ThreatQuotient

Kaspersky Threat Intelligence CDF

Version 2.2.6

May 28, 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

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.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	2.2.6
Compatible with ThreatQ Versions	>= 5.20.0
Support Tier	ThreatQ Supported

Introduction

The Kaspersky Threat Intelligence CDF ingests threat intelligence data from Kaspersky Threat Intelligence.

The CDF ingests threat data from the following feeds:

- **Kaspersky Botnet C&C URL Exact** - ingests indicators and malware together with their attributes.
- **Kaspersky Phishing URL Exact** - ingests sets of web address masks covering phishing websites and web pages.
- **Kaspersky Malicious URL Exact** - ingests sets of web address masks covering malicious websites and web pages..
- **Kaspersky Ransomware URL** - ingests sets of web addresses, domains, and hosts covering ransomware links and websites.
- **Kaspersky IoT URL** - ingests sets of web addresses covering websites used to host malware that infect Internet of Things (IoT) devices. Hashes of the malware are also provided.
- **Kaspersky Mobile Botnet C&C URL** - ingests set of web addresses covering mobile botnet C&C servers.
- **Kaspersky Malicious Hash** - returns a list of STIX bundles, each of them containing Indicators related in `TAXII_Malicious_Hash_Data_Feed_Indicators` (stix2) collection.
- **Kaspersky Mobile Malicious Hash** - ingests sets of file hashes covering the detection of malicious objects that infect mobile Android and iPhone platforms.
- **Kaspersky ICS Hash** - ingests sets of file hashes with corresponding context covering the most dangerous, prevalent, or emerging malware that infect devices used in ICS.
- **Kaspersky IP Reputation** - ingests sets of IP addresses covering malicious hosts.
- **Kaspersky APT IPs** - ingests sets of IP addresses that are part of infrastructure used in malicious APT campaigns.
- **Kaspersky APT URLs** - ingests sets of domains that are part of an infrastructure used in malicious APT campaigns.
- **Kaspersky APT Hashes** - ingests sets of hashes covering malicious artifacts used by APT actors to conduct APT campaigns.

The integration ingests the following system objects:

- Indicators
  - Indicator Attributes
- Malware
  - Malware Attributes
- Signatures

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(s).

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).

