ThreatQuotient

Intel 471 Indicators - Malware Intelligence Guide

Version 1.1.0

Monday, September 28, 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: Monday, September 28, 2020

Contents

Intel 471 Indicators - Malware Intelligence Guide 1

Warning and Disclaimer 2

Contents 3

Versioning 4

Introduction 5

Installation 6

Configuration 7

ThreatQ Mapping 8

Intel471 Indicators - Malware Intelligence 8

Change Log 15

Versioning

- Current integration version: `1.1.0`
- Supported on ThreatQ versions >= `4.37.0`

Introduction

The Intel 471 Indicators - Malware Intelligence feed returns a list of Indicators that match filter criteria.

Malware Intelligence is a different product from Intel 471 to adversary intelligence.

Intel 471 Indicators - Malware Intelligence ingests threat intelligence data from the following endpoint:

- `https://api.intel471.com/v1/indicators`

Notes:

- Uses basic HTTP authentication based on email address and API key.

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 **Intel 471 Indicators Malware** 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 **Commercial** 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 **Commercial** tab.
3. Click on the **Feed Settings** link for the feed.
4. Under the **Connection** tab, enter the following configuration parameters:

Parameter	Description
Indicator Type	Search indicators by type (file, ipv4, url). If no types are selected for this parameter, all types will be returned.
Email Address	Intel 471 account email address.
API Key	Intel 471 account API key.
Count	Maximum number of records to retrieve from the provider per request.

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

ThreatQ Mapping

Intel471 Indicators - Malware Intelligence

'GET https://api.intel471.com/v1/indicators'

JSON response sample:


```
{
    "indicatorTotalCount": 224181,
    "indicators": [
        {
            "data": {
                "indicator_id": "c8c1385ee0411410463b-
b39a8a944c2ec7025d09",
                "threat": {
                    "type": "malware",
                    "uid": "b38ef686caf0103866339452d3d1c4fb",
                    "data": {
                        "malware_family_profile_uid": "b38e-
f686caf0103866339452d3d1c4fb",
                        "family": "dridex"
                    }
                },
                "expiration": 1622192350000,
                "confidence": "medium",
                "context": {
                    "description": "plugin downloaded by dri-
dex malware family"
                },
```

```
                "mitre_tactics": "stage_capabilities",
                "indicator_type": "file",
                "indicator_data": {
                    "file": {
                        "md5": "c444f89248e673d3b-
c22ed125c4ed162",
                        "sha1":
"c652139e29b209757d497e026bfc187ef3bfadc7",
                        "sha256": "cd7b-
c57e2d614137de1594ac0b04004b936797f0e5b402ace3e75a7138e61370",
                        "type": "PEDLL_x86",
                        "size": 382976,
                        "download_url": "https://ap-
i.in-
tel471.-
com/v1/-
down-
load/mal-
wareIn-
tel/cd7b-
c57e2d614137de1594ac0b04004b936797f0e5b402ace3e75a7138e61370.z-
ip"
                    }
                },
                "intel_requirements": [
                    "1.3.4",
                    "1.1.4"
                ]
            },
```

```
            "meta": {
                "version": "0.1"
            },
            "last_updated": 1590656362056,
            "uid": "b366979d1abdedf51f985fe03d0fc19e",
            "activity": {
                "first": 1590503428000,
                "last": 1590656350000
            }
        }
    ]
}
```

ThreatQ provides the following default mapping for this feed:

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.indicators[].data.threat.type	Indicator.Attribute	Malware Type	.indicators[].data.activity.first	malware	
.indicators[].data.threat.uid	Indicator.Attribute	Threat UID	.indicators[].data.activity.first	b38ef686caf01038 66339452d3d1c4fb	
.indicators[].data.-threat.data.malware_family_profile_uid	Indicator.Attribute	Malware Family Profile UID	.indicators[].data.activity.first	b38ef686caf010386 6339452d3d1c4fb	
.indicators[].data.-threat.data.family	Indicator.Attribute	Malware Family	.indicators[].data.activity.first	dridex	
.indicators[].data.expiration	Indicator.Attribute	Expires At	.indicators[].data.activity.first	1622712015000	
.indicators[].data.confidence	Indicator.Attribute	Confidence	.indicators[].data.activity.first	medium	
.indicators[].data.-	Indicator.Description	N/A	.indicators	plugin downloaded by	

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
context.description			[].data.activity.first	dridex malware family	
.indicators[].data.mitre_tactics	Indicator.Attribute	MITRE Tactics	.indicators [].data.activity.first	stage_capabilities	
.indicators[].data.indicator_data.file.md5	Indicator.Value	MD5	.indicators [].data.activity.first	05f7722289b1b8a7 7b77a15ba192adb8	Indicator from type File
.indicators[].data.indicator_data.file.sha1	Indicator.Value	SHA-1	.indicators [].data.activity.first	1b38f9ae60d1cb05 9f15139c5c6919f14 503bca9	Indicator from type File
.indicators[].data.indicator_data.file.sha256	Indicator.Value	SHA-256	.indicators [].data.activity.first	3ce665e28a462697 3d252af6d1a6d969 f378e2d9aaf120c0f8 62061fd6384b5e	Indicator from type File
.indicators[].data.indicator_data.url	Indicator.Value	URL	.indicators [].data.activity.first	http://mailchristen.at	Indicator from type URL
.indicators[].data.indicator_data.address	Indicator.Value	IP Address	.indicators [].data.activity.first	54.38.22.65	Indicator from type IPv4

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.indicators[].data.intel_requirements	Indicator.Attribute	Intelligence Requirement	.indicators[].data.activity.first	1.3.4	
.indicators[].data.-meta.version	Indicator.Attribute	Document Version	.indicators[].data.activity.first	0.1	
.indicators[].data.last_updated	Indicator.Attribute	Last Updated At	.indicators[].data.activity.first	1591176018215	
.indicators[].data.uid	Indicator.Attribute	Indicator UID	.indicators[].data.activity.first	55464586356a9bde14b86e5488673620	
.indicators[].data.activity.first	Indicator.Attribute	Active Period First	.indicators[].data.activity.first	1591172700000	
.indicators[].data.activity.last	Indicator.Attribute	Active Period Last	.indicators[].data.activity.first	1591176015000	
.indicators[].data.indicator_data.file.download_url	Indicator.Attribute	Download URL	.indicators[].data.activity.first	https://api.intel471.com/v1/download/malware Intel/3ce665e28a4626	This attribute is only for MD5, SHA-1 and SHA-

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
				973d252af6d1a6d969f378e2d9aaf120c0f862061fd6384b5e.zip	256
.indicators[].data.indicator_data.file.type	Indicator.Attribute	File Type	.indicators[].data.activity.first	PEDLL_x86	This attribute is only for MD5, SHA-1 and SHA-256
.indicators[].data.indicator_data.file.size	Indicator.Attribute	File Size	.indicators[].data.activity.first	382976	This attribute is only for MD5, SHA-1 and SHA-256

Change Log

- **Version 1.1.0**
  - Added the option to ingest all indicator types at once. The Indicator Type configuration parameter no longer requires the user to select a specific type. If no types are selected for this parameter, all types will be returned.
- **Version 1.0.0**
  - Initial Release