ThreatQuotient

Kaspersky Threat Intelligence CDF Guide

Version 2.1.1

February 01, 2022

ThreatQuotient
11400 Commerce Park Dr., Suite 200
Reston, VA 20191

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

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.

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.

Versioning

- Current integration version: `2.1.1`
- Compatible with ThreatQ versions >= `4.37.0`

Introduction

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

- 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
- Kaspersky Malicious Hash
- Kaspersky Mobile Malicious Hash
- Kaspersky ICS Hash
- Kaspersky IP Reputation
- Kaspersky APT IPs
- Kaspersky APT URLs
- Kaspersky APT Hashes

The integration ingests the following system objects:

- Indicators
  - Indicator Attributes

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 file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the integration file using one of the following methods:
   - Drag and drop the file into the dialog box
   - Select **Click to Browse** to locate the integration 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.
6. If prompted, select the individual feeds to install and click **Install**. The feed 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 **Commercial** 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 to open its details page.
4. Enter the following parameters under the **Configuration** tab:

PARAMETER	DESCRIPTION
Kaspersky PEM File	Your Kaspersky Client Certificate for authentication.
Entries	The number of entries to be retrieved. The default to 10,000.

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

ThreatQ Mapping

URL Feeds

The following feeds all follow the same JSON response data format and have the same ThreatQ data mapping:

- Kaspersky Botnet C&C URL Exact - `GET https://wlinfo.kaspersky.com/api/v1.0/feeds/115/updates`
- Kaspersky Phishing URL Exact - `GET https://wlinfo.kaspersky.com/api/v1.0/feeds/116/updates`
- Kaspersky Malicious URL Exact - `GET https://wlinfo.kaspersky.com/api/v1.0/feeds/117/updates`
- Kaspersky Ransomware URL - `GET https://wlinfo.kaspersky.com/api/v1.0/feeds/99/updates`
- Kaspersky IoT URL - `GET https://wlinfo.kaspersky.com/api/v1.0/feeds/126/updates`
- Kaspersky Mobile Botnet C&C URL - `GET https://wlinfo.kaspersky.com/api/v1.0/feeds/139/updates`

JSON response sample:


```
[
    {
        "bot_urls": [
            {
                "bot_url": "one.saltapparel.club/accept.php"
            }
        ],
        "category": "Malware",
        "domains": [
            {
                "domain": "saltapparel.club"
            }
        ],
        "files": [
            {
                "MD5": "51D2B6222891CD0F444C1CF8E542A003",
                "SHA1": "E18F994827E26C2393832532142BB99D611B0B82",
                "SHA256": "EEF0CABE42B36B9544DD8E3BB3ACE0002D82579DDD4E40060C2397D510CD5EAE"
            },
            {
                "MD5": "CC7755D599A83C3CC1A56334D9398CB8"
            }
        ],
        "first_seen": "12.11.2019 13:46",
        "geo": "ru, de, in, dz, fr, it, br, vn, pl, ua",
```

```
        "hosts": [
            {
                "host": "one.saltapparel.club"
            }
        ],
        "id": 39724587,
        "industry": "Global Internet Portal",
        "IP": "54.88.21.193, 143.95.237.77, 146.112.51.207, 66.253.35.206",
        "last_seen": "29.03.2020 11:40",
        "mask": "saltapparel.club",
        "popularity": 5,
        "port": 80,
        "protocol": "http",
        "threat": "Trojan.Win32.Generic",
        "type": 1,
        "urls": [
            {
                "url": "one.saltapparel.club/offer.php"
            }
        ],
        "whois": {
            "country": "PA",
            "created": "12.11.2019",
            "domain": "saltapparel.club",
            "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.",
            "expires": "12.11.2020",
            "MX": "eforward1.registrar-servers.com, eforward2.registrar-servers.com, eforward3.registrar-servers.com,
eforward4.registrar-servers.com, eforward5.registrar-servers.com",
            "MX_ips": "162.255.118.51, 162.255.118.52, 162.255.118.61, 162.255.118.62",
            "NS": "dns1.registrar-servers.com, dns2.registrar-servers.com",
            "NS_ips": "156.154.132.200, 156.154.133.200",
            "org": "WhoisGuard, Inc.",
            "registrar_email": "abuse@namecheap.com",
            "registrar_name": "NameCheap, Inc.",
            "updated": "17.11.2019"
        }
    },
    ...
]
```


