ThreatQuotient for IMAP Application

September 14, 2018

Version 3.1.0

11400 Commerce Park Dr
Suite 200,
Reston, VA
20191, USA
https://www.threatq.com/
Support: support@threatq.com
Sales: sales@threatq.com

Contents

List of Figures and Tables

1 Introduction

1.1 Application Function

The ThreatQuotient for IMAP Application provides IoC and Spear Phish parsing capabilities on general messages sent to an IMAP enabled email inbox. It is common practice in many different organizations that general mailbox accounts are setup to receive threat intelligence information, sometimes from sources like a national CERT, Open Source CTI, and internal malware and forensic analysis teams.

The IMAP Integration can be installed many different times using different names and configured for a variety of inboxes.

1.2 Preface

This guide provides the information necessary to implement the ThreatQuotient for IMAP Application. This document is not specifically intended as a site reference guide. It is assumed that the implementation engineer has experience installing and commissioning ThreatQuotient Apps and integrations covered within the document, as well as experience necessary to troubleshoot at a basic level.

1.3 Audience

This document is intended for use by the following parties:

1. ThreatQ and IMAP/Exchange Engineers
2. ThreatQuotient Professional Services Project Team & Engineers

1.4 Scope

This document covers the implementation of the ThreatQuotient for IMAP Application only.

Table 1: ThreatQuotient Software & App Version Information

Software/App Name	File Name	Version
ThreatQ	Version 3.6.x or greater	
ThreatQuotient for IMAP Application	3.1.0	

1.5 Assumptions

The following criteria is assumed to be in place and functional to allow the implementation of the ThreatQuotient for IMAP Application into the managed estate:

- All ThreatQuotient equipment is online and in service.
- All required firewall ports have been opened.

Table 2: ThreatQuotient Firewall Port Requirements

Source	Destination	Port	Description
ThreatQ Instance	IMAP Server	993	This is the default requirement, and uses SSL Encrypted IMAP (this may require setting up certificates)
		143	This is used if the -ds flag is used. This uses unencrypted IMAP.

2 Implementation Overview

This document will show how to install the ThreatQuotient for IMAP Application.

2.1 Prerequisites

Throughout this implementation document, we will refer to several files and directories, some of which will be symbolic, and others may change depending on specifics of the environmental setup.

Accounts needed for the application and IMAP requirements:

Table 3: Application Account Requirements

Service	Account	Description
ThreatQ	Integration	This account will be used as the source for the integration and will be used during installation. It is recommended that a user be created for the purpose of integrations in general.
IMAP	User/Inbox	This is the inbox that will be setup. The username and password for this account are required during the configuration steps.

Ensure all ThreatQ devices are set to the correct time, time zone and date, and using a clock source available to all.

To identify which time zone is closest to your present location, use the `timedatectl` command with the `list-timezones` command line option. For example, to list all available time zones in Europe, type:

Figure 1: Time Zone List Example

```
timedatectl list-timezones | grep Europe
Europe/Amsterdam
Europe/Athens
Europe/Belgrade
Europe/Berlin
```

To change the time zone to Europe/Prague, type as root:

Figure 2: Time Zone Change Example

```
timedatectl set-timezone UTC
```

2.2 Security and Privacy

For ThreatQuotient Professional Services engineers to configure the system, local network access is required to connect to the managed estate. Therefore, the implementation must occur at an office or data center location.

Passwords have not been provided in this document. Please contact your project team for this information, if required.

All engineers are reminded that all data belonging and pertaining to the business is strictly confidential and should not be disclosed to any unauthorized parties.

The data held within this document is classed as confidential due to its nature.

