

# MISP Objects

# MISP Objects

|                     |    |
|---------------------|----|
| Introduction        | 1  |
| Funding and Support | 2  |
| MISP objects        | 3  |
| ail-leak            | 3  |
| android-permission  | 4  |
| annotation          | 6  |
| asn                 | 7  |
| av-signature        | 8  |
| bank-account        | 9  |
| cap-alert           | 11 |
| cap-info            | 14 |
| cap-resource        | 17 |
| coin-address        | 18 |
| cookie              | 19 |
| course-of-action    | 20 |
| cowrie              | 21 |
| credential          | 22 |
| credit-card         | 23 |
| ddos                | 24 |
| diameter-attack     | 25 |
| domain-ip           | 26 |
| elf                 | 27 |
| elf-section         | 29 |
| email               | 32 |
| fail2ban            | 33 |
| file                | 34 |
| geolocation         | 36 |
| gtp-attack          | 37 |
| http-request        | 38 |
| ip-port             | 39 |
| ja3                 | 40 |
| legal-entity        | 41 |
| macho               | 41 |
| macho-section       | 42 |
| microblog           | 43 |
| mutex               | 44 |
| netflow             | 44 |
| network-connection  | 46 |

|                     |    |
|---------------------|----|
| network-socket      | 47 |
| passive-dns         | 50 |
| paste               | 52 |
| pe                  | 53 |
| pe-section          | 55 |
| person              | 56 |
| phone               | 58 |
| process             | 60 |
| r2graphity          | 61 |
| regex               | 63 |
| registry-key        | 63 |
| report              | 65 |
| rtir                | 65 |
| sandbox-report      | 66 |
| sb-signature        | 67 |
| ss7-attack          | 68 |
| stix2-pattern       | 70 |
| suricata            | 71 |
| target-system       | 71 |
| timecode            | 72 |
| timesketch-timeline | 72 |
| timestamp           | 73 |
| tor-node            | 74 |
| transaction         | 75 |
| url                 | 76 |
| victim              | 78 |
| virustotal-report   | 80 |
| vulnerability       | 80 |
| whois               | 81 |
| x509                | 82 |
| yabin               | 84 |
| yara                | 84 |
| Relationships       | 85 |

# 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](#).



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

## 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 |
|------------------|---------------------|---|---------------------|
| type             | text                | Type of information leak as discovered and classified by an AIL module. ['Credential', 'CreditCards', 'Mail', 'Onion', 'Phone', 'Keys'] | —                   |
| text             | text                | A description of the leak which could include the potential victim(s) or description of the leak.                                       | ✓                   |
| 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.   | —                   |
| duplicate        | text                | Duplicate of the existing leaks.  | —                   |
| original-date    | datetime            | When the information available in the leak was created. It's usually before the first-seen.   | ✓                   |

| Object attribute | MISP attribute type | Description  | Disable correlation |
|------------------|---------------------|--|---------------------|
| sensor           | text                | The AIL sensor uuid where the leak was processed and analysed.           | —                   |
| first-seen       | datetime            | When the leak has been accessible or seen for the first time.            | ✓                   |
| raw-data         | attachment          | Raw data as received by the AIL sensor compressed and encoded in Base64. | ✓                   |
| duplicate_number | counter             | Number of known duplicates.  | —                   |

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

| Object attribute | MISP attribute type | Description   | Disable correlation |
|------------------|---------------------|---|---------------------|
| permission       | text                | Android permission<br>['ACCESS_CHECKIN_PROPERTIES',<br>'ACCESS_COARSE_LOCATION',<br>'ACCESS_FINE_LOCATION',<br>'ACCESS_LOCATION_EXTRA_COMMANDS',<br>'ACCESS_NETWORK_STATE',<br>'ACCESS_NOTIFICATION_POLICY',<br>'ACCESS_WIFI_STATE',<br>'ACCOUNT_MANAGER',<br>'ADD_VOICEMAIL',<br>'ANSWER_PHONE_CALLS', 'BATTERY_STATS',<br>'BIND_ACCESSIBILITY_SERVICE',<br>'BIND_APPWIDGET',<br>'BIND_AUTOFILL_SERVICE',<br>'BIND_CARRIER_MESSAGING_SERVICE',<br>'BIND_CHOOSER_TARGET_SERVICE',<br>'BIND_CONDITION_PROVIDER_SERVICE',<br>'BIND_DEVICE_ADMIN',<br>'BIND_DREAM_SERVICE',<br>'BIND_INCALL_SERVICE',<br>'BIND_INPUT_METHOD',<br>',<br>'BIND_MIDI_DEVICE_SERVICE',<br>'BIND_NFC_SERVICE',<br>'BIND_NOTIFICATION_LISTENER_SERVICE',<br>'BIND_PRINT_SERVICE',<br>'BIND_QUICK_SETTINGS_TILE',<br>'BIND_REMOTEVIEWS',<br>'BIND_SCREENING_SERVICE',<br>'BIND_TELECOM_CONN | -                   |



# 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](#).

'ACTION\_SERVICE',  
'BIND\_TEXT\_SERVICE',  
'BIND\_TV\_INPUT',  
'BIND\_VISUAL\_VOICEM  
ALL\_SERVICE',  
'BIND\_VOICE\_INTERAC  
TION',

| Object attribute  | MISP attribute type | Description   | Disable correlation |
|-------------------|---------------------|---|---------------------|
| type              | text                | Type of the annotation<br>['Annotation',<br>'Executive Summary',<br>'Introduction',<br>'Conclusion',<br>'Disclaimer',<br>'Keywords',<br>'Acknowledgement',<br>'Other', 'Copyright',<br>'Authors', 'Logo'] | ✓                   |
| text              | text                | Raw text of the annotation  | —                   |
| ref               | link                | Reference(s) to the annotation  | —                   |
| creation-date     | datetime            | Initial creation of the annotation  | —                   |
| format            | text                | Format of the annotation ['text',<br>'markdown',<br>'asciidoc',<br>'MultiMarkdown',<br>'GFM', 'pandoc',<br>'Fountain',<br>'CommonWork',<br>'kramdown-rfc2629',<br>'rfc7328', 'Extra']                     | ✓                   |
| modification-date | datetime            | Last update of the annotation   | —                   |

'DIAGNOSTIC',  
'DISABLE\_KEYGUARD',  
'DUMP',  
'EXPAND\_STATUS\_BAR',  
'FACTORY\_TEST',

# asn

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



asn is a MISP object available in JSON format at [this location](#) The JSON format can be freely reused in your application or automatically enabled in [MISP](#).

| Object attribute | MISP attribute type | Description   | Disable correlation |
|------------------|---------------------|---|---------------------|
| last-seen        | datetime            | Last time the ASN was seen  | ✓                   |
| import           | text                | The inbound IPv4 routing policy of the AS in RFC 2622 – Routing Policy Specification Language (RPSL) format   | –                   |
| export           | text                | The outbound routing policy of the AS in RFC 2622 – Routing Policy Specification Language (RPSL) format   | –                   |
| country          | text                | Country code of the main location of the autonomous system  | –                   |
| 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  | –                   |
| description      | text                | Description of the autonomous system  | –                   |

| Object attribute | MISP attribute type | Description   | Disable correlation |
|------------------|---------------------|---|---------------------|
| first-seen       | datetime            | First time the ASN was seen   | ✓                   |
| asn              | AS                  | Autonomous System Number  | —                   |
| 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 | —                   |

## 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 applications, or automatically enabled in MISP.

| Object attribute | MISP attribute type | Description                           | Disable correlation |
|------------------|---------------------|---------------------------------------|---------------------|
| text             | text                | Free text value to attach to the file | ✓                   |
| signature        | text                | Name of detection signature           | —                   |
| datetime         | datetime            | Datetime                              | ✓                   |
| software         | text                | Name of antivirus software            | ✓                   |

'MEDIA\_CONTENT\_CONTROL',  
'MODIFY\_AUDIO\_SETTINGS',  
'MODIFY\_PHONE\_STATE',  
'MOUNT\_UNMOUNT\_FILESYSTEMS',  
'MOUNT\_UNMOUNT\_FILESYSTEMS',

', 'READ\_INPUT\_STATE',  
'READ\_LOGS',  
'READ\_PHONE\_NUMBERS',  
'READ\_PHONE\_STATE',

# 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 |
|---------------------|---------------------|--|---------------------|
| opened              | datetime            | When the account was opened.   | ✓                   |
| comments            | text                | Comments about the bank account.   | ✓                   |
| account-name        | text                | A field to freely describe the bank account details.   | —                   |
| currency-code       | text                | Currency of the account. ['USD', 'EUR']  | ✓                   |
| status-code         | text                | Account status at the time of the transaction processed. ['A - Active', 'B - Inactive', 'C - Dormant'] | ✓                   |
| client-number       | text                | Client number as seen by the bank.   | —                   |
| closed              | datetime            | When the account was closed.   | ✓                   |
| aba-rtn             | aba-rtn             | ABA routing transit number   | —                   |
| beneficiary-comment | text                | Comment about the final beneficiary.   | ✓                   |
| iban                | iban                | IBAN of the bank account.  | —                   |
| institution-name    | text                | Name of the bank or financial organisation.  | ✓                   |

| Object attribute      | MISP attribute type | Description   | Disable correlation |
|-----------------------|---------------------|---|---------------------|
| account               | bank-account-nr     | Account number  | –                   |
| date-balance          | datetime            | When the balance was reported.  | ✓                   |
| 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'] | ✓                   |
| personal-account-type | text                | Account type. ['A - Business', 'B - Personal Current', 'C - Savings', 'D - Trust Account', 'E - Trading Account', 'O - Other']  | ✓                   |

