ThreatQuotient

Intel 471 Indicators - Malware Intelligence Guide

Version 1.1.1

December 15, 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.

Contents

Versioning

- Current integration version: `1.1.1`
- Supported on ThreatQ versions >= `4.41.0`

Introduction

The Intel 471 Indicators - Malware Intelligence integration returns a list of indicators that match filter criteria from the following endpoint:

- Intel 471 Indicator - Malware Intelligence

> Users should be using ThreatQ version 4.41 or later to upgrade to this integration version.

Notes

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

Installation

Perform the following steps to install the integration:

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

1. Log into https://marketplace.threatq.com/.
2. Locate and download the integration file.
3. Navigate to the My Integrations page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the integration 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.
6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

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. Navigate to the My Integrations page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Email Address	Your Intel 471 account email address.
API Key	Your Intel 471 account API key.
Indicator Type	Search indicators by type (file, ipv4, url). > If no option is selected, all indicator types are queried.
Count	The maximum number of records to retrieve from the provider per request.

5. Review the **Settings** configuration, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

Intel 471 Indicators - Malware Intelligence

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

JSON response sample:


```
{
    "indicatorTotalCount": 224181,
    "indicators": [
        {
            "data": {
                "indicator_id": "c8c1385ee0411410463bb39a8a944c2ec7025d09",
                "threat": {
                    "type": "malware",
                    "uid": "b38ef686caf0103866339452d3d1c4fb",
                    "data": {
                        "malware_family_profile_uid": "b38ef686caf0103866339452d3d1c4fb",
                        "family": "dridex"
                    }
                },
                "expiration": 1622192350000,
                "confidence": "medium",
                "context": {
                    "description": "plugin downloaded by dridex malware family"
                },
                "mitre_tactics": "stage_capabilities",
                "indicator_type": "file",
                "indicator_data": {
                    "file": {
                        "md5": "c444f89248e673d3bc22ed125c4ed162",
                        "sha1": "c652139e29b209757d497e026bfc187ef3bfadc7",
                        "sha256": "cd7bc57e2d614137de1594ac0b04004b936797f0e5b402ace3e75a7138e61370",
                        "type": "PEDLL_x86",
                        "size": 382976,
                        "download_url": "https://api.intel471.com/v1/download/malwareIntel/
cd7bc57e2d614137de1594ac0b04004b936797f0e5b402ace3e75a7138e61370.zip"
                    }
                },
                "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	b38ef686ca f010386633 9452d3d1c4 fb	
.indicators[].data.threat.data. malware_family_profile_uid	Indicator.Attribute	Malware Family Profile UID	.indicators[].data.activity.first	b38ef686caf0 10386633945 2d3d1c4fb	
.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	16227120150 00	
.indicators[].data.confidence	Indicator.Attribute	Confidence	.indicators[].data.activity.first	medium	
.indicators[].data.context. description	Indicator.Description	N/A	.indicators[].data.activity.first	plugin downloaded by 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 f378e2d9aaf120c0f 862061fd6384b5e	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
.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	55464586356a9bde 14b86e5488673620	
.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/m	This attribute is

FEED DATA	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
				alwareIntel/3ce665e2 8a4626973d252af6d1 a6d969f378e2d9aaf12 0c0f862061fd6384b5e.zip	only for MD5, SHA-1 and SHA-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

Average Feed Run

METRIC	RESULT
Run Time	3 minutes
Indicators	983
Indicator Attributes	16,304

Feed runtime is 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. The values from this run were based on the indicator type File with a count of 10.

Change Log

- **Version 1.1.1**
  - Fixed an issue with the feed name.
- **Version 1.1.0**
  - Added ability to ingest all indicator types at once.
- **Version 1.0.0**
  - Initial release.