ThreatQuotient

Project Zero: 0Day 'In the Wild' Feed Guide

Version 1.0.0

Friday, June 26, 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: Friday, June 26, 2020

Contents

Versioning

- Current integration version `1.0.0`
- Supported on ThreatQ versions >= `4.27.0`

Introduction

This Project Zero: 0day 'In the Wild' integration consumes data from the Project Zero: 0day 'In the Wild' spreadsheet that tracks known cases of zero-day exploits found in the wild. The spreadsheet is provided by Project Zero as a community resource and not a feed.

There are no guarantees around the timeliness of the data provided and it may become unmaintained at any point. Only enable this data source if you accept these limitations.

The spreadsheet can be found at:

https://-docs.google.com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY

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 **Project Zero: 0Day 'In the Wild'** integration 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 feed will be added to the **OSINT** 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 **OSINT** tab.
3. Click on the **Feed Settings** link for the feed.
4. Under the **Connection** tab, enter the following configuration parameter:

Parameter	Description
Ingest CVEs As	Select whether to ingest CVEs as ThreatQ Vulnerability objects, Indicator objects, or both. The default is to ingest only Vulnerability objects.

5. Click on **Save Changes**.
6. Click on the toggle switch next to the feed name to enable it.

ThreatQ Mapping

The feed is provided in CSV format.

```
GET https://-
doc-
s.google.-
com/spreadsheets/d/1lkNJ0uQwbeC1ZTRrxdtuPLCIl7mlUreoKfSIgajnSyY/export?format=csv&gid=1123292625
```

```
CVE,Vendor,Product,Type,Description,Date Discovered,Date Patched,Advisory,Analysis URL,Claimed Attribution,Claimed Attribution URL,
CVE-2020-6819,Mozilla,Firefox,Memory Corruption,Use-after-free while running the nsDocShell destructor,???,2020-04-03,https://www.mozilla.org/en-US/security/advisories/mfsa2020-11/,???,???,???,
CVE-2020-8467,TrendMicro,Apex One/OfficeScan,Unspecified,Unspecified vulnerability in a migration tool component,???,2020-03-16,https://success.trendmicro.com/solution/000245571,???,???,???,
CVE-2019-1458,Microsoft,Windows,Memory Corruption,Memory corruption in window switching,???,2019-12-10,https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-1458,ht-tps://securelist.com/windows-0-day-exploit-cve-2019-1458-used-in-operation-wiz-ardopium/95432/,WizardOpium,https://securelist.com/windows-0-day-exploit-cve-2019-1458-used-in-operation-wizardopium/95432/,
```

```
CVE-2019-1429,Microsoft,Internet Explorer,Memory Corruption,Unspecified memory corruption in
Internet Explorer,???,2019-11-12,https://portal.msrc.microsoft.com/en-us/security-guid-
ance/advisory/CVE-2019-1429,???,???,???,
CVE-2019-13720,Google,Chrome,Memory Corruption,Use-after-free in audio,???,2019-10-31,ht-
tps://chromereleases.googleblog.com/2019/10/stable-channel-update-for-desktop_31.htm-
l,https://securelist.com/chrome-0-day-exploit-cve-2019-13720-used-in-operation-
wizardopium/94866/,WizardOpium,https://securelist.com/chrome-0-day-exploit-cve-2019-13720-used-
in-operation-wizardopium/94866/,
CVE-2019-18187,Trend Micro,OfficeScan,Logic/Design Flaw,Directory traversal in ZIP file extrac-
tion,???,2019-10-28,ht-
tps://success.trendmicro.com/solution/000151730,???,Tick,https://www.zdnet.com/article/trend-
micro-antivirus-zero-day-used-in-mitsubishi-electric-hack/,
CVE-2019-2215,Google,Android,Memory Corruption,Use-after-free in Binder,2019-09-26,2019-10-06,ht-
tps://source.android.com/security/bulletin/2019-10-01.html#kernel-b,ht-
tps://bugs.chromium.org/p/project-zero/issues/detail?id=1942,NSO
Group,https://bugs.chromium.org/p/project-zero/issues/detail?id=1942#c7,
CVE-2019-1367,Microsoft,Windows,Memory Corruption,Unspecified memory corruption in Internet
Explorer,???,2019-09-23,https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-
2019-1367,???,Dark Hotel,https://twitter.com/craiu/status/1176525773869649921, ~
```

ThreatQ provides the following default mapping for this feed:

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
0 (first token)	Vulnerability.Value, Indicator.Value	CVE	N/A	CVE-2019-1458	Vulnerability and Indicator objects are conditionally ingested depending on the value of the `Ingest CVEs As` configuration parameter.
1 (second token)	Vulnerability.Attribute, Indicator.Attribute, Adversary.Attribute	Vendor	N/A	Mozilla	
2 (third token)	Vulnerability.Attribute, Indicator.Attribute, Adversary.Attribute	Product	N/A	Firefox	
3 (fourth token)	Vulnerability.Attribute, Indicator.Attribute, Adversary.Attribute	Type	N/A	Memory Corruption	
4 (fifth	Vulnerability.Attribute,	Description	N/A	Use-after-free while running the	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
token)	Indicator.Attribute			nSDocShell destructor	
5 (sixth token)	Vulnerability.Attribute, Indicator.Attribute	Date Discovered	N/A	2020-04-03	May be `???` in response if no data is available
6 (seventh token)	Vulnerability.Attribute, Indicator.Attribute	Date Patched	N/A	2020-04-03	May be `???` in response if no data is available
7 (eighth token)	Vulnerability.Attribute, Indicator.Attribute	Advisory	N/A	https://www.mozilla.org/en-US/security/advisories/mfsa2020-11/	
8 (ninth token)	Vulnerability.Attribute, Indicator.Attribute	Analysis URL	N/A	https://bugs.chromium.org/p/project-zero/issues/detail?id=1942	
9 (tenth token)	Adversary.Value	N/A	N/A	NSO Group	
10 (eleventh token)	Vulnerability.Attribute, Indicator.Attribute, Adversary.Attribute	Reference URL	N/A	https://bugs.chromium.org/p/project-zero/issues/detail?id=1942#c7	

Feed Data Path	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
N/A	Vulnerability.Attribute, Indicator.Attribute	Exploit Exists	N/A	True	Will always be `True`
N/A	Vulnerability.Attribute, Indicator.Attribute	Observed as 0-day	N/A	True	Will always be `True`

Average Feed Run

Average Feed Run results for Project Zero 0day 'In the wild':

Metric	Result
Run Time	< 1 minute
Indicators	120
Indicator Attributes	1100
Vulnerabilities	120
Vulnerability Attributes	1100
Adversaries	50

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.

Known Issues/Limitations

Due to the feed's update frequency, it is recommended to run this feed **daily** as opposed to hourly.

Changelog

- **Version 1.0.0**
  - Initial release