ThreatQuotient

Kaspersky APT Reports Feed Implementation Guide

Version 1.0.1

Monday, January 6, 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, January 6, 2020

Contents

Versioning

- Current integration version `1.0.1`
- Supported on ThreatQ versions >= `4.27.0`

Introduction

The Kaspersky APT Reports feed ingests threat intelligence data from the following endpoints:

- **Kaspersky APT Reports Get List** - https://tip.kaspersky.com/api/publications/get_list
- **Kaspersky APT Reports Get One** - https://tip.kaspersky.com/api/publications/get_one

Notes:

- A username, password, client certificate, and client private key are used for HTTP authentication.

  > ThreatQuotient does not issue third-party credentials. Contact Kaspersky for the required credentials.

- Time constrained data fetching is possible.

Installation

Complete the following steps to install the feed:

> The steps below can also be used to update the feed.

1. Log into https://marketplace.threatq.com.
2. Download the **Kaspersky APT Reports yaml** file.
3. From the ThreatQ user interface, select the **Settings icon > Incoming Feeds**.
4. Click **Add New Feed**.
5. In the Add New Feed dialog box, complete one of the following actions:
   - Drag and drop the yaml file into the dialog box.
   - Select **Click to browse** to locate the yaml 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 appear under the **Commercial** feeds heading.

You will still need to configure then enable the feed. See the Configuration section.

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 vendor-supplied email address and API key.

   The Kaspersky APT Reports feed supports multiple configuration parameters:

Parameter	Description
Username	You Kaspersky Username.
Password	Your Kaspersky Password.
Client Private Key	The Kaspersky Client Private Key.
Client Certificate	The Kaspersky Certificate.
Language	Language in which the execsum and pdf files are fetched. Available languages: • English • Portuguese • Russian

Parameter	Description
	- Spanish Note that if a file is not available in the selected language, the file will not be downloaded.

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

ThreatQ Mapping

The Kaspersky APT Reports feed provides an API that users can use to extract data in JSON format.

Each response from the provider contains the following parameters:

Kaspersky to ThreatQ Indicator Type Mapping

```
md5: MD5
sha256: SHA-256
IP: IP Address
UrlHistoryItem/URL: URL
Network/DNS: FQDN
FileItem/Md5sum: MD5
FileItem/Sha256sum: SHA-256
FileItem/FileName: Filename
RegistryItem/KeyPath: Registry Key
RouteEntryItem/Destination: FQDN
```

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.report_yara	signature.value	Signature Value	<base_64_encoded_gziped_data>	YARA - parsed
.report_pdf	attachment	Threat File	<pdf_base_64_encoded_gziped_data>	*
.report_execsum	attachment	Threat File	<execsum_base_64_encoded_gziped_data>	*

* The format will be as follows: **Kaspersky_PDF_<id>_<lang>.pdf** and **Kaspersky_Execsum_<id>_<lang>.pdf** files are created where <id> is the id of the publication and <lang> is the language of the documents.

Feed Data (.report_iocs.ioc)	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.description	indicator.attribute	Report Name	"Latin America bank contractors..."	
.authored_date	indicator.attribute	Detection Date	"2017-10-23T00:00:00"	
.definition.Indicator.IndicatorItem.Content ['#text']	indicator.value	Indicator Value	"86f8787f891eaaae5bcc62e892d503f3"	

Feed Data (.report_iocs.ioc)	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.definition.Indicator.IndicatorItem. Content ['@type'] / Context['@search']	indicator.type	Indicator Type	"md5"	*
.definition.Indicator.IndicatorItem['@id']	indicator.attribute	UID	"59f72d95-fab8-450d-9017-3c3fc0a85a81"	
* Only indicators that can be mapped using the 'Kaspersky Indicator Type to ThreatQ Indicator Type Mapping' are ingested into ThreatQ.				

Get List

JSON Response Sample

```
{
    "status": "ok",
    "status_msg": "",
    "return_data": {
        "count": 1,
        "publications": [
            {
                "id": "28-fin",
                "updated": 1508878740,
                "published": 1508792340,
                "name": "Latin? America? bank? contractors?
and employees? under Cobalt Strike? attack",
                "desc": "In the first week of September, an
unknown threat actor registered a domain ...",
                "report_group": "fin",
                "tags": [
                    "Chile",
                    "Financial institutions",
                    "Mexico"
                ],
                "tags_actors": [
                  "BlueNoroff",
                  "Lazarus"
                ],
                "tags_industry": [
                    "Financial institutions"
                ],
                "tags_geo": [
                    "Chile",
                    "Mexico"
                ],
                "pdfs": [
                    "en"
                ],
                "exec_sums": [
                    "en"
                ]
            }
        ]
    }
}
```

The mapping table is listed on the next page.

