ThreatQuotient

Intel 471 Malware Intelligence CDF Guide

Version 1.1.0

August 08, 2022

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

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.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ⚠ ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.1.0
Compatible with ThreatQ Versions	>= 4.21.0
Support Tier	ThreatQ Supported
ThreatQ Marketplace	https://marketplace.threatq.com/details/intel471-malware-intelligence

Introduction

Malware Intelligence Reports provides analysis of malware families and features, network traffic, how to identify, detect and decode it, extract and parse its configuration, control server(s) encryption key and campaign IDYARA Rules and IDS Signatures to accurately identify the identification and detection of malware families, malicious network traffic and improve detection systems. ThreatQ integration Brings Malware Reports with associated IOCs and Signatures all in with a 1-click experience

Intel471 Malware Feed ingests threat intelligence data from the following endpoints:

- **Malware Reports** - `https://api.intel471.com/v1/malwareReports`
- **Malware Indicators** - `https://api.intel471.com/v1/indicators/stream`
- **Malware Signatures** - `https://api.intel471.com/v1/yara`

Important Notes

- An email address and API key are used for HTTP basic authentication.
- Time constrained data fetching is possible.

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 integrations management 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 integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **OSINT/Commercial/Labs** 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 entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Email Address	Your Intel471 Account email address.
API Key	Your Intel471 Account API key.
Count	The maximum number of records that can be returned per response from the provider. The default setting is 10. > This only affects the Malware Reports and Malware Signatures feeds. The Malware Indicators feed is hardcoded with a value of 100.

5. Review any additional settings, 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

Malware Reports

High-level summary of what info the feed does

`GET https://api.intel471.com/v1/malwareReports`

Sample Response:


```
{
    "malwareReportTotalCount": 14,
    "malwareReports": [
        {
            "data": {
                "threat": {
                    "uid": "d972018da6adf284cce963c2552df80b",
                    "type": "malware",
                    "data": {
                        "family": "bokbot",
                        "malware_family_profile_uid": "d972018da6adf284cce963c2552df80b"
                    }
                },
                "malware_report_data": {
                    "text": "foo <div>bar</div>",
                    "released_at": 1566552377000,
                    "title": "BokBot - The evolution of Vawtrak",
                    "version": "1.8"
                }
            },
            "meta": {
                "version": "0.1"
            },
            "last_updated": 1566748352307,
            "uid": "1a36e81e75c363d4cb7022f007e1182b",
            "activity": {
                "first": 1566550742000,
                "last": 1566552377000
            }
        }
    ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.data.malware_report_data.title	report.value	Report Title	"BokBot - The evolution of Vawtrak"	
.data.malware_report_data.text	report.description	Report Description	"foo bar "	*
.uid	report.attribute	UID	"1a36e81e75c363d4cb7022f007e1182b"	
.last_updated	report.attribute	Modified At	1566748352307	formatted
.data.threat.uid	report.attribute	Threat UID	"d972018da6adf284cce963c2552df80b"	
.data.threat.type	report.attribute	Threat Type	"malware"	
.data.threat.data.family	report.attribute	Malware Family	"bokbot"	
.data.threat.data.malware_family_profile_uid	report.attribute	Malware Family Profile ID	"d972018da6adf284cce963c2552df80b"	
.data.threat.data.version	report.attribute	Threat Version	"1.8"	
.data.malware_report_data.released_at	report.attribute	Released At	1566552377000	formatted
.meta.version	report.attribute	Document Version	"0.1"	
.activity.first	report.attribute	Active Period First	1566550742000	formatted
.activity.last	report.attribute	Active Period Last	1566552377000	formatted
.data.malware_report_data.released_at	report.published_at	N/A	1566552377000	formatted

***** Stripped tags, trimmed to first paragraph, added link for full description.

Malware Indicators

High-level summary of what info the feed does

`GET https://api.intel471.com/v1/indicators/stream`

Sample Response:


```
{
    "indicatorTotalCount": 102158,
    "indicators": [
        {
            "data": {
                "confidence": "medium",
                "expiration": 1572707778000,
                "context": {
                    "description": "danabot exfiltration URL"
                },
                "threat": {
                    "uid": "0e3263ebcdc7611ae808f82e58353ac5",
                    "type": "malware",
                    "data": {
                        "family": "danabot",
                        "malware_family_profile_uid": "0e3263ebcdc7611ae808f82e58353ac5"
                    }
                },
                "mitre_tactics": "command_and_control",
                "intel_requirements": [
                    "1.1.4",
                    "1.1.16"
                ],
                "indicator_type": "url",
                "indicator_data": {
                    "url": "tcp://195.123.246.209:443"
                }
            },
            "meta": {
                "version": "0.1"
            },
            "last_updated": 1570115782701,
            "uid": "428f4c3517ffd31e65ad240d2a7dc37c",
            "activity": {
                "first": 1565902923000,
                "last": 1570115778000
            }
        },
        {
            "data": {
                "confidence": "high",
                "expiration": 1601723409000,
                "context": {
                    "description": "sample of vidar malware family"
                },
                "threat": {
                    "uid": "bcf1b5b912722362f2f928f5a32e2272",
                    "type": "malware",
```

```
                    "data": {
                        "family": "vidar",
                        "malware_family_profile_uid": "22594e13276480dd456a8441babc227b",
                        "version": "13.6"
                    }
                },
                "mitre_tactics": "command_and_control",
                "intel_requirements": [
                    "1.1.5",
                    "1.1.6"
                ],
                "indicator_type": "file",
                "indicator_data": {
                    "file": {
                        "md5": "d4b9734b3f06ce112f88e2f7d88e3513",
                        "sha1": "d0400b8ef915d633dc6f3db0878d4c3ae3f8eaaa",
                        "sha256": "900a568f4e95dd8d7e93707a214e43a76653b17aea43fc3a7adf4ae89668efea",
                        "download_url": "https://api.intel471.com/v1/download/malwareIntel/
900a568f4e95dd8d7e93707a214e43a76653b17aea43fc3a7adf4ae89668efea.zip"
                    }
                }
            },
            "meta": {
                "version": "0.1"
            },
            "last_updated": 1570187418736,
            "uid": "de38abab91098b99072fc5b10ad279e2",
            "activity": {
                "first": 1570187409000,
                "last": 1570187409000
            }
        },
        {
            "data": {
                "confidence": "medium",
                "expiration": 1572779544000,
                "context": {
                    "description": "lokibot controller IPv4"
                },
                "threat": {
                    "uid": "22e7a5f41d4f3cc5c704758ffa505556",
                    "type": "malware",
                    "data": {
                        "family": "lokibot",
                        "malware_family_profile_uid": "20eb1f82621001883ea0c2085aff5729",
                        "version": "1.8"
                    }
                },
                "mitre_tactics": "command_and_control",
                "intel_requirements": [
                    "1.1.5",
                    "1.1.6"
                ],
                "indicator_type": "ipv4",
                "indicator_data": {
                    "address": "8.208.76.80"
                }
            },
            "meta": {
                "version": "0.1"
            },
```

```
            "last_updated": 1570187545255,
            "uid": "30b5c9b5e16179132f0369d8b6f74738",
            "activity": {
                "first": 1569808002000,
                "last": 1570187544000
            }
        }
    ]
}
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
.data.indicator_type	indicator.type	Indicator Type	"url" / "ipv4" / "file"	*
.data.indicator_data	indicator.value	Indicator Value	* See note	*
.uid	indicator.attribute	Indicator UID	"048fe252afced217d487600349355bbc"	
.last_updated	indicator.attribute	Modified At	1556258716643	formatted
.data.threat.uid	indicator.attribute	Threat UID	"45c17dfa1b60fb295f377836da5454c5"	
.data.threat.type	indicator.attribute	Threat Type	"malware"	
.data.threat.data.family	indicator.attribute	Malware Family	"arkei"	
.data.threat.data.malware_family_profile_uid	indicator.attribute	Malware Family Profile ID	"45c17dfa1b60fb295f377836da5454c5"	
.data.threat.data.version	indicator.attribute	Threat Version	"1.8"	
.meta.version	indicator.attribute	Document Version	"0.1"	
.activity.first	indicator.attribute	Active Period First	1566550742000	formatted
.activity.last	indicator.attribute	Active Period Last	1566552377000	formatted
.data.confidence	indicator.attribute	Confidence	"high"	
.data.intel_requirements	indicator.attribute	Intelligence Requirement	["1.1.5","1.1.6"]	
.data.expiration	indicator.attribute	Expires At	1572779544000	formatted
.data.context.description	indicator.attribute	Description	"lokibot controller IPv4"	
.data.mitre_tactics	indicator.attribute	Mitre Tactics	"command_and_control"	
[see note 4]	indicator.attribute	Released At	1566552377000	formatted
[see note 4]	indicator.published_at	N/A	1566552377000	formatted

