

ThreatQuotient



DNS Twister CDF

Version 1.0.0

June 25, 2024

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 3

Support 4

Integration Details..... 5

Introduction 6

Installation..... 7

Configuration 8

ThreatQ Mapping..... 10

 DNS Twister 10

 Get Domain Fuzz (Supplemental)..... 11

 Get Domain IP (Supplemental) 13

 Get Domain MX (supplemental) 14

Average Feed Run..... 15

Known Issues / Limitations 16

Change Log 17

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 © 2024 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.

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	1.0.0
Compatible with ThreatQ Versions	>= 5.24.1
Support Tier	ThreatQ Supported

Introduction

DNS fuzzing is an automated workflow that aims to uncover potentially malicious domains that target your organization by generating a comprehensive list of permutations based on a provided domain name, and subsequently verifies whether any of these permutations are in use in DNS currently.

The DNS Twister CDF can ingest all variations or just currently active variants. Additionally, you can add known-good variants to avoid creating unwanted indicators.

The integration provides the following feed:

- **DNS Twister** - performs fuzzing of corporate domains and lookup in DNS.

The integration ingests indicator system objects.

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 yaml file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration yaml file using one of the following methods:
 - Drag and drop the file into the dialog box
 - Select **Click to Browse** to locate the file on your local machine
6. Select the individual feeds to install, when prompted and click **Install**.



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 feed(s) 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 **OSINT** 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
Source Domain	Enter a line-delimited list of domains to fuzz with DNS Twister.
Domains to Ignore	<p>Enter a line-delimited list of domains to ignore.</p> <p>Example: If your primary domain is <code>brandname.com</code>, you might already have <code>brandname.org</code> and <code>brandname.net</code> that you wouldn't want to ingest each time. These alternatives can be added to the list to be skipped.</p>
Ingest All Variations	<p>Enable this option to ingest all variations. This option is not enabled by default, which means the integration will ingest only those variations that have DNS entries to resolve.</p> <div>  Exercise caution before enabling this configuration option. </div>

< DNS Twister



Disabled Enabled

Run Integration

Uninstall

Additional Information

Integration Type: Feed

Version:

Configuration Activity Log

Source Domains

bbc.com

New line delimited list of the domains we want to fuzz with DnsTwister

Domains To Ignore

jbc.com

rbc.com

New line delimited list of the domains we don't want to ingest (known variations)

☐ Ingest All Variations

Choose whether to ingest all variations or just those that resolve.

- Set indicator status to...

Active

Run Frequency

Every 24 Hours

Next scheduled run:

2024-06-20 04:12am (-04:00)

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

ThreatQ Mapping

DNS Twister

The DNS Twister feed takes the FQDN provided and converts it to the hexadecimal format required by the fuzzer.

GET https://dnstwister.report/api/to_hex/<domain>

Sample Response:

```
{
  "domain": "bbc.com",
  "domain_as_hexadecimal": "6262632e636f6d",
  "fuzz_url": "https://dnstwister.report/api/fuzz/6262632e636f6d",
  "has_mx_url": "https://dnstwister.report/api/mx/6262632e636f6d",
  "parked_score_url": "https://dnstwister.report/api/parked/6262632e636f6d",
  "resolve_ip_url": "https://dnstwister.report/api/ip/6262632e636f6d",
  "url": "https://dnstwister.report/api/to_hex/bbc.com"
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
main	Attribute	Original Domain	N/A	bbc.com	This represents the original domain that seeded the fuzzer. It's added as an attribute rather than indicator to avoid needing to store whitelisted indicators.

Get Domain Fuzz (Supplemental)

The Get Domain Fuzz supplemental feed generates a list of fuzzed domains based on the hexadecimal variant of your initial brand domain.

GET <https://dnstwister.report/api/fuzz/<domain-as-hex>>

Sample Response:

```
{
  "domain": "bbc.com",
  "domain_as_hexadecimal": "6262632e636f6d",
  "fuzzy_domains":
  [
    {
      "domain": "bbc.com",
      "domain_as_hexadecimal": "6262632e636f6d",
      "fuzz_url": "https://dnstwister.report/api/fuzz/6262632e636f6d",
      "fuzzer": "Original",
      "has_mx_url": "https://dnstwister.report/api/mx/6262632e636f6d",
      "parked_score_url": "https://dnstwister.report/api/parked/
6262632e636f6d",
      "resolve_ip_url": "https://dnstwister.report/api/ip/6262632e636f6d"
    },
    {
      "domain": "cbc.com",
      "domain_as_hexadecimal": "6362632e636f6d",
      "fuzz_url": "https://dnstwister.report/api/fuzz/6362632e636f6d",
      "fuzzer": "Bitsquatting",
      "has_mx_url": "https://dnstwister.report/api/mx/6362632e636f6d",
      "parked_score_url": "https://dnstwister.report/api/parked/
6362632e636f6d",
      "resolve_ip_url": "https://dnstwister.report/api/ip/6362632e636f6d"
    },
    {
      "domain": "fbc.com",
      "domain_as_hexadecimal": "6662632e636f6d",
      "fuzz_url": "https://dnstwister.report/api/fuzz/6662632e636f6d",
      "fuzzer": "Bitsquatting",
      "has_mx_url": "https://dnstwister.report/api/mx/6662632e636f6d",
      "parked_score_url": "https://dnstwister.report/api/parked/
6662632e636f6d",
      "resolve_ip_url": "https://dnstwister.report/api/ip/6662632e636f6d"
    }
  ],
  "has_mx_url": "https://dnstwister.report/api/mx/6262632e636f6d",
  "parked_score_url": "https://dnstwister.report/api/parked/6262632e636f6d",
  "resolve_ip_url": "https://dnstwister.report/api/ip/6262632e636f6d",
  "url": "https://dnstwister.report/api/fuzz/6262632e636f6d"
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
fuzzy_domains[].domain	Indicator	FQDN	N/A	cbc.com	Primary output from the feed, a domain created by fuzzing the original
fuzzy_domains[].domain_as_hexadecimal	Attribute	Domain as Hex	N/A	6362632e636f6d	An unambiguous representation of the fuzzed domain ingested.
fuzzy_domains[].fuzzer	Attribute	Fuzz Method	N/A	Bitsquatting	The method used to turn the original domain into the ingested domain.

Get Domain IP (Supplemental)

The Get Domain IP supplemental feed collects the IP that is behind the domain, if it resolves.

GET <https://dnstwister.report/api/ip/<domain-as-hex>>

Sample Response:

```
{
  "domain": "cbc.com",
  "domain_as_hexadecimal": "6362632e636f6d",
  "error": false,
  "fuzz_url": "https://dnstwister.report/api/fuzz/6362632e636f6d",
  "has_mx_url": "https://dnstwister.report/api/mx/6362632e636f6d",
  "ip": "121.78.127.249",
  "parked_score_url": "https://dnstwister.report/api/parked/6362632e636f6d",
  "url": "https://dnstwister.report/api/ip/6362632e636f6d"
}
```

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	Indicator	IP	N/A	121.78.127. .249	Secondary output from the feed, an IP that the fuzzed domain maps to. Added as Indirect status

Get Domain MX (supplemental)

GET <https://dnstwister.report/api/mx/<domain-as-hex>>

Sample Response:

```
{
  "domain": "cbc.com",
  "domain_as_hexadecimal": "6362632e636f6d",
  "error": false,
  "fuzz_url": "https://dnstwister.report/api/fuzz/6362632e636f6d",
  "mx": true,
  "parked_score_url": "https://dnstwister.report/api/parked/6362632e636f6d",
  "resolve_ip_url": "https://dnstwister.report/api/ip/6362632e636f6d",
  "url": "https://dnstwister.report/api/mx/6362632e636f6d"
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
mx	Attribute	Domain has MX	N/A	Yes	Whether the domain has an MX record for this domain, the value of true or false is mapped to "Yes" or "No", respectively.

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.

METRIC	RESULT
Run Time	3 minutes
Indicators	150
Indicator Attributes	600

Known Issues / Limitations

- Excessive use can result in temporary rejection of requests due to rate limiting. The feed has some built-in rate limiting to assist with this.

Change Log

- Version 1.0.0
 - Initial release