1,  
'UPDATE\_DEVICE\_STAT

| Object attribute        | MISP attribute type | Description   | Disable correlation |
|-------------------------|---------------------|---|---------------------|
| 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. | ✓                   |
| text                    | text                | A description of the bank account.  | ✓                   |
| beneficiary             | text                | Final beneficiary of the bank account.  | ✓                   |
| institution-code        | text                | Institution code of the bank.   | ✓                   |
| balance                 | text                | The balance of the account after the suspicious transaction was processed.  | ✓                   |
| swift                   | bic                 | SWIFT or BIC as defined in ISO 9362.  | ✓                   |
| branch                  | text                | Branch code or name   | ✓                   |

## 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 |
|------------------|---------------------|--|---------------------|
| 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.  | ✓                   |
| scope            | text                | The code denoting the intended distribution of the alert message. ['Public', 'Restricted', 'Private']  | ✓                   |
| 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 |
|------------------|---------------------|---|---------------------|
| 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.  | ✓                   |
| code             | text                | The code denoting the special handling of the alert message.  | ✓                   |
| sent             | datetime            | The time and date of the origination 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.   | ✓                   |
| identifier       | text                | The identifier of the alert message in a number or string uniquely identifying this message, assigned by the sender.  | ✓                   |



| Object attribute | MISP attribute type | Description  | Disable correlation |
|------------------|---------------------|--|---------------------|
| note             | text                | The text describing the purpose or significance of the alert message.  | ✓                   |
| status           | text                | The code denoting the appropriate handling of the alert message. ['Actual', 'Exercise', 'System', 'Test', 'Draft']   | —                   |
| 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. | ✓                   |

## 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 |
|------------------|---------------------|--|---------------------|
| language         | text                | The code denoting the language of the info sub-element of the alert message. | ✓                   |

| <b>Object attribute</b> | <b>MISP attribute type</b> | <b>Description</b>   | <b>Disable correlation</b> |
|-------------------------|----------------------------|--|----------------------------|
| senderName              | text                       | The text naming the originator of the alert message.   | ✓                          |
| responseType            | text                       | The code denoting the type of action recommended for the target audience. ['Shelter', 'Evacuate', 'Prepare', 'Execute', 'Avoid', 'Monitor', 'Assess', 'AllClear', 'None']  | ✓                          |
| onset                   | datetime                   | The expected time of the beginning of the subject event of the alert message.  | ✓                          |
| audience                | text                       | The text describing the intended audience of the alert message.  | ✓                          |
| effective               | datetime                   | The effective time of the information of the alert message.  | ✓                          |
| web                     | link                       | The identifier of the hyperlink associating additional information with the alert message.   | ✓                          |
| 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'] | ✓                          |

| <b>Object attribute</b> | <b>MISP attribute type</b> | <b>Description</b>  | <b>Disable correlation</b> |
|-------------------------|----------------------------|---|----------------------------|
| parameter               | text                       | A system-specific additional parameter associated with the alert message.   | ✓                          |
| event                   | text                       | The text denoting the type of the subject event of the alert message.   | ✓                          |
| expires                 | datetime                   | The expiry time of the information of the alert message.  | ✓                          |
| urgency                 | text                       | The code denoting the urgency of the subject event of the alert message. ['Immediate', 'Expected', 'Future', 'Past', 'Unknown'] | ✓                          |
| contact                 | text                       | The text describing the contact for follow-up and confirmation of the alert message.  | ✓                          |
| instruction             | text                       | The text describing the recommended action to be taken by recipients of the alert message.                                      | ✓                          |
| eventCode               | text                       | A system-specific code identifying the event type of the alert message.   | ✓                          |
| description             | text                       | The text describing the subject event of the alert message.   | ✓                          |

| Object attribute | MISP attribute type | Description   | Disable correlation |
|------------------|---------------------|---|---------------------|
| severity         | text                | The code denoting the severity of the subject event of the alert message. ['Extreme', 'Severe', 'Moderate', 'Minor', 'Unknown']   | ✓                   |
| 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'] | ✓                   |
| headline         | text                | The text headline of 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 |
|------------------|---------------------|--|---------------------|
| derefUri         | attachment          | The base-64 encoded data content of 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.         | —                   |

| Object attribute | MISP attribute type | Description   | Disable correlation |
|------------------|---------------------|---|---------------------|
| contentType      | mime-type           | The identifier of the MIME content type and sub-type describing the resource file.            | ✓                   |
| digest           | sha1                | The code representing the digital digest (“hash”) computed from the resource file (OPTIONAL). | —                   |

## 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 |
|------------------|---------------------|---|---------------------|
| last-seen        | datetime            | Last time this payment destination address has been seen  | ✓                   |
| text             | text                | Free text value   | ✓                   |
| symbol           | text                | The (uppercase) symbol of the cryptocurrency used. Symbol should be from <a href="https://coinmarketcap.com/all/views/all/">https://coinmarketcap.com/all/views/all/</a> ['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'] | ✓                   |

| Object attribute | MISP attribute type | Description   | Disable correlation |
|------------------|---------------------|---|---------------------|
| first-seen       | datetime            | First time this payment destination address has been seen | ✓                   |
| address          | btc                 | Address used as a payment destination in a cryptocurrency | —                   |

## cookie

An HTTP cookie (web cookie, browser cookie) is a small piece of data that a server sends to the user's web browser. The browser may store it and send it back with the next request to the same server. Typically, it's used to tell if two requests came from the same browser — keeping a user logged-in, for example. It remembers stateful information for the stateless HTTP protocol. (as defined by the Mozilla foundation..)



cookie is a MISP object available in JSON format at [this location](#) The JSON format can be freely reused in your application or automatically enabled in [MISP](#).

| Object attribute | MISP attribute type | Description   | Disable correlation |
|------------------|---------------------|---|---------------------|
| cookie-name      | text                | Name of the cookie (if splitted)  | —                   |
| text             | text                | A description of the cookie.  | ✓                   |
| cookie-value     | text                | Value of the cookie (if splitted)   | —                   |
| type             | text                | Type of cookie and how it's used in this specific object. ['Session management', 'Personalization', 'Tracking', 'Exfiltration', 'Malicious Payload', 'Beaconing'] | —                   |
| cookie           | cookie              | Full cookie   | —                   |

# 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 |
|------------------|---------------------|--|---------------------|
| 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'] | ✓                   |
| impact           | text                | The estimated impact of applying the course of action. ['High', 'Medium', 'Low', 'None', 'Unknown']  | ✓                   |
| cost             | text                | The estimated cost of applying the course of action. ['High', 'Medium', 'Low', 'None', 'Unknown']  | ✓                   |
| efficacy         | text                | The estimated efficacy of applying the course of action. ['High', 'Medium', 'Low', 'None', 'Unknown']  | ✓                   |

| Object attribute | MISP attribute type | Description   | Disable correlation |
|------------------|---------------------|---|---------------------|
| stage            | text                | The stage of the threat management lifecycle that the course of action is applicable to. ['Remedy', 'Response'] | ✓                   |
| description      | text                | A description of the course of action.  | ✓                   |
| objective        | text                | The objective of the course of action.  | ✓                   |
| name             | text                | The name used to identify the course of action.   | ✓                   |

## 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 |
|------------------|---------------------|-------------------------------------|---------------------|
| macCS            | text                | SSH MAC supported in the session    | ✓                   |
| username         | text                | Username related to the password(s) | —                   |
| isError          | text                | isError                             | ✓                   |
| session          | text                | Session id                          | —                   |
| password         | text                | Password                            | —                   |
| src_port         | port                | Source port of the session          | ✓                   |
| src_ip           | ip-src              | Source IP address of the session    | —                   |



| Object attribute | MISP attribute type | Description   | Disable correlation |
|------------------|---------------------|---|---------------------|
| timestamp        | datetime            | When the event happened                                     | ✓                   |
| dst_port         | port                | Destination port of the session                             | ✓                   |
| encCS            | text                | SSH symmetric encryption algorithm supported in the session | ✓                   |
| dst_ip           | ip-dst              | Destination IP address of the session                       | ✓                   |
| keyAlgs          | text                | SSH public-key algorithm supported in the session           | ✓                   |
| eventid          | text                | Eventid of the session in the cowrie honeypot               | ✓                   |
| message          | text                | Message of the cowrie honeypot                              | ✓                   |
| sensor           | text                | Cowrie sensor name  | ✓                   |
| input            | text                | Input of the session  | —                   |
| system           | text                | System origin in cowrie honeypot                            | ✓                   |
| compCS           | text                | SSH compression algorithm supported in the session          | ✓                   |
| protocol         | text                | Protocol used in the cowrie honeypot                        | ✓                   |

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

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

## ddos

DDoS object describes a current DDoS activity from a specific or/and to a specific target. Type of DDoS can be attached to the object as a taxonomy.



ddos is a MISP object available in JSON format at [this location](#) The JSON format can be freely reused in your application or automatically enabled in [MISP](#).

| Object attribute | MISP attribute type | Description                 | Disable correlation |
|------------------|---------------------|-----------------------------|---------------------|
| src-port         | port                | Port originating the attack | —                   |
| text             | text                | Description of the DDoS     | ✓                   |
| last-seen        | datetime            | End of the attack           | ✓                   |

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

## diameter-attack

Attack as seen on diameter authentication against a GSM, UMTS or LTE network.