* If .data.indicator_type == 'ipv4', the value of the indicator will be equal to .data.indicator_data.address (8.208.76.80) and the type of the indicator will be "IP Address"

* If .data.indicator_type == 'url', the value of the indicator will be equal to .data.indicator_data.url (tcp://195.123.246.209:443) and the type of the indicator will be "URL"

* If .data.indicator_type == 'file', 3 indicators will be added with types 'MD5','SHA-1','SHA-256' and the value of the indicators will be extracted from .value.file.md5/sha1/sha256

** The 'Released At' attribute and the indicator.published_at values are fetched from the '.data.malware_report_data.released_at' value of the Malware Reports feed response.

Malware Signatures

`GET https://api.intel471.com/v1/yara`

Sample Response:


```
{
    "yaraTotalCount": 3,
    "yaras": [
        {
            "data": {
                "confidence": "high",
                "yara_data": {
                    "title": "arkei",
                    "signature": "rule arkei\n{\n  meta: \n    author = \"Intel 471\"\n  strings:\n    $config = \"/
server/grubConfig\" fullword ascii\n    $gate = \"/server/gate\" fullword ascii\n    $arkei = \"Arkei\"\n
$filezilla1 = \"\\\\files\\\\filezilla_recentservers.xml\" fullword\n    $filezilla2 = \"\\\\files\\\
\filezilla_sitemanager.xml\" fullword\n    $info_log = \"files\\\\information.log\"\n    $passwords_log = \"files\\\
\passwords.log\" fullword wide\n    $stats1 = \"MachineID: %s\"\n    $stats2 = \"Windows Username: %s\"\n    $stats3
= \"Videocard: %s\" \n    $desktop = \"Desktop.zip\"\n    $ipgeo1 = \"http://ip-api.com/line/?fields=countryCode\"
fullword wide\n    $ipgeo2 = \"http://ip-api.com/line/?fields=query\" fullword wide\n\n  condition:\n    uint16(0) ==
0x5a4d and (all of them)\n}\n"
                },
                "threat": {
                    "data": {
                        "family": "arkei",
                        "malware_family_profile_uid": "45c17dfa1b60fb295f377836da5454c5"
                    },
                    "type": "malware",
                    "uid": "45c17dfa1b60fb295f377836da5454c5",
                    "version": "1.6"
                },
                "intel_requirements": [
                    "1.1.5",
                    "1.1.6"
                ]
            },
            "meta": {
                "version": "0.1"
            },
            "last_updated": 1556258716643,
            "uid": "048fe252afced217d487600349355bbc",
            "activity": {
                "first": 1550066320000,
                "last": 1550066320000
            }
        }
    ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	EXAMPLES	NOTES
-	signature.type	Signature Type	"YARA"	
.data.yara_data.title	signature.name	Signature Name	"arkei"	
.data.yara_data.signature	signature.value	Signature Value	"rule arkei\n{\n meta: \n author = ..."	
.uid	signature.attribute	Signature UID	"048fe252afced217d487600349355bbc"	
.last_updated	signature.attribute	Modified At	1556258716643	formatted
.data.threat.uid	signature.attribute	Threat UID	"45c17dfa1b60fb295f377836da5454c5"	
.data.threat.type	signature.attribute	Threat Type	"malware"	
.data.threat.data.family	signature.attribute	Malware Family	"arkei"	
.data.threat.data.malware_family_profile_uid	signature.attribute	Malware Family Profile ID	"45c17dfa1b60fb295f377836da5454c5"	
.data.threat.data.version	signature.attribute	Threat Version	"1.6"	
.meta.version	signature.attribute	Document Version	"0.1"	
.activity.first	signature.attribute	Active Period First	1566550742000	formatted
.activity.last	signature.attribute	Active Period Last	1566552377000	formatted
.data.confidence	signature.attribute	Confidence	"high"	
.data.intel_requirements	signature.attribute	Intelligence Requirement	["1.1.5","1.1.6"]	
[see note 1]	signature.attribute	Released At*	1566552377000	formatted
[see note 1]	signature.published_at	N/A	1566552377000	formatted

* The 'Released At' attribute and the signature.published_at values are fetched from the '.data.malware_report_data.released_at' value of the Malware Reports feed response.

Change Log

- **Version 1.1.0**
  - Updated the **Malware Indicators** supplemental feed endpoint to use the streaming API.
- **Version 1.0.2**
  - N/A
- **Version 1.0.1**
  - N/A