ThreatQuotient

Kaspersky Threat Intelligence Feed Implementation Guide

Version 1.1.0

Tuesday, June 30, 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: Tuesday, June 30, 2020

Contents

Versioning

- Current integration version: `1.1.0`
- Supported on ThreatQ versions >= `4.36.1`

Introduction

The Kaspersky Threat Intelligence connectors ingests threat intelligence data from the following feeds:

- Kaspersky Botnet C&C URL Exact
- Kaspersky Phishing URL Exact
- Kaspersky Malicious URL Exact
- Kaspersky Malicious Hash
- Kaspersky Mobile Malicious Hash
- Kaspersky IP Reputation
- Kaspersky P-SMS Trojan
- Kaspersky Ransomware URL
- Kaspersky IoT URL
- Kaspersky Mobile Botnet C&C URL
- Kaspersky ICS Hash

The Kaspersky feeds need two http calls for downloading the threat data. The first call (endpoints above) will return a link if the requested data is available. By fetching the data from the returned link a zip file containing the threat data will be fetched.

Notes:

- A client certificate is used for HTTP authentication.
- 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 Threat Intelligence** 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 Threat Intelligence feeds support the following configuration parameters:

Parameter	Description
Kaspersky PEM File	The Kaspersky Client Certificate.
Entries	The number of entries to be retrieved. Each JSON response is sorted by importance. The recommended entries fetched for each of the feeds are: • Kaspersky Botnet C&C URL Exact: 8000 • Kaspersky Phishing URL Exact: 8000 • Kaspersky Malicious URL Exact: 10,000 • Kaspersky Malicious Hash: 10,000 • Kaspersky Mobile Malicious Hash: 10,000 • Kaspersky IP Reputation: 4000 • Kaspersky P-SMS Trojan: 10,000

Parameter	Description
	• Kaspersky Ransomware URL: 8000 • Kaspersky IoT URL: 8000 • Kaspersky Mobile Botnet C&C URL: 8000 • Kaspersky ICS Hash: 10,000

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

ThreatQ Mapping

URL Feeds

Which include:

- Kaspersky Botnet C&C URL Exact
- Kaspersky Phishing URL Exact
- Kaspersky Malicious URL Exact
- Kaspersky Ransomware URL
- Kaspersky IoT URL
- Kaspersky Mobile Botnet C&C URL


```
{
  "id": 39724587,
  "type": 1,
  "mask": "saltapparel.club",
  "urls": [
    {
      "url": "one.saltapparel.club/offer.php"
    }
  ],
  "hosts": [
    {
      "host": "one.saltapparel.club"
    }
  ],
  "domains": [
    {
```

```
        "domain": "saltapparel.club"
      }
    ],
    "first_seen": "12.11.2019 13:46",
    "last_seen": "29.03.2020 11:40",
    "popularity": 5,
    "geo": "ru, de, in, dz, fr, it, br, vn, pl, ua",
    "IP": "54.88.21.193, 143.95.237.77, 146.112.51.207,
66.253.35.206",
    "threat": "Trojan.Win32.Generic",
    "files": [
      {
        "MD5": "51D2B6222891CD0F444C1CF8E542A003",
        "SHA1": "E18F994827E26C2393832532142BB99D611B0B82",
        "SHA256":
"EEF0CABE42B36B9544DD8E3BB3ACE0002D82579DDD4E40060C2397D510CD5-
EAE"
      },
      {
        "MD5": "CC7755D599A83C3CC1A56334D9398CB8"
      }
    ],
    "whois": {
      "domain": "saltapparel.club",
      "created": "12.11.2019",
      "updated": "17.11.2019",
      "expires": "12.11.2020",
      "org": "WhoisGuard, Inc.",
      "country": "PA",
```

```
      "email": "please query the rdds service of the registrar
of record identified in this output for information on how to
contact the registrant, admin, or tech contact of the queried
domain name.",
      "registrar_name": "NameCheap, Inc.",
      "registrar_email": "abuse@namecheap.com",
      "NS": "dns1.registrar-servers.com, dns2.registrar-serv-
ers.com",
      "NS_ips": "156.154.132.200, 156.154.133.200",
      "MX": "eforward1.registrar-servers.com, efor-
ward2.registrar-servers.com, eforward3.registrar-servers.com,
eforward4.registrar-servers.com, eforward5.registrar-serv-
ers.com",
      "MX_ips": "162.255.118.51, 162.255.118.52,
162.255.118.61, 162.255.118.62"
    }
  }
```

