ThreatQuotient

Bambenek Feeds Implementation Guide

Version 2.1.1

Monday, August 17, 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.

Last Updated: Monday, August 17, 2020

Contents

Versioning

- Current integration version `2.1.1`
- Supported on ThreatQ versions >= `4.27.0`

Introduction

The following feeds/endpoints are included in the Bambenek version 2.1.0 download.

- Bambenek Consulting - C2 IP
- Bambenek Consulting - C2 Domain
- Bambenek Consulting - C2 All Indicators
- Bambenek Consulting - DGA Domain
- Bambenek Consulting - High-Confidence C2 IP
- Bambenek Consulting - High-Confidence C2 Domain
- Bambenek Consulting - High-Confidence C2 All Indicators
- Bambenek Consulting - High-Confidence DGA Domain
- Bambenek Consulting - Bamital Master
- Bambenek Consulting - Banjori Master
- Bambenek Consulting - Bebloh/URLZone Master
- Bambenek Consulting - Bedep Master
- Bambenek Consulting - Beebone Master
- Bambenek Consulting - Chinad Master
- Bambenek Consulting - Corebot Master
- Bambenek Consulting - Cryptolocker Master
- Bambenek Consulting - Dircrypt Master
- Bambenek Consulting - Dromedan Master
- Bambenek Consulting - Dyre Master
- Bambenek Consulting - Fobber Master
- Bambenek Consulting - G01 Master
- Bambenek Consulting - Geodo Master
- Bambenek Consulting - Gozi Master
- Bambenek Consulting - Hesperbot Master
- Bambenek Consulting - Kraken Master
- Bambenek Consulting - Locky Master
- Bambenek Consulting - Madmax Master
- Bambenek Consulting - Matsnu Master
- Bambenek Consulting - Mirai Master
- Bambenek Consulting - Murofet Master
- Bambenek Consulting - Necurs Master
- Bambenek Consulting - Nymaim Master
- Bambenek Consulting - P2P GOZ Master
- Bambenek Consulting - Pandabanker Master
- Bambenek Consulting - PT GOZ / New GOZ Master
- Bambenek Consulting - Padcrypt Master
- Bambenek Consulting - Pizd Master
- Bambenek Consulting - Proslikefan Master
- Bambenek Consulting - Pushdo Master
- Bambenek Consulting - Pykspa Master
- Bambenek Consulting - Qadars Master
- Bambenek Consulting - Qakbot Master
- Bambenek Consulting - Ramdo Master
- Bambenek Consulting - Ramnit Master
- Bambenek Consulting - Ranbyus Master

- Bambenek Consulting - Shifu Master
- Bambenek Consulting - Simda Master
- Bambenek Consulting - Sisron Master
- Bambenek Consulting - Sphinx Master
- Bambenek Consulting - Suppobox Master
- Bambenek Consulting - Symmi Master
- Bambenek Consulting - Tempedreve Master
- Bambenek Consulting - Tinba / TinyBanker Master
- Bambenek Consulting - Tinynuke Master
- Bambenek Consulting - Tofsee Master
- Bambenek Consulting - Unknowndropper Master
- Bambenek Consulting - Unknownjs Master
- Bambenek Consulting - Vawtrak Master
- Bambenek Consulting - Vidro Master
- Bambenek Consulting - Virut Master
- Bambenek Consulting - Volatile Cedar / Explosive Master

Installation

Perform the following steps to install the feed:

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

1. Log into https://marketplace.threatq.com/.
2. Locate and download the **Bambenek** feeds file.
3. Navigate to your ThreatQ instance.
4. Click on the **Settings** icon and select **Incoming feeds**.
5. Click on the **Add New Feed** button.
6. Upload the feed file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the feed 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.

The feeds will be added to the **Commercial** tab for Incoming Feeds. 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 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.
URL	Bambenek Consulting URL (only for display purposes).

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

ThreatQ Mapping

Feeds containing 'Master' or 'All Indicators' in their name mapping

Text format with comma separated values.