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 |
|------------------|---------------------|--|---------------------|
| Destination-Host | text                | Destination-Host.                          | —                   |
| Username         | text                | Username (in this case, usually the IMSI). | —                   |
| Origin-Realm     | text                | Origin-Realm.                              | —                   |
| Origin-Host      | text                | Origin-Host.                               | —                   |
| SessionId        | text                | Session-ID.                                | —                   |

| Object attribute  | MISP attribute type | Description  | Disable correlation |
|-------------------|---------------------|--|---------------------|
| IdrFlags          | text                | IDR-Flags.   | ✓                   |
| first-seen        | datetime            | When the attack has been seen for the first time.  | ✓                   |
| Destination-Realm | text                | Destination-Realm.   | —                   |
| text              | text                | A description of the attack seen.  | ✓                   |
| CmdCode           | text                | A decimal representation of the diameter Command Code.   | ✓                   |
| category          | text                | Category. ['Cat0', 'Cat1', 'Cat2', 'Cat3', 'CatSMS']   | ✓                   |
| ApplicationId     | text                | Application-ID is used to identify for which Diameter application the message is applicable. Application-ID is a decimal representation. | —                   |

## domain-ip

A domain and IP address seen as a tuple in a specific time frame..



domain-ip is a MISP object available in JSON format at [this location](#) The JSON format can be freely reused in your application or automatically enabled in [MISP](#).

| Object attribute | MISP attribute type | Description                       | Disable correlation |
|------------------|---------------------|-----------------------------------|---------------------|
| last-seen        | datetime            | Last time the tuple has been seen | ✓                   |
| text             | text                | A description of the tuple        | ✓                   |

| Object attribute | MISP attribute type | Description                        | Disable correlation |
|------------------|---------------------|------------------------------------|---------------------|
| first-seen       | datetime            | First time the tuple has been seen | ✓                   |
| ip               | ip-dst              | IP Address                         | —                   |
| domain           | domain              | Domain 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 |
|------------------|---------------------|--|---------------------|
| type             | text                | Type of ELF ['CORE', 'DYNAMIC', 'EXECUTABLE', 'HIPROC', 'LOPROC', 'NONE', 'RELOCATABLE'] | —                   |

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

| Object attribute   | MISP attribute type | Description  | Disable correlation |
|--------------------|---------------------|--|---------------------|
| os_abi             | text                | Header operating system application binary interface (ABI) ['AIX', 'ARM', 'AROS', 'C6000_ELFABI', 'C6000_LINUX', 'CLOUDABI', 'FENIXOS', 'FREEBSD', 'GNU', 'HPUX', 'HURD', 'IRIX', 'MODESTO', 'NETBSD', 'NSK', 'OPENBSD', 'OPENVMS', 'SOLARIS', 'STANDALONE', 'SYSTEMV', 'TRU64'] | ✓                   |
| number-sections    | counter             | Number of sections   | ✓                   |
| text               | text                | Free text value to attach to the ELF   | ✓                   |
| entrypoint-address | text                | Address of the entry point   | ✓                   |

## 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](#).

'TILE64', 'TILEPRO',  
'CUDA', 'TILEGX',  
'CLOUDSHIELD',  
'COREA\_1ST',  
'COBIA\_2ND',  
'ARC\_COMPACT2',  
'OPENJSON',  
'JRL78',  
'VIDEOCORE5',  
'ARCH\_78KOR',  
'ARCH\_56800EX', 'BA1',  
'BA2', 'XCORE',  
'MCHP\_PIC', 'INTEL205',  
'INTEL206', 'INTEL207',  
'INTEL208', 'INTEL209',  
'KM32', 'KMX32',  
'KMX16', 'KMX8',  
'KVARC', 'CDP', 'COGE',  
'COOL', 'NORC',  
'CSR\_KALIMBA',  
'AMDGPU']



| Object attribute | MISP attribute type | Description   | Disable correlation |
|------------------|---------------------|---|---------------------|
| type             | text                | Type of the section<br>['NULL', 'PROGBITS',<br>'SYMTAB', 'STRTAB',<br>'RELA', 'HASH',<br>'DYNAMIC', 'NOTE',<br>'NOBITS', 'REL', 'SHLIB',<br>'DYNYSYM',<br>'INIT_ARRAY',<br>'FINI_ARRAY',<br>'PREINIT_ARRAY',<br>'GROUP',<br>'SYMTAB_SHNDX',<br>'LOOS',<br>'GNU_ATTRIBUTES',<br>'GNU_HASH',<br>'GNU_VERDEF',<br>'GNU_VERNEED',<br>'GNU_VERSYM', 'HIOS',<br>'LOPROC', 'ARM_EXIDX',<br>'ARM_PREEMPTMAP',<br>'HEX_ORDERED',<br>'X86_64_UNWIND',<br>'MIPS_REGINFO',<br>'MIPS_OPTIONS',<br>'MIPS_ABIFLAGS',<br>'HIPROC', 'LOUSER',<br>'HIUSER'] | ✓                   |
| size-in-bytes    | size-in-bytes       | Size of the section, in bytes   | ✓                   |

| Object attribute | MISP attribute type | Description  | Disable correlation |
|------------------|---------------------|--|---------------------|
| flag             | text                | Flag of the section<br>['ALLOC', 'EXCLUDE',<br>'EXECINSTR', 'GROUP',<br>'HEX_GPREL',<br>'INFO_LINK',<br>'LINK_ORDER',<br>'MASKOS', 'MASKPROC',<br>'MERGE', 'MIPS_ADDR',<br>'MIPS_LOCAL',<br>'MIPS_MERGE',<br>'MIPS_NAMES',<br>'MIPS_NODUPES',<br>'MIPS_NOSTRIP',<br>'NONE',<br>'OS_NONCONFORMING',<br>'STRINGS', 'TLS',<br>'WRITE',<br>'XCORE_SHF_CP_SECTION'] | ✓                   |
| entropy          | float               | Entropy of the whole section   | ✓                   |
| sha1             | sha1                | [Insecure] Secure Hash Algorithm 1 (160 bits)  | —                   |
| md5              | md5                 | [Insecure] MD5 hash (128 bits)   | —                   |
| sha224           | sha224              | Secure Hash Algorithm 2 (224 bits)   | —                   |
| sha512/224       | sha512/224          | Secure Hash Algorithm 2 (224 bits)   | —                   |
| sha512           | sha512              | Secure Hash Algorithm 2 (512 bits)   | —                   |
| ssdeep           | ssdeep              | Fuzzy hash using context triggered piecewise hashes (CTPH)   | —                   |

| Object attribute | MISP attribute type | Description                              | Disable correlation |
|------------------|---------------------|--|---------------------|
| sha256           | sha256              | Secure Hash Algorithm 2 (256 bits)       | —                   |
| text             | text                | Free text value to attach to the section | ✓                   |
| sha512/256       | sha512/256          | Secure Hash Algorithm 2 (256 bits)       | —                   |
| name             | text                | Name of the section                      | ✓                   |
| sha384           | sha384              | Secure Hash Algorithm 2 (384 bits)       | —                   |

## email

Email object describing an email with meta-information.



email is a MISP object available in JSON format at [this location](#). The JSON format can be freely reused in your application or automatically enabled in [MISP](#).

| Object attribute  | MISP attribute type    | Description                | Disable correlation |
|-------------------|------------------------|----------------------------|---------------------|
| cc                | email-dst              | Carbon copy                | ✓                   |
| message-id        | email-message-id       | Message ID                 | ✓                   |
| screenshot        | attachment             | Screenshot of email        | ✓                   |
| to                | email-dst              | Destination email address  | ✓                   |
| from-display-name | email-src-display-name | Display name of the sender | —                   |
| header            | email-header           | Full headers               | ✓                   |
| return-path       | email-src              | Message return path        | —                   |

| Object attribute | MISP attribute type    | Description   | Disable correlation |
|------------------|------------------------|---|---------------------|
| x-mailer         | email-x-mailer         | X-Mailer generally tells the program that was used to draft and send the original email | ✓                   |
| send-date        | datetime               | Date the email has been sent  | ✓                   |
| subject          | email-subject          | Subject   | —                   |
| eml              | attachment             | Full EML  | ✓                   |
| email-body       | email-body             | Body of the email   | ✓                   |
| thread-index     | email-thread-index     | Identifies a particular conversation thread   | ✓                   |
| to-display-name  | email-dst-display-name | Display name of the receiver  | —                   |
| reply-to         | email-reply-to         | Email address the reply will be sent to   | —                   |
| user-agent       | text                   | User Agent of the sender  | ✓                   |
| mime-boundary    | email-mime-boundary    | MIME Boundary   | ✓                   |
| from             | email-src              | Sender email address  | —                   |
| attachment       | email-attachment       | Attachment  | —                   |