ThreatQ provides the following default mapping for these feeds:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
[]bot_urls[].bot_url	Related Indicator.Value	URL	[].first_seen	www.boturlsample.com	Ingested with the `Indirect` status. Value is dropped if it is equal to `[].mask`. Related to the primary `[].mask` Indicator
[]category	Indicator.Attribute	Category	[].first_seen	Malware	Applied to all non-Whois Indicators
[]domains[].domain	Related Indicator.Value	FQDN	[].first_seen	saltapparel.club	Value is dropped if it is equal to `[].mask`. Ingested with the `Indirect` status. Related to the primary `[].mask` Indicator. Inter-related with other `[].domains[].domain` and `.hosts[].host` Indicators

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
[].files[].Behaviour	Related Indicator.Attribute	Behaviour	[].first_seen	Hide itself	Only applied to `[].files[]` Indicators
[].files[].MD5	Related Indicator.Value	MD5	[].first_seen	51D2B6222891CD0F444C1CF8E542A003	Related to primary `[].mask` Indicator. Inter-related with other `[].files[]` Indicators.
[].files[].SHA1	Related Indicator.Value	SHA-1	[].first_seen	E18F994827E26C2393832532142BB99D611B0B82	Related to primary `[].mask` Indicator. Inter-related with other `[].files[]` Indicators.
[].files[].SHA256	Related Indicator.Value	SHA256	[].first_seen	EEF0CABE42B36B9544DD8E3BB3ACE0002D82579DDD4E40060C2397D510CD5EAE	Related to primary `[].mask` Indicator. Inter-related with other `[].files[]` Indicators.
[].files[].Threat	Related Indicator.Attribute	Threat	[].first_seen	HEUR:Trojan.Script.Generic	Only applied to `[].files[]` Indicators
[].geo	Indicator.Attribute	Country Code	[].first_seen	ru	Value is split on `', '`. Applied to all non-Whois Indicators
[].hosts[].host	Related Indicator.Value	FQDN	[].first_seen	one.saltapparel.club	Value is dropped if it is equal to `[].mask`. Ingested with the `Indirect` status. Related to the primary `[].mask` Indicator. Inter-related with other `[].domains[].domain` and `.hosts[].host` Indicators
[].id	Indicator.Attribute	Kaspersky ID	[].first_seen	39724587	Applied to all non-Whois Indicators
[].industry	Indicator.Attribute	Industry	[].first_seen	Global Internet Portal	Applied to all non-Whois Indicators
[].IP	Related Indicator.Value	IP Address	[].first_seen	54.88.21.193	Value is split on `', '`. Ingested with the `Indirect` status. Related to primary `[].mask` Indicator
[].last_seen	Indicator.Attribute	Last Seen	[].first_seen	29.03.2020 11:40	Applied to all non-Whois Indicators
[].mask	Indicator.Value	See Kaspersky Type Mapping table	[].first_seen	saltapparel.club	N/A
[].popularity	Indicator.Attribute	Popularity	[].first_seen	5	Applied to all non-Whois Indicators
[].port	Indicator.Attribute	Port	[].first_seen	80	Applied to all non-Whois Indicators
[].protocol	Indicator.Attribute	Protocol	[].first_seen	http	Applied to all non-Whois Indicators
[].threat	Indicator.Attribute	Threat	[].first_seen	Trojan.Win32.Generic	Applied to all non-Whois Indicators
[].urls[].url	Related Indicator.Value	URL	[].first_seen	one.saltapparel.club/offer.php	Ingested with the `Indirect` status. Value is dropped if it is equal to `[].mask`. Related to the primary `[].mask` Indicator
[].whois.city	Related Indicator.Attribute	Whois City	[].whois.created	San Mateo	Only applied to Whois Indicators
[].whois.country	Related Indicator.Attribute	Whois Country Code	[].whois.created	PA	Only applied to Whois Indicators

