ThreatQuotient

Malware Patrol CDF User Guide

Version 2.0.1

July 17, 2023

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

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.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	2.0.1
Compatible with ThreatQ Versions	>= 4.28.0
Support Tier	ThreatQ Supported

Introduction

The Malware Patrol CDF for ThreatQ ingests threat intelligence data from several Malware Patrol feeds:

- Malware URLs (Sanitized)
- Command and Control Server Addresses (Sanitized)
- Malware Hashes
- Malicious IP Addresses
- Real Time DDoS Attacks
- Domains Generated via DGA
- Malware Patrol - Phishing
- Malware Patrol - Anti Mining

The integration ingests indicators and indicator attributes into the ThreatQ platform.

Installation

Perform the following steps to install the integration:

> The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the integration file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the integration 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.

6. If prompted, select the individual feeds to install and click **Install**. The feed will be added to the integrations page.

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 integration-related credentials.

To configure the integration:

1. Navigate to your integrations management page in ThreatQ.
2. Select the **Commercial** option from the *Category* dropdown (optional).

   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Username	Your Malware Patrol account username.
Password	Your Malware Patrol account password.
Domain	The domain name of the feeds hosting server (E.g. .malwarepatrol.net)

5. Review any additional settings, make any changes if needed, and click on **Save**.
6. Click on the toggle switch, located above the *Additional Information* section, to enable it.

ThreatQ Mapping

Malware Patrol Malware URLs (Sanitized)

Gunzipped JSON Sample Response:


```
[
    {
        "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"
    },
    ...
]
```


ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	NOTES
.[].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	.[].detection_timestamp		Trojan-Banker.Win32.Banker.etk	
.[].ASN	indicator.attribute	Classification	.[].detection_timestamp		Trojan-Banker.Win32.Banker.etk	
.[].MBL_ID	indicator.attribute	Classification	.[].detection_timestamp		12479	See Above

Malware Patrol Command and Control Server Addresses (Sanitized)

Gunzipped JSON Sample Response:

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

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	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`
.[].malware_family	indicator.attribute	Malware Family		.[].detection_timestamp	ZeuS	

Malware Patrol Malware Hashes

Gunzipped JSON Sample Response:

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

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
[].md5	indicator.value	MD5	.[].timestamp	fe516740fb2a7b7fe8411963fa5e0e57	
.[].sha1	indicator.value	SHA1	.[].timestamp	7c9c5ed13022df06545be28b3193ee6baeb2e4b5	
. [].classification	indicator.attribute	Malware Classification	.[].timestamp	TrojanBanker.Win32.Banker.etk	

Malware Patrol Malicious IP Addresses

Gunzipped JSON Sample Response:

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

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.[].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	

Malware Patrol Real Time DDoS Attacks

CSV Sample Response:

```
20181117034914,hpot,US-DC02,132.232.237.18,11211,N/A,Amplification/
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,Amplification/
Reflection,3,3,2
20181116134950,hpot,US-DC02,66.240.205.221,1900,12,Amplification/
Reflection,3,3,2
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	NOTES
1 (second token)	indicator.attribute	Source	0 (first token)		hpot	
2 (third token)	indicator.attribute	Node	0 (first token)		US-DC02	
3 (fourth token)	indicator.value	IP Address		0 (first token)	132.232.237.18	
4 (fifth token)	indicator.attribute	Port	0 (first token)		11211	
5 (sixth token)	indicator.attribute	Count	0 (first token)		12	
6 (eighth token)	indicator.attribute	Type	0 (first token)		3	
8 (ninth token)	indicator.attribute	Reliability	0 (first token)		3	
9 (tenth token)	indicator.attribute	Credibility	0 (first token)		2	

Malware Patrol Domains Generated via DGA

Gunzipped JSON Sample Response:

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

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	NORMALIZATION	PUBLISHED DATE	EXAMPLES	NOTES
.[].domain	indicator.value	FQDN		.[].timestamp	zpjnllaabettingk.com	
.[].classification	indicator.attribute	Malware Classification	.[].timestamp		Banjori	

Malware Patrol - Anti Mining

Gunzipped JSON Sample Response:

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

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.[].domain	indicator.value	FQDN		tovar4ka.ru	
.[].IP	indicator.value	IP Address		5.101.152.21	
.[].rank	indicator.attribute	Rank		30M	
.[].domain	indicator.value	FQDN		.[].timestamp	zpjnllaabettingk.com
.[].classification	indicator.attribute	Malware Classification	.[].timestamp		Banjori

Malware Patrol - Phishing

Gunzipped JSON Sample Response:

```
[
    {
        "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"
    },
    ...
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES
.[].domain	indicator.value	FQDN	.[].detection_timestamp	"shamoc.com"
.[].screenshot_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_screenshot	indicator.attribute	Flag Screenshot	.[].detection_timestamp	"1"
.[].detection_timestamp	indicator.attribute	Detected At	.[].detection_timestamp	"2019-09-23 21:35:54"
.[].brand	indicator.attribute	Brand	.[].detection_timestamp	"Microsoft"
.[].score	indicator.attribute	Score	.[].detection_timestamp	"100"
.[].domain_ranking	indicator.attribute	Domain Ranking	.[].detection_timestamp	"0"

Average Feed Run

> Object counts and Feed runtime are 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.

Malware Patrol Malware URLs (Sanitized)

METRIC	RESULT
Run Time	1 minute
Indicators	0
Indicator Attributes	0

Malware Patrol Command And Control Server Addresses (Sanitized)

METRIC	RESULT
Run Time	2 minutes
Indicators	1,189
Indicator Attributes	3,537

Malware Patrol Hashes

METRIC	RESULT
Run Time	58 minutes
Indicators	72,248
Indicator Attributes	72,258

Malware Patrol Malicious IP Addresses

METRIC	RESULT
Run Time	53 minutes
Indicators	10,167
Indicator Attributes	76,351

Malware Patrol Real Time DDoS Attacks

METRIC	RESULT
Run Time	11 minutes
Indicators	4,002
Indicator Attributes	25,066

Malware Patrol Domains Generated via DGA

METRIC	RESULT
Run Time	37 minutes
Indicators	56,969
Indicator Attributes	57,261

Malware Patrol - Anti Mining

METRIC	RESULT
Run Time	1 minute
Indicators	856
Indicator Attributes	894

Malware Patrol - Phishing

METRIC	RESULT
Run Time	4 minutes
Indicators	858
Indicator Attributes	8,533

Change Log

- **Version 2.0.1**
  - Removed deprecated feed - **Malware Patrol Sinkhole IP Addresses**.
  - Resolved a parsing issue with the **Malware Patrol Real Time DDoS Attacks** feed.
- **Version 2.0.0**
  - N/A
- **Version 1.2.0**
  - N/A
- **Version 1.0.0**
  - N/A