Feed Data	ThreatQEntity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.IP	indicator.value	IP Address	.first_seen	'54.88.21.193, 143.95.237.77, ...'	split-up
.mask	indicator.value	*	.first_seen	'saltapparel.club'	*See the IOC mapping table listed below.
.first_seen	indicator.attribute	First Seen	.first_seen	'12.11.2019 13:46'	formatted
.last_seen	indicator.attribute	Last Seen	.first_seen	'29.03.2020 11:40'	formatted
.geo	indicator.attribute	Country Code	.first_seen	'ru, de, in, dz, fr, it, br, vn, pl, ua'	split-up
.id	indicator.attribute	Kaspersky ID	.first_seen	39724587	
.popularity	indicator.attribute	Popularity	.first_seen	5	
.industry	indicator.attribute	Industry	.first_seen	'Global Internet Portal'	
.category	indicator.attribute	Category	.first_seen	'Malware'	
.threat	indicator.attribute	Threat	.first_seen	'Trojan.Win32.Generic'	
.port	indicator.attribute	Port	.first_seen	80	

Feed Data	ThreatQEntity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.protocol	indicator.attribute	Protocol	.first_seen	'http'	
.urls[].url	indicator.value	URL	.first_seen	'one.saltapparel.club/offer.php'	
.bot_urls[].bot_url	indicator.value	URL	.first_seen	'www.boturlsample.com'	
.hosts[].host	indicator.value	FQDN	.first_seen	'one.saltapparel.club'	
.domains[].domain	indicator.value	FQDN	.first_seen	'saltapparel.club'	
.files[].MD5	indicator.value	MD5	.first_seen	'51D2B6222891CD0F444C1CF8E542A003'	
.files[].SHA1	indicator.value	SHA1	.first_seen	'E18F994827E26C2393832532142BB99D611B0B82'	
.files[].SHA256	indicator.value	SHA256	.first_seen	'EEF0CABE42B36B9544DD8E3BB3ACE0002D82579DDD4E40060C2397D510CD5EAE'	
.files[].Threat	indicator.attribute	Threat	.first_seen	'HEUR:Trojan.Script.Generic'	only for .file[] indic-

Feed Data	ThreatQEntity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
					ators
.files[].Behaviour	indicator.attribute	Behavior	.first_seen	'Hide itself'	only for .file[] indicators
.whois.registrar_email	indicator.value	Email Address	.whois.created	'abuse@namecheap.com'	
.whois.email	indicator.value	Email Address	.whois.created	'abuse1@namecheap.com'	filtered
.whois.NS	indicator.value	FQDN	.whois.created	'dns1.registrar-servers.com, dns2.registrar-servers.com'	split-up
.whois.MX	indicator.value	FQDN	.whois.created	'eforward1.registrar-servers.com, eforward2.registrar-servers.com..'	split-up
.whois.domain	indicator.value	FQDN	.whois.created	'saltapparel.club'	
.whois.NS_ips	indicator.value	IP Address	.whois.created	'156.154.132.200, 156.154.133.200'	split-up
.whois.MX_ips	indicator.value	IP Address	.whois.created	'162.255.118.51, 162.255.118.52,...'	split-up
.whois.created	indicator.attribute	Whois Created	.whois.created	'12.11.2019'	only for .whois indic-

Feed Data	ThreatQEntity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
					ators, formatted
.whois.updated	indicator.attribute	Whois Update	.whois.created	'17.11.2019'	only for .whois indicators, formatted
.whois.expires	indicator.attribute	Whois Expires	.whois.created	'12.11.2020'	only for .whois indicators, formatted
.whois.name	indicator.attribute	Whois Name	.whois.created	'Provate Whois'	only for .whois indicators
.whois.registrar_name	indicator.attribute	Whois Registrar Name	.whois.created	'URL SOLUTIONS INC.'	only for .whois indicators
.whois.org	indicator.attribute	Whois Organization	.whois.created	'WhoisGuard, Inc.'	only for .whois indicators
.whois.country	indicator.attribute	Whois Country	.whois.created	'PA'	only for .whois indicators
.whois.city	indicator.attribute	Whois City	.whois.created	'San Mateo'	only for .whois indicators

*IOC value formatted and its type created based on the `.type` key:

.type	Threat Indicator Type	Formatted as	Example	Formatted example
1	FQDN	n/a	'domain.ru'	'domain.ru'
2	FQDN	n/a	'subdomain.domain.com'	'subdomain.domain.com'
3	URL	n/a	'domain.com/fxry/_tgpz'	'subdomain.domain.com'
4	URL	n/a	'domain.com/get.php?id=2'	'domain.com/get.php?id=2'
19	FQDN	lstrip('*.')	'*.domain.1143.net.cn/'	'domain.1143.net.cn/*'
20	URL	rstrip('/*')	'domain.cn/1/*'	'domain.cn/1'
21	URL	rstrip('*')	'domain.com/vbulletin_menu.js?*'	'domain.com/vbulletin_menu.js?'

