ThreatFox | Data exposed through Real Time Intelligence Feed v. publicly available data

ThreatFox provides context-rich signal from abuse.ch, sharing indicators of compromise (IOCs) associated with malware.

Users can access this data via the Real Time Intelligence Feed, or via publicly available APIs. These access methods provide different metadata outputs, as highlighted in this document.

The Real Time Intelligence Feed is the only access method to receive all observed threat signals.

Metadata field	Metadata description	Real Time Feed	Publicly available data
IOC additions			
`_idx`	Is an integer representing the incremental number of the message.	✓	✗
`_ts`	Is the Unix timestamp, indicating when the message was received by the real time infrastructure.	✓	✓*
`uuid`	Is an internal, unique identifier for the message. This is the property that should be used to dedupe the incoming flows where necessary.	✓	✗
`type`	Defines the type of message. It's always 'ioc_addition'.	✓	✓
`id`	Is the ThreatFox ID of the IOC. You can also use this ID to craft the link to see the entry on the ThreatFox platform (https:// threatfox.abuse.ch/ioc/id/).	✓	✓
`ioc`	Is the IOC (value).	✓	✓
`ioc_type`	Is the type of the IOC (example: ip:port). A list of possible values is available through the API: https://threatfox.abuse.ch/api/#types	✓	✓
`confidence_level`	Is the confidence level of this IOC (set by the reporter). The value is between 0 and 100.	✓	✓
`threat_type`	Is the type of threat - a list of possible values is available through the API: https://threatfox.abuse.ch/api/#types	✓	✓
`threat_type_ description`	Is a short description, human-readable description, of `threat_type`.	✓	✓*
`malware`	Is the malware family (using the Malpedia naming scheme).	✓	✓*
`malware_printable`	Printable name of malware family (Malpedia)	✓	✓
`malware_alias`	Malware aliases (Malpedia)	✓	✓
`sightings`	Indicates how many times this IOC has been reported/observed.	✓	✗
`anonymous`	Boolean that indicates whether the submitter or this IOC wants to remain anonymous or not.	✓	✓
`reporter`	Is the abuse.ch handle of the submitter of this file (or 'null').	✓	✓
`reward`	List of rewards (credits) the reporter received from other users for this submission	✓	✓*
`tags`	Is a List of tags associated with this file. A list of current tags is available through the API: https://threatfox.abuse.ch/api/#tag-list	✓	✓
`reference`	Reference (URL)	✓	✓
`comment`	Is a human-readable string comment from the reporter on this IOC.	✓	✓
IOC changes			
`_idx`	Is an integer representing the incremental number of the message.	✓	✗
`_ts`	Is the Unix timestamp, indicating when the message was received by the real time infrastructure.	✓	✗
`uuid`	Is an internal, unique identifier for the message. This is the property that should be used to dedupe the incoming flows where necessary.	✓	✗
`type`	Defines the type of message. It's always 'ioc_change'.	✓	✗
`id`	Is the ThreatFox ID of the IOC. You can also use this ID to craft the link to see the entry on the ThreatFox platform (https:// threatfox.abuse.ch/ioc/id/).	✓	✗
`ioc`	Is The IOC (value).	✓	✗
`ioc_type`	This is the type of the IOC (example: ip:port). A list of possible values is available through the API: https://threatfox.abuse.ch/api/#types	✓	✗
`threat_type`	This is the threat type. A list of possible values is available through the API: https://threatfox.abuse.ch/api/#types	✓	✗
`threat_type_ description`	This is a short description, human-readable, of threat_type.	✓	✗
`field`	Shows the affected field where the change occurred.	✓	✗
`value`	Is the new value of the affected field.	✓	✗
`action`	Is an enumerated field that describes the action. May contain `add`, `remove`, `change`.	✓	✗
IOC removal			
`_idx`	Is an integer representing the incremental number of the message.	✓	✗
`_ts`	Is the Unix timestamp, indicating when the message was received by the real time infrastructure.	✓	✗
`uuid`	Is an internal, unique identifier for the message. This is the property that should be used to dedupe the incoming flows where necessary.	✓	✗
`type`	Defines the type of message. It's always 'file_removal'.	✓	✗
`id`	Is the ThreatFox ID of the IOC. You can also use this ID to craft the link to see the entry on the ThreatFox platform (https:// threatfox.abuse.ch/ioc/id/).	✓	✗
`ioc`	Is the IOC (value).	✓	✗
`ioc_type`	This is the type of the IOC (example: ip:port). A list of possible values is available through the API: https://threatfox.abuse.ch/api/#types	✓	✗
`threat_type`	This is the threat type. A list of possible values is available through the API: https://threatfox.abuse.ch/api/#types	✓	✗
`threat_type_ description`	This is a short description, human-readable, of `threat_type`.	✓	✗
`removal_note`	Is a string containing any removal note.	✓	✗

*** Comparable data for this field is provided via publicly available data, however the field names are not an exact match.**
If you require the comparable field name, please speak with your Spamhaus contact.