ThreatQuotient

Mr.Looquer IOC Feed Guide

Version 1.0.0

Thursday, June 4, 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: Thursday, June 4, 2020

Contents

Versioning

- Current integration version: `1.0.0`
- Supported on ThreatQ versions >= `4.34.0`

Introduction

Mr.Looquer has created the first threat feed focused on systems with dual stack. Since IPv6 protocol has begun to be part of malware and fraud communications, it is necessary to detect and mitigate the threats in both protocols (IPv4 and IPv6). The threat feed is analyzed and generated daily.

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 **Mr.Looquer IOC** 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 field is for display purposes only.

5. Click on **Save Changes**.
6. Click on the toggle switch next to the feed name to enable it.

ThreatQ Mapping

Mr.Looquer IOCFeed

```
GET https://iocfeed.mrlooquer.com/feed.json
```

JSON response sample:


```
[
   {
      "ip4" : "145.14.145.239",
      "ip4Asn" : "204915",
      "subcategory" : "phishing",
      "category" : "fraud",
      "ip6Asn" : "204915",
      "ip6Portlist" :
         [
            80,
            32768,
            443,
            8080,
            32767
         ],
      "ip4Portlist" :
         [
            443,
            80,
            2049,
            32768,
            8080,
```

```
            32767
         ],
      "ip6" : "2a02:4780:dead:c893::1",
      "dualstak" : true,
      "ip4NumCve" : 0,
      "ip6NumCve" : 0,
      "twin_config" : false,
      "lastSeen" : "05/14/20-03:11",
      "domain" : "hortatory-headsets.000webhostapp.com",
      "ip6Prefix" : "2a02:4780:dead:c893::",
      "type" : "bulkphishing"
   },
   ...
]
```

ThreatQ provides the following default mapping for this feed:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.[].ip4	Indicator	IP Address	.[].lastSeen	145.14.145.239	Indicators created for .[].domain, .[].ip4Asn, .[].ip6 and .[].ip6Asn are related
.[].ip4Asn	Attribute	ASN	.[].lastSeen	204915	N/A
.[].ip4Portlist	Attribute	Port	.[].lastSeen	443	Only applied to IP Address Indicators
.[].ip6	Indicator	IPv6 Address	.[].lastSeen	2a02:4780:dead:c893::1	Indicators created for .[].domain, .[].ip4, .[].ip4Asn, and .[].ip6Asn are related
.[].ip6Prefix	Attribute	Prefix	.[].lastSeen	2a02:4780:dead:c893::	Only applied to IPv6 Address Indicators
.[].ip6Asn	Attribute	ASN	.[].lastSeen	204915	N/A
.[].ip6Portlist	Attribute	Port	.[].lastSeen	32767	Only applied to IPv6 Address Indicators

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.[].domain	Indicator	FQDN	.[].lastSeen	hortatory-head-sets.000webhostapp.com	Indicators created for .[].domain, .[].ip4, .[].ip4Asn, .[].ip6 and .[].ip6Asn are related
.[].type	Attribute	Type	.[].lastSeen	bulkphishing	Applied to all objects
.[].sub-category	Attribute	Subcategory	.[].lastSeen	phishing	Applied to all objects
.[].category	Attribute	Category	.[].lastSeen	fraud	Applied to all objects
.[].dualstak	Attribute	Dualstak	.[].lastSeen	False	Applied to all objects
.[].twin_config	Attribute	Twin Config	.[].lastSeen	True	Applied to all objects
.[].lastSeen	N/A	N/A	N/A	05/14/20-03:11	Publish date for all objects and attributes

Average Feed Run

Average Feed Run results for Mr.Looquer IOCFeed:

Metric	Result
Run Time	24 minutes
Indicators	5754
Indicator Attributes	67466

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