3 IMAP Application Installation

3.1 Setting up the Integration

From the ThreatQuotient Repository:

To install this TQIS app from the ThreatQuotient repository with YUM credentials, complete the following steps:

1. Install the IMAP application by using the following commands.

Figure 3: Installing from the ThreatQuotient Repository (Example Output)

```
sudo pip install -i
https://<USERNAME>:<PASSWORD>@extensions.threatq.com/threatq/integrations tqIMAP
Downloading https://extensions.threatq.com/threatq/integrations-
dev/+f/9c2/131c319f2bb32/tqIMAP-3.1.0-py2-none-any.whl
Requirement already satisfied (use --upgrade to upgrade): threatqsdk>=1.6.2 in
/usr/lib/python2.7/site-packages (from tqIMAP)
Requirement already satisfied (use --upgrade to upgrade): threatqcc>=1.1.2 in
/usr/lib/python2.7/site-packages (from tqIMAP)
Collecting PySocks==1.6.7 (from tqIMAP)
  Downloading
https://extensions.threatq.com/root/pypi/+f/d00/329f27efa157d/PySocks-1.6.7.tar.gz
(282kB)
    100% |████████████████████████████████| 286kB 4.3MB/s
Requirement already satisfied (use --upgrade to upgrade): requests>=2.9.1 in
/usr/lib/python2.7/site-packages (from threatqsdk>=1.6.2->tqIMAP)
Requirement already satisfied (use --upgrade to upgrade): six>=1.5 in
/usr/lib/python2.7/site-packages (from python-dateutil>=2.6.1->tqIMAP)
Requirement already satisfied (use --upgrade to upgrade): MarkupSafe in
/usr/lib64/python2.7/site-packages (from jinja2==2.8->threatqcc>=1.1.2->tqIMAP)
Installing collected packages: PySocks, python-dateutil, tqIMAP
Successfully installed PySocks-1.6.7 python-dateutil-2.7.3 tqIMAP-3.1.0
```

Offline From the .whl File:

To install this IMAP application from a wheel file, the wheel file (.whl) file `tqIMAP-3.1.0-py2-none-any.whl` will need to be copied via SCP into your ThreatQ instance. the dependencies will need to be installed PySocks, python_dateutil including the latest ThreatqSDK and Threatqcc.

1. Install the .whl file using the following command.

Figure 4: Installing .whl File (Inc Example Output)

```
$> sudo pip install /file/path/to/app/tqIMAP-3.1.0-py2-none-any.whl
You are using pip version 7.1.0, however version 9.0.1 is available.
You should consider upgrading via the 'pip install --upgrade pip' command.
Processing ./tqIMAP-3.1.0-py2-none-any.whl
Requirement already satisfied (use --upgrade to upgrade): threatqsdk>=1.6.2 in
/usr/lib/python2.7/site-packages (from tqIMAP==2.0.1)
Requirement already satisfied (use --upgrade to upgrade): threatqcc>=1.1.2 in
Requirement already satisfied (use --upgrade to upgrade): PySocks>=1.6.7 in
/usr/lib/python2.7/site-packages (from tqIMAP==3.1.0)
Installing collected packages: python-dateutil, tqIMAP
      Successfully uninstalled python-dateutil-2.6.0
Successfully installed python-dateutil-2.7.0 tqIMAP-3.1.0
```

Once the application has been installed, a directory structure must be created for all configuration, logs and files, using the `mkdir -p` command. See example below:

Figure 5: Creating Integration Directories (Example)

```
mkdir -p /opt/tq-integrations/imap
mkdir -p /opt/tq-integrations/imap/config
mkdir -p /opt/tq-integrations/imap/logs
```

A driver called `tqIMAP` or `tqimap` is installed.

2. Issue the following commands to initialize the integration.

   You will be asked the following questions:

   a. **ThreatQ Host:** This is the host of the ThreatQ instance, either the IP Address or Hostname as resolvable by ThreatQ.
   b. **Client ID:** This is the OAuth id that can be found at **Settings** > **OAuth Management**.
   c. **E-mail Address:** This is the *User in the ThreatQ System* for integrations.
   d. **Password:** The password for the above ThreatQ account
   e. **Status:** This is the default status for IoCs that are created by this Integration. It is common to set this status to "Review", but organization SOPs should be respected when determining a setting.

