Malware Patrol 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: Tuesday, September 18, 2018

Contents

Introduction

This Malware Patrol Connector ingests threat intelligence data in seven feeds from the **Malware Patrol** vendor. The connector definition file maps how the feed data for each of those feeds is mapped to ThreatQ specific indicators and their related attributes. Threat intelligence data from the following seven feeds is ingested in ThreatQ:

- Sinkhole IP Addresses Data Feed
- Malware URLs (Sanitized)
- Command and Control Server Addresses (Sanitized)
- Malware Hashes
- Malicious IP Addresses
- Real Time DDoS Attacks
- Domains Generated via DGA

Installation

The installation instructions for this integration differ based on the ThreatQ version you have installed.

ThreatQ Versions Before 4.9

It is assumed that the user has python installed with a minimum version of `2.7.5` and the following packages (use `pip` to install these packages):

- ruamel.yaml
- threatqsdk

threatqsdk is installed typically by making changes to the **pip.conf** file as follows:

```
[global]
       index-url = https://system-updates.threatq.com/pypi
         extra-index-url = https://username:password
         @extensions.threatq.com/threatq/integrations
         https://username:password@extensions.threatq.com/threatq/sdk
```

After satisfying the above requirements, the integration can be installed as follows:

```
python bulk_create_cdf.py -c tq.config -y malware_
patrol.yaml -f '{"username": {"value":
"<YOURUSER>", "label": "Username"}, "password":
{"value": "<YOURPASS>", "label": "Password",
"type": "password"}, "domain": {"value":
"<YOURDOMAIN>", "label": "Domain"}}'
```

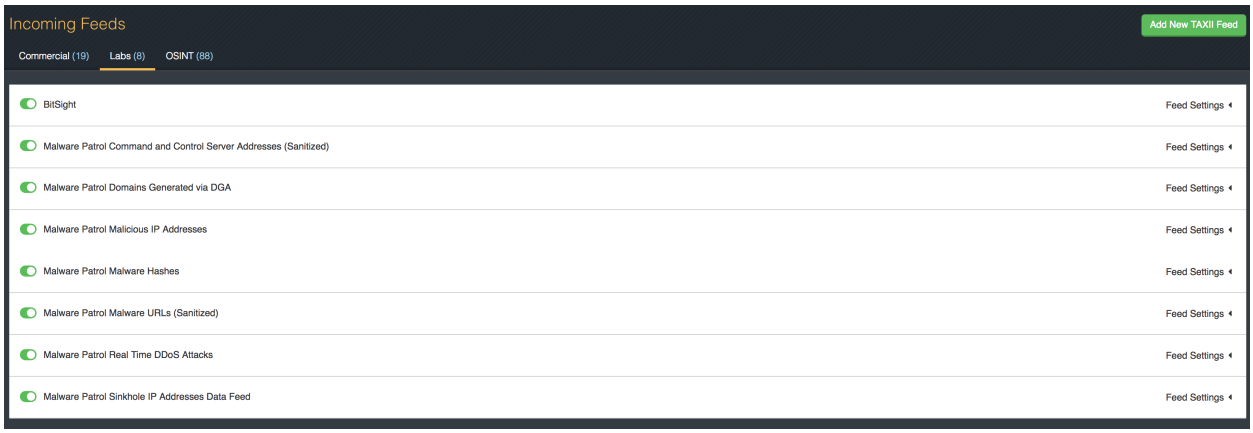
ThreatQ Version 4.9 or Later

The following artisan command on the platform will install it.

```
sudo php artisan threatq:feed-install malware_
patrol.yaml
```

ThreatQ User Interface Configuration

The connector installs as a feed under **Labs** as shown below. The Malware Patrol button must be enabled for the feed to begin ingesting data.



All Malware Patrol Feeds have the same configuration parameters as shown in the picture below. The descriptions are:

- Username: The Malware Patrol account username
- Password: The Malware Patrol account password
- Domain: The domain name of the feeds hosting server (Ex. eval-.malwarepatrol.net)

Known Issues

If users are using a ThreatQ Version before 4.9.0, we recommend that you check the json arguments being passed (after the `-f` flag) using a json validator tool, since the script does not do any validation. If the `json arguments` were passed incorrectly, the UI feeds page is unable to parse those arguments and the whole feeds page fails to load. If ever this problem occurred regardless while using the script above, drop the connector from the database.