ThreatQuotient

Spamhaus Don't Route or Peer List (DROP) Guide

Version 1.0.1

Friday, August 7, 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: Friday, August 7, 2020

Contents

Versioning

- Current integration version: `1.0.1`
- Supported on ThreatQ versions >= `4.3.0`

Introduction

The Spamhaus Don't Route Or Peer List (DROP) feed allows a user to ingest CIDR Block indicators from netblocks allocated directly by an established Regional Internet Registry (RIR) or National Internet Registry (NIR) that are "hijacked" or leased by professional spam or cyber-crime operations (used for dissemination of malware, trojan downloaders, botnet controllers).

Installation

Perform the following steps to install the feed:

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 **Spamhaus Don't Route or Peer List (Drop)** integration 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. Review the configuration under the **Settings** tab and make any updates as needed.
5. Click on **Save Changes**.
6. Click on the toggle switch to the left of the feed name to enable the feed.

ThreatQ Mapping

Spamhaus DROP List

```
GET http://www.spamhaus.org/drop/drop.txt
```

Text response sample:

```
; Spamhaus DROP List 2020/07/30 - (c) 2020 The Spamhaus Pro-
ject
; https://www.spamhaus.org/drop/drop.txt
; Last-Modified: Sat, 25 Jul 2020 08:39:55 GMT
; Expires: Thu, 30 Jul 2020 16:52:29 GMT
1.10.16.0/20 ; SBL256894
1.19.0.0/16 ; SBL434604
1.32.128.0/18 ; SBL286275
2.56.255.0/24 ; SBL444288
2.59.200.0/22 ; SBL463003
5.134.128.0/19 ; SBL270738
5.183.60.0/22 ; SBL463004
5.188.10.0/23 ; SBL402741
23.92.80.0/20 ; SBL372561
23.239.64.0/19 ; SBL372562
24.233.0.0/19 ; SBL210084
27.126.160.0/20 ; SBL257064
27.146.0.0/16 ; SBL326434
36.0.8.0/21 ; SBL225949
36.37.48.0/20 ; SBL258006
36.116.0.0/16 ; SBL303895
36.119.0.0/16 ; SBL303894
```

```
37.252.220.0/22 ; SBL461634
41.77.240.0/21 ; SBL478585
41.93.128.0/17 ; SBL464277
```

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	CIDR Block	N/A	223.254.0.0/16	
1 (second token)	Indicator.Attribute	SBL ID	N/A	SBL212803	
1 (second token)	Indicator.Attribute	SBL Link	N/A	https://www.spamhaus.org/sbl/query/SBL212803	The base url `https://www.spamhaus.org/sbl/query/` is always prepended to the second token value

Spamhaus EDROP List

Spamhaus Extended DROP List (EDROP) is an extension of the DROP list that includes suballocated netblocks controlled by spammers or cyber criminals.

```
GET http://www.spamhaus.org/drop/edrop.txt
```

Text response sample:

```
; Spamhaus EDROP List 2020/07/30 - (c) 2020 The Spamhaus Pro-
ject
; https://www.spamhaus.org/drop/edrop.txt
; Last-Modified: Sat, 04 Jul 2020 01:32:55 GMT
; Expires: Fri, 31 Jul 2020 15:00:38 GMT
5.188.11.0/24 ; SBL402809
27.112.32.0/19 ; SBL237955
31.184.237.0/24 ; SBL419884
37.9.42.0/24 ; SBL394633
38.39.160.0/20 ; SBL460585
42.140.0.0/17 ; SBL253830
43.57.0.0/16 ; SBL271294
43.181.0.0/16 ; SBL271295
45.190.220.0/24 ; SBL487277
46.148.112.0/24 ; SBL394634
46.148.120.0/24 ; SBL394635
46.148.127.0/24 ; SBL394636
58.2.0.0/17 ; SBL249532
59.254.0.0/15 ; SBL230802
62.112.16.0/21 ; SBL237227
```

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	CIDR Block	N/A	62.112.16.0/21	
1 (second token)	Indicator.Attribute	SBL ID	N/A	SBL230802	
1 (second token)	Indicator.Attribute	SBL Link	N/A	https://www.spamhaus.org/sbl/query/SBL230802	The base url `https://www.spamhaus.org/sbl/query/` is always prepended to the second token value

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.

Spamhaus DROP List

Metric	Result
Run Time	1 minute
Indicators	777
Indicator Attributes	1554

Spamhaus EDROP List

Metric	Result
Run Time	1 minute
Indicators	87
Indicator Attributes	178

Change Log

- **Version 1.0.1**
  - Updated yaml with `namespace` and `category` fields.
- **Version 1.0.0**
  - Initial release.