ThreatQuotient

Abuse.ch Feeds Guide

Version 1.5.0

September 28, 2021

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

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.

Support

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

Support Email: 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.

Versioning

- Current integration version: `1.5.0`
- Supported on ThreatQ versions >= `4.33.0`

Introduction

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

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
- SSLBL SSL IP Blacklist
- SSLBL Response Policy Zones (RPZ)

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

- URLhaus Database Dump
- URLhaus Response Policy Zones
- URLhaus Plain-Text URL List
- URLhaus Plain-Text URL List Recent

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).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration to open its details page.
4. Enter the following parameter under the **Configuration** tab:

   All Feeds Except URLhaus Plain-Text URL List Feed

PARAMETER	DESCRIPTION
Feed URL	Display only field that denotes the abuse.ch endpoint hit by the feed. Changing this user field in the UI will **not** affect feed behavior.

   URLhaus Plain-Text URL List Feed

PARAMETER	DESCRIPTION
Feed URL	Use the dropdown to select whether to ingest all data or the most recent. Options include: • **All Data** - Ingest all the data • **Recent Data** - Data from the last 30 days.

5. Review the **Settings** configuration, 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 Response Policy Zones (RPZ)

```
GET https://sslbl.abuse.ch/blacklist/sslbl.rpz
```

RPZ response sample:

```
32.122.2.149.77.rpz-ip CNAME . ; AsyncRAT C&C, see https://sslbl.abuse.ch/browse/
32.149.162.59.139.rpz-ip CNAME . ; BuerLoader C&C, see https://sslbl.abuse.ch/browse/
```

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	IP Address	0 (first token)	77.149.2.122	Text ".rpz-ip CNAME . ;" is stripped from the IP Address. The reverse IP lookup, eg "32.122.2.149.77", is reversed and the final octet is dropped (e.g., 32).
1 (second token)	Indicator.Attribute	Malware Family	0 (first token)	AsyncRAT C&C	Text ", see https://sslbl.abuse.ch/browse/" is stripped from the Malware Family

SSLBL IP Blacklist

`GET https://sslbl.abuse.ch/blacklist/sslipblacklist.csv`

CSV response sample:

```
2019-01-21 23:21:15,46.183.223.10,7650
2019-01-21 20:15:06,185.244.30.121,4379
```

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)	46.183.223.10	N/A
2 (third token)	Indicator.Attribute	Destination Port	0 (first token)	7650	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,f10c6f69a0252454792fc3cbcdd7f0e7bab3bb2b,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)	http://rest-tv.top/administrator/cache/ssj.jpg	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)	https://urlhaus.abuse.ch/url/107221/	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/
```

CSV response sample:

```
http://yayasansumurmuslim.org/wp-content/themes/ace-corporate/js/sserv.jpg
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	http://yayasansumurmuslim.org/wp-content/themes/ace-corporate/js/sserv.jpg	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)	https://urlhaus.abuse.ch/host/0qixri.thule.su	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 Response Policy Zones (RPZ)

METRIC	RESULT
Run Time	< 1 minute
Indicators	104
Indicator Attributes	108

SSLBL IP Blacklist

METRIC	RESULT
Run Time	< 1 minute
Indicators	106
Indicator Attributes	106

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
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 1.5.0**
  - 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 `.sslbl-rpz` indicators. Also, added logic to reverse the reverse IP-lookup format supplied by Abuse.