Hash Feeds

Which include:

- Kaspersky Malicious Hash
- Kaspersky Mobile Malicious Hash
- Kaspersky ICS Hash


```
  {
    "MD5": "82865FF17BC664C711EFA674759F9991",
    "SHA1": "1603F72897CBD81F473A906C328A83C0413C5FB5",
    "SHA256":
"F85CD6F93BA18E642D50BEC7FC6AEB9D8751CC49B3BE5650DD5C556628545-
524",
    "first_seen": "15.11.2017 00:00",
    "last_seen": "31.03.2020 10:51",
    "popularity": 5,
    "threat": "HackTool.Win32.KMSAuto.i",
    "geo": "br, tw, dz, ru, de, cn, ma, th, vn, es",
    "file_size": 77824,
    "file_type": "PE",
    "file_names": "kmservice.exe, keygen.exe, kmsact.exe, act_
office14_kms.exe, mini-kms_activator_v1.052.exe, mini-kms_
activator_v1.051.exe, 12, upx, o1.6.exe, mini-kms_activator_
v1.1_office.2010.vl.eng.exe",
    "IP": "177.74.57.151, 36.91.164.33, 213.13.26.154,
82.64.49.223",
    "urls": [
      {
        "url":
```

```
"nuvem.belem.pa.gov.br/remote.php/dav/files/ca91a71e-7d52-
102c-8242-ade1aef9bba1/projetos-cad/arquivos suporte_cin-
besa/renato back/software-win7-office-2010/office 2010 pt-br
x86/ativador/ativador/activator_v1.052.rar"
      },
      {
        "url": "smkn1-
cikampek.-
powered-
byclear.com/data/software/iso/office2010/creck/keygen.exe"
      }
    ]
  }
```

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.MD5	indicator.value	Indicator Value	'82865FF17BC664C711EFA674759F9991'	indicator type - MD5
.SHA1	indicator.value	Indicator Value	'1603F72897CBD81F473A906C328A83C0413C5FB5'	indicator type - SHA1
.SHA256	indicator.value	Indicator Value	'F85CD6F93BA18E642D50BEC7FC6AEB9D8751CC49B3BE5650DD5C556628545524'	indicator type - SHA256
.IP	indicator.value	Indicator Value	'177.74.57.151, 36.91.164.33, 213.13.26.154, 82.64.49.223'	indicator type - IP Address, split-up
.urls[].url	indicator.value	Indicator Value	'nuvem.belem.pa.gov.br/remote.php/dav/files/...'	indicator type - URL
.first_seen	indicator.published_at	Indicator Published At	'15.11.2017 00:00'	formatted
.first_seen	indicator.attribute	First Seen	'15.11.2017 00:00'	formatted
.last_seen	indicator.attribute	Last Seen	'31.03.2020 10:51'	formatted
.geo	indicator.attribute	Country Code	'br, tw, dz, ru, de, cn, ma, th, vn, es'	split-up

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Examples	Notes
.threat	indicator.attribute	Threat	'HackTool.Win32.KMSAuto.i'	
.popularity	indicator.attribute	Popularity	5	
.file_ names	indicator.attribute	File Names	'kmservice.exe, keygen.exe, kmsact.exe, ...'	split-up
.file_size	indicator.attribute	File Size	77824	
.file_type	indicator.attribute	File Type	'PE'	

SMS Feeds

Which include:

- Kaspersky P-SMS Trojan


```
{
      "MD5":"0005565DEDFC19A28961DB191FD12383",
      "AV Verdict":"Trojan-SMS.AndroidOS.Opfake.a",
      "Date":"2/12/2019 12:35:50 AM",
      "details": [
        {
              "SMS Number":"3601",
              "SMS text":"4291500112791 041 123",
              "mcc":"250",
              "Country":"ru"
        },
        {
              "SMS Number":"3602",
              "SMS text":"4291500112791 041 123",
              "mcc":"250",
              "Country":"ru"
        }
      ]
}
```

