	link	Archive of the original comment (Internet Archive, Archive.is, etc).	✔	✔
attachment	attachment	A screen capture or exported comment.	—	✔
channel-name	text	The name of the channel where it was posted.	—	✔
comment	text	The raw text of the YouTube video comment.	—	—
description	text	A description of the comment.	✔	—
embedded-link	url	Link embedded in the comment (potentially malicious).	—	✔
embedded-safe-link	link	Link embedded in the comment (supposed safe).	—	✔

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
hashtag	text	Hashtag used in the comment.	—	✔
link	link	Original link to the comment (supposed harmless).	—	—
url	url	Original URL location of the comment (potentially malicious).	—	—
user-account	text	The user account that commented on the YouTube video.	—	—
username-quoted	text	Username who are quoted in the comment.	—	✔
video-title	text	The title of the YouTube video.	—	—

youtube-playlist

A YouTube playlist.

> youtube-playlist 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	Multiple
archive	link	Archive of the playlist (Internet Archive, Archive.is, etc).	✔	✔
attachment	attachment	A screen capture or exported list of contacts etc.	—	✔
description	text	A description of the playlist.	✔	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
link	link	Original link to the playlist page (supposed harmless).	—	—
playlist-id	text	Playlist id.	—	—
playlist-name	text	Playlist name.	—	—
url	url	Original URL location of the page (potentially malicious).	—	—
video-link	link	Link to the video in playlist (supposed harmless).	—	—

youtube-video

A YouTube video.

youtube-video 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	Multiple
archive	link	Archive of the original YouTube video (Internet Archive, Archive.is, etc).	✔	✔
attachment	attachment	A screen capture or exported YouTube video.	—	✔
channel-name	text	The name of the channel where it was posted.	—	✔
creator	text	The user account that created the YouTube video.	—	—

Object attribute	MISP attribute type	Description	Disable correlation	Multiple
description	text	A description of the YouTube video.	✔	—
embedded-link	url	Link embedded in the YouTube video description (potentially malicious).	—	✔
embedded-safe-link	link	Link embedded in the YouTube video description (supposed safe).	—	✔
hashtag	text	Hashtag used to identify or promote the YouTube video.	—	✔
link	link	Original link to the YouTube video (supposed harmless).	—	—
url	url	Original URL location of the YouTube video (potentially malicious).	—	—
username-quoted	text	Username who are quoted in the YouTube video or description.	—	✔
video-title	text	The title of the YouTube video.	—	—
video-transcript	text	The YouTube video transcript (closed captions).	—	—

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', 'alfred']
executes	This relationship describes an object which executes another object.	['misp']
shares	This relationship describes an object which shares another object.	['misp']
shared-by	This relationship describes an object which was shared by another object.	['misp']
publishes	This relationship describes an object which publishes another object.	['misp']
published-by	This relationship describes an object which was published by another object.	['misp']
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.	['alfred', 'followthemoney', 'misp', 'stix-2.0']
connected-to	The referenced source is connected to the target object.	['misp', 'stix-1.1']
connected-from	The referenced source is connected from the target object.	['misp', 'stix-1.1']
contains	The referenced source is containing the target object.	['misp', 'stix-1.1', 'alfred']
contained-by	The referenced source is contained by the target object.	['misp', 'stix-1.1']
contained-within	The referenced source is contained within the target object.	['misp', 'stix-1.1']
characterized-by	The referenced source is characterized by the target object.	['misp', 'stix-1.1']
characterizes	The referenced source is characterizing the target object.	['misp', 'stix-1.1']

Name of relationship	Description	Format
properties-queried	The referenced source has queried the target object.	['misp', 'stix-1.1']
properties-queried-by	The referenced source is queried by the target object.	['misp', 'stix-1.1']
extracted-from	The referenced source is extracted from the target object.	['misp', 'stix-1.1']
supra-domain-of	The referenced source is a supra domain of the target object.	['misp', 'stix-1.1']
sub-domain-of	The referenced source is a sub domain of the target object.	['misp', 'stix-1.1']
dropped	The referenced source has dropped the target object.	['misp', 'stix-1.1']
dropped-by	The referenced source is dropped by the target object.	['misp', 'stix-1.1']
downloaded	The referenced source has downloaded the target object.	['misp', 'stix-1.1']
downloaded-from	The referenced source has been downloaded from the target object.	['misp', 'stix-1.1']
resolved-to	The referenced source is resolved to the target object.	['misp', 'stix-1.1']
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', 'alfred']
indicates	This relationship describes that the source object indicates the target object.	['misp', 'stix-2.0']
indicated-by	This relationship describes that the source object is indicated by the target object.	['misp', 'stix-2.1']
mentions	This relationship describes that the source object mentions the target object.	['misp']