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

## 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 |
|------------------|---------------------|--|---------------------|
| size-in-bytes    | size-in-bytes       | Size of the file, in bytes   | ✓                   |
| path             | text                | Path of the filename complete or partial   | ✓                   |
| state            | text                | State of the file ['Malicious', 'Harmless', 'Signed', 'Revoked', 'Expired', 'Trusted'] | ✓                   |
| malware-sample   | malware-sample      | The file itself (binary)   | —                   |

| Object attribute | MISP attribute type   | Description  | Disable correlation |
|------------------|-----------------------|--|---------------------|
| sha256           | sha256                | Secure Hash Algorithm 2 (256 bits)   | —                   |
| sha1             | sha1                  | [Insecure] Secure Hash Algorithm 1 (160 bits)  | —                   |
| md5              | md5                   | [Insecure] MD5 hash (128 bits)   | —                   |
| sha224           | sha224                | Secure Hash Algorithm 2 (224 bits)   | —                   |
| sha512/224       | sha512/224            | Secure Hash Algorithm 2 (224 bits)   | —                   |
| sha512           | sha512                | Secure Hash Algorithm 2 (512 bits)   | —                   |
| ssdeep           | ssdeep                | Fuzzy hash using context triggered piecewise hashes (CTPH)                                     | —                   |
| authentihash     | authentihash          | Authenticode executable signature hash   | —                   |
| certificate      | x509-fingerprint-sha1 | Certificate value if the binary is signed with another authentication scheme than authenticode | —                   |
| text             | text                  | Free text value to attach to the file  | ✓                   |
| sha512/256       | sha512/256            | Secure Hash Algorithm 2 (256 bits)   | —                   |
| entropy          | float                 | Entropy of the whole file  | ✓                   |

| Object attribute | MISP attribute type | Description  | Disable correlation |
|------------------|---------------------|--|---------------------|
| pattern-in-file  | pattern-in-file     | Pattern that can be found in the file              | —                   |
| tlsh             | tlsh                | Fuzzy hash by Trend Micro: Locality Sensitive Hash | —                   |
| filename         | filename            | Filename on disk                                   | ✓                   |
| mimetype         | mime-type           | Mime type  | ✓                   |
| sha384           | sha384              | Secure Hash Algorithm 2 (384 bits)                 | —                   |

## geolocation

An object to describe a geographic location..



geolocation is a MISP object available in JSON format at [this location](#) The JSON format can be freely reused in your application or automatically enabled in [MISP](#).

| Object attribute | MISP attribute type | Description  | Disable correlation |
|------------------|---------------------|--|---------------------|
| last-seen        | datetime            | When the location was seen for the last time.  | ✓                   |
| text             | text                | A generic description of the location.   | ✓                   |
| latitude         | float               | The latitude is the decimal value of the latitude in the World Geodetic System 84 (WGS84) reference. | ✓                   |
| region           | text                | Region.  | —                   |
| altitude         | float               | The altitude is the decimal value of the altitude in the World Geodetic System 84 (WGS84) reference. | —                   |

| Object attribute | MISP attribute type | Description   | Disable correlation |
|------------------|---------------------|---|---------------------|
| zipcode          | text                | Zip Code.   | —                   |
| city             | text                | City.   | —                   |
| longitude        | float               | The longitude is the decimal value of the longitude in the World Geodetic System 84 (WGS84) reference | ✓                   |
| first-seen       | datetime            | When the location was seen for the first time.  | ✓                   |
| country          | text                | Country.  | —                   |
| address          | text                | Address.  | —                   |

## gtp-attack

GTP attack object as seen on a GSM, UMTS or LTE network.



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 |
|------------------|---------------------|--|---------------------|
| GtpVersion       | text                | GTP version ['0', '1', '2']                          | ✓                   |
| PortSrc          | port                | Source port.   | ✓                   |
| ipDest           | ip-dst              | IP destination address.                              | —                   |
| GtpImei          | text                | GTP IMEI (International Mobile Equipment Identity).  | —                   |
| GtpImsi          | text                | GTP IMSI (International mobile subscriber identity). | —                   |
| first-seen       | datetime            | When the attack has been seen for the first time.    | ✓                   |



| Object attribute  | MISP attribute type | Description  | Disable correlation |
|-------------------|---------------------|--|---------------------|
| text              | text                | A description of the GTP attack.   | ✓                   |
| 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. | ✓                   |
| GtpInterface      | text                | GTP interface. ['S5', 'S11', 'S10', 'S8', 'Gn', 'Gp']  | ✓                   |
| PortDest          | text                | Destination port.  | ✓                   |
| GtpMsisdn         | text                | GTP MSISDN.  | —                   |
| ipSrc             | ip-src              | IP source address.   | —                   |
| GtpServingNetwork | text                | GTP Serving Network.   | ✓                   |

## 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 |
|------------------|---------------------|--|---------------------|
| 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 | —                   |

| Object attribute   | MISP attribute type | Description   | Disable correlation |
|--------------------|---------------------|---|---------------------|
| host               | hostname            | The domain name of the server   | —                   |
| uri                | uri                 | Request URI   | —                   |
| 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  | ✓                   |
| method             | http-method         | HTTP Method invoked (one of GET, POST, PUT, HEAD, DELETE, OPTIONS, CONNECT)                                 | ✓                   |
| url                | url                 | Full HTTP Request URL   | —                   |
| proxy-password     | text                | HTTP Proxy Password   | —                   |
| basicauth-password | text                | HTTP Basic Authentication Password  | —                   |
| proxy-user         | text                | HTTP Proxy Username   | —                   |
| user-agent         | user-agent          | The user agent string of the user agent   | —                   |

## 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 |
|------------------|---------------------|------------------------------------|---------------------|
| last-seen        | datetime            | Last time the tuple has been seen  | ✓                   |
| text             | text                | Description of the tuple           | ✓                   |
| src-port         | port                | Source port                        | —                   |
| domain           | domain              | Domain                             | —                   |
| hostname         | hostname            | Hostname                           | —                   |
| first-seen       | datetime            | First time the tuple has been seen | ✓                   |
| ip               | ip-dst              | IP Address                         | —                   |
| dst-port         | port                | Destination port                   | ✓                   |

## ja3

JA3 is a new technique for creating SSL client fingerprints that are easy to produce and can be easily shared for threat intelligence. Fingerprints are composed of Client Hello packet; SSL Version, Accepted Ciphers, List of Extensions, Elliptic Curves, and Elliptic Curve Formats. <https://github.com/salesforce/ja3>.



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 |
|------------------|---------------------|--|---------------------|
| last-seen        | datetime            | Last seen of the SSL/TLS handshake             | ✓                   |
| description      | text                | Type of detected software ie software, malware | —                   |
| first-seen       | datetime            | First seen of the SSL/TLS handshake            | ✓                   |
| ip-src           | ip-src              | Source IP Address                              | —                   |

| Object attribute    | MISP attribute type | Description             | Disable correlation |
|---------------------|---------------------|-------------------------|---------------------|
| ja3-fingerprint-md5 | md5                 | Hash identifying source | —                   |
| ip-dst              | ip-dst              | Destination IP address  | —                   |

## 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 |
|---------------------|---------------------|---|---------------------|
| text                | text                | A description of the entity.                                | ✓                   |
| registration-number | text                | Registration number of an entity in the relevant authority. | —                   |
| phone-number        | phone-number        | Phone number of an entity.                                  | —                   |
| legal-form          | text                | Legal form of an entity.                                    | —                   |
| business            | text                | Business area of an entity.                                 | —                   |
| name                | text                | Name of an entity.  | —                   |
| commercial-name     | text                | Commercial name of an entity.                               | —                   |

## macho

Object describing a file in Mach-O format..



macho is a MISP object available in JSON format at [this location](#) The JSON format can be freely reused in your application or automatically enabled in [MISP](#).

| Object attribute   | MISP attribute type | Description   | Disable correlation |
|--------------------|---------------------|---|---------------------|
| type               | text                | Type of Mach-O ['BUNDLE', 'CORE', 'DSYM', 'DYLIB', 'DYLIB_STUB', 'DYLINKER', 'EXECUTE', 'FVMLIB', 'KEXT_BUNDLE', 'OBJECT', 'PRELOAD'] | —                   |
| text               | text                | Free text value to attach to the Mach-O file  | ✓                   |
| number-sections    | counter             | Number of sections  | ✓                   |
| name               | text                | Binary's name   | —                   |
| entrypoint-address | text                | Address of the entry point  | ✓                   |

## 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 |
|------------------|---------------------|---|---------------------|
| size-in-bytes    | size-in-bytes       | Size of the section, in bytes                 | ✓                   |
| entropy          | float               | Entropy of the whole section                  | ✓                   |
| sha1             | sha1                | [Insecure] Secure Hash Algorithm 1 (160 bits) | —                   |
| md5              | md5                 | [Insecure] MD5 hash (128 bits)                | —                   |
| sha224           | sha224              | Secure Hash Algorithm 2 (224 bits)            | —                   |

| Object attribute | MISP attribute type | Description  | Disable correlation |
|------------------|---------------------|--|---------------------|
| sha512/224       | sha512/224          | Secure Hash Algorithm 2 (224 bits)                         | —                   |
| sha512           | sha512              | Secure Hash Algorithm 2 (512 bits)                         | —                   |
| ssdeep           | ssdeep              | Fuzzy hash using context triggered piecewise hashes (CTPH) | —                   |
| sha256           | sha256              | Secure Hash Algorithm 2 (256 bits)                         | —                   |
| text             | text                | Free text value to attach to the section                   | ✓                   |
| sha512/256       | sha512/256          | Secure Hash Algorithm 2 (256 bits)                         | —                   |
| name             | text                | Name of the section  | ✓                   |
| sha384           | sha384              | Secure Hash Algorithm 2 (384 bits)                         | —                   |