Figure 6: Running the Integration

```
$>tq-imap -c /file/path/to/config/ -ll /file/path/to/logs/ -f /file/path/to files/
-v 3  --files files
ThreatQ Host: <IP ADDRESS>
Client ID: <ClientID>
E-Mail Address: <EMAIL ADDRESS>
Password: <PASSWORD>
Status: Active
Connector configured.  Set information in UI. 2018-03-16 18:05:46 - Intelligence
Mailbox CRITICAL: Connector has been created, please use UI for final configuration
```

The driver will run once, where it will connect to the ThreatQ instance and install the user interface component of the connector.

If multiple instances are required, use the -n flag, as shown below.

Figure 7: Running the Integration with -n flag

```
$>tq-imap -n <Bespoke_Name> -c /file/path/to/config/ -ll /file/path/to/logs/ -f
/file/path/to files/ -v 3  --files files
ThreatQ Host: <IP ADDRESS>
Client ID: <ClientID>
E-Mail Address: <EMAIL ADDRESS>
Password: <PASSWORD>
Status: Active
Connector configured.  Set information in UI. 2018-03-16 18:05:46 - Intelligence
Mailbox CRITICAL: Connector has been created, please use UI for final configuration
```

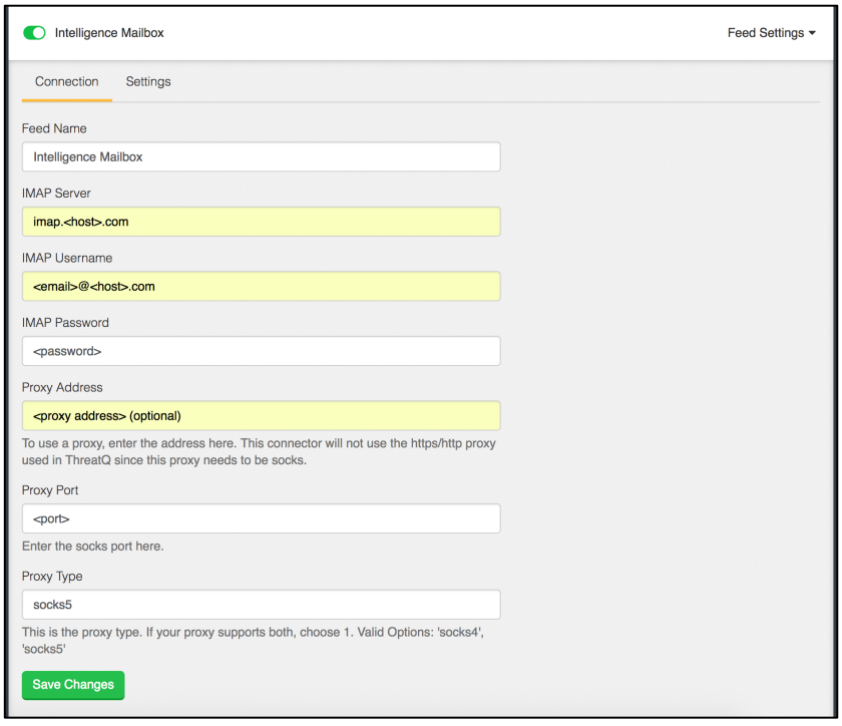
3.2 Configuring the connector

Once the steps from the previous section are complete, go to the ThreatQ user interface and navigate to **Settings** > **Incoming Feeds** > **ThreatQ Labs** and find the *Intelligence Mailbox* feed.
To edit the configuration, go to the **Incoming Feeds** page within ThreatQ, click the **ThreatQ Labs** tab, then expand the Feed Settings for the **Intelligence Mailbox** section.

The following information will need to be entered as described below.

