ThreatQuotient

PassiveTotal Guide

Version 1.1.0

Monday, August 10, 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, August 10, 2020

Contents

Versioning

- Current integration version: `1.1.0`
- Supported on ThreatQ versions: `4.18.0` or higher

Introduction

The PassiveTotal feed retrieves data from RiskIQ Community API, using the following end-points:

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

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 publishes information grouped as "projects". For each project a call to the api is made to load the associated indicators (called artifacts in Passive Total). The objects that are saved in ThreatQ are the indicators, while the properties of the projects will be attributes of those indicators.

The API uses HTTP basic authentication. The response data is in json format.

PassiveTotal Project

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


```
{
    "success": true,
    "results": [
        {
            "featured": true,
            "links": {
                "self": "/v2/project?project=182d1a3a-5be3-dad4-76b8-67f8f79e8488",
                "artifact": "/v2/artifact?project=182d1a3a-5be3-dad4-76b8-67f8f79e8488",
                "tag": "/v2/project/tag?project=182d1a3a-5be3-dad4-76b8-67f8f79e8488"
```

```
            },
            "description": "Browser exploit kit used for distribution of malware to vulnerable
computers",
            "collaborators": [],
            "organization": "riskiq",
            "can_edit": false,
            "tags": [
                "crimeware",
                "exploit kit",
                "rig"
            ],
            "owner": "riskiq",
            "subscribers": [
                "yonathan@riskiq.net",
                "zann@riskiq.net"
            ],
            "visibility": "community",
            "guid": "182d1a3a-5be3-dad4-76b8-67f8f79e8488",
            "creator": "mike.wyatt@riskiq.net",
            "name": "RIG Exploit Kit",
            "active": true,
```

```
            "created": "2016-11-16T05:55:00.425000"
        }
    ]
}
```

ThreatQ provides the following default mapping for this feed:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute	Published Date	Examples
.results[].name	Indicator.Attribute	Project Name	.results[].created	RIG Exploit Kit
.results[].active	Indicator.Attribute	Active	.results[].created	true
.results[].tags[]	Indicator.Attribute	Tag	.results[].created	crimeware
.results[].visibility	Indicator.Attribute	Visibility	.results[].created	community
.results[].organization	Indicator.Attribute	Organization	.results[].created	riskiq
.results[].owner	Indicator.Attribute	Owner	.results[].created	riskiq
.results[].featured	Indicator.Attribute	Featured	.results[].created	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute	Published Date	Examples
.results[].description	Indicator.Attribute	Description	.results[].created	
.results[].guid	Indicator.Attribute	Project ID	.results[].created	83276f14-5069-8b12-11ff-2ba73f1b9c3e

PassiveTotal Artifacts

PassiveTotal Artifacts `GET https://api.passivetotal.org/v2/artifact?project=project_id`


```
{
	"artifacts": [
		{
			"monitor": false,
			"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"
			},
			"creator": "mike.wyatt@riskiq.net",
			"guid": "83276f14-5069-8b12-11ff-2ba73f1b9c3e",
			"query": "aavm50cc.top",
			"tag_meta": {},
			"user_tags": [],
			"monitor": true,
			"created": "2017-02-15T13:31:41.256000",
			"project": "182d1a3a-5be3-dad4-76b8-67f8f79e8488",
```

```
                    "system_tags": [],
                    "type": "domain",
                    "tags": [],
                    "organization": "riskiq",
                    "owner": "riskiq"
                }
        ]
}
```

ThreatQ provides the following default mapping for this feed:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute	Published Date	Examples
.artifacts[].query	Indicator.Value	Derived from .artifacts[].type. See PassiveTotal Type to ThreatQ Indicator Type Mapping table.	.artifacts[].created	aavm50cc.top
.artifacts[].monitor	Indicator.Attribute	Monitor	.artifacts[].created	true
.artifacts[].creator	Indicator.Attribute	Creator	.artifacts[].created	mike.wyatt@riskiq.net
.artifacts[].created	Indicator.Attribute	Created	.artifacts[].created	2017-02-15T13:31:41.256000

PassiveTotal Artifacts Enrichment

PassiveTotal Artifacts Enrichment `POST https://api.passivetotal.org/v2/enrichment/bulk`


```
{
    "results": {
        "146.0.72.186": {
            "dynamicDns": false,
            "classification": null,
            "sinkhole": false,
            "everCompromised": false,
            "queryType": "ip",
            "queryValue": "146.0.72.186",
            "autonomousSystemNumber": 57043,
            "autonomousSystemName": "HOSTKEY B.V.",
            "network": "146.0.72.0/24",
            "country": "NL",
            "longitude": 4.899499893188477,
            "latitude": 52.38240051269531,
            "subdomains": [],
            "tag_meta": {},
```

```
            "global_tags": [
                "hostkey"
            ],
            "tags": [],
            "system_tags": [
                "routable",
                "HOSTKEY-B.V."
            ]
        }
    }
}
```

ThreatQ provides the following default mapping for this feed:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute	Published Date	Examples
.results.`indicator.value`.dynamicDns	Indicator.Attribute	Dynamic Dns		false
.results.`indicator.value`.tag	Indicator.Attribute	Tag		
.results.`indicator.value`.system_tags	Indicator Attribute	System Tag		["routable"]
.results.`indicator.value`.global_tags	Indicator.Attribute	Global Tag		["hostkey"]
.results.`indicator.value`.subdomains	Indicator.Attribute	Subdomain		
.results.`indicator.value`.country	Indicator.Attribute	Country		NZ
.results.`indicator.value`.latitude	Indicator.Attribute	Latitude		4.89124343434323
.results.`indicator.value`.classification	Indicator.Attribute		Classification	
.results.`indicator.value`.everCompromised	Indicator.Attribute	Ever Compromised		false
.results.`indicator.value`.primaryDomain	Indicator.Attribute		Primary Domain	
.results.`indicator.value`.autonomusSys-temNumber	Indicator.Value	ASN		57043

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute	Published Date	Examples
.results.`indicator.value`.autonomusSystemName	Indicator.Attribute	Autonomus System Name		HOSTKEY B.V.

PassiveTotal Type to Indicator Type Mapping

The mapping between the indicator types in Passive Total and ThreatQ is:

Passive Total	ThreatQ
domain	FQDN
Email	Email Address
ip	IP Address
MD5 Hash	MD5
autonomusSystemNumber	ASN

Average Feed Run

Average Feed Run results for PassiveTotal:

Metric	Result
Run Time	1 hour
Indicators	20,120
Indicator Attributes	221,122

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.

Known Issues

- Projects that have associated a large number of indicators(~ >5000) will usually fail when trying to retrieve indicators, throwing a `504 Gateway Time-out` error. This is caused by the Passive Total servers and will not stop the feed run.
- If a project has no indicators when trying to load them, Passive Total will return a `404 NOT FOUND` error. This will not stop the feed run.

Change Log

- **Version 1.1.0**
  - Added ASN indicator ingestion.
- **Version 1.0.1**
  - Initial release.