ThreatQuotient

Intel 471 Reports, Actors, and Indicators Feed Implementation Guide

Version 1.0.0

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.

Last Updated: Monday, November 18, 2019

Contents

Versioning

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

Introduction

Intel 471 Reports Feed ingests threat intelligence data from the following endpoints:

- **Intel 471 Reports** - https://api.intel471.com/v1/report
- **Intel 471 Detailed Reports - Supplemental** - https://api.intel471.com/v1/reports/:report_uid

Notes

- The supplemental feed is called for each record returned from Intel471 Reports and also for each UID in its similar_reports.
- Time constrained data fetching is possible.
- Uses basic HTTP authentication based on email address and API key.

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

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 Reports** feed 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 feed 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 vendor-supplied email address and API key.

   The Intel 471 Reports, Actors and Indicators feed supports multiple configuration parameters:

Parameter	Description
Count	Maximum number of records to retrieve from the provider per request. Default value: 10. Size range: 0-100.
Report Location	Display reports related to a certain country or region. Examples: "European Union" (as a region), "United Kingdom" (as a country). It can only search for one location at a time.
Report Tag	Display reports related to a certain tag. Examples: "Banking & Finance", "Tools", "Airlines", "Phishing", "Spam", "Credit Card Fraud". It can only search for one tag at a time.

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

ThreatQ Mapping

Intel 471 provides an API that users can use to extract data in JSON format.

Each response from the provider contains the following parameters:

```
  indicator_type_map:
    MD5: MD5
    IPAddress: IP Address
    ActorDomain: FQDN
    ActorWebsite: URL
    EmailAddress: Email Address
    MaliciousURL: URL
    SHA256: SHA-256
    SHA1: SHA-1
    URL: URL
```

Intel 471 Reports

JSON response sample

```
{
    "reportTotalCount": 2,
    "reports": [
        {
            "uid": "625bf3a87263f00e06b3cb-
f6cc7b6380d83fff93b7ef201d0c9e599fb6bd95bf",
            "admiraltyCode": "F4",
            "motivation": [
                "CC"
            ],
```

```
            "subject": "Possible Ukrainian actor MentoS128
(aka Silver128, PapoKarlo) offers hacking service; Possible
victims identified",
            "created": 1571659854000,
            "dateOfInformation": 1571115600000,
            "sourceCharacterization": "Information was derived
from Russian-language cybercrime forum XSS and our sensitive
and reliable source.",
            "entities": [
                {
                    "type": "EmailAddress",
                    "value": "kremz@mail.ua"
                },
                {
                    "type": "EmailAddress",
                    "value": "silver_mix@ukr.net"
                },
                {
                    "type": "Handle",
                    "value": "aleksandrkremnikonov"
                }

            ],
            "locations": [
                {
                    "region": "Asia",
                    "country": "India",
                    "link": "impacts"
                },
```

```
                {
                    "region": "Asia",
                    "country": "Taiwan",
                    "link": "impacts"
                }
            ],
            "tags": [
                "Database Dumps",
                "Extortion",
                "Injects",
                "IoT (Internet of Things)",
                "Ransomware"
            ],
            "portalReportUrl": "https://ti-
tan.intel471.com/report/10757ae14960b92e04733023130fce5e",
            "lastUpdated": 1571660657176,
            "actorSubjectsOfReport": [
                {
                    "handle": "MentoS128",
                    "aliases": [
                        "Silver128",
                        "PapoKarlo"
                    ]
                }
            ],
            "similarReports": [
                {
                    "uid": "aa210760432ea8b-
f21ed3bf42068c365bf8fa34fd4c678d321ef066055625e45",
```

```
                    "admiraltyCode": "B2",
                    "motivation": [
                        "CC"
                    ],
                    "subject": "Russian actor, bulletproof
hoster yalishanda's (aka downlow, stas_vl) new control panel
for fast-flux service reviewed",
                    "dateOfInformation": 1545976800000,
                    "sourceCharacterization": "Information was
derived from the Russian-language cybercrime forum Exploit,
our actors' database, and our sensitive and reliable source.",
                    "portalReportUrl": "https://ti-
tan.intel471.com/report/4cd457bd47c42dae80f8dbf0305c3a76"
                }
            ]
        }
    ]
}
```


The mapping table is below.