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
[]whois.domain	Related Indicator.Value	FQDN	[]whois.created	saltapparel.club	Ingested with the `Indirect` status. Value is dropped if it is equal to `[].mask`. Related to the primary `[].mask` Indicator
[]whois.email	Related Indicator.Value	Email Address	[]whois.created	abuse1@namecheap.com	Ingested with the `Indirect` status. Related to the primary `[].mask` Indicator
[]whois.expires	Related Indicator.Attribute	Whois Expires	[]whois.created	12.11.2020	Only applied to Whois Indicators
[]whois.MX	Related Indicator.Value	FQDN	[]whois.created	eforward1.registrar-servers.com	Value is dropped if it is equal to `[].mask`. Value is split on `', '`. Ingested with the `Indirect status`. Related to the primary `[].mask` Indicator
[]whois.MX_ips	Related Indicator.Value	IP Address	[]whois.created	162.255.118.51	Value is dropped if it is equal to `[].mask`. Value is split on `', '`. Ingested with the `Indirect status`. Related to the primary `[].mask` Indicator
[]whois.name	Related Indicator.Attribute	Whois Name	[]whois.created	Provate Whois	Only applied to Whois Indicators
[]whois.NS	Related Indicator.Value	FQDN	[]whois.created	dns1.registrar-servers.com	Value is dropped if it is equal to `[].mask`. Value is split on `', '`. Ingested with the `Indirect status`. Related to the primary `[].mask` Indicator
[]whois.NS_ips	Related Indicator.Value	IP Address	[]whois.created	156.154.132.200	Value is dropped if it is equal to `[].mask`. Value is split on `', '`. Ingested with the `Indirect status`. Related to the primary `[].mask` Indicator
[]whois.org	Related Indicator.Attribute	Whois Organization	[]whois.created	WhoisGuard, Inc.	Value is dropped if it is equal to `??`. Only applied to Whois Indicators
[]whois.registrar_email	Related Indicator.Value	Email Address	[]whois.created	abuse@namecheap.com	Ingested with the `Indirect status`. Related to the primary `[].mask` Indicator
[]whois.registrar_name	Related Indicator.Attribute	Whois Registrar Name	[]whois.created	URL SOLUTIONS INC.	Only applied to Whois Indicators
[]whois.updated	Related Indicator.Attribute	Whois Updated	[]whois.created	17.11.2019	Only applied to Whois Indicators

Hash Feeds

The following feeds all follow the same JSON response data format and have the same ThreatQ data mapping:

- Kaspersky Malicious Hash - `GET https://wlinfo.kaspersky.com/api/v1.0/feeds/66/updates`
- Kaspersky Mobile Malicious Hash - `GET https://wlinfo.kaspersky.com/api/v1.0/feeds/67/updates`
- Kaspersky ICS Hash - `GET https://wlinfo.kaspersky.com/api/v1.0/feeds/141/updates`

