

ThreatQuotient



Intel 471 Malware Intelligence Feed Implementation Guide

Version 1.0.1

Monday, November 18, 2019

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.

Copyright © 2019 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

Last Updated: Monday, November 18, 2019

Contents

Intel 471 Malware Intelligence Feed Implementation Guide	1
Warning and Disclaimer	2
Contents	3
Versioning	4
Introduction	4
Prerequisites	5
Installation	6
ThreatQ Mapping	7
Malware Reports	7
Malware Indicators	10
Malware Signatures	18

Versioning

- Current integration version `1.0.0`
- Supported on ThreatQ versions `>= 4.21.0`

Introduction

The Intel 471 Malware Intelligence feed ingests threat intelligence data from the following endpoints:

- **Intel 471 Malware Reports** - <https://api.intel471.com/v1/malwareReports>
- **Intel 471 Malware Indicators** - <https://api.intel471.com/v1/indicators>
- **Intel 471 Malware Signatures** - <https://api.intel471.com/v1/yara>

Notes:

- An email address and API key are used for HTTP basic authentication.
- The number of pages requested per call is user configurable and affects all the endpoints (defaults to 10).
- Time constrained data fetching is possible.

Prerequisites

ThreatQ version 4.25 included the full STIX 2.0 object set. If you have not upgraded your ThreatQ instance to version 4.25 or later, Report objects (STIX 2.0 custom object) must be installed prior to running the feed.

The commands to install the custom objects are as follows:

1. `cd /var/www/api`
2. `sudo php artisan threatq:create-custom-objects`
3. `sudo php artisan threatq:make-object-set --
file=/var/www/api/database/seeds/data/custom_
objects/stix2_0.json`
4. `sudo php artisan up`

Installation

Complete the following steps to install the connector:

1. Log into <https://marketplace.threatq.com>.
2. Download the **Intel 471 yaml** file.
3. From the ThreatQ user interface, select the **Settings icon > Incoming Feeds**.
4. Click **Add New Feed**.
5. In the Add New Feed dialog box, complete one of the following actions:
 - Drag and drop the yaml file into the dialog box.
 - **Click to browse** to the yaml file and select it.

The connector installs as a feed on **Commercial** tab.

6. Under Intel 471 Malware Intelligence, click **Feed Settings**.



ThreatQuotient does not issue third-party credentials. Contact the specific vendor.

7. For Email Address, enter your Intel 471 email account.
8. For Password, enter your Intel 471 account password.
9. Enter a value for **Count**, which is maximum number of records that can be returned per response from the provider.
10. Click the toggle button next to Intel 471 Malware Intelligence to enable the feed.
11. Click **Save Changes**.

The feed will appear under the **Commercial** feeds heading.

ThreatQ Mapping

Intel 471 Malware Intelligence feed provides an API that users can use to programmatically extract data in JSON format. The response contains a list of reports, signatures, and indicators.

Malware Reports

Endpoint Example:

```
{
  "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
    }
}
]
```

ThreatQ provides the following default mapping for the connector:

Feed Data	ThreatQ Entity	Threat-Q 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"	*stripped tags
.uid	report.at-	UID		

Feed Data	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Examples	Notes
	tribute		"1a36e81e75c363d4cb7022f0-07e1182b"	
.last_updated	report.attribute	Modified At	1566748352307	formatted
.data.threat.uid	report.attribute	Threat UID	"d972018da6ad-f284cce963c2552df80b"	
.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	"d972018da6ad-f284cce963c2552df80b"	
.data.-threat.data.version	report.attribute	Threat Version	"1.8"	
.data.malware_report_data.re-	report.attribute	Releas-	1566552377000	formatted

Feed Data	ThreatQ Entity	Threat-Q Object Type or Attribute Key	Examples	Notes
leased_at		ed At		
.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



* The description field will return the first paragraph with the tagging stripped. A link to the report will be included.

Malware Indicators

Endpoint Example:

```
{
  "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": "0e3263e-
bcd7611ae808f82e58353ac5"
        }
      },
      "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":
"22594e13276480dd456a8441babbc227b",
          "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": "d0400b8e-
f915d633dc6f3db0878d4c3ae3f8eaaa",
                "sha256":
"900a568f4e95d-
d8d7e93707a214e43a76653b17aea43fc3a7adf4ae89668efea",
                "download_url":
"https://ap-
i.in-
tel471.-
com/v1/-
down-
load/mal-
wareIn-
tel/900a568f4e95d-
d8d7e93707a214e43a76653b17aea43fc3a7adf4ae89668efea.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
  }
}
]
```

ThreatQ provides the following default mapping for the connector:

Feed Data	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	"048fe252afced217d4876003-49355bbc"	

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.last_updated	indicator.attribute	Modified At	1556258716643	formatted
.data.threat.uid	indicator.attribute	Threat UID	"45c17d-fa1b60f-b295f377836da5454c5"	
.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	"45c17d-fa1b60f-b295f377836da5454c5"	
.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

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.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"	



*

- 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', 4 indicators will be added with



types 'MD5','SHA-1','SHA-256','URL' and the value of the indicators will be extracted from .value.-
file.md5/sha1/sha256/download_url

Malware Signatures

Endpoint Example:

```
{
  "yaraTotalCount": 3,
  "yaras": [
    {
      "data": {
        "confidence": "high",
        "yara_data": {
          "title": "arkei",
          "signature": "rule arkei\n{\n  meta: \n\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": "45c17d-
falb60fb295f377836da5454c5"
      },
      "type": "malware",
      "uid": "45c17dfalb60fb295f377836da5454c5",
      "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
  }
}
]
```

ThreatQ provides the following default mapping for the connector:

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
-	sig-nature.type	Sig-nature Type	"YARA"	
.data.yara_data.title	sig-nature.-name	Sig-nature Name	"arkei"	
.data.yara_data.sig-nature	sig-nature.-value	Sig-nature Value	"rule arkei\n{\n meta: \n author = ..."	
.uid	report.at-tribute	Sig-nature UID	"048fe252afced217d4876003-49355bbc"	
.last_updated	report.at-tribute	Modified At	1556258716643	format- ted
.data.threat.uid	report.at-tribute	Threat UID	"45c17d-fa1b60f-b295f377836da5454c5"	
.data.threat.type	report.at-tribute	Threat Type	"malware"	
.data.-threat.data.family	report.at-tribute	Malware Family	"arkei"	

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.data.-threat.data.malware_family_profile_uid	report.attribute	Malware Family Profile ID	"45c17d-fa1b60f-b295f377836da5454c5"	
.data.-threat.data.version	report.attribute	Threat Version	"1.6"	
.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.confidence	report.attribute	Confidence	"high"	
.data.intel_requirements	report.attribute	Intelligence Requirement	["1.1.5","1.1.6"]	