### Types

* **md5**: You are encouraged to use filename|md5 instead. A checksum in md5 format, only use this if you don't know the correct filename
* **sha1**: You are encouraged to use filename|sha1 instead. A checksum in sha1 format, only use this if you don't know the correct filename
* **sha256**: You are encouraged to use filename|sha256 instead. A checksum in sha256 format, only use this if you don't know the correct filename
* **filename**: Filename
* **pdb**: Microsoft Program database (PDB) path information
* **filename|md5**: A filename and an md5 hash separated by a | (no spaces)
* **filename|sha1**: A filename and an sha1 hash separated by a | (no spaces)
* **filename|sha256**: A filename and an sha256 hash separated by a | (no spaces)
* **ip-src**: A source IP address of the attacker
* **ip-dst**: A destination IP address of the attacker or C&C server. Also set the IDS flag on when this IP is hardcoded in malware
* **hostname**: A full host/dnsname of an attacker. Also set the IDS flag on when this hostname is hardcoded in malware
* **domain**: A domain name used in the malware. Use this instead of hostname when the upper domain is important or can be used to create links between events.
* **domain|ip**: A domain name and its IP address (as found in DNS lookup) separated by a | (no spaces)
* **email-src**: The email address (or domainname) used to send the malware.
* **email-dst**: A recipient email address that is not related to your constituency.
* **email-subject**: The subject of the email
* **email-attachment**: File name of the email attachment.
* **url**: url
* **http-method**: HTTP method used by the malware (e.g. POST, GET, ...).
* **user-agent**: The user-agent used by the malware in the HTTP request.
* **regkey**: Registry key or value
* **regkey|value**: Registry value + data separated by |
* **AS**: Autonomous system
* **snort**: An IDS rule in Snort rule-format. This rule will be automatically rewritten in the [NIDS](https://www.circl.lu/doc/misp/GLOSSARY.html#nids) exports.
* **pattern-in-file**: Pattern in file that identifies the malware
* **pattern-in-traffic**: Pattern in network traffic that identifies the malware
* **pattern-in-memory**: Pattern in memory dump that identifies the malware
* **yara**: Yara signature
* **vulnerability**: A reference to the vulnerability used in the exploit
* **attachment**: Please upload files using the *Upload Attachment* button.
* **malware-sample**: Please upload files using the *Upload Attachment* button.
* **link**: Link to an external information
* **comment**: Comment or description in a human language. This will not be correlated with other attributes
* **text**: Name, ID or a reference
* **other**: Other attribute
* **named pipe**: Named pipe, use the format .\pipe\
* **mutex**: Mutex, use the format \BaseNamedObjects\
* **target-user**: Attack Targets Username(s)
* **target-email**: Attack Targets Email(s)
* **target-machine**: Attack Targets Machine Name(s)
* **target-org**: Attack Targets Department or Organization(s)
* **target-location**: Attack Targets Physical Location(s)
* **target-external**: External Target Organizations Affected by this Attack
* **btc**: Bitcoin Address
* **iban**: International Bank Account Number
* **bic**: Bank Identifier Code Number
* **bank-account-nr**: Bank account number without any routing number
* **aba-rtn**: ABA routing transit number
* **bin**: Bank Identification Number
* **cc-number**: Credit-Card Number
* **prtn**: Premium-Rate Telephone Number
* **threat-actor**: A string identifying the threat actor
* **campaign-name**: Associated campaign name
* **campaign-id**: Associated campaign ID
* **malware-type**:
* **uri**: Uniform Resource Identifier
* **authentihash**: You are encouraged to use filename|authentihash instead. Authenticode executable signature hash, only use this if you don't know the correct filename
* **ssdeep**: You are encouraged to use filename|ssdeep instead. A checksum in the SSDeep format, only use this if you don't know the correct filename
* **imphash**: You are encouraged to use filename|imphash instead. A hash created based on the imports in the sample, only use this if you don't know the correct filename
* **pehash**: PEhash - a hash calculated based of certain pieces of a PE executable file
* **sha224**: You are encouraged to use filename|sha224 instead. A checksum in sha224 format, only use this if you don't know the correct filename
* **sha384**: You are encouraged to use filename|sha384 instead. A checksum in sha384 format, only use this if you don't know the correct filename
* **sha512**: You are encouraged to use filename|sha512 instead. A checksum in sha512 format, only use this if you don't know the correct filename
* **sha512/224**: You are encouraged to use filename|sha512/224 instead. A checksum in sha512/224 format, only use this if you don't know the correct filename
* **sha512/256**: You are encouraged to use filename|sha512/256 instead. A checksum in sha512/256 format, only use this if you don't know the correct filename
* **tlsh**: You are encouraged to use filename|tlsh instead. A checksum in the Trend Micro Locality Sensitive Hash format, only use this if you don't know the correct filename
* **filename|authentihash**: A checksum in md5 format
* **filename|ssdeep**: A checksum in ssdeep format
* **filename|imphash**: Import hash - a hash created based on the imports in the sample.