Name of relationship	Description	Format
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', 'alfred']
impersonates	This relationship describes a source object which impersonates the target object	['misp', 'stix-2.0']
retrieved-from	This relationship describes an object retrieved from the target object.	['misp']
authored-by	This relationship describes the author of a specific object.	['misp']
is-author-of	This relationship describes an object being author by someone.	['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']
includes	This relationship describes an object that includes an other 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']
drops	This relationship describes an object which drops another object	['misp']
executed-by	This relationship describes an object executed by another object.	['misp']

Name of relationship	Description	Format
affects	This relationship describes an object that affects another object.	['misp', 'alfred']
affected-by	This relationship describes an object affected by another object.	['misp']
beacons-to	This relationship describes an object beaconing to another object.	['misp', 'alfred']
abuses	This relationship describes an object which abuses another object.	['misp']
exfiltrates-to	This relationship describes an object exfiltrating to another object.	['misp', 'alfred']
identifies	This relationship describes an object which identifies another object.	['misp', 'alfred']
intercepts	This relationship describes an object which intercepts another object.	['misp', 'alfred']
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']
followed-by	This relationship describes an object which is followed by another object. This can be used when a time reference is missing but a sequence is known.	['misp']
preceded-by	This relationship describes an object which is preceded by another object. This can be used when a time reference is missing but a sequence is known.	['misp']
triggers	This relationship describes an object which triggers another object.	['misp']

Name of relationship	Description	Format
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']
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', 'stix-2.1']
hosts	This relationship describes an object which hosts another object.	['stix-2.1']
hosted-by	This relatiobship describes an object hosted by another object.	['stix-2.1']
consists	This relationship describes an object which consists of one or more object(s).	['stix-2.1']
delivers	This relationship describes an object which delivers to one or more object(s).	['stix-2.1']
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']

Name of relationship	Description	Format
belongs-to	This relationship describes an object which belongs to another object.	['cert-eu', 'followthemoney']
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']
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']

Name of relationship	Description	Format
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', 'alfred']
publishes-method-for	This relationship describes an object which publishes method for another object.	['cert-eu']
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']

Name of relationship	Description	Format
released	This relationship describes an object which release another object.	['cert-eu']
exploits	This relationship describes an object (like a PoC/exploit) which exploits another object (such as a vulnerability object).	['misp']
signed-by	This relationship describes an object signed by another object.	['misp']
delivered-by	This relationship describes an object by another object (such as exploit kit, dropper).	['misp']
controls	This relationship describes an object which controls another object.	['misp']
annotates	This relationships describes an object which annotates another object.	['misp']
references	This relationships describes an object which references another object or attribute.	['misp']
child-of	A child semantic link to a parent.	['alfred']
parent-of	A parent semantic link to a child.	['alfred', 'misp']
compromised	Represents the semantic link of having compromised something.	['alfred']
connects	The initiator of a connection.	['alfred']
connects-to	The destination or target of a connection.	['alfred']
cover-term-for	Represents the semantic link of one thing being the cover term for another.	['alfred']
disclosed-to	Semantic link indicating where information is disclosed to.	['alfred']
downloads	Represents the semantic link of one thing downloading another.	['alfred']

Name of relationship	Description	Format
downloads-from	Represents the semantic link of malware being downloaded from a location.	['alfred']
generated	Represents the semantic link of an alert generated from a signature.	['alfred']
implements	One data object implements another.	['alfred']
initiates	Represents the semantic link of a communication initiating an event.	['alfred', 'misp']
initiated-by	The source object initiated the target object.	['misp']
instance-of	Represents the semantic link between a FILE and FILE_BINARY.	['alfred']
issuer-of	Represents the semantic link of being the issuer of something.	['alfred']
linked-to	Represents the semantic link of being associated with something.	['alfred', 'followthemoney']
not-relevant-to	Represents the semantic link of a comm that is not relevant to an EVENT.	['alfred']
part-of	Represents the semantic link that defines one thing to be part of another in a hierachial structure from the child to the parent.	['alfred']
processed-by	Represents the semantic link of something has been processed by another program.	['alfred']
produced	Represents the semantic link of something having produced something else.	['alfred']
queried-for	The IP Address or domain being queried for.	['alfred']
query-returned	The IP Address or domain returned as the result of a query.	['alfred']