## microblog

Microblog post like a Twitter tweet or a post on a Facebook wall..



microblog is a MISP object available in JSON format at [this location](#) The JSON format can be freely reused in your application or automatically enabled in [MISP](#).

| Object attribute | MISP attribute type | Description  | Disable correlation |
|------------------|---------------------|--|---------------------|
| type             | text                | Type of the microblog post ['Twitter', 'Facebook', 'LinkedIn', 'Reddit', 'Google+', 'Instagram', 'Forum', 'Other'] | ✓                   |
| removal-date     | datetime            | When the microblog post was removed  | —                   |

| Object attribute  | MISP attribute type | Description                                     | Disable correlation |
|-------------------|---------------------|---|---------------------|
| post              | text                | Raw post  | —                   |
| url               | url                 | Original URL location of the microblog post     | —                   |
| username          | text                | Username who posted the microblog post          | —                   |
| creation-date     | datetime            | Initial creation of the microblog post          | —                   |
| username-quoted   | text                | Username who are quoted into the microblog post | —                   |
| modification-date | datetime            | Last update of the microblog post               | —                   |
| link              | url                 | Link into the microblog post                    | —                   |

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

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



| Object attribute | MISP attribute type | Description  | Disable correlation |
|------------------|---------------------|--|---------------------|
| protocol         | text                | Protocol used for this flow ['TCP', 'UDP', 'ICMP', 'IP'] | —                   |
| ip-dst           | ip-dst              | IP address destination of the netflow                    | —                   |
| dst-port         | port                | Destination port of the netflow                          | —                   |
| ip_version       | counter             | IP version of this 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 |
|-------------------|---------------------|--|---------------------|
| layer7-protocol   | text                | Layer 7 protocol of the network connection. ['HTTP', 'HTTPS', 'FTP'] | —                   |
| first-packet-seen | datetime            | Datetime of the first packet seen.                                   | —                   |
| src-port          | port                | Source port of the network connection.                               | —                   |
| layer3-protocol   | text                | Layer 3 protocol of the network connection. ['IP', 'ICMP', 'ARP']    | —                   |
| layer4-protocol   | text                | Layer 4 protocol of the network connection. ['TCP', 'UDP']           | —                   |
| hostname-dst      | hostname            | Destination hostname of the network connection.                      | —                   |

| Object attribute | MISP attribute type | Description                                       | Disable correlation |
|------------------|---------------------|---|---------------------|
| ip-dst           | ip-dst              | Destination IP address of the network connection. | —                   |
| hostname-src     | hostname            | Source hostname of the network connection.        | —                   |
| dst-port         | port                | Destination port of the network connection.       | —                   |
| ip-src           | ip-src              | Source IP address of the network connection.      | —                   |

## 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 |
|------------------|---------------------|---|---------------------|
| 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', 'PF_VSOCK', 'PF_KCM', 'PF_MAX'] | —                   |
| src-port         | port                | Source (local) port of the network socket connection.   | —                   |
| state            | text                | State of the socket connection. ['blocking', 'listening']   | —                   |

| <b>Object attribute</b> | <b>MISP attribute type</b> | <b>Description</b>  | <b>Disable correlation</b> |
|-------------------------|----------------------------|---|----------------------------|
| dst-port                | port                       | Destination port of the network socket connection.                | —                          |
| option                  | text                       | Option on the socket connection.                                  | —                          |
| hostname-dst            | hostname                   | Destination hostname of the network socket connection.            | —                          |
| protocol                | text                       | Protocol used by the network socket. ['TCP', 'UDP', 'ICMP', 'IP'] | —                          |
| hostname-src            | hostname                   | Source (local) hostname of the network socket connection.         | —                          |
| ip-src                  | ip-src                     | Source (local) IP address of the network socket connection.       | —                          |

| Object attribute | MISP attribute type | Description  | Disable correlation |
|------------------|---------------------|--|---------------------|
| address-family   | text                | Address family who specifies the address family type (AF_*) of the socket connection.<br>[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', 'AF_KCM', 'AF_MAX'] | —                   |
| ip-dst           | ip-dst              | Destination IP address of the network socket connection.   | —                   |

## passive-dns

Passive DNS records as expressed in draft-dulaunoy-dnsop-passive-dns-cof-01.



passive-dns is a MISP object available in JSON format at [this location](#) The JSON format can be freely reused in your application or automatically enabled in [MISP](#).

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

| Object attribute | MISP attribute type | Description  | Disable correlation |
|------------------|---------------------|--|---------------------|
| rrtype           | text                | Resource Record type as seen by the passive DNS. ['A', 'AAAA', 'CNAME', 'PTR', 'SOA', 'TXT', 'DNAME', 'NS', 'SRV', 'RP', 'NAPTR', 'HINFO', 'A6'] | ✓                   |
| zone_time_last   | datetime            | Last time that the unique tuple (rrname, rrtype, rdata) record has been seen via master file import.   | ✓                   |
| rrname           | text                | Resource Record name of the queried resource.  | —                   |
| bailiwick        | text                | Best estimate of the apex of the zone where this data is authoritative   | ✓                   |

## 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 |
|------------------|---------------------|---|---------------------|
| last-seen        | datetime            | When the paste has been accessible or seen for the last time. | ✓                   |
| paste            | text                | Raw text of the paste or post                                 | —                   |

| Object attribute | MISP attribute type | Description  | Disable correlation |
|------------------|---------------------|--|---------------------|
| origin           | text                | Original source of the paste or post. ['pastebin.com', 'pastebin.com_pro', 'pastie.org', 'slexy.org', 'gist.github.com', 'codepad.org', 'safebin.net', 'hastebin.com', 'ghostbin.com'] | —                   |
| url              | url                 | Link to the original source of the paste or post.  | —                   |
| title            | text                | Title of the paste or post.  | —                   |
| first-seen       | datetime            | When the paste has been accessible or seen for the first time.   | ✓                   |

## 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 |
|-------------------|---------------------|--|---------------------|
| type              | text                | Type of PE ['exe', 'dll', 'driver', 'unknown']       | ✓                   |
| impfuzzy          | impfuzzy            | Fuzzy Hash (ssdeep) calculated from the import table | —                   |
| internal-filename | filename            | InternalFilename in the resources                    | ✓                   |
| file-description  | text                | FileDescription in the resources                     | ✓                   |



| Object attribute               | MISP attribute type | Description  | Disable correlation |
|--------------------------------|---------------------|--|---------------------|
| compilation-timestamp          | datetime            | Compilation timestamp defined in the PE header   | —                   |
| file-version                   | text                | FileVersion in the resources   | ✓                   |
| pehash                         | pehash              | Hash of the structural information about a sample. See <a href="https://www.usenix.org/legacy/event/leet09/tech/full_papers/wicherski/wicherski_html/">https://www.usenix.org/legacy/event/leet09/tech/full_papers/wicherski/wicherski_html/</a> | —                   |
| original-filename              | filename            | OriginalFilename in the resources  | ✓                   |
| legal-copyright                | text                | LegalCopyright in the resources  | ✓                   |
| text                           | text                | Free text value to attach to the PE  | ✓                   |
| company-name                   | text                | CompanyName in the resources   | ✓                   |
| number-sections                | counter             | Number of sections   | ✓                   |
| product-version                | text                | ProductVersion in the resources  | ✓                   |
| entrypoint-section-at-position | text                | Name of the section and position of the section in the PE  | ✓                   |
| imphash                        | imphash             | Hash (md5) calculated from the import table  | —                   |
| product-name                   | text                | ProductName in the resources   | ✓                   |

| Object attribute   | MISP attribute type | Description                | Disable correlation |
|--------------------|---------------------|----------------------------|---------------------|
| lang-id            | text                | Lang ID in the resources   | ✓                   |
| entrypoint-address | text                | Address of the entry point | ✓                   |

## 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 |
|------------------|---------------------|---|---------------------|
| size-in-bytes    | size-in-bytes       | Size of the section, in bytes                                 | ✓                   |
| characteristic   | text                | Characteristic of the section ['read', 'write', 'executable'] | —                   |
| entropy          | float               | Entropy of the whole section                                  | ✓                   |
| sha1             | sha1                | [Insecure] Secure Hash Algorithm 1 (160 bits)                 | —                   |
| md5              | md5                 | [Insecure] MD5 hash (128 bits)                                | —                   |
| sha224           | sha224              | Secure Hash Algorithm 2 (224 bits)                            | —                   |
| sha512/224       | sha512/224          | Secure Hash Algorithm 2 (224 bits)                            | —                   |
| sha512           | sha512              | Secure Hash Algorithm 2 (512 bits)                            | —                   |

| Object attribute | MISP attribute type | Description   | Disable correlation |
|------------------|---------------------|---|---------------------|
| ssdeep           | ssdeep              | Fuzzy hash using context triggered piecewise hashes (CTPH)          | —                   |
| sha256           | sha256              | Secure Hash Algorithm 2 (256 bits)                                  | —                   |
| text             | text                | Free text value to attach to the section                            | ✓                   |
| sha512/256       | sha512/256          | Secure Hash Algorithm 2 (256 bits)                                  | —                   |
| name             | text                | Name of the section ['.rsrc', '.reloc', '.rdata', '.data', '.text'] | ✓                   |
| sha384           | sha384              | Secure Hash Algorithm 2 (384 bits)                                  | —                   |

