# ThreatQuotient

## PassiveTotal Guide

Version 2.0.0

Monday, October 5, 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, October 5, 2020

# Contents

# Versioning

- Current integration version: `2.0.0`
- Supported on ThreatQ versions >= `4.34.0`

# Introduction

The Passive Total feed retrieves data from RiskIQ Community API, using the following endpoints:

- `https://api.passivetotal.org/v2/project`
- `https://api.passivetotal.org/v2/artifact`
- `https://api.passivetotal.org/v2/enrichment/bulk`

PassiveTotal publishes information grouped as `Project`s. PassiveTotal's `Artifact` endpoint is called for each `Project`, retrieving associated indicators (called artifacts in PassiveTotal). These associated Indicators are enriched via PassiveTotal's Bulk Artifact Enrichment endpoint. ThreatQ ingests these Indicators with the `Project` context as Attributes.

# 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 **PassiveTotal** 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 |
|---|---|
| Username | The PassiveTotal account Username. |
| API Key | The PassiveTotal account API key. |

5. Click on **Save Changes**.
6. Click on the toggle switch next to the feed name to enable it.

# ThreatQ Mapping

PassiveTotal's API endpoints use HTTP basic authentication.

## PassiveTotal

```
GET https://api.passivetotal.org/v2/project
```

JSON response sample:

```
{
    "success": true,
    "results": [
        {
            "active": true,
            "can_edit": false,
            "collaborators": [],
            "created": "2016-11-16T05:55:00.425000",
            "creator": "mike.wyatt@riskiq.net",
            "description": "Browser exploit kit used for distribution of malware to vulnerable
computers",
```

```
    "featured": true,
    "guid": "182d1a3a-5be3-dad4-76b8-67f8f79e8488",
    "link": null,
    "links": {
        "artifact": "/v2/artifact?project=182d1a3a-5be3-dad4-76b8-67f8f79e8488",
        "self": "/v2/project?project=182d1a3a-5be3-dad4-76b8-67f8f79e8488",
        "tag": "/v2/project/tag?project=182d1a3a-5be3-dad4-76b8-67f8f79e8488"
    },
    "name": "RIG Exploit Kit",
    "organization": "riskiq",
    "owner": "riskiq",
    "subscribers": [
        "yonathan@riskiq.net",
        "zann@riskiq.net"
    ],
    "success": true,
    "tags": [
        "crimeware",
        "exploit kit",
        "rig"
    ],
```

```
            "visibility": "community"
        },
        ...
    ]
}
```

ThreatQ provides the following default mapping for this feed:

| Feed Data Path | ThreatQ Entity | ThreatQ Object Type or Attribute Key | Published Date | Examples | Notes |
|---|---|---|---|---|---|
| .results[].active | Report.Attribute | Active | .results[].created | true | Formatted as a title-cased string |
| .results[].name / .results[].guid | Report.Value | N/A | .results[].created | RIG Exploit Kit | Formatted as `{{.results[].name}} - {{.results[].guid}}` |
| .results[].tags[] | Report.Attribute | Tag | .results[].created | crimeware | N/A |
| .results[].visibility | Report.Attribute | Visibility | .results[].created | community | N/A |
| .results[].organization | Report.Attribute | Organization | .results[].created | riskiq | N/A |
| .results[].owner | Report.Attribute | Owner | .results[].created | riskiq | N/A |
| .results[].fea- | Report.Attribute | Featured | .results | true | N/A |

| Feed Data Path | ThreatQ Entity | ThreatQ Object Type or Attribute Key | Published Date | Examples | Notes |
|---|---|---|---|---|---|
| tured | | | [].created | | |
| .results[].description | Report.Description | N/A | N/A | Browser exploit kit used for distribution of malware to vulnerable computers | N/A |
| .results[].guid | Report.Attribute & Indicator.Attribute | Project ID | .results[].created | 83276f14-5069-8b12-11ff-2ba73f1b9c3e | N/A |

