Passive Total Connector Implementation Guide

Version 1.0.0

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: Thursday, April 25, 2019

Contents

Versioning

- Current integration version: `1.0.0`
- Supported on ThreatQ versions: `4.18.0` or higher

Introduction

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

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

Installation

Complete the following steps to install the connector:

1. Login to https://download.threatq.com/integrations/.
2. Download the **passivetotal.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 **LABS** tab.

6. Under Passive Total, click **Feed Settings**.
7. For Username, enter the Passive Total account Username.
8. For API Key, enter the Passive Total account API key.
9. Click the toggle button next to Passive Total to enable the feed.
10. Click **Save Changes**.

ThreatQ Mapping

Passive Total 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.

Projects - `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"
        }
    ]
}
```


Artifacts (Indicators) - `https://api-i.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 the connector:

Passive Total Key	ThreatQ Entity	ThreatQ Name	Examples
Project			

Passive Total Key	ThreatQ Entity	ThreatQ Name	Examples
name	indicator.attribute	Project Name	RIG Exploit Kit
active	indicator.attribute	Active	true
tags[]	indicator.attribute	Tag	crimeware
visibility	indicator.attribute	Visibility	community
organization	indicator.attribute	Organization	riskiq
owner	indicator.attribute	Owner	riskiq
featured	indicator.attribute	Featured	
description	indicator.attribute	Description	Browser exploit kit used...
guid	indicator.attribute	Project ID	182d1a3a-5be3-dad4-76b8-67f8f79e8488
Artifact(Indicator)			
artifacts[].query	indicator.value		aavm50cc.top
artifacts[].type	indicator.type		domain
artifacts[].monitor	indicator.attribute	Monitor	true

Passive Total Key	ThreatQ Entity	ThreatQ Name	Examples
artifacts[].creator	indicator.attribute	Creator	john.smith@riskiq.net
artifacts[].created	indicator.attribute	Created	2017-02-15T13:31:41.256000

The mapping between the indicator types in Passive Total and ThreatQ are displayed below:

AlienVault	ThreatQ
domain	FQDN
Email	Email Address
ip	IP Address
MD5 Hash	MD5
FileHash-SHA1	SHA-1

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.