JSON response sample:

```
[
    {
        "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",
        "file_size": 77824,
        "file_type": "PE",
        "first_seen": "15.11.2017 00:00",
        "geo": "br, tw, dz, ru, de, cn, ma, th, vn, es",
        "IP": "177.74.57.151, 36.91.164.33, 213.13.26.154, 82.64.49.223",
        "last_seen": "31.03.2020 10:51",
        "MD5": "82865FF17BC664C711EFA674759F9991",
        "popularity": 5,
        "SHA1": "1603F72897CBD81F473A906C328A83C0413C5FB5",
        "SHA256": "F85CD6F93BA18E642D50BEC7FC6AEB9D8751CC49B3BE5650DD5C556628545524",
        "threat": "HackTool.Win32.KMSAuto.i",
        "urls": [
            {
                "url": "nuvem.belem.pa.gov.br/remote.php/dav/files/ca91a71e-7d52-102c-8242-ade1aef9bba1/projetos-cad/
arquivos suporte_cinbesa/renato back/software-win7-office-2010/office 2010 pt-br x86/ativador/ativador/
activator_v1.052.rar"
            },
            {
                "url": "smkn1cikampek.poweredbyclear.com/data/software/iso/office2010/creck/keygen.exe"
            }
        ]
    },
    ...
]
```

FEED DATA	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
[].file_names	Related Indicator.Value	Filename	[].first_seen	kmservice.exe	Value is split on `', '`. Ingested with the `Indirect` status. Related to the primary `[].MD5` Indicator
[].file_size	Indicator.Attribute	File Size	[].first_seen	77824	Applied to hash Indicators
[].file_type	Indicator.Attribute	File Type	[].first_seen	PE	Applied to hash Indicators
[].geo	Indicator.Attribute	Country Code	[].first_seen	br	Value is split on `', '`. Applied to hash Indicators

FEED DATA	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
[].IP	Related Indicator.Value	IP Address	[].first_seen	177.74.57.151	Value is split on `', '`. Ingested with the `Indirect` status. Related to the primary `[].MD5` Indicator
[].last_seen	Indicator.Attribute	Last Seen	[].first_seen	31.03.2020 10:51	Applied to hash Indicators
[].MD5	Indicator.Value	MD5	[].first_seen	82865FF17BC664C711EFA674759F9991	Inter-related with other hash indicators.
[].popularity	Indicator.Attribute	Popularity	[].first_seen	5	Applied to hash Indicators
[].SHA1	Related Indicator.Value	SHA1	[].first_seen	1603F72897CBD81F473A906C328A83C0413C5FB5	Inter-related with other hash Indicators
[].SHA256	Indicator.Value	SHA256	[].first_seen	F85CD6F93BA18E642D50BEC7FC6AEB9D8751CC49B3BE5650DD5C556628545524	Inter-related with other hash indicators.
[].threat	Indicator.Attribute	Threat	[].first_seen	HackTool.Win32.KMSAuto.i	Applied to hash Indicators
[].urls[].url	Indicator.Value	URL	[].first_seen	nuvem.belem.pa.gov.br/remote.php/dav/files/...	Ingested with the `Indirect` status. Related to the primary `[].MD5` Indicator

Kaspersky APT IPs

`GET https://wlinfo.kaspersky.com/api/v1.0/feeds/142/updates`

JSON response sample:

```
[
    {
        "detection_date": "20.04.2017 00:00",
        "id": 16453205,
        "ip": "69.64.59.133",
        "publication_name": "ShadowBrokers Lost in translation leak - SWIFT attacks analysis"
    },
    ...
]
```

FEED DATA	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
[].ip	Indicator.Value	IP Address	[].detection_date	69.64.59.133	N/A
[].publication_name	Indicator.Attribute	Publication	[].detection_date	ShadowBrokers Lost in translation leak - SWIFT attacks analysis	N/A

Kaspersky APT URLs

`GET https://wlinfo.kaspersky.com/api/v1.0/feeds/143/updates`

JSON response sample:

```
[
    {
        "detection_date": "09.03.2017 00:00",
        "id": 16451625,
        "mask": "ec2-52-74-203-151.ap-southeast-1.compute.amazonaws.com",
        "publication_name": "APT10 Spearphishes Japanese Policy Experts late 2016 to early 2017",
        "type": 2
    },
    ...
]
```