## PassiveTotal Artifacts

Endpoint to get related Indicator `Artifact`s for each PassiveTotal `Project`.

```
GET https://api.passivetotal.org/v2/artifact?project=<Project-GUID>
```

JSON response sample:


```
{
    "artifacts": [
        {
            "created": "2017-02-15T13:31:41.256000",
            "creator": "mike.wyatt@riskiq.net",
            "enterprise": false,
            "guid": "83276f14-5069-8b12-11ff-2ba73f1b9c3e",
            "links": {
                "tag": "/v2/artifact/tag?artifact=83276f14-5069-8b12-11ff-2ba73f1b9c3e",
                "self": "/v2/artifact?artifact=83276f14-5069-8b12-11ff-2ba73f1b9c3e",
                "project": "/v2/project?project=182d1a3a-5be3-dad4-76b8-67f8f79e8488"
            },
            "monitor": true,
            "monitorable": false,
            "organization": "riskiq",
            "owner": "riskiq",
```

```
            "project": "182d1a3a-5be3-dad4-76b8-67f8f79e8488",
            "query": "aavm50cc.top",
            "system_tags": [],
            "tag_meta": {},
            "tags": [],
            "type": "domain",
            "user_tags": []
        },
        ...
    ]
}
```

ThreatQ provides the following default mapping for this feed:

| Feed Data Path | ThreatQ Entity | ThreatQ Object Type or Attribute | Published Date | Examples | Notes |
|---|---|---|---|---|---|
| .artifacts[].creator | Indicator.Attribute | Creator | .artifacts[].created | mike.wyatt@riskiq.net | N/A |
| .artifacts[].enterprise | Indicator.Attribute | Enterprise | .artifacts[].created | False | Formatted as a title-cased string |
| .artifacts[].monitor | Indicator.Attribute | Monitor | .artifacts[].created | true | Formatted as a title-cased string |
| .artifacts[].monitorable | Indicator.Attribute | Monitorable | .artifacts[].created | False | Formatted as a title-cased string |
| .artifacts[].organization | Indicator.Attribute | Organization | .artifacts[].created | riskiq | N/A |
| .artifacts[].owner | Indicator.Attribute | Owner | .artifacts[].owner | riskiq | N/A |
| .artifacts[].query | Indicator.Value | See `PassiveTotal to ThreatQ Indicator Type Mapping` below | .artifacts[].created | aavm50cc.top | Derived from `.artifacts[].type`. Only types supported via PassiveTotal to ThreatQ Indicator |

| Feed Data Path | ThreatQ Entity | ThreatQ Object Type or Attribute | Published Date | Examples | Notes |
|---|---|---|---|---|---|
| | | | | | Type Mapping below will be ingested. |

## Indicator Type Mapping

PassiveTotal to ThreatQ Indicator Type Mapping:

| PassiveTotal | ThreatQ |
|---|---|
| domain | FQDN |
| Email | Email Address |
| ip | IP Address |
| MD5 Hash | MD5 |
| autonomusSystemNumber | ASN |

## PassiveTotal Bulk Artifacts Enrichment

Endpoint to get enrichment data for each related Indicator `Artifact` returned by the PassiveTotal Artifacts endpoint. This endpoint expects a JSON data body with the request containing the `Artifact`s to enrich structured like so:

```
{
    "query": ["146.0.72.186", "192.168.0.1", ...]
}
```

```
GET https://api.passivetotal.org/v2/enrichment/bulk
```