Name of relationship	Description	Format
registered	Represents the semantic link of someone registered some thing.	['alfred']
registered-to	Represents the semantic link of something being registered to.	['alfred']
relates	Represents the semantic link between HBS Comms and communication addresses.	['alfred']
relevant-to	Represents the semantic link of a comm that is relevant to an EVENT.	['alfred']
resolves-to	Represents the semantic link of resolving to something.	['alfred']
responsible-for	Represents the semantic link of some entity being responsible for something.	['alfred']
seeded	Represents the semantic link of a seeded domain redirecting to another site.	['alfred']
sends	A sends semantic link meaning 'who sends what'.	['alfred']
sends-as-bcc-to	A sends to as BCC semantic link meaning 'what sends to who as BCC'.	['alfred']
sends-as-cc-to	A sends to as CC semantic link meaning 'what sends to who as CC'.	['alfred']
sends-to	A sends to semantic link meaning 'what sends to who'.	['alfred']
spoofer-of	The represents the semantic link of having spoofed something.	['alfred']
subdomain-of	Represents a domain being a subdomain of another.	['alfred']
supersedes	One data object supersedes another.	['alfred']
triggered-on	Represents the semantic link of an alert triggered on an event.	['alfred']
uploads	Represents the semantic link of one thing uploading another.	['alfred']

Name of relationship	Description	Format
user-of	The represents the semantic link of being the user of something.	['alfred']
works-for	Represents the semantic link of working for something.	['alfred']
works-with	Represents an object working with another one.	['misp']
witness-of	Represents an object being a witness of something.	['misp']
injects-into	Represents an object injecting something into something	['misp']
injected-into	Represents an object which is injected something into something	['misp']
creates	Represents an object that creates something.	['misp', 'haxpak']
screenshot-of	Represents an object being the screenshot of something.	['misp']
knows	Represents an object having the knowledge of another object.	['misp']
describes	Represents the semantic link of describing another object.	['misp']
extends	Represents the semantic link of extending another object.	['misp']
writes	Reprensents an object which writes towards another object or attribute	['misp']
ranked-with	Represents the semantic link of an asn object being ranked with a bgp-ranking object	['misp']
owns	owns	['followthemoney']
awarded-to	awarded-to	['followthemoney']
directs	directs	['followthemoney']
involved-in	involved-in	['followthemoney']
associated-with	associated-with	['followthemoney']
represents	represents	['followthemoney']
owes	owes	['followthemoney']
preceeds	preceeds	['followthemoney']

Name of relationship	Description	Format
documents	documents	['followthemoney']
paid	paid	['followthemoney']
leaks	leaks	['misp']
leaked-by	leaked-by	['misp']
doxed-by	doxed-by	['misp']
alerts	alerts about a specific object	['misp']
legal-address-of	The referenced source object is the legal address of the target.	['misp']
shipping-address-of	The referenced source object is a shipping address of the target.	['misp']
visited	The referenced source object visited the target (for example an address).	['misp']
office-of	The referenced source object is an office of the target.	['misp']
picture-of	The referenced source object is a picture (photo/image) of the target.	['misp']
pictured-by	The referenced source object is pictured by the target (photo/image).	['misp']
found-on	The referenced source object has been found on the target (device, server).	['misp']
found-in	The referenced source object has been found in the target (document).	['misp']
drives	The referenced source object drives the target described (often a vehicule).	['misp']
rewrite	The referenced source object is a rewrite specified in the target object. The rewrite can be for a computer program text but also any rewrite of a text.	['misp']
friend-of	The referenced source object is a friend of the target object.	['foaf']

Name of relationship	Description	Format
acquaintance-of	The referenced source object is an acquaintance of the target object.	['foaf']
sibling-of	The referenced source object is a sibling of the target object.	['foaf']
grandchild-of	The referenced source object is a grandchild of the target object.	['foaf']
spouse-of	The referenced source object is a spouse of the target object.	['foaf']
enemy-of	The referenced source object is an enemy of the target object.	['foaf']
antagonist-of	The referenced source object is an antagonist of the target object.	['foaf']
ambivalient-of	The referenced source object is an ambivalent of the target object.	['foaf']
is-a-translation-of	The referenced source object is a translation of the target object.	['misp']
has-met	The referenced source object has met with the target object.	['misp']
submitted	The referenced source object submitted the referenced target object (to an online anti virus scanner).	['misp']
submitted-by	The referenced source object was submitted (to an online anti virus scanner) by the referenced target object.	['misp']
does-not-target	This relationship describes that the source object does not target the target object.	['misp']
is-targeted-by	This relationship describes that the source object is targeted by the target object.	['misp']
is-not-targeted-by	This relationship describes that the source object is not targeted by the target object.	['misp']