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.MD5	indicator.value	MD5	.first_seen	'82865FF17BC664C711EF A674759F9991'	
.SHA1	indicator.value	SHA1	.first_seen	'1603F72897CBD81F473A 906C328A83C0413C5FB5'	
.SHA256	indicator.value	SHA256	.first_seen	'F85CD6F93BA18E642D5 0BEC7FC6AEB9D8751C C49B3BE5650DD5C5566 28545524'	
.IP	indicator.value	IP Address	.first_seen	'177.74.57.151, 36.91.164.33, 213.13.26.154, 82.64.49.223'	split-up
.urls[].url	indicator.value	URL	.first_seen	'nuvem.belem.pa.gov.br/remote.php/dav/files/...'	
.file_ names	indicator.value	Filename	.first_seen	'kmservice.exe, keygen.exe, kmsact.exe, ...'	
.first_seen	indicator.attribute	First Seen	.first_seen	'15.11.2017 00:00'	formatted
.last_seen	indicator.attribute	Last Seen	.first_seen	'31.03.2020 10:51'	formatted
.geo	indicator.attribute	Country Code	.first_seen	'br, tw, dz, ru, de, cn, ma, th, vn, es'	split-up

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.threat	indicator.attribute	Threat	.first_seen	'HackTool.Win32.KMSAuto.i'	
.popularity	indicator.attribute	Popularity	.first_seen	5	
.file_size	indicator.attribute	File Size	.first_seen	77824	
.file_type	indicator.attribute	File Type	.first_seen	'PE'	

IP Feeds

Which include:

- Kaspersky IP Reputation


```
  {
    "ip": "163.172.219.20",
    "threat_score": 100,
    "category": "malware",
    "first_seen": "12.12.2019 02:23",
    "last_seen": "31.03.2020 12:23",
    "popularity": 5,
    "ip_geo": "nl",
    "users_geo": "dz, sa, fr, eg, ma, br, om, ae, ps, iq",
    "ip_whois": {
      "net_range": "163.0.0.0 - 163.255.255.255",
      "net_name": "ERX-NETBLOCK",
      "descr": "Early registration addresses",
      "created": "28.08.2015",
      "country": "AU"
    },
    "domains": "a.top4top.io, 1.top4top.io",
    "files": [
      {
        "MD5": "07690B14706EA196171069A8A63D358A",
        "SHA1": "05888E5B6829E31CA4345579B5EC386D9A8DDCCB",
        "SHA256":
"343875A9A6265FEE8D28FA180094B0A6B9A53ED8B671189E3B5B4009BBEC5-
1F4",
```

```
        "threat": "UDS:DangerousObject.Multi.Generic"
      },
      {
        "MD5": "C603006543FFB7F3096183C8558FC991",
        "SHA1": "7C6DA0D4595545EDE0E0A43392F647336355F7EF",
        "SHA256":
"1262E31895447A2F1E94E3FD325EF7CE965E23826A0606A30DAFB15F6A2E2-
BBC",
        "threat": "UDS:DangerousObject.Multi.Generic"
      }
    ]
  }
```

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.ip	indicator.value	IP Address	.first_seen	'163.172.219.20'	
.domains	indicator.value	FQDN	.first_seen	'a.top4top.io, 1.top4top.io'	split-up
.first_seen	indicator.attribute	First Seen	.first_seen	'12.12.2019 02:23'	formatted
.last_seen	indicator.attribute	Last Seen	.first_seen	'31.03.2020 12:23'	formatted
.popularity	indicator.attribute	Popularity	.first_seen	5	
.threat_score	indicator.attribute	Threat Score	.first_seen	100	
.users_geo	indicator.attribute	Users Country Code	.first_seen	'dz, sa, fr, eg, ma, br, om, ae, ps, iq'	split-up
.ip_geo	indicator.attribute	IP Country Code	.first_seen	'nl'	
.category	indicator.attribute	Category	.first_seen	'malware'	
.files[].MD5	indicator.value	MD5	.first_seen	'07690B14706EA19617106 9A8A63D358A'	
.files[].SHA1	indicator.value	SHA1	.first_seen	'05888E5B6829E31CA434 5579B5EC386D9A8DDCCB'	