FEED DATA	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
[].mask	Indicator.Value	See Kaspersky Type Mapping table	[].detection_date	ec2-52-74-203-151.ap-southeast-1.compute.amazonaws.com	N/A
[].publication_name	Indicator.Attribute	Publication	[].detection_date	ShadowBrokers Lost in translation leak - SWIFT attacks analysis	N/A

Kaspersky APT Hashes

`GET https://wlinfo.kaspersky.com/api/v1.0/feeds/144/updates`

JSON response sample:

```
[
    {
        "detection_date": "23.06.2017 00:00",
        "id": 16456071,
        "MD5": "F805882CC276B583D9CA7E16AD957E7B",
        "publication_name": "Ismdoor - possible Shamoon attack vector found in Saudi Arabia",
        "SHA1": "2E4DB721DBD2ACEFD851BEDF95492BF789F588FD",
        "SHA256": "D76024256AC35424EB02B6A47565F8859B12050F5DE49EF16DEC449A61DA1EFC"
    },
    ...
]
```

FEED DATA	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
[].MD5	Indicator.Value	MD5	[].detection_date	F805882CC276B583D9CA7E16AD957E7B	Inter-related with other hash Indicators
[].SHA1	Indicator.Value	SHA-1	[].detection_date	2E4DB721DBD2ACEFD851BEDF95492BF789F588FD	Inter-related with other hash Indicators

FEED DATA	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
[].SHA256	Indicator.Value	SHA256	[].detection_date	D76024256AC35424EB02B6A47565F8859B12050F5DE49EF16DEC449A61DA1EFC	Inter-related with other hash Indicators
[].publication_name	Indicator.Attribute	Publication	[].detection_date	ShadowBrokers Lost in translation leak - SWIFT attacks analysis	N/A

Kaspersky IP Reputation

`GET https://wlinfo.kaspersky.com/api/v1.0/feeds/68/updates`

JSON response sample:


```
[
    {
        "category": "malware",
        "domains": "a.top4top.io, 1.top4top.io",
        "files": [
            {
                "MD5": "07690B14706EA196171069A8A63D358A",
                "SHA1": "05888E5B6829E31CA4345579B5EC386D9A8DDCCB",
                "SHA256": "343875A9A6265FEE8D28FA180094B0A6B9A53ED8B671189E3B5B4009BBEC51F4",
                "threat": "UDS:DangerousObject.Multi.Generic"
            },
            {
                "MD5": "C603006543FFB7F3096183C8558FC991",
                "SHA1": "7C6DA0D4595545EDE0E0A43392F647336355F7EF",
                "SHA256": "1262E31895447A2F1E94E3FD325EF7CE965E23826A0606A30DAFB15F6A2E2BBC",
                "threat": "UDS:DangerousObject.Multi.Generic"
            }
        ],
        "first_seen": "12.12.2019 02:23",
        "ip": "163.172.219.20",
        "ip_geo": "nl",
        "ip_whois": {
            "asn": 49981,
            "contact_abuse_country": "US",
            "contact_abuse_email": "xengine@mail.ru",
            "contact_abuse_name": "Abuse",
            "contact_owner_city": "Seattle",
            "contact_owner_code": "HUN8",
            "contact_owner_country": "EC",
            "contact_owner_email": "xengine123@mail.ru",
            "contact_owner_name": "ONLINE SAS",
            "country": "AU",
            "created": "28.08.2015",
            "descr": "Early registration addresses",
            "net_name": "ERX-NETBLOCK",
            "net_range": "163.0.0.0 - 163.255.255.255",
            "updated": "28.08.2015"
        },
        "last_seen": "31.03.2020 12:23",
        "popularity": 5,
        "threat_score": 100,
```

```
        "users_geo": "dz, sa, fr, eg, ma, br, om, ae, ps, iq"
    },
    ...
]
```

