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

Feodo Tracker rovides context-rich signal from abuse.ch, sharing botnet C&C infrastructure associated with major malware threats that facilitate ransomware attacks. This data helps network owners to protect their users.

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
Observed C2s			
`_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 'observed_c2'.	✓	✓
`ip_address`	Is the IPv4 or IPv6 address of the botnet C2.	✓	✓ *
`port`	Is the port of the botnet C2.	✓	✓ *
`protocol`	Is the protocol the botnet C2 uses.	✓	✓ *
`malware_malpedia`	Is the malware family associated with this botnet C2 (using the Malpedia naming scheme).	✓	✓
`as_number`	Is the Autonomous System (AS) number associated with the botnet C2 (ip_address).	✓	✓
`as_name`	Is the AS name associated with the botnet C2.	✓	✓
`country`	Is the geo-located country of the botnet C2 (two-letter country code).	✓	✓
`first_seen`	Is the Unix timestamp when this botnet C2 has been observed for the first time.	✓	✓ *
`first_seen`	Is the Unix timestamp when this botnet C2 has been (re-)validated by Feodo Tracker last time.	✓	✓ *
`last_online`	Is the Unix timestamp when this botnet C2 has been seen active (online) for the last time.	✓	✓ *
C2 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 'c2_removal'.	✓	✗
`ip_address`	Is the IPv4 of the botnet C2.	✓	✗
`port`	Is the port of the botnet C2.	✓	✗
`protocol`	Is the protocol the botnet C2 uses.	✓	✗
`malware_malpedia`	Is the malware family associated with this botnet C2 (using the Malpedia naming scheme).	✓	✗
`removal_note`	Contains the reason why the botnet C2 has been removed.	✓	✗

*** 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.