ThreatQuotient

Malware Patrol Connector Implementation Guide

Version 2.0.0

Wednesday, January 15, 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.

Copyright © 2020 ThreatQuotient, Inc.

All rights reserved. This document and the software product it describes are licensed for use under a software license agreement. Reproduction or printing of this document is permitted in accordance with the license agreement.

ThreatQuotient and Malware Patrol are trademarks of their respective companies.

Last Updated: Wednesday, January 15, 2020

Contents

Versioning

- Current integration version `2.0.0`
- Supported on ThreatQ versions `4.28` and later

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
- Phishing
- Anti Mining

ThreatQ Mapping

ThreatQ provides the following default mapping for the feed. The mapping summarizes how the information from each field from the feed is converted to ThreatQ specific objects.

Sinkhole IP Addresses Feed

This is in .csv format. For example:

```
104.155.11.149,15169,104.155.0.0/19,US,arin,2014-07-09
104.244.12.1,393667,104.244.12.0/24,US,arin,2014-11-06
104.244.12.10,393667,104.244.12.0/24,US,arin,2014-11-06
104.244.12.100,393667,104.244.12.0/24,US,arin,2014-11-06
```

ThreatQ mapping information is summarized below:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples
0 (first token)	indicator.value	IP Address	5 (Sixth Token)	104.155.11.149
1 (first token)	indicator.attribute	ASN	5 (Sixth Token)	15169
2 (first token)	indicator.value	CIDR Block	5 (Sixth Token)	104.155.0.0/19
3 (first token)	indicator.attribute	Country Code	5 (Sixth Token)	US
4 (first token)	indicator.attribute	Registry Entity	5 (Sixth Token)	arin

Malware URLs (Sanitized)

This is in gzipped json format. For example:

```
[
   {
      "malware_classification":"Trojan-Banker-
.Win32.Banker.etk",
      "malware_
SHA1":"7c9c5ed13022df06545be28b3193ee6baeb2e4b5",
      "ASN":"12479",
      "detection_timestamp":"20060119150041",
      "AS_information":"UNI2-AS Uni2 Autonomous System",
      "domain":"perso.wanadoo.es",
      "malware_URL":"http://perso.wanadoo.es/selviba101",
      "MBL_ID":"MBL#14021",
      "malware_extension":"exe",
      "malware_MD5":"fe516740fb2a7b7fe8411963fa5e0e57"
   },
   ...
]
```

ThreatQ mapping information is summarized below:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples
malware_URL	indicator.value	URL	.[].detection_timestamp	http://perso.wanadoo.es/selviba101
malware_SHA1	indicator.value	SHA1	.[].detection_timestamp	7c9c5ed13022df06545be28b3193ee6baeb2e4b5
malware_MD5	indicator.value	MD5	.[].detection_timestamp	fe516740fb2a7b7fe8411963fa5e0e57
malware_classification	indicator.attribute	Malware Classification		Trojan-Banker.Win32.Banker.etk
ASN	indicator.attribute	Classification		Trojan-Banker.Win32.Banker.etk
MBL_ID	indicator.attribute	Classification		12479

Command and Control Server Addresses (Sanitized)

This is in gzipped json format. For example:

```
[
   {
       "C2_URL":"http://www.technlip.com/wp-includes/-
pomo/joe/cp.php",
       "malware_family":"ZeuS",
       "detection_timestamp":"2014-03-30 19:14:47"
   },
   ...
]
```

ThreatQ mapping information is summarized below:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.[].C2_URL	indicator.value	URL	.[].detection_timestamp	http://www.technlip.com/wp-includes/-pomo/joe/cp.php	If it's a URL
.[].C2_URL	indicator.value	IP Address	.[].detection_timestamp	http://190.128.29.1:8080/webalizer/opt/cp.php	If it's an IP Address
.[].C2_URL	indicator.attribute	Scheme	.[].detection_timestamp	`tcp`, `udp`, `http` or `https`	
.[].C2_URL	indicator.attribute	Port	.[].detection_timestamp	8080	If the format is `url:port` or `ip:-port`
.[].mal-ware_fam-ily	indicator.attribute	Malware Family	.[].detection_timestamp	ZeuS	

Malware Hashes

This is in gzipped json format. For example:

```
[
   {
       "timestamp":"20060119150041",
       "md5":"fe516740fb2a7b7fe8411963fa5e0e57",
       "sha1":"7c9c5ed13022df06545be28b3193ee6baeb2e4b5",
       "classification":"TrojanBanker.Win32.Banker.etk"
   },
   ...
]
```

ThreatQ mapping information is summarized below:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples
.[].md5	indicator.value	MD5	.[].timestamp	fe516740fb2a7b7fe8411963fa5e0e57
.[].md5sha1	indicator.value	SHA1	.[].timestamp	7c9c5ed13022df06545be28b3193ee6baeb2e4b5
.[].m-d5classification	indicator.attribute	Malware Classification	.[].timestamp	TrojanBanker.Win32.Banker.etk