FEED DATA	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
[].category	Indicator.Attribute	Category	[].first_seen	malware	Applied to non-ip_whois Indicators
[].domains	Related Indicator.Value	FQDN	[].first_seen	a.top4top.io	Value is split on `', '`. Ingested with the `Indirect` status. Related to the primary `[].ip` Indicator
[].files[].Behaviour	Related Indicator.Attribute	Behaviour	[].first_seen	Hide itself	Only applied to `[].files[]` Indicators
[].files[].MD5	Related Indicator.Value	MD5	[].first_seen	51D2B6222891 CD0F444C1CF8 E542A003	Related to primary `[].ip` Indicator. Inter-related with other `[].files[]` Indicators
[].files[].SHA1	Related Indicator.Value	SHA-1	[].first_seen	E18F994827E26C 2393832532142B B99D611B0B82	Related to primary `[].ip` Indicator. Inter-related with other `[].files[]` Indicators
[].files[].SHA256	Related Indicator.Value	SHA256	[].first_seen	EEF0CABE42B36B9 544DD8E3BB3ACE0 002D82579DDD4E4 0060C2397D510CD5 EAE	Related to primary `[].ip` Indicator. Inter-related with other `[].files[]` Indicators
[].files[].Threat	Related Indicator.Attribute	Threat	[].first_seen	HEUR:Trojan.Script.Generic	Only applied to `[].files[]` Indicators
[].ip	Indicator.Value	IP Address	[].first_seen	163.172.219.20	N/A
[].ip_geo	Indicator.Attribute	IP Country Code	[].first_seen	nl	Applied to non-ip_whois Indicators
[].ip_whois.asn	Related Indicator.Attribute	IP Whois ASN	[].ip_whois.created	49981	Only applied to ip_whois Indicators
[].ip_whois.contact_abuse_country	Related Indicator.Attribute	IP Whois Contact Abuse Country	[].ip_whois.created	US	Only applied to ip_whois Indicators
[].ip_whois.contact_abuse_email	Related Indicator.Value	Email Address	[].ip_whois.created	xengine@mail.ru	Ingested with the `Indirect` status. Related to primary `[].ip` Indicator
[].ip_whois.contact_abuse_name	Related Indicator.Attribute	IP Whois Contact Abuse Name	[].ip_whois.created	Abuse	Only applied to ip_whois Indicators
[].ip_whois.contact_owner_city	Related Indicator.Attribute	IP Whois Contact Owner City	[].ip_whois.created	Seattle	Only applied to ip_whois Indicators
[].ip_whois.contact_owner_code	Related Indicator.Attribute	IP Whois Contact Owner Code	[].ip_whois.created	HUN8	Only applied to ip_whois Indicators

FEED DATA	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
[].ip_whois.contact_owner_country	Related Indicator.Attribute	IP Whois Contact Owner Country	[].ip_whois.created	EC	Only applied to ip_whois Indicators
[].ip_whois.contact_owner_email	Related Indicator.Value	Email Address	[].ip_whois.created	xengine123@mail.ru	Ingested with the `Indirect` status. Related to primary `[].ip` Indicator
[].ip_whois.contact_owner_name	Related Indicator.Attribute	IP Whois Contact Owner Name	[].ip_whois.created	ONLINE SAS	Only applied to ip_whois Indicators
[].ip_whois.country	Related Indicator.Attribute	IP Whois Country	[].ip_whois.created	ru	Only applied to ip_whois Indicators
[].ip_whois.descr	Related Indicator.Attribute	IP Whois Description	[].ip_whois.created	Early registration addresses	Only applied to ip_whois Indicators
[].ip_whois.net_name	Related Indicator.Attribute	IP Whois Network Name	[].ip_whois.created	ERX-NETBLOCK	Only applied to ip_whois Indicators
[].ip_whois.net_range	Related Indicator.Value	CIDR Block	[].ip_whois.created	163.0.0.0 - 163.255.255.255	CIDR Block is derived from the given IP range. Ingested with the `Indirect` status. Related to primary `[].ip` Indicator
[].ip_whois.updated	Related Indicator.Attribute	IP Whois Updated	[].ip_whois.created	01.01.2020	Only applied to ip_whois Indicators
[].last_seen	Indicator.Attribute	Last Seen	[].first_seen	31.03.2020 12:23	Applied to non-ip_whois Indicators
[].popularity	Indicator.Attribute	Popularity	[].first_seen	5	Applied to non-ip_whois Indicators
[].threat_score	Indicator.Attribute	Threat Score	[].first_seen	100	Applied to non-ip_whois Indicators
[].users_geo	Indicator.Attribute	Users Country Code	[].first_seen	dz	Value is split on `', '`. Applied to non-ip_whois Indicators