* **filename|pehash**: A filename and a PEhash separated by a |
* **filename|sha224**: A filename and a sha-224 hash separated by a |
* **filename|sha384**: A filename and a sha-384 hash separated by a |
* **filename|sha512**: A filename and a sha-512 hash separated by a |
* **filename|sha512/224**: A filename and a sha-512/224 hash separated by a |
* **filename|sha512/256**: A filename and a sha-512/256 hash separated by a |
* **filename|tlsh**: A filename and a Trend Micro Locality Sensitive Hash separated by a |
* **windows-scheduled-task**: A scheduled task in windows
* **windows-service-name**: A windows service name. This is the name used internally by windows. Not to be confused with the windows-service-displayname.
* **windows-service-displayname**: A windows service's displayname, not to be confused with the windows-service-name. This is the name that applications will generally display as the service's name in applications.
* **whois-registrant-email**: The e-mail of a domain's registrant, obtained from the WHOIS information.
* **whois-registrant-phone**: The phone number of a domain's registrant, obtained from the WHOIS information.
* **whois-registrant-name**: The name of a domain's registrant, obtained from the WHOIS information.
* **whois-registrar**: The registrar of the domain, obtained from the WHOIS information.
* **whois-creation-date**: The date of domain's creation, obtained from the WHOIS information.
* **x509-fingerprint-sha1**: X509 fingerprint in SHA-1 format
* **dns-soa-email**: RFC1035 mandates that DNS zones should have a SOA (Statement Of Authority) record that contains an email address where a PoC for the domain could be contacted. This can sometimes be used for attribution/linkage between different domains even if protected by whois privacy
* **size-in-bytes**: Size expressed in bytes
* **counter**: An integer counter, generally to be used in objects
* **datetime**: Datetime in the ISO 8601 format
* **cpe**: Common platform enumeration
* **port**: Port number
* **ip-dst|port**: IP destination and port number seperated by a |
* **ip-src|port**: IP source and port number seperated by a |
* **hostname|port**: Hostname and port number seperated by a |
* **email-dst-display-name**: Email destination display name
* **email-src-display-name**: Email source display name
* **email-header**: Email header
* **email-reply-to**: Email reply to header
* **email-x-mailer**: Email x-mailer header
* **email-mime-boundary**: The email mime boundary separating parts in a multipart email
* **email-thread-index**: The email thread index header
* **email-message-id**:
* **github-username**: A github user name
* **github-repository**: A github repository
* **github-organisation**: A github organisation
* **jabber-id**: Jabber ID
* **twitter-id**: Twitter ID
* **first-name**: First name of a natural person
* **middle-name**: Middle name of a natural person
* **last-name**: Last name of a natural person
* **date-of-birth**: Date of birth of a natural person (in YYYY-MM-DD format)
* **place-of-birth**: Place of birth of a natural person
* **gender**: The gender of a natural person (Male, Female, Other, Prefer not to say)
* **passport-number**: The passport number of a natural person
* **passport-country**: The country in which the passport was issued
* **passport-expiration**: The expiration date of a passport
* **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
* **nationality**: The nationality of a natural person
* **visa-number**: Visa number
* **issue-date-of-the-visa**: The date on which the visa was issued
* **primary-residence**: The primary residence of a natural person
* **country-of-residence**: The country of residence of a natural person
* **special-service-request**: A Special Service Request is a function to an airline to provide a particular facility for A Passenger or passengers.
* **frequent-flyer-number**: The frequent flyer number of a passenger
* **travel-details**: Travel details
* **payment-details**: Payment details
* **place-port-of-original-embarkation**: The orignal port of embarkation
* **place-port-of-clearance**: The port of clearance
* **place-port-of-onward-foreign-destination**: A Port where the passenger is transiting to
* **passenger-name-record-locator-number**: The Passenger Name Record Locator is a key under which the reservation for a trip is stored in the system. The PNR contains, among other data, the name, flight segments and address of the passenger. It is defined by a combination of five or six letters and numbers.
* **mobile-application-id**: The application id of a mobile application