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.uid	report	Call Intel 471 Detailed Report		
.similarReports.uid	report	Call Intel 471 Detailed Report		

Intel 471 Detailed Reports

JSON response sample


```
{
    "uid": "cc00f36d-
fd4cdb899637546cb86e1a2be4dd96e2096db0dfe7da9e2557469dbc",
    "admiraltyCode": "B4",
    "motivation": [
        "CC"
    ],
    "subject": "Possible Russian actor SOLDATKIN (aka dDonry,
Hellpein, lOoOl, Rocfor, Soldat554, 2+2=5000, Joker5218)
offers to sell remote access trojan based on remote manip-
ulator system malware",
    "researcherComments": "<p><strong>Assessment of cred-
ibil-
ity</strong></p>\r\n\r\n<p><strong>SOLDATKIN </strong>is
a Russian-speaking ...",
    "rawText": "<p>On Oct. 1, 2019, the actor
((strong>SOLDATKIN</strong)) posted the following on the XSS
forum:<br />\r\n---</p>\r\n\r\n....",
    "rawTextTranslated": "<p>On Oct. 1, 2019, the act-
or <strong>SOLDATKIN</strong> posted the following
on the XSS forum:<br />\r.....",
    "created": 1570534310000,
    "dateOfInformation": 1569906000000,
    "sourceCharacterization": "Information was derived from
the Russian-language cybercrime forum XSS and our sensitive
and reliable source.",
    "entities": [
```

```
        {
            "type": "EmailAddress",
            "value": "denis.soldatkin@bk.ru"
        },
        {
            "type": "Handle",
            "value": "2+2=5000"
        },
        {
            "type": "Handle",
            "value": "dDonry"
        },
        {
            "type": "Handle",
            "value": "Denis Soldatkin"
        },
        {
            "type": "Handle",
            "value": "GGGGG IOILA"
        }
    ],
    "locations": [
        {
            "region": "Europe",
            "country": "Russia",
            "link": "originated_from"
        }
    ],
    "tags": [
```

```
        "Crypters & Packers",
        "Malware",
        "Tools"
    ],
    "portalReportUrl": "https://ti-
tan.intel471.com/report/08ec0068f2a36e01b8066f0e67420824",
    "lastUpdated": 1570534757790,
    "actorSubjectsOfReport": [
        {
            "handle": "SOLDATKIN",
            "aliases": [
                "dDonry",
                "Hellpein",
                "lOoOl",
                "Rocfor",
                "Soldat554",
                "2+2=5000",
                "Joker5218"
            ]
        }
    ],
    "reportAttachments": [
        {
            "fileName": "attachment-157017573009333.zip",
            "url": "https://ap-
i.in-
tel471.-
com/v1/re-
```

```
ports/c-
c00f36d-
fd4cd-
b899637546cb86e1a2be4d-
d96e2096d-
b0d-
fe7da9e2557469d-
bc/download/23cc2a8b7e4eaf7fe1a982da34f24c8f/attachment-
157017573009333.zip",
            "fileSize": 49680
        }
    ],
    "similarReports": [
        {
            "uid": "aa210760432ea8b-
f21ed3bf42068c365bf8fa34fd4c678d321ef066055625e45",
            "admiraltyCode": "B2",
            "motivation": [
                "CC"
            ],
            "subject": "Russian actor, bulletproof hoster yal-
ishanda’s (aka downlow, stas_vl) new control panel for fast-
flux service reviewed",
            "dateOfInformation": 1545976800000,
            "sourceCharacterization": "Information was derived
from the Russian-language cybercrime forum Exploit, our act-
ors’ database, and our sensitive and reliable source.",
            "portalReportUrl": "https://ti-
tan.intel471.com/report/4cd457bd47c42dae80f8dbf0305c3a76"
```

```
            }
        ]
}
```

The mapping table is below.

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.subject	report.value	Value	"Possible Russian actor SOLDATKIN (aka dDonny, Hellpein, lOoOl, Rocfor, Soldat554, 2+2=5000, Joker5218)…."	
.researcherComments	report.description	Descrip-tion	"sample comment"	
.created or .dateOfIn-formation	report.published_at	Pub-lished At	"1570534310000"	format-ted
.uid	report.uid	Intel471 Report ID	"cc00f36d-fd4cd-b899637546cb86e1a2be4dd96e2096db0dfe7da9e2557469dbc"	
.sourceCharacterization	report.-sourceCharacterization	Intel471 Source	"Information was derived from the Russian-language cybercrime forum XSS and our sensitive and reliable source."	
.locations.region	report.region	Region	"Russia"	
.locations.country	report.country	Country	"United States"	
.portalReportURL	report.url	Intel471 Portal URL	"https://ti-tan.intel471.com/report/08ec0068f2a36e01b8066f0e67420824"	
.tags	report.tags	Intel471 Tags	["Crypters & Packers", "Malware", "Tools"]	
.admiralityCode[0]	report.ad-	Intel471	"B"	

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
	miralityReliability	Admiralty Reli-ability		
.admiralityCode[1]	report.ad-miralityCredibility	Intel471 Admiralty Cred-ibility	"4"	
.motivation	report.attribute	Intel471 Motiv-ation	"CC"	
.entities.value	adversary.name if ["type"] == "Handle"		"coolcat"	
.entities.value	indicator.value if ["type"] != "Handle"		"ch4rgui@hotmail.fr"	
.entities.type	indicator.type if ["type"] != "Handle		"EmailAddress"	indic-ator_type_map
.act-orSub-jectsOfReport.aliases	adversary.attribute	Aliases	["dDonny", "Hellpein"]	*

* Where actorSubjectsOfReport.handle == adversary.name