JSON response sample:

```
{
    "results": {
        "146.0.72.186": {
            "autonomousSystemName": "HOSTKEY B.V.",
            "autonomousSystemNumber": 57043,
            "classification": null,
            "country": "NL",
            "dynamicDns": false,
            "everCompromised": false,
            "global_tags": [
```

```
            "hostkey"
        ],
        "latitude": 52.38240051269531,
        "longitude": 4.899499893188477,
        "network": "146.0.72.0/24",
        "primaryDomain": "particulieren-bank.nl",
        "queryType": "ip",
        "queryValue": "146.0.72.186",
        "sinkhole": false,
        "subdomains": [
            "mail"
        ],
        "system_tags": [
            "routable",
            "HOSTKEY-B.V."
        ],
        "tag_meta": {},
        "tags": [],
        "tld": "net"
    },
    ...
```

```
        }
}
```

ThreatQ provides the following default mapping for this feed:

| Feed Data Path | ThreatQ Entity | ThreatQ Object Type or Attribute | Published Date | Examples | Notes |
|---|---|---|---|---|---|
| .results.`artifact`.autonomousSystemName | Indicator.Attribute | Autonomous System Name | N/A | HOSTKEY B.V. | Only applies to the ASN Indicator created from `.result`s.`artifact`.autonomusSystemNumber |
| .results.`artifact`.autonomousSystemNumber | Indicator.Value | ASN | N/A | 57043 | N/A |
| .results.`artifact`.classification | Indicator.Attribute | Classification | N/A | null | Only created if present |
| .results.`artifact`.country | Indicator.Attribute | Country | N/A | NZ | N/A |
| .results.`artifact`.dynamicDns | Indicator.Attribute | Dynamic Dns | N/A | false | Formatted as a title-cased string |

| Feed Data Path | ThreatQ Entity | ThreatQ Object Type or Attribute | Published Date | Examples | Notes |
|---|---|---|---|---|---|
| .results.artifact.everCompromised | Indicator.Attribute | Ever Compromised | N/A | false | Formatted as a title-cased string |
| .results.artifact.global_tags | Indicator.Attribute | Global Tag | N/A | hostkey | N/A |
| .results.artifact.latitude | Indicator.Attribute | Latitude | N/A | 52.38240051269531 | N/A |
| .results.artifact.longitude | Indicator.Attribute | Longitude | N/A | 4.899499893188477 | N/A |
| .results.artifact.network | Indicator.Value | CIDR Block | N/A | 146.0.72.0/24 | N/A |
| .results.artifact.primaryDomain | Indicator.Attribute | Primary Domain | N/A | particulieren-bank.nl | N/A |
| .results.artifact.sinkhole | Indicator.Attribute | Sinkhole | N/A | false | Formatted as a title-cased string |

| Feed Data Path | ThreatQ Entity | ThreatQ Object Type or Attribute | Pub-lished Date | Examples | Notes |
|---|---|---|---|---|---|
| .results.`artifact`.sys-tem_tags | Indic-ator.Attribute | System Tag | N/A | routable | N/A |
| .results.`artifact`.tags | Indic-ator.Attribute | Tag | N/A | hostkey | N/A |
| .results.`artifact`.tld | Indic-ator.Attribute | TLD | N/A | net | N/A |

# Average Feed Runs

Object counts and Feed runtime are 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.

### Hourly PassiveTotal Scheduled Run

| Metric | Result |
|---|---|
| Run Time | 2 minutes |
| Indicators | 136 |
| Indicator Attributes | 1492 |
| Reports | 2 |
| Report Attributes | 10 |

### PassiveTotal Manual Run (01/01/2020 - 9/29/2020)

| Metric | Result |
|---|---|
| Run Time | 1 hour 2 minutes |
| Indicators | 15311 |
| Indicator Attributes | 159606 |
| Reports | 381 |
| Report Attributes | 2166 |

# Change Log

- **Version 2.0.0**
  - Added Manual Run support
  - Added primary Report objects linking to PassiveTotal's `Project`s. These Report objects are related to their Indicator `Artifact`s.
  - Removed `subdomain` Attributes from Indicators.
  - Refactor Feed
- **Version 1.1.0**
  - Added ASN indicator ingestion
- **Version 1.0.1**
  - Initial release