Malware Patrol Connector Implementation Guide

Version 1.2.0

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, November 27, 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

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	IP Address	5 (Fifth Token)	104.155.11.149
1 (first token)	Indicator Attribute	ASN	5 (Fifth Token)	15169
2 (first token)	Indicator	CIDR Block	5 (Fifth Token)	104.155.0.0/19
3 (first token)	Indicator Attribute	Country Code	5 (Fifth Token)	US
4 (first token)	Indicator Attribute	Registry Entity	5 (Fifth 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	URL	detection_timestamp	http://perso.wanadoo.es/selviba101
malware_SHA1	Indicator	SHA1	detection_timestamp	7c9c5ed13022d-f06545be28b3193ee6baeb2e4b5
malware_	Indicator	MD5	detection_	fe516740f-b2a7b7fe8411963fa5e0e57

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples
MD5			timestamp	
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
C2_URL	Indicator	URL	detection_timestamp	http://www.technlip.com/wp-includes/-pomo/joe/cp.php
C2_URL	Indicator	IP Address	detection_timestamp	http://190.128.29.1:8080/webalizer/opt/cp.php
C2_URL	Indicator Attribute	Scheme		`tcp`, `udp`, `http` or `https`

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples
C2_URL	Indicator Attribute	Port		8080
malware_family	Indicator Family	Malware Family		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	MD5	timestamp	fe516740f-b2a7b7fe8411963fa5e0e57
sha1	Indicator	SHA1	timestamp	7c9c5ed13022d-f06545be28b3193ee6baeb2e4b5
classification	Indicator Attribute	Malware Classification		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	IP Address	detection_timestamp	122.226.188.6
MBL_ID	Indicator Attribute	MBL ID		MBL-M-11386919
classification	Indicator Attribute	Malware Classification		Win32.210.Eldorado
type	Indicator Attribute	Type		malware_url

Real Time DDoS Attacks

This is in .csv format. For example:

```
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
```

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	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	FQDN	timestamp	zpjnllaabettingk.com
classification	Indicator Attribute	Malware Classification		Banjori

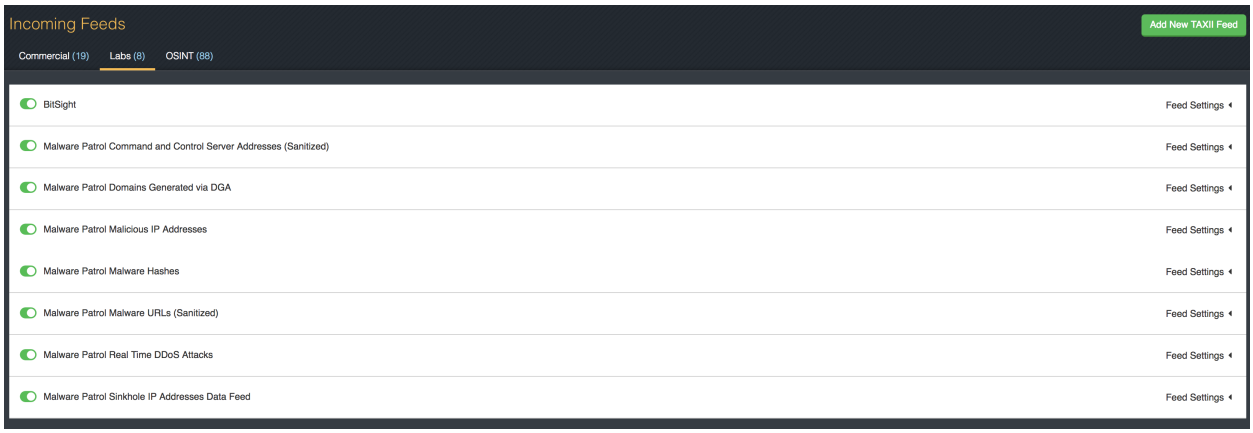
Installation

The following artisan command will install the feed definition (in `yaml` format) on the ThreatQ platform.

```
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)