## 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 |
|------------------|---------------------|---|---------------------|
| 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. | —                   |
| last-name        | last-name           | Last name of a natural person.  | —                   |
| alias            | text                | Alias name or known as.   | —                   |

| <b>Object attribute</b> | <b>MISP attribute type</b> | <b>Description</b>   | <b>Disable correlation</b> |
|-------------------------|----------------------------|--|----------------------------|
| passport-number         | passport-number            | The passport number of a natural person.   | —                          |
| redress-number          | redress-number             | The Redress Control Number is the record identifier for people who apply for redress through the DHS Travel Redress Inquiry Program (DHS TRIP). DHS TRIP is for travelers who have been repeatedly identified for additional screening and who want to file an inquiry to have erroneous information corrected in DHS systems. | —                          |
| identity-card-number    | identity-card-number       | The identity card number of a natural person.  | —                          |
| first-name              | first-name                 | First name of a natural person.  | ✓                          |
| place-of-birth          | place-of-birth             | Place of birth of a natural person.  | ✓                          |
| gender                  | gender                     | The gender of a natural person. ['Male', 'Female', 'Other', 'Prefer not to say']   | ✓                          |
| text                    | text                       | A description of the person or identity.   | ✓                          |
| social-security-number  | text                       | Social security number   | —                          |
| 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 |
|---------------------|---------------------|--|---------------------|
| nationality         | nationality         | The nationality of a natural person.                   | ✓                   |
| title               | text                | Title of the natural person such as Dr. or equivalent. | ✓                   |
| passport-country    | passport-country    | The country in which the passport was issued.          | ✓                   |
| passport-expiration | passport-expiration | The expiration date of a passport.                     | ✓                   |

## 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 |
|------------------|---------------------|--|---------------------|
| last-seen        | datetime            | When the phone has been accessible or seen for the last time.                                | ✓                   |
| text             | text                | A description of the phone.  | ✓                   |
| 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). | —                   |
| serial-number    | text                | Serial Number.   | —                   |

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

| Object attribute | MISP attribute type | Description   | Disable correlation |
|------------------|---------------------|---|---------------------|
| guti             | text                | Globally Unique Temporary UE Identity (GUTI) is a temporary identification to not reveal the phone (user equipment in 3GPP jargon) composed of GUMMEI and the M-TMSI. | —                   |

## 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 |
|------------------|---------------------|---|---------------------|
| port             | src-port            | Port(s) owned by the process.                     | —                   |
| start-time       | datetime            | Local date/time at which the process was started. | ✓                   |
| pid              | text                | Process ID of the process.                        | —                   |
| parent-pid       | text                | Process ID of the parent process.                 | —                   |
| creation-time    | datetime            | Local date/time at which the process was created. | ✓                   |
| child-pid        | text                | Process ID of the child(ren) process.             | —                   |
| name             | text                | Name of the process                               | —                   |

# 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 |
|--------------------|---------------------|---|---------------------|
| refsglobalvar      | counter             | Amount of API calls outside of code section (glob var, dynamic API)     | ✓                   |
| total-functions    | counter             | Total amount of functions in the file.                                  | ✓                   |
| create-thread      | counter             | Amount of calls to CreateThread   | ✓                   |
| callback-average   | counter             | Average size of a callback  | ✓                   |
| total-api          | counter             | Total amount of API calls   | ✓                   |
| get-proc-address   | counter             | Amount of calls to GetProcAddress                                       | ✓                   |
| miss-api           | counter             | Amount of API call reference that does not resolve to a function offset | ✓                   |
| callback-largest   | counter             | Largest callback  | ✓                   |
| memory-allocations | counter             | Amount of memory allocations  | ✓                   |
| r2-commit-version  | text                | Radare2 commit ID used to generate this object                          | ✓                   |
| ratio-api          | float               | Ratio: amount of API calls per kilobyte of code section                 | ✓                   |



| Object attribute               | MISP attribute type | Description   | Disable correlation |
|--------------------------------|---------------------|---|---------------------|
| not-referenced-strings         | counter             | Amount of not referenced strings  | ✓                   |
| referenced-strings             | counter             | Amount of referenced strings  | ✓                   |
| shortest-path-to-create-thread | counter             | Shortest path to the first time the binary calls CreateThread   | ✓                   |
| ratio-string                   | float               | Ratio: amount of referenced strings per kilobyte of code section  | ✓                   |
| callbacks                      | counter             | Amount of callbacks (functions started as thread)   | ✓                   |
| ratio-functions                | float               | Ratio: amount of functions per kilobyte of code section   | ✓                   |
| text                           | text                | Description of the r2graphity object  | ✓                   |
| unknown-references             | counter             | Amount of API calls not ending in a function (Radare2 bug, probalby)  | ✓                   |
| gml                            | attachment          | Graph export in Graph Modelling Language format   | ✓                   |
| 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.) | ✓                   |
| local-references               | counter             | Amount of API calls inside a code section   | ✓                   |

# regexp

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



regexp is a MISP object available in JSON format at [this location](#) The JSON format can be freely reused in your application or automatically enabled in [MISP](#).

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

# registry-key

Registry key object describing a Windows registry key with value and last-modified timestamp.



registry-key is a MISP object available in JSON format at [this location](#) The JSON format can be freely reused in your application or automatically enabled in [MISP](#).

| Object attribute | MISP attribute type | Description  | Disable correlation |
|------------------|---------------------|--|---------------------|
| hive             | text                | Hive used to store the registry key (file on disk) | ✓                   |

| Object attribute | MISP attribute type | Description  | Disable correlation |
|------------------|---------------------|--|---------------------|
| key              | regkey              | Full key path  | —                   |
| data             | text                | Data stored in the registry key  | —                   |
| 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'] | ✓                   |
| name             | text                | Name of the registry key   | —                   |
| last-modified    | datetime            | Last time the registry key has been modified   | —                   |

| Object attribute | MISP attribute type | Description  | Disable correlation |
|------------------|---------------------|--|---------------------|
| 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'] | ✓                   |

## report

Metadata used to generate an executive level report.



report is a MISP object available in JSON format at [this location](#) The JSON format can be freely reused in your application or automatically enabled in [MISP](#).

| Object attribute | MISP attribute type | Description                     | Disable correlation |
|------------------|---------------------|---------------------------------|---------------------|
| summary          | text                | Free text summary of the report | —                   |
| case-number      | text                | Case number                     | —                   |

## rtir

RTIR - Request Tracker for Incident Response.



rtir is a MISP object available in JSON format at [this location](#) The JSON format can be freely reused in your application or automatically enabled in [MISP](#).

| Object attribute | MISP attribute type | Description   | Disable correlation |
|------------------|---------------------|---|---------------------|
| ip               | ip-dst              | IPs automatically extracted from the RTIR ticket  | —                   |
| subject          | text                | Subject of the RTIR ticket  | —                   |
| ticket-number    | text                | ticket-number of the RTIR ticket  | —                   |
| status           | text                | Status of the RTIR ticket ['new', 'open', 'stalled', 'resolved', 'rejected', 'deleted'] | —                   |
| constituency     | text                | Constituency of the RTIR ticket   | —                   |
| classification   | text                | Classification of the RTIR ticket   | —                   |
| queue            | text                | Queue of the RTIR ticket ['incident', 'investigations', 'blocks', 'incident reports']   | —                   |

## 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 |
|------------------|---------------------|---------------------|---------------------|
| permalink        | link                | Permalink reference | —                   |

| Object attribute   | MISP attribute type | Description  | Disable correlation |
|--------------------|---------------------|--|---------------------|
| web-sandbox        | text                | A web sandbox where results are publicly available via an URL ['malwr', 'hybrid-analysis']   | ✓                   |
| 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'] | ✓                   |
| results            | text                | Freetext result values   | ✓                   |
| raw-report         | text                | Raw report from sandbox  | ✓                   |
| sandbox-type       | text                | The type of sandbox used ['on-premise', 'web', 'saas']   | ✓                   |
| score              | text                | Score  | ✓                   |
| saas-sandbox       | text                | A non-on-premise sandbox, also results are not publicly available ['forticloud-sandbox', 'joe-sandbox-cloud', 'symantec-cas-cloud']                                      | ✓                   |

## 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 |
|------------------|---------------------|---|---------------------|
| text             | text                | Additional signature description  | ✓                   |
| signature        | text                | Name of detection signature - set the description of the detection signature as a comment | —                   |
| datetime         | datetime            | Datetime  | ✓                   |
| software         | text                | Name of Sandbox software  | ✓                   |

## ss7-attack

SS7 object of an attack seen on a GSM, UMTS or LTE network via SS7 logging..



