

# ThreatQuotient



## **abuse.ch CDF User Guide**

**Version 1.7.0**

June 03, 2025

### **ThreatQuotient**

20130 Lakeview Center Plaza Suite 400  
Ashburn, VA 20147

 **ThreatQ Supported**

### **Support**

Email: [support@threatq.com](mailto:support@threatq.com)

Web: [support.threatq.com](https://support.threatq.com)

Phone: 703.574.9893

# Contents

Warning and Disclaimer .....	3
Support .....	4
Integration Details.....	5
Introduction .....	6
Installation.....	7
Configuration .....	8
All Feeds .....	8
URLhaus Plain-Text URL List Feed .....	8
URLhaus Database Dump Feed .....	9
<b>ThreatQ Mapping.....</b>	<b>10</b>
Feodo Tracker Botnet C2 IP Blocklist .....	10
SSLBL SSL Blacklist.....	11
URLhaus Database Dump.....	12
URLhaus Plain-Text URL List.....	13
URLhaus Response Policy Zones .....	14
<b>Average Feed Run.....</b>	<b>15</b>
Feodo Tracker Botnet C2 IP Blocklist .....	15
SSLBL SSL Blacklist.....	15
URLhaus Database Dump.....	15
URLhaus Plain-Text URL List.....	16
URLhaus Response Policy Zones .....	16
<b>Known Issues / Limitations .....</b>	<b>16</b>
<b>Change Log .....</b>	<b>18</b>

# Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Copyright © 2025 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

# Support

This integration is designated as **ThreatQ Supported**.

**Support Email:** [support@threatq.com](mailto:support@threatq.com)

**Support Web:** <https://support.threatq.com>

**Support Phone:** 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.



ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

# Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.7.0
Compatible with ThreatQ Versions	>= 5.29.0
Support Tier	ThreatQ Supported

# Introduction

abuse.ch provides community driven threat intelligence on cyber threats. It is the home of a couple of projects that help internet service providers and network operators protect their infrastructure from malware. IT-Security researchers, vendors and law enforcement agencies rely on data from abuse.ch to make the internet a safer place.

Feodo Tracker is a project of abuse.ch with the goal of sharing botnet C&C servers associated with the Feodo malware family (Dridex, Emotet/Heodo). It offers various blocklists helping network owners to protect their users from Dridex and Emotet/Heodo.

- **Feodo Tracker Botnet C2 IP Blocklist** - <https://feodotracker.abuse.ch/downloads/ipblocklist.csv>

The SSL Blacklist (SSLBL) is a project of abuse.ch with the goal of detecting malicious SSL connections, by identifying and blacklisting SSL certificates used by botnet C&C servers. In addition, SSLBL identifies JA3 fingerprints that helps you to detect block malware botnet C&C communication on the TCP layer.

Feeds included:

- **SSLBL SSL Blacklist** - <https://sslbl.abuse.ch/blacklist/sslblacklist.csv>

abuse.ch URLHaus ingests threat intelligence data from feeds published by abuse.ch vendor. Feeds included:

- **URLhaus Database Dump** - <https://urlhaus.abuse.ch/downloads/csv/>
- **URLhaus Response Policy Zones** - <https://urlhaus.abuse.ch/downloads/rpz/>
- **URLhaus Plain-Text URL List** - [https://urlhaus.abuse.ch/downloads/text\\_recent/](https://urlhaus.abuse.ch/downloads/text_recent/)
- **URLhaus Plain-Text URL List Recent** - [https://urlhaus.abuse.ch/downloads/text\\_recent/](https://urlhaus.abuse.ch/downloads/text_recent/)



In order to run the **URLhaus Plain-Text URL List Recent** feed, the user will need to run the **URLhaus Plain-Text URL List** feed and select the option Recent Data from the **Feed URL** parameter.

The Abuse.ch Feeds integration ingests Indicators and Indicator Attribute types into the ThreatQ Platform.

# Installation

Perform the following steps to install the integration:



The same steps can be used to upgrade the integration to a new version.

1. Log into <https://marketplace.threatq.com/>.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
  - Drag and drop the file into the dialog box
  - Select **Click to Browse** to locate the integration file on your local machine



ThreatQ will inform you if the feed already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the feed contains changes to the user configuration. The new user configurations will overwrite the existing ones for the feed and will require user confirmation before proceeding.

6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

You will still need to [configure and then enable](#) the feed.

