ThreatQuotient

Abuse.ch Feeds Implementation Guide

Version 1.3.1

Tuesday, February 18, 2020

ThreatQuotient

11400 Commerce Park Dr., Suite 200

Reston, VA 20191

Support

Email: support@threatq.com

Web: support.threatq.com

Phone: 703.574.9893

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.

Last Updated: Tuesday, February 18, 2020

Contents

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
- Feodo Tracker Malware Hashes

SSLBL: 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.

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

abuse.ch URLHaus ingests threat intelligence data from three feeds published by abuse.ch vendor. The three feeds are:

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

Versioning

- Current integration version `1.3.1`
- Supported on ThreatQ versions >= `4.15.0`

Installation

The abuse.ch feeds are automatically installed when you upgrade your ThreatQ instance to version 4.30 or later. You can also install the abuse.ch feeds using the ThreatQ UI - see the steps below.

Perform the following steps to install the feeds:

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

1. Log into https://marketplace.threatq.com/.
2. Locate and download the **abuse.ch** feeds file.
3. Navigate to your ThreatQ instance.
4. Click on the **Settings** icon and select **Incoming feeds**.
5. Click on the **Add New Feed** button.
6. Upload the feed file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the feed 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.

The feeds will be added to the **OSINT** tab for Incoming Feeds. 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 feed-related credentials.

To configure the feed:

1. Click on the **Settings** icon and select **Incoming Feeds**.
2. Locate the feed under the **OSINT** tab.
3. Click on the **Feed Settings** link for the feed.
4. Select your desired settings under the **Connection** tab.
5. Click on **Save Changes**.
6. Click on the toggle switch to the left of each feed name to enable the feed.

ThreatQ Mapping

Feodo Tracker Botnet C2 IP Blocklist

This is in csv format. Example:

```
2019-01-21 12:11:05,74.58.188.22,8080,Heodo
2019-01-21 12:10:42,114.79.134.49,80,Heodo
2019-01-21 12:10:37,50.99.132.7,465,Heodo
2019-01-21 12:10:11,83.110.212.100,443,Heodo
```

The mapping table is below.

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Normalization	Published Date	Examples
1 (second token)	Indicator	IP Address		0 (first token)	74.58.188.22
2 (third token)	Indicator Attribute	Destination Port		0 (first token)	8080
3 (fourth token)	Indicator Attribute	Malware Type		0 (first token)	Heodo

Feodo Tracker Malware Hashes

This is in csv format. Example:

```
2019-01-21 15:08:23,e8974e0386f256bb4dc003fe55d195f2,Heodo
2019-01-21 15:08:22,bcd2fa4f4d4289ca0a7996d07f163824,Heodo
2019-01-21 15:08:22,c84b714d090df882fb0f120b6d1f37f0,Heodo
```

The mapping table is below.

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Normalization	Published Date	Examples
1 (second token)	Indicator	MD5		0 (first token)	e8974e0386f256bb4dc003fe55d195f2
2 (third token)	Indicator Attribute	Malware Type		0 (first token)	Heodo

SSLBL SSL Blacklist

This is in csv format. Example:

```
2019-01-21 10:08:50,b8e3ed1b-
b59bac1a0d18725e751a7b43b462df59,Malware C&C
2019-01-21 09:21:38,f10c6f69a0252454792fc3cb-
cdd7f0e7bab3bb2b,Malware C&C
2019-01-20 09:50:10,5c19c-
c1f79f68f542a5f31349b48798310c9f1e4,Gozi C&C
```

The mapping table is below.

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Normalization	Published Date	Examples
1 (second token)	Indicator	SHA-1		0 (first token)	b8e3ed1bb59bac1a0d18725e751a7b43b462df59
2 (third token)	Indicator Attribute	Malware Family		0 (first token)	Malware C&C

SSLBL IP Blacklist

This is in csv format. Example:

```
2019-01-21 23:21:15,46.183.223.10,7650
2019-01-21 20:15:06,185.244.30.121,4379
2019-01-21 17:59:34,68.111.123.100,449
```

The mapping table is below.

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Normalization	Published Date	Examples
1 (second token)	Indicator	IP Address		0 (first token)	46.183.223.10
2 (third token)	Indicator Attribute	Destination Port		0 (first token)	7650

SSLBL Response Policy Zones (RPZ)

This is in rpz format. Example:

```
10.223.183.46.sslbl-rpz CNAME . ; Adwind C&C, see
https://sslbl.abuse.ch/browse/
121.30.244.185.sslbl-rpz CNAME . ; Adwind C&C, see
https://sslbl.abuse.ch/browse/
100.123.111.68.sslbl-rpz CNAME . ; TrickBot C&C, see
https://sslbl.abuse.ch/browse/
```

The mapping table is below.

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Normalization	Published Date	Examples
1 (second token)	Indicator	IP Address		0 (first token)	10.223.183.46
2 (third token)	Indicator Attribute	Malware Family		0 (first token)	TrickBot C&C

URLhaus Database Dump

This is in csv format. Example:

```
"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/"
```

The mapping table is below.

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Normalization	Published Date	Examples
0 (first token)	Indicator Attribute	URL Haus ID		1 (second token)	107221
2 (third token)	Indicator	URL		1 (second token)	http://rest-tv.top/administrator/cache/ssj.jpg
3 (fourth token)	Indicator Attribute	URL Status		1 (second token)	online
4 (fifth token)	Indicator Attribute	Threat Type		1 (second token)	malware_download
5 (sixth token)	Indicator Attribute	URLHaus Tags		1 (second token)	exe
6 (seventh token)	Indicator Attribute	URLHaus Link		1 (second token)	https://urlhaus.abuse.ch/url/107221/

URLhaus Response Policy Zones

It has the following format:

```
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/
```

The mapping table is below.

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Normalization	Published Date	Examples
0 (first token)	Indicator	FQDN		1 (second token)	0qixri.thule.su
2 (third token)	Indicator	URL		1 (second token)	https://urlhaus.abuse.ch/host/0qixri.thule.su

URLhaus Plain-Text URL List

This is a list. Example:

```
http://yayasansumurmuslim.org/wp-content/themes/ace-corporate/js/sserv.jpg
http://velerosa.it/wp-admin/css/Payment_details/012019/
```

The mapping table is below.

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Normalization	Published Date	Examples
0 (first token)	Indicator	URL			http://yayasansumurmuslim.org/wp-content/themes/ace-corporate/js/sserv.jpg