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 |
|-----------------------|---------------------|---|---------------------|
| SccpCgGT              | text                | Signaling Connection Control Part (SCCP) CgGT - Phone number. | —                   |
| MapSmsTP-DCS          | text                | MAP SMS TP-DCS.   | ✓                   |
| MapUssdCoding         | text                | MAP USSD Content.   | ✓                   |
| MapSmscGT             | text                | MAP SMSC. Phone number.                                       | —                   |
| MapGmlc               | text                | MAP GMLC. Phone number.                                       | —                   |
| MapApplicationContext | text                | MAP application context in OID format.                        | ✓                   |
| MapOpCode             | text                | MAP operation codes - Decimal value between 0-99.             | ✓                   |

| <b>Object attribute</b> | <b>MISP attribute type</b> | <b>Description</b>   | <b>Disable correlation</b> |
|-------------------------|----------------------------|--|----------------------------|
| MapMscGT                | text                       | MAP MSC GT. Phone number.  | —                          |
| SccpCgPC                | text                       | Signaling Connection Control Part (SCCP) CgPC - Phone number.  | —                          |
| MapSmsText              | text                       | MAP SMS Text. Important indicators in SMS text.  | —                          |
| MapUssdContent          | text                       | MAP USSD Content.  | —                          |
| MapMsisdn               | text                       | MAP MSISDN. Phone number.  | —                          |
| MapImsi                 | text                       | MAP IMSI. Phone number starting with MCC/MNC.  | —                          |
| SccpCdGT                | text                       | Signaling Connection Control Part (SCCP) CdGT - Phone number.  | —                          |
| SccpCgSSN               | text                       | Signaling Connection Control Part (SCCP) - Decimal value between 0-255.                              | ✓                          |
| Category                | text                       | Category ['Cat0', 'Cat1', 'Cat2.1', 'Cat2.2', 'Cat3.1', 'Cat3.2', 'Cat3.3', 'CatSMS', 'CatSpoofing'] | ✓                          |
| first-seen              | datetime                   | When the attack has been seen for the first time.  | ✓                          |
| MapVlrGT                | text                       | MAP VLR GT. Phone number.  | —                          |
| SccpCdPC                | text                       | Signaling Connection Control Part (SCCP) CdPC - Phone number.  | —                          |



| Object attribute | MISP attribute type | Description   | Disable correlation |
|------------------|---------------------|---|---------------------|
| text             | text                | A description of the attack seen via SS7 logging.                       | ✓                   |
| MapSmsTP-OA      | text                | MAP SMS TP-OA. Phone number.  | —                   |
| MapSmsTypeNumber | text                | MAP SMS TypeNumber.   | ✓                   |
| MapVersion       | text                | Map version. ['1', '2', '3']  | ✓                   |
| MapGsmScfGT      | text                | MAP GSMSCF GT. Phone number.  | —                   |
| SccpCdSSN        | text                | Signaling Connection Control Part (SCCP) - Decimal value between 0-255. | ✓                   |
| MapSmsTP-PID     | text                | MAP SMS TP-PID.   | ✓                   |

## 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 |
|------------------|---------------------|---|---------------------|
| comment          | comment             | A description of the stix2-pattern.     | —                   |
| stix2-pattern    | stix2-pattern       | STIX 2 pattern                          | —                   |
| version          | text                | Version of STIX 2 pattern. ['stix 2.0'] | —                   |

# suricata

An object describing a Suricata rule along with its version and context.



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 |
|------------------|---------------------|--|---------------------|
| ref              | link                | Reference to the Suricata rule such as origin of the rule or alike.                          | —                   |
| comment          | comment             | A description of the Suricata rule.  | —                   |
| suricata         | suricata            | 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 |
|-----------------------|---------------------|----------------------------|---------------------|
| targeted_machine      | target-machine      | Targeted system            | ✓                   |
| targeted_ip_of_system | ip-src              | Targeted system IP address | ✓                   |
| timestamp_seen        | datetime            | Registered date and time   | ✓                   |

# 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 |
|-----------------------|---------------------|--|---------------------|
| end-marker-timecode   | text                | End marker timecode in the format hh:mm:ss;ff    | —                   |
| recording-date        | datetime            | Date of recording of the video sequence          | —                   |
| start-marker-timecode | text                | Start marker timecode in the format hh:mm:ss;ff  | —                   |
| end-timecode          | text                | End marker timecode in the format hh:mm:ss.mms   | —                   |
| description           | text                | Description of the video sequence                | —                   |
| 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 |
|------------------|---------------------|----------------------------------|---------------------|
| message          | text                | Informative message of the event | —                   |

| Object attribute | MISP attribute type | Description  | Disable correlation |
|------------------|---------------------|--|---------------------|
| timestamp_desc   | text                | Text explaining what type of timestamp is it                 | —                   |
| datetime         | datetime            | When the log entry was seen                                  | —                   |
| timestamp        | timestamp-microsec  | When the log entry was seen in microseconds since Unix epoch | —                   |

## 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 |
|------------------|---------------------|--|---------------------|
| last-seen        | datetime            | First time that the linked object or attribute has been seen.  | ✓                   |
| text             | text                | Description of the time object.  | ✓                   |
| first-seen       | datetime            | First time that the linked object or attribute has been seen.  | ✓                   |
| precision        | text                | Timestamp precision represents the precision given to first_seen and/or last_seen in this object. ['year', 'month', 'day', 'hour', 'minute', 'full'] | ✓                   |

# 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 |
|------------------|---------------------|---|---------------------|
| last-seen        | datetime            | When the Tor node designed by the IP address has been seen for the last time.     | ✓                   |
| version_line     | text                | versioning information reported by the node.                                      | —                   |
| fingerprint      | text                | router's fingerprint.   | —                   |
| document         | text                | Raw document from the consensus.  | ✓                   |
| flags            | text                | list of flag associated with the node.  | —                   |
| description      | text                | Tor node description.   | ✓                   |
| nickname         | text                | router's nickname.  | —                   |
| version          | text                | parsed version of tor, this is None if the relay's using a new versioning scheme. | —                   |
| text             | text                | Tor node comment.   | ✓                   |
| first-seen       | datetime            | When the Tor node designed by the IP address has been seen for the first time.    | ✓                   |

| Object attribute | MISP attribute type | Description   | Disable correlation |
|------------------|---------------------|---|---------------------|
| published        | datetime            | router's publication time. This can be different from first-seen and last-seen. | ✓                   |
| address          | ip-src              | IP address of the Tor node seen.  | —                   |

## 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 |
|--------------------|---------------------|--|---------------------|
| to-country         | text                | Target country of a transaction.   | —                   |
| 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'] | ✓                   |
| from-country       | text                | Origin country of a transaction.   | —                   |
| transaction-number | text                | A unique number identifying a transaction.   | —                   |
| authorized         | text                | Person who authorized the transaction.   | —                   |

| Object attribute  | MISP attribute type | Description   | Disable correlation |
|-------------------|---------------------|---|---------------------|
| transmode-code    | text                | How the transaction was conducted.  | —                   |
| 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'] | ✓                   |
| date              | datetime            | Date and time of the transaction.   | —                   |
| text              | text                | A description of the transaction.   | ✓                   |
| location          | text                | Location where the transaction took place.  | —                   |
| amount            | text                | The value of the transaction in local currency.   | —                   |
| teller            | text                | Person who conducted the transaction.   | —                   |
| transmode-comment | text                | Comment describing transmode-code, if needed.   | —                   |
| date-posting      | datetime            | Date of posting, if different from date of transaction.   | —                   |

## 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 |
|--------------------|---------------------|---|---------------------|
| last-seen          | datetime            | Last time this URL has been seen  | ✓                   |
| scheme             | text                | Scheme ['http', 'https', 'ftp', 'gopher', 'sip']  | ✓                   |
| url                | url                 | Full URL  | —                   |
| domain             | domain              | Full domain   | —                   |
| host               | hostname            | Full hostname   | —                   |
| first-seen         | datetime            | First time this URL has been seen   | ✓                   |
| tld                | text                | Top-Level Domain  | ✓                   |
| text               | text                | Description of the URL  | —                   |
| query_string       | text                | Query (after path, preceded by '?')   | —                   |
| port               | port                | Port number   | ✓                   |
| fragment           | text                | Fragment identifier is a short string of characters that refers to a resource that is subordinate to another, primary resource. | —                   |
| domain_without_tld | text                | Domain without Top-Level Domain   | —                   |
| subdomain          | text                | Subdomain   | ✓                   |
| resource_path      | text                | Path (between hostname:port and query)  | —                   |



| Object attribute | MISP attribute type | Description                     | Disable correlation |
|------------------|---------------------|---------------------------------|---------------------|
| credential       | text                | Credential (username, password) | —                   |

