ThreatQuotient

DomainTools COVID-19 Threat List Feed Guide

Version 1.0.0

Tuesday, June 2, 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, June 2, 2020

Contents

Versioning

- Current integration version: `1.0.0`
- Supported on ThreatQ versions >= `4.30.0`

Introduction

DomainTools is providing a free, curated list of high-risk COVID-19-related domains to support the community during the Coronavirus crisis. The list will be updated daily and is available as a gzipped CSV file.

For more information, see: https://www.domaintools.com/resources/blog/free-covid-19-threat-list-domain-risk-assessments-for-coronavirus-threats

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 **DomainTools COVID-19 Threat List** 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. Under the **Connection** tab, enter the following configuration parameters:

Parameter	Description
Feed URL	This parameter is for display purposes only.

5. Click on **Save Changes**.
6. Click on the toggle switch to the left of the feed name to enable the feed.

ThreatQ Mapping

DomainTools COVID-19

DomainTools provides the list of COVID-19 related domains as a gzipped tab-delimited CSV file:

```
covid19medicinaintegral.com     2020-04-19      99
covid19renaissance.info        2020-04-19      99
2020quarantine.info    2020-04-19      99
ncov24h.live   2020-04-19      99
thecovid-19.site       2020-04-19      99
```

ThreatQ provides the following default mapping for this feed:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
First Token	Indicator	FQDN	Second Token	covid19medicinaintegral.com	
Second Token	Indicator.Attribute	First Seen	Second Token	2020-04-19	Converted to a timestamp

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
Third Token	Indicator.Attribute	Risk Score	Second Token	99	
N/A	Indicator.Attribute	COVID-19 Malicious Activity	Second Token	Suspected	Hard-coded value; allows searching of all COVID-19 threats

Average Feed Run

Run Time	Indicators	Indicators Attributes
160 minutes	148,829	446,487
Object counts and Feed run time are supplied as generalities only - objects returned by a provider can differ based on credential configurations and Feed run time may vary based on system resources and load.		

Change Log

- **Version 1.0.0**
  - Initial Release