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.name	report.value	Report Title	"Latin? America? bank? contractors? ..."	
.desc	report.description	Report Description	"In the first week of September, an ..."	
.published	report.published_at	Report Published At	1508792340	formatted
.id	report.attribute	Publication ID	"28-fin"	
.updated	report.attribute	Updated At	1508878740	formatted
.report_group	report.attribute	Report Group	"fin"	
.tags_industry	report.attribute	Industry	["Financial institutions"]	
.tags_geo	report.attribute	Geography	["Chile", "Mexico"]	
.tags_actors	adversary.name	Adversary Name	["BlueNoroff", "Lazarus"]	

Get One

JSON Response Sample

```
{
    "status": "ok",
    "status_msg": "",
    "return_data": {
        "id": "28-fin",
        "report_group": "fin",
        "updated": 1508878740,
        "published": 1508792340,
        "name": "Latin? America? bank? contractors? and employ-
ees? under Cobalt Strike? attack",
        "desc": "In the first week of September, an unknown
threat actor registered a domain ...",
        "tags": [
            "Chile",
            "Financial institutions",
            "Mexico"
        ],
        "tags_industry": [
            "Financial institutions"
        ],
        "tags_geo": [
            "Chile",
            "Mexico"
        ],
        "tags_actors": [
          "BlueNoroff",
          "Lazarus"
        ],
        "report_yara": "<yara_base_64_encoded_gziped_data>",
        "report_iocs": "<iocs_base_64_encoded_gziped_data>",
        "report_pdf": "<pdf_base_64_encoded_gziped_data>",
        "report_execsum": "<execsum_base_64_encoded_gziped_
data>"
    }
}
```

Decoded and unzipped `yara_base_64_encoded_gziped_data`:

```
    import "pe"

    rule APT_ZZ_CobaltStrike_Cometer {
    meta:
        copyright = "Kaspersky Lab"
        description = "Attack through Central Bank of Chile
fake web-sites"
        last_modified = "2017-10-18"
        author = "Kaspersky Lab"
        hash = "0344EEEBFD183AA48E049BB3A8101CCE"
        hash = "5890917A52314280E0FC6D999104491B"
        hash = "AE8CFD1A33F604FEE0A48CA0B51CC538"
        hash = "ef6f128eb6f4167a494ac6c085cdf4e4"
        version = "1.0"

    strings:
        $a1 = {69 60 69 6A 69 E9 24 06 13 00 05 05 08 46 5? 47
59 49 41 0A 06 04 19 08 1D 00 0B 05 0C 52 49 24 3A 20 2C 49}
```

```
    condition:
        uint16(0) == 0x5A4D and
        filesize < 1000000 and
        1 of them and
        (pe.exports ("SystemUpdater") or pe.exports ("_SystemUpdater"))
    }
```

Decoded and unzipped `iocs_base_64_encoded_gziped_data`:

```
    <ioc xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema" id="59f72c61-f830-44ae-860f-3b73c0a85a81" last-modified="2017-10-23T00:00:00" xmlns="http://schemas.mandiant.com/2010/ioc">
      <short_description>DISTRIBUTION IS FORBIDDEN. DO NOT UPLOAD TO ANY MULTISCANNER OR SHARE ON ANY THREAT INTEL PLATFORM</short_description>
      <description>Latin America bank contractors and employees under Cobalt Strike attack IOCs v.1.0</description>
      <keywords />
      <authored_by>Kaspersky Lab</authored_by>
      <authored_date>2017-10-23T00:00:00</authored_date>
      <links />
      <definition>
        <Indicator operator="OR" id="59f9e930-50b4-4499-b215-0f44c0a85a81">
          <IndicatorItem id="59f72d35-aef8-4089-b3a4-3b5fc0a85a81" condition="is">
            <Context document="FileItem"
```

```
search="FileItem/Md5sum" type="mir" />
            <Content type-
e="md5">86f8787f891eaaae5bcc62e892d503f3</Content>
          <IndicatorItem id="59f72d95-fab8-450d-9017-
3c3fc0a85a81" condition="is">
            <Context document="Network" search="Network/DNS"
type="mir" />
            <Content type="string">banco-central.cl</Content>
          </IndicatorItem>
          </IndicatorItem>
        </Indicator>
      </definition>
    </ioc>
```