## 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 |
|------------------|---------------------|---|---------------------|
| user             | target-user         | The username(s) of the user targeted.   | —                   |
| node             | target-machine      | Name(s) of node that was targeted.  | —                   |
| ip-address       | ip-dst              | IP address(es) of the node targeted.  | —                   |
| email            | target-email        | The email address(es) of the user targeted.   | —                   |
| description      | text                | Description of the victim   | —                   |
| regions          | target-location     | The list of regions or locations from the victim targeted. ISO 3166 should be used. | —                   |

| Object attribute | MISP attribute type | Description   | Disable correlation |
|------------------|---------------------|---|---------------------|
| sectors          | text                | The list of sectors that the victim belong to ['agriculture', 'aerospace', 'automotive', 'communications', 'construction', 'defence', 'education', 'energy', 'engineering', 'entertainment', 'financial services', 'government national', 'government regional', 'government local', 'government public services', 'healthcare', 'hospitality leisure', 'infrastructure', 'insurance', 'manufacturing', 'mining', 'non profit', 'pharmaceuticals', 'retail', 'technology', 'telecommunications', 'transportation', 'utilities'] | —                   |
| external         | target-external     | External target organisations affected by this attack.  | —                   |
| name             | target-org          | The name of the department(s) or organisation(s) targeted.  | —                   |
| classification   | text                | The type of entity being targeted. ['individual', 'group', 'organization', 'class', 'unknown']  | ✓                   |
| roles            | text                | The list of roles targeted within the victim.   | —                   |

# virustotal-report

VirusTotal report.



virustotal-report is a MISP object available in JSON format at [this location](#). The JSON format can be freely reused in your application or automatically enabled in [MISP](#).

| Object attribute | MISP attribute type | Description                  | Disable correlation |
|------------------|---------------------|------------------------------|---------------------|
| community-score  | text                | Community Score              | ✓                   |
| permalink        | link                | Permalink Reference          | —                   |
| last-submission  | datetime            | Last Submission              | —                   |
| first-submission | datetime            | First Submission             | —                   |
| comment          | text                | Comment related to this hash | —                   |
| detection-ratio  | text                | Detection Ratio              | ✓                   |

# vulnerability

Vulnerability object describing a common vulnerability enumeration which can describe 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 |
|------------------|---------------------|--|---------------------|
| text             | text                | Description of the vulnerability   | —                   |
| id               | vulnerability       | Vulnerability ID (generally CVE, but not necessarily). The id is not required as the object itself has an UUID and the CVE id can updated later. | —                   |

| Object attribute         | MISP attribute type | Description   | Disable correlation |
|--------------------------|---------------------|---|---------------------|
| references               | link                | External references   | —                   |
| modified                 | datetime            | Last modification date  | ✓                   |
| created                  | datetime            | First time when the vulnerability was discovered  | ✓                   |
| published                | datetime            | Initial publication date  | ✓                   |
| 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'] | ✓                   |
| summary                  | text                | Summary of the vulnerability  | —                   |
| vulnerable_configuration | text                | The vulnerable configuration is described in CPE format   | —                   |

## 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 |
|------------------|---------------------|-------------------------------|---------------------|
| expiration-date  | datetime            | Expiration of the whois entry | ✓                   |

| Object attribute  | MISP attribute type    | Description                         | Disable correlation |
|-------------------|------------------------|-------------------------------------|---------------------|
| domain            | domain                 | Domain of the whois entry           | –                   |
| creation-date     | datetime               | Initial creation of the whois entry | ✓                   |
| registrant-phone  | whois-registrant-phone | Registrant phone number             | –                   |
| registrant-org    | whois-registrant-org   | Registrant organisation             | –                   |
| nameserver        | hostname               | Nameserver                          | ✓                   |
| registrar         | whois-registrar        | Registrar of the whois entry        | –                   |
| text              | text                   | Full whois entry                    | ✓                   |
| registrant-email  | whois-registrant-email | Registrant email address            | –                   |
| ip-address        | ip-src                 | IP address of the whois entry       | –                   |
| modification-date | datetime               | Last update of the whois entry      | ✓                   |
| registrant-name   | whois-registrant-name  | Registrant name                     | –                   |
| comment           | text                   | Comment of the whois entry          | –                   |

## 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 |
|------------------|---------------------|----------------|---------------------|
| is_ca            | boolean             | CA certificate | –                   |

| Object attribute        | MISP attribute type     | Description  | Disable correlation |
|-------------------------|-------------------------|--|---------------------|
| x509-fingerprint-md5    | x509-fingerprint-md5    | [Insecure] MD5 hash (128 bits)                     | —                   |
| pubkey-info-modulus     | text                    | Modulus of the public key                          | —                   |
| text                    | text                    | Free text description of the certificate           | —                   |
| x509-fingerprint-sha256 | x509-fingerprint-sha256 | Secure Hash Algorithm 2 (256 bits)                 | —                   |
| validity-not-after      | datetime                | Certificate invalid after that date                | —                   |
| pubkey-info-algorithm   | text                    | Algorithm of the public key                        | —                   |
| serial-number           | text                    | Serial number of the certificate                   | —                   |
| version                 | text                    | Version of the certificate                         | —                   |
| pem                     | text                    | Raw certificate in PEM format (Unix-like newlines) | —                   |
| subject                 | text                    | Subject of the certificate                         | —                   |
| pubkey-info-size        | text                    | Length of the public key (in bits)                 | —                   |
| pubkey-info-exponent    | text                    | Exponent of the public key                         | —                   |
| dns_names               | text                    | DNS names  | —                   |
| issuer                  | text                    | Issuer of the certificate                          | —                   |
| raw-base64              | text                    | Raw certificate base64 encoded (DER format)        | —                   |

| Object attribute      | MISP attribute type   | Description                                   | Disable correlation |
|-----------------------|-----------------------|---|---------------------|
| self_signed           | boolean               | Self-signed certificate                       | —                   |
| validity-not-before   | datetime              | Certificate invalid before that date          | —                   |
| x509-fingerprint-sha1 | x509-fingerprint-sha1 | [Insecure] Secure Hash Algorithm 1 (160 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 |
|------------------|---------------------|---|---------------------|
| yara-hunt        | yara                | Wide yara rule generated from -yh.  | ✓                   |
| yara             | yara                | Yara rule generated from -y.  | ✓                   |
| comment          | comment             | A description of Yara rule generated.                                     | —                   |
| whitelist        | comment             | Whitelist name used to generate the rules.                                | —                   |
| version          | comment             | yabin.py and regex.txt version used for the generation of the yara rules. | —                   |

## yara

An object describing a YARA rule 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 |
|------------------|---------------------|--|---------------------|
| yara             | yara                | YARA rule.   | —                   |
| comment          | comment             | A description of the YARA rule.  | —                   |
| context          | text                | Context where the YARA rule can be applied ['all', 'disk', 'memory', 'network']                | —                   |
| version          | text                | Version of the YARA rule depending where the yara rule is known to work as expected. ['3.7.1'] | —                   |

## Relationships

Default type of relationships in MISP objects.

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

| Name of relationship | Description  | Format               |
|----------------------|--|----------------------|
| derived-from         | The information in the target object is based on information from the source object. | ['misp', 'stix-2.0'] |
| duplicate-of         | The referenced source and target objects are semantically duplicates of each other.  | ['misp', 'stix-2.0'] |
| related-to           | The referenced source is related to the target object.                               | ['misp', 'stix-2.0'] |
| connected-to         | The referenced source is connected to the target object.                             | ['misp', 'stix-1.1'] |
| contains             | The references source is containing 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'] |



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

| <b>Name of relationship</b> | <b>Description</b>  | <b>Format</b> |
|-----------------------------|---|---------------|
| beacons-to                  | This relationship describes an object beacons to another object.  | ['misp']      |
| abuses                      | This relationship describes an object which abuses another object.  | ['misp']      |
| exfiltrates-to              | This relationship describes an object exfiltrating to another object.   | ['misp']      |
| identifies                  | This relationship describes an object which identifies another object.  | ['misp']      |
| intercepts                  | This relationship describes an object which intercepts another object.  | ['misp']      |
| calls                       | This relationship describes an object which calls another objects.  | ['misp']      |
| detected-as                 | This relationship describes an object which is detected as another object.  | ['misp']      |
| 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']      |
| preceding-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']      |
| 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']   |

| <b>Name of relationship</b>  | <b>Description</b>  | <b>Format</b> |
|------------------------------|---|---------------|
| 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']   |
| affiliated                   | This relationship describes an object which is affiliated with another object.                          | ['cert-eu']   |
| alleged-founder-of           | This relationship describes an object which is the alleged founder of another object.                   | ['cert-eu']   |
| attacking-other-group        | This relationship describes an object which attacks another object.                                     | ['cert-eu']   |
| belongs-to                   | This relationship describes an object which belongs to another object.                                  | ['cert-eu']   |
| business-relations           | This relationship describes an object which has business relations with another object.                 | ['cert-eu']   |
| claims-to-be-the-founder-of  | This relationship describes an object which claims to be the founder of another object.                 | ['cert-eu']   |
| cooperates-with              | This relationship describes an object which cooperates with another object.                             | ['cert-eu']   |
| former-member-of             | This relationship describes an object which is a former member of another object.                       | ['cert-eu']   |
| successor-of                 | This relationship describes an object which is a successor of another object.                           | ['cert-eu']   |
| has-joined                   | This relationship describes an object which has joined another object.                                  | ['cert-eu']   |
| member-of                    | This relationship describes an object which is a member of another object.                              | ['cert-eu']   |

| <b>Name of relationship</b> | <b>Description</b>   | <b>Format</b> |
|-----------------------------|--|---------------|
| 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']   |
| 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']   |

| Name of relationship | Description   | Format      |
|----------------------|---|-------------|
| 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'] |
| released             | This relationship describes an object which release another object.                 | ['cert-eu'] |