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.files[].SHA256	indicator.value	SHA256	.first_seen	'343875A9A6265FEE8D28F A180094B0A6B9A53ED8B6 71189E3B5B4009BBEC51F4'	
.files[].Threat	indicator.attribute	Threat	.first_seen	'UDS:DangerousObject.Multi.Generic'	only for .file[] indicators
.files[].Behaviour	indicator.attribute	Behavior	.first_seen	'Hide itself'	only for .file[] indicators
.ip_whois.contact_ abuse_email	indicator.value	Email Address	.ip_whois.cre-ated	'xengine@mail.ru'	
.ip_whois.contact_ owner_email	indicator.value	Email Address	.ip_whois.cre-ated	'xengine123@mail.ru'	
.ip_whois.net_ range	indicator.value	IPAddress	.ip_whois.cre-ated	'163.0.0.0 - 163.255.255.255'	
.ip_whois.created	indicator.attribute	IP Whois Created	.ip_whois.cre-ated	'28.08.2015'	only for .ip_whois indicators, format-ted

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.ip_whois.updated	indicator.attribute	IP Whois Update	.ip_whois.created	'01.01.2020'	only for .ip_whois indicators, formatted
.ip_whois.descr	indicator.attribute	IP Whois Description	.ip_whois.created	'Early registration addresses'	only for .ip_whois indicators
.ip_whois.country	indicator.attribute	IP Whois Country	.ip_whois.created	'ru'	only for .ip_whois indicators
.ip_whois.asn	indicator.attribute	IP Whois ASN	.ip_whois.created	'49981'	only for .ip_whois indicators
.ip_whois.net_name	indicator.attribute	IP Whois Network Name	.ip_whois.created	'ERX-NETBLOCK'	only for .ip_whois indicators
.ip_whois.contact_owner_code	indicator.attribute	IP Whois Contact Owner Code	.ip_whois.created	'HUN8'	only for .ip_whois indicators
.ip_whois.contact_owner_name	indicator.attribute	IP Whois Contact Owner Name	.ip_whois.created	'ONLINE SAS'	only for .ip_whois indicators

Feed Data	ThreatQ Entity	ThreatQ Object Type or Attribute Key	Published Date	Examples	Notes
.ip_whois.contact_owner_country	indicator.attribute	IP Whois Contact Owner Country	.ip_whois.created	'EC'	only for .ip_whois indicators
.ip_whois.contact_owner_city	indicator.attribute	IP Whois Contact Owner City	.ip_whois.created	'Seattle'	only for .ip_whois indicators
.ip_whois.contact_abuse_name	indicator.attribute	IP Whois Contact Abuse Name	.ip_whois.created	'Abuse'	only for .ip_whois indicators
.ip_whois.contact_abuse_country	indicator.attribute	IP Whois Contact Abuse Country	.ip_whois.created	'US'	only for .ip_whois indicators

Average Feed Runs

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.

Kaspersky Botnet C&C URL Exact

Metric	Result
Run Time	~30 hours
Indicators	121442
Indicator Attributes	922697

Kaspersky Phishing URL Exact

Metric	Result
Run Time	~50 hours
Indicators	57674
Indicator Attributes	872181

Kaspersky Malicious URL Exact

Metric	Result
Run Time	~60 hours
Indicators	111066
Indicator Attributes	1333949

Kaspersky Malicious Hash

Metric	Result
Run Time	~20 hours
Indicators	55123
Indicator Attributes	904227

Kaspersky Mobile Malicious Hash

Metric	Result
Run Time	~5 hours
Indicators	28496
Indicator Attributes	200703

Kaspersky IP Reputation

Metric	Result
Run Time	~2 hours
Indicators	8654
Indicator Attributes	68212

Kaspersky P-SMS Trojan

Metric	Result
Run Time	~12 hours
Indicators	10000
Indicator Attributes	635536

Kaspersky Ransomware URL

Metric	Result
Run Time	~11 hours
Indicators	20369
Indicator Attributes	211376

Kaspersky IoT URL

Metric	Result
Run Time	~15 hours
Indicators	12034
Indicator Attributes	673431

Kaspersky Mobile Botnet C&C URL

Metric	Result
Run Time	~13 hours
Indicators	50367
Indicator Attributes	321056

Kaspersky ICS Hash

Metric	Result
Run Time	~1 hour
Indicators	26885
Indicator Attributes	240127

Change Log

- **Version 1.1.0**
  - Added new feed to integration: Kaspersky ICS Hash
- **Version 1.0.0**
  - Initial Release