Name of relationship	Description	Format
serves	This relationship describes that the source object provides services described in the target object.	['misp']
Friend	The source object considers the target object as a friend. Is not necessarily symmetric.	['XFN']
Acquaintance	The source object considers the target object as a acquaintance. Is not necessarily symmetric.	['XFN']
Contact	The source object have information to contact and/or get in touch with the target object.	['XFN']
Met	The source object have physically met the target object.	['XFN']
Co-worker	The source object shares an employer with the target object. This relationship is not geographically limited.	['XFN']
Colleague	The source object regards the target object as a peer, someone who they feel is on their level and has skills and interests similar to their own. A colleague does not have to be a co-worker, although of course can be.	['XFN']
Co-resident	The source object is co-resident with the target object, which means they share a street address with the target object. Co-resident is symmetric.	['XFN']
Neighbor	The source object is neighbor with the target object. This is not limited to next door neighbor.	['XFN']
Child	The target object is the child of the source object.	['XFN']
Parent	The target object is the parent of the source object.	['XFN']

Name of relationship	Description	Format
Sibling	The source object share a parent with the target object. Brothers, sisters, half-brothers, and half-sisters are all examples of siblings.	['XFN']
Spouse	The source object is -or feels themself to be- married, whether legally or not, to the target object.	['XFN']
Kin	The target object is a relative of the source object.	['XFN']
Muse	The source object is inspired in some way by the target object.	['XFN']
Crush	The source object is attracted -romantically speaking- to the target object.	['XFN']
Date	The source object is dating the target object.	['XFN']
Sweetheart	The source object is intimate, whether physically or emotionally, with the target object.	['XFN']
Me	The source object refers to the target object as themself or a representation of themself. Can be a profile on social-networking for example. This value is exclusive of all other XFN values.	['XFN']
redirects-to	The source object is redirected to the target object.	['misp']
rendered-as	The source object is rendered to the target object.	['misp']
known-as	The source object is known as the target object.	['misp']
led-to	The source object is led to the target object.	['stix-2.1']
impacts	The source object has an impact on the target.	['stix-2.1']
impacted-by	The source object is impacted by the target.	['misp']

Name of relationship	Description	Format
located-at	An object occured at a specific location.	['stix-2.1']
contact-for	The source object should be considered a point of contact for the target.	['stix-2.1']
detects	The source object was responsible for detecting the target object.	['stix-2.1']
detected-by	The source object is detected by the target object.	['misp']
observed	The target object was observed as part of a source event.	['stix-2.1']
observed-by	The source object was observed by the target object.	['misp']
based-on	The source object is based on the target.	['stix-2.1']
performed	The source object performed the target event.	['stix-2.1']
performed-by	The source object was performed by the target.	['misp']
blocks	The source object blocks the target object.	['stix-2.1']
blocked-by	The source object is blocked by the target object.	['misp']
causes	The source object causes the target event.	['stix-2.1']
caused-by	The source object is caused by the target object.	['misp']
errored-to	The source object is followed by the target because of an error.	['stix-2.1']
assigned	The source object has been assigned the target.	['stix-2.1']
participated-in	The source object participated in the target task.	['stix-2.1']
targeted-by	The source object is targeted by the target object.	['misp']
created-by	The source object was created by the target object.	['misp']

Name of relationship	Description	Format
sample-of	The source object is the sample of the target object.	['stix-2.1']
is-allied-with	This relationship describes an object which is allied with another object.	['misp']
acquires	The source object acquires the target object.	['misp']
is-acquired-by	The source object is acquired by the target object.	['misp']
supports	The source object supports the target object.	['misp']
supported-by	The source object is supported by the target object.	['misp']
sponsors	The source object sponsors the target object.	['misp']
sponsored-by	The source object is sponsored by the target object.	['misp']
operates-from	The source object operates from the target object.	['misp']
deploys	The source object deploys the target object.	['misp']
is-deployed-by	The source object is deployed by the target object.	['misp']
interacts-with	The source object interacts with the target object.	['misp']
injects	The source object injects the target object.	['misp']
is-injected-by	The source object is injected by the target object.	['misp']
interviews	The source object interviews the target object.	['misp']
is-interviewed-by	The source object is interviewed by the target object.	['misp']
summarizes	The source object summarizes the target object.	['misp']
summarized-by	The source object is summarized by the target object.	['misp']

Name of relationship	Description	Format
releasable-to	The source object is releasable to the target object.	['misp']
weakened-by	The source object is weakened by the target weakness.	['misp']
weakens	The source weakness weakens the target object.	['misp']