Example:

```
aakamen.com,78.24.9.52,ns2.vshosting.cz |
ns.aakamen.com|poski.vshosting.cz,78.24.9.52 |
89.235.0.2,Master Indicator Feed for banjori non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/banjori.txt

aaskmen.com,103.224.212.222,ns15.above.com |
ns16.above.com,103.224.212.5 | 103.224.212.6,Master Indicator
Feed for banjori non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/banjori.txt

aifamen.com,157.52.223.233,juming.dnsdun.com |
juming.dnsdun.net | v1.dnsdun.com |
v1.dnsdun.net,47.96.179.127 | 104.152.45.130 | 104.152.45.131
| 116.1.237.4 | 122.228.80.247 | 172.247.255.190,Master
Indicator Feed for banjori non-sinkholed
domains,http://osint.bambenekconsulting.com/manual/banjori.txt
```

The mapping table is below.

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Example
1 (first token)	indicator.value	FQDN	aakamen.com
2 (second token)	indicator.value	IP Address	78.24.9.52
3 (third token)	indicator.value	FQDN	vshosting.cz, ns.aakamen.com, poski.vshosting.cz
4 (fourth token)	indicator.value	IP Address	78.24.9.52, 89.235.0.2
5 (fifth token)	indicator.attribute	Description	Master Indicator Feed for banjori non-sinkholed domains
6 (sixth token)	indicator.attribute	Source	http://osint.bambenekconsulting.com/manual/banjori.txt

Feeds containing 'IP' in their name mapping

Text format with comma separated values.

Example:

```
5.79.79.209,IP used by banjori C&C,2019-11-20
19:03,http://osint.bambenekconsulting.com/manual/banjori.txt

14.192.4.35,IP used by banjori C&C,2019-11-20
19:03,http://osint.bambenekconsulting.com/manual/banjori.txt

18.213.250.117,IP used by banjori C&C,2019-11-20
19:03,http://osint.bambenekconsulting.com/manual/banjori.txt
```

The mapping table is below.

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Example
1 (first token)	indicator.value	IP Address	5.79.79.209
2 (second token)	indicator.attribute	Description	IP used by banjori C&C
3 (third token)	indicator.published_at	Published At	2019-11-20 19:03
4 (fourth token)	indicator.attribute	Source	http://osint.bambenekconsulting.com/manual/banjori.txt

Feeds containing 'Domain' in their name mapping

Text format with comma separated values.

Example:

```
jaxwolcxabjzcexx0p.com,Domain used by bedep,2019-11-20
19:08,http://osint.bambenekconsulting.com/manual/bedep.txt

llyamcjgytzaw5n.com,Domain used by bedep,2019-11-20
19:08,http://osint.bambenekconsulting.com/manual/bedep.txt

yjkcbwknkzqdnirl.com,Domain used by bedep,2019-11-20
19:08,http://osint.bambenekconsulting.com/manual/bedep.txt
```

The mapping table is below.

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Example
1 (first token)	indicator.value	FQDN	axwolcxabjzcexx0p.com
2 (second token)	indicator.attribute	Description	Domain used by bedep
3 (third token)	indicator.published_at	Published At	2019-11-20 19:08
4 (fourth token)	indicator.attribute	Source	http://osint.bambenekconsulting.com/manual/bedep.txt

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.

Feeds containing 'Master' or 'All Indicators' in their name mapping.

Metric	Result
Run Time	10 minutes
Indicators	800
Indicator Attributes	1,600

Feeds containing 'IP' in their name mapping.

Metric	Result
Run Time	3 minutes
Indicators	150
Indicator Attributes	320

Feeds containing 'Domain' in their name mapping.

Metric	Result
Run Time	4 hours
Indicators	350,000
Indicator Attributes	740,000

Change Log

- **Version 2.1.1**
  - Changed feed category from OSINT to Commercial.
- **Version 2.1.0**
  - Updated Nameserver from Attribute to Indicator.
- **Version 2.0.0**
  - Initial Release