Malicious IP Addresses

This is in gzipped json format. For example:

```
[
   {
       "MBL_ID": "MBL-M-11386919",
       "IP_address": "122.226.188.6",
       "type": "malware_url",
       "classification": "Win32.210.Eldorado",
       "detection_timestamp": "20180714231621"
   },
   ...
]
```

ThreatQ mapping information is summarized below:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples
.[].IP_Address	indicator.value	IP Address	.[].detection_timestamp	122.226.188.6
.[].MBL_ID	indicator.attribute	MBL ID	.[].detection_timestamp	MBL-M-11386919
.[].classification	indicator.attribute	Malware Classification	.[].detection_timestamp	Win32.210.Eldorado
.[].type	indicator.attribute	Type	.[].detection_timestamp	malware_url

Real Time DDoS Attacks

This is in .csv format. For example:

```
20181117034914,hpot,US-DC02,132.232.237.18,11211,N/A,Am-
plification/Reflection,3,3,2
20181116020037,hpot,US-
DC02,197.219.208.66,11211,N/A,Amplification/Reflection,3,3,2
20181116170931,hpot,US-DC01,221.229.196.61,11211,N/A,Am-
plification/Reflection,3,3,2
20181116134950,hpot,US-
DC02,66.240.205.221,1900,12,Amplification/Reflection,3,3,2
```

ThreatQ mapping information is summarized below:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples
1 (second token)	indicator.attribute	Source		hpot
2 (third token)	indicator.attribute	Node		US-DC02
3 (fourth token)	indicator.value	IP Address	0 (first token)	132.232.237.18
4 (fifth token)	indicator.attribute	Port		11211
5 (sixth token)	indicator.attribute	Count		12
6 (eighth token)	indicator.attribute	Type		3
8 (ninth token)	indicator.attribute	Reliability		3
9 (tenth token)	indicator.attribute	Credibility		2

Domains Generated via DGA

This is in gzipped json format. For example:

```
[
   {
       "domain": "zpjnllaabettingk.com",
       "classification": "Banjori",
       "timestamp": "0000-00-00 00:00:00"
   },
   ...
]
```

ThreatQ mapping information is summarized below:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples
.[].domain	indicator.value	FQDN	.[].timestamp	zpjnllaabettingk.com
.[].classification	indicator.attribute	Malware Classification		Banjori

Phishing

This is in gzipped json format. For example:

```
[
   {
       "domain": "shamoc.com",
       "language": "ro",
       "brand": "Microsoft",
       "id": "396390",
       "screenshot_file_name": "cd5c732c566ada475ef2acdc5fdfd081",
       "domain_ranking": "0",
       "score": "100",
       "flag_screenshot": "1",
       "detection_timestamp": "2019-09-23 21:35:54",
       "url": "http://www.christianbeaulieu.com/wp-includes/-
pomo/dol/uy131aguhv8lqpk9tsq63z1r.php"
   },
   ...
]
```

ThreatQ mapping information is summarized below:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples
.[].domain	indicator.value	FQDN	detection_timestamp	shamoc.com
.[].screen-shot_file_name	indicator.value	Filename	detection_timestamp	cd5c732c566ada475ef2acdc5fdfd081
.[].url	indicator.value	URL	detection_timestamp	http://www.christianbeaulieu.com/wp-includes/-pomo/dol/uy131aguhv8lqpk9tsq63z1r.php
.[].language	indicator.attribute	Language	detection_timestamp	ro
.[].id	indicator.attribute	ID	detection_timestamp	396390
.[].flag_screen-shot	indicator.attribute	Flag Screenshot	detection_timestamp	1
.[].detection_timestamp	indicator.attribute	Detected At	detection_timestamp	2019-09-23 21:35:54

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples
.[].brand	indicator.attribute	Brand	detection_timestamp	Microsoft
.[].score	indicator.attribute	Score	detection_timestamp	100
.[].domain_ranking	indicator.attribute	Domain Ranking	detection_timestamp	0

Anti Mining

This is in gzipped json format. For example:

```
[
   {
       "domain": "tovar4ka.ru",
       "IP":"5.101.152.21"
       "rank":">30M"
   },
   ...
]
```

ThreatQ mapping information is summarized below:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples
.[].domain	indicator.value	FQDN	tovar4ka.ru
.[].IP	indicator.value	IP Address	5.101.152.21
.[].rank	indicator.attribute	Rank	30M

Installation

Complete the following steps to install the connector:

1. Log into https://marketplace.threatq.com.
2. Download the **Malware Patrol 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 the **Commercial** tab. You will still need to configure and then enable the feed.

ThreatQ User Interface Configuration

All Malware Patrol Feeds have the same configuration parameters as detailed below.

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 vendor-supplied username.
Password	The vendor-supplied password.
Domain	The domain name of the feeds hosting server (E.g. .malwarepatrol.net)

5. Click on **Save Changes**.
6. Click on the toggle switch to the left of the feed name to enable the feed.