Kaspersky Type Mapping

[].TYPE VALUE	INDICATOR TYPE VALUE	NOTES
1, 2	FQDN	N/A
3, 4	URL	N/A
19	FQDN	Value is formatted with `lstrip('*.')`
20	URL	Value is formatted with `rstrip('/*')`
21	URL	Value is formatted with `rstrip('*')`

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.

Kaspersky Botnet C&C URL Exact

METRIC	RESULT
Run Time	13 hours
Indicators	172,990
Indicator Attributes	1,166,318

Kaspersky Phishing URL Exact

METRIC	RESULT
Run Time	14 hours
Indicators	70,179
Indicator Attributes	882,094

Kaspersky Malicious URL Exact

METRIC	RESULT
Run Time	8 hours 10 minutes
Indicators	104,730
Indicator Attributes	1,086,859

Kaspersky Ransomware URL

METRIC	RESULT
Run Time	2 hours 15 minutes
Indicators	25,402
Indicator Attributes	192,779

Kaspersky IoT URL

METRIC	RESULT
Run Time	4 hours 15 minutes
Indicators	45,577
Indicator Attributes	696,466

Kaspersky Mobile Botnet C&C URL

METRIC	RESULT
Run Time	2 hours 45 minutes
Indicators	77,649
Indicator Attributes	386,710

Kaspersky Malicious Hash

METRIC	RESULT
Run Time	2.5 hours
Indicators	53,711
Indicator Attributes	371,878

Kaspersky Mobile Malicious Hash

METRIC	RESULT
Run Time	1 hour
Indicators	25,823
Indicator Attributes	149,425

Kaspersky ICS Hash

METRIC	RESULT
Run Time	1 hour 10 minutes
Indicators	33,003
Indicator Attributes	193,858

Kaspersky APT IPs

METRIC	RESULT
Run Time	1 minute
Indicators	35
Indicator Attributes	35

Kaspersky APT URLs

METRIC	RESULT
Run Time	1 minute
Indicators	42
Indicator Attributes	42

Kaspersky APT Hashes

METRIC	RESULT
Run Time	1 minute
Indicators	431
Indicator Attributes	431

Kaspersky IP Reputation

METRIC	RESULT
Run Time	1 hour 10 minutes
Indicators	16,651
Indicator Attributes	96,666

Change Log

- **Version 2.1.1**
  - Fixed a relationship bug that would cause feed run performance issues.
- **Version 2.1.0**
  - Refactored feeds.
  - Ensure all Indicators related to main pivot Indicators ingest with the `Indirect` status
  - Added object relations between main pivot Indicators and related Indirect Indicators.
  - Fixed a bug that caused relations to hash indicators to fail.
  - Added the following APT Feeds:
    - Kaspersky APT IPs
    - Kaspersky APT URLs
    - Kaspersky APT Hashes
  - Changed the status to `Active` for related indicators of type `MD5`, `SHA-1`, `SHA-256`.
  - Removed Kaspersky P-SMS Trojan feed.
- **Version 1.2.0**
  - Updated URL Feeds - `.whois` related indicators ingested as indirect
- **Version 1.1.0**
  - Added new feed to integration: Kaspersky ICS Hash Feed
- **Version 1.0.0**
  - Initial release