# Configuration



ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:


1. Navigate to your integrations management page in ThreatQ.
2. Select the **OSINT** option from the *Category* dropdown (optional).
3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

## All Feeds

PARAMETER	DESCRIPTION
Auth Key	Enter your abuse.ch authentication key.
Enable SSL Certificate Verification	Enable this for the feed to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the feed should not honor proxies set in the ThreatQ UI.

## URLhaus Plain-Text URL List Feed

PARAMETER	DESCRIPTION
Dump Type	Use the dropdown to select whether to ingest all data or the most recent. Options include: <b>All Data</b> - Ingest all the data <b>Recent Data</b> - Data from the last 30 days.



In order to run the **URLhaus Plain-Text URL List Recent** feed, the user will need to run the **URLhaus Plain-Text URL List** feed and select the option **Recent Data** from the **Feed URL** parameter.



## URLhaus Database Dump Feed

PARAMETER	DESCRIPTION
Only Ingest New Indicators	Enabling this parameter will filter out indicators that are not new since the last time the feed ran.
Only Ingest Online Indicators	Enabling this parameter will filter out indicators that have a status of <b>offline</b> .
Context Selection	Select which pieces of context to ingest into ThreatQ with each indicator: URL Haus ID, URL Status, Threat Type, URLHaus Tag, URLHaus Link

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

# ThreatQ Mapping

## Feodo Tracker Botnet C2 IP Blocklist

GET <https://feodotracker.abuse.ch/downloads/ipblocklist.csv>

CSV response sample:

```
"2021-01-17 07:30:05","67.213.75.205","443","offline","2021-02-04","Dridex"
"2021-01-17 07:44:46","192.73.238.101","443","online","2021-02-04","Dridex"
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
1 (second token)	Indicator.Value	IP Address	0 (first token)	74.58.188.22	N/A
2 (third token)	Indicator.Attribute	Destination Port	0 (first token)	8080	N/A
3 (fourth token)	Indicator.Attribute	C2 Status	0 (first token)	online	N/A
4 (sixth token)	Indicator.Attribute	Malware Type	0 (first token)	Dridex	N/A

## SSLBL SSL Blacklist

GET <https://sslbl.abuse.ch/blacklist/sslblacklist.csv>

CSV response sample:

```
2019-01-21 10:08:50,b8e3ed1bb59bac1a0d18725e751a7b43b462df59,Malware C&C
2019-01-21 09:21:38,f10c6f69a0252454792fc3cbcd7f0e7bab3bb2b,Malware C&C
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
1 (second token)	Indicator.Value	SHA-1	0 (first token)	b8e3ed1bb59bac1a0d18725e751a7b43b462df59	N/A
2 (third token)	Indicator.Attribute	Malware Family	0 (first token)	Malware C&C	N/A

# URLhaus Database Dump

GET <https://urlhaus.abuse.ch/downloads/csv/>

CSV response sample extracted from ZIP archive:

```
"107221","2019-01-22 12:38:12","http://rest-tv.top/administrator/cache/ssj.jpg","online","malware_download","exe","https://urlhaus.abuse.ch/url/107221/"
"107230","2019-01-22 12:58:02","http://velerosa.it/wp-admin/css/Payment_details/012019/","online","malware_download","doc,emotet,epoch1","https://urlhaus.abuse.ch/url/107230/"
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
0 (first token)	Indicator.Attribute	URL Haus ID	1 (second token)	107221	N/A
2 (third token)	Indicator.Value	URL	1 (second token)	<a href="http://rest-tv.top/administrator/cache/ssj.jpg">http://rest-tv.top/administrator/cache/ssj.jpg</a>	N/A
3 (fourth token)	Indicator.Attribute	URL Status	1 (second token)	online	N/A
4 (fifth token)	Indicator.Attribute	Threat Type	1 (second token)	malware_download	N/A
5 (sixth token)	Indicator.Attribute	URLHaus Tags	1 (second token)	exe	N/A
6 (seventh token)	Indicator.Attribute	URLHaus Link	1 (second token)	<a href="https://urlhaus.abuse.ch/url/107221/">https://urlhaus.abuse.ch/url/107221/</a>	N/A

# URLhaus Plain-Text URL List

## All Data Configuration Option:

GET <https://urlhaus.abuse.ch/downloads/text/>

## Recent Data Configuration Option (last 30 days):

GET [https://urlhaus.abuse.ch/downloads/text\\_recent/](https://urlhaus.abuse.ch/downloads/text_recent/)

CSV response sample:

<http://yayasansumurmuslim.org/wp-content/themes/ace-corporate/js/sserv.jpg>

[http://velerosa.it/wp-admin/css/Payment\\_details/012019/](http://velerosa.it/wp-admin/css/Payment_details/012019/)

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
0 (first token)	Indicator.Value	URL	N/A	<a href="http://yayasansumurmuslim.org/wp-content/themes/ace-corporate/js/sserv.jpg">http://yayasansumurmuslim.org/wp-content/themes/ace-corporate/js/sserv.jpg</a>	N/A

# URLhaus Response Policy Zones

GET <https://urlhaus.abuse.ch/downloads/rpz/>

RPZ response sample:

```
0qixri.thule.su CNAME . ; Malware download (2019-01-17), see https://
urlhaus.abuse.ch/host/0qixri.thule.su/
188mbnews.com CNAME . ; Malware download (2018-12-30), see https://
urlhaus.abuse.ch/host/188mbnews.com/
```

ThreatQ provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
0 (first token)	Indicator	FQDN	1 (second token)	0qixri.thule.su	Text " CNAME . ; Malware download (" is stripped from the FQDN
2 (third token)	Indicator.Attribute	URL	1 (second token)	<a href="https://urlhaus.abuse.ch/host/0qixri.thule.su">https://urlhaus.abuse.ch/host/0qixri.thule.su</a>	Text "), see " is stripped from the URL

# Average Feed Run



Object counts and Feed runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed runtime may vary based on system resources and load.

## Feodo Tracker Botnet C2 IP Blocklist

METRIC	RESULT
Run Time	1 minutes
Indicators	326
Indicator Attributes	987

## SSLBL SSL Blacklist

METRIC	RESULT
Run Time	4 minutes
Indicators	3,737
Indicator Attributes	3,737

## URLhaus Database Dump

METRIC	RESULT
Run Time	28 hours

METRIC	RESULT
Indicators	949,860
Indicator Attributes	7,539,856

## URLhaus Plain-Text URL List

METRIC	RESULT
Run Time	9.5 hours
Indicators	947,573
Indicator Attributes	1,521,759

## URLhaus Response Policy Zones

METRIC	RESULT
Run Time	1 minute
Indicators	1,050
Indicator Attributes	1,050

## Known Issues / Limitations

### URLhaus Database Dump

- This feed brings back a very large (~170MB) list of URLhaus data. As a result, Feed Runs for this feed take a longer time. You should configure URLhaus Database Dump to pull data on a daily basis or consider disabling it after a successful run and re-enabling it sparingly.

### URLhaus Plain-Text URL List



- 
- This feed brings back a large (~11MB) list of URLhaus URLs when the All Data user field value is selected, as a result the execution of this feed can take a longer time. To prevent long run times, one can select the Recent Data user field option which only brings the most recent data (last 30 days) from URLhaus.

# Change Log

- **Version 1.7.0**
  - Added support for authenticating with the API.
  - Removed deprecated feeds: abuse.ch SSLBL Response Policy Zones (RPZ) and abuse.ch SSLBL IP Blacklist
  - Changed Minimum ThreatQ version to 5.29.
  - Introduced a new design for user fields.
  - Added the option to to enable SSL certificate verification and/or disable proxies.
  - Added a **Context Selection** configuration option for abuse.ch URLhaus Database Dump.
- **Version 1.6.0**
  - Added the following new configuration parameters:
    - **Only Ingest New Indicators** - filter out indicators that are not new since the last time the feed ran.
    - **Only Ingest Online Indicators** - filter out indicators that have a status of offline.
  - Updated the **URLHAUS Tags** attribute name to **URLHAUS Tag**.
- **Version 1.5.1**
  - Updated the URLhaus Plain-Text URL List feed default behavior to fetch recent data.
- **Version 1.5.0**
  - Added new parameter for the URLhaus Plain-Text URL List. You can now select to bring in **All Data** or **Recent Data** (last 30 days).
- **Version 1.4.0**
  - Fixed a bug with abuse.ch Feodo Tracker Botnet C2 IP Blocklist that caused an "Error creating objects from threat data" exception to be raised
  - Added a new C2 Status attribute to abuse.ch Feodo Tracker Botnet C2 IP Blocklist
  - Removed the now defunct abuse.ch Feodo Tracker Malware Hashes feed
  - Updated abuse.ch SSLBL Response Policy Zones (RPZ) in order to support `.rpz-ip` indicators in addition to the previously supported `.sslb1-rpz` indicators. Also, added logic to reverse the reverse IP-lookup format supplied by Abuse.