1. **IMAP Server**: This is the IMAP server associated with the email provider.
2. **IMAP Username**: The username/email address to be accessed.
3. **IMAP Password**: The password associated with the username/email address.
4. **Proxy Address**: This is the socks proxy address needed to connect to the IMAP server.
    - The proxy cannot be a HTTP/HTTPS proxy. This field is optional. If a socks proxy is not used, this field can be left blank.
5. **Proxy Port**: The port associated with the proxy address field.
    - This will only be used if you are using a proxy.
6. **Proxy Type**: This is the type of proxy to use. Since there are two sock proxy versions, the options are 'socks4' and 'socks5.'
    - The proxy cannot be a HTTP/HTTPS proxy. This field is optional. If a socks proxy is not used, this field can be left blank.
7. Click **Save Changes** and ensure that the toggle next to the name of the integration is enabled (Displaying green).

Figure 8: ThreatQ User Interface Configuration



Once completed, the integration is ready for operation.

3.3 CRON

To run this script on a reoccurring basis use CRON or some other system schedule. The argument in the cron script **must** specify the config and log locations.

This can be run multiple times a day and should not be run more often than once per hour.

3.3.1 Setting Up the CRONJOB

1. Login via a CLI terminal session to your ThreatQ host.
2. Input the commands below.

Figure 9: Command Line Crontab Command

```
$> crontab -e
```

This will enable the editing of the crontab, using vi.

Depending on how often you wish the cronjob to run, you will need to adjust the time to suit the environment.

3. Input the commands below – this example shows every **4 Hours.**

Figure 10: Command Line Crontab tqIMAP Command

```
0 */4 * * * $> tqIMAP -c /path/to/config/directory/ -ll
/path/to/log/directory/ -f /path/to/files/directory --files files/
```

Figure 11: Command Line Crontab tqIMAP Command (Bespoke Name)

```
0 */4 * * * $> tq-imap -n <Bespoke_Name> -c /path/to/config/directory/ -
ll /path/to/log/directory/ -f /path/to/files/directory --files files/
```

To run this script on a reoccurring basis, use CRON or some other on system schedule. CRON is shown here.

The argument in the cron script **must** specify the config and log locations.

This can be run multiple times a day and should **not** be run more often than once per hour.

For further reference, see the ThreatQ Help Center.

Appendix A: Supplementary Information

IMAP Application Notes

- Running the ThreatQuotient for IMAP Application connector will look for all unread emails. Once the connector is run, it will 'read' the unread emails, making them display marked as read.
- This ThreatQuotient for IMAP Application will read the entire email including the attachments. If an attachment is present, it will upload the attachment to ThreatQ as a file. It will also attempt to parse the file and the email body looking for any indicators. If indicators are found, they will be related to the email's attachment.

Uninstalling the Connector

```
sudo pip uninstall tqIMAP
```

tq-imap command line options

The tqIMAP/tq-imap Driver has several command line arguments that will help you and your customers execute this. They are listed below. You can see these by executing `/usr/bin/tqIMAP --help.`

```
usage: tqIMAP Connector [-h] [-ll LOGLOCATION][-c CONFIG] [-v VERBOSITY]

tqIMAP
```

optional arguments:

```
  -h, --help
```

Shows the help message and exit

```
  -ll LOGLOCATION, --loglocation LOGLOCATION
```

This sets the logging location for this connector. The location should exist and be writable by the current user. A special value of 'stdout' means to log to the console (this happens by default).

```
  -c CONFIG, --config CONFIG
```

This is the location of the configuration file for the connector. This location must have read and write permissions for the current user. If no config file is given, the current directory will be used. This file is also where some information from each run of the connector may be put (e.g. last run time, private OAuth, etc).

```
  -v {1,2,3}, --verbosity {1,2,3}
```

This is the logging verbosity level. The Default is 1 (Warning).

Trademarks and Disclaimers

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR THREATQUOTIENT REPRESENTATIVE FOR A COPY.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THIRD PARTY SUPPLIERS ARE PROVIDED “AS IS” WITH ALL FAULTS. THREATQUOTIENT AND THIRD-PARTY SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL THREATQUOTIENT OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF THREATQUOTIENT OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

ThreatQuotient and the ThreatQuotient Logo are trademarks of ThreatQuotient, Inc. and/or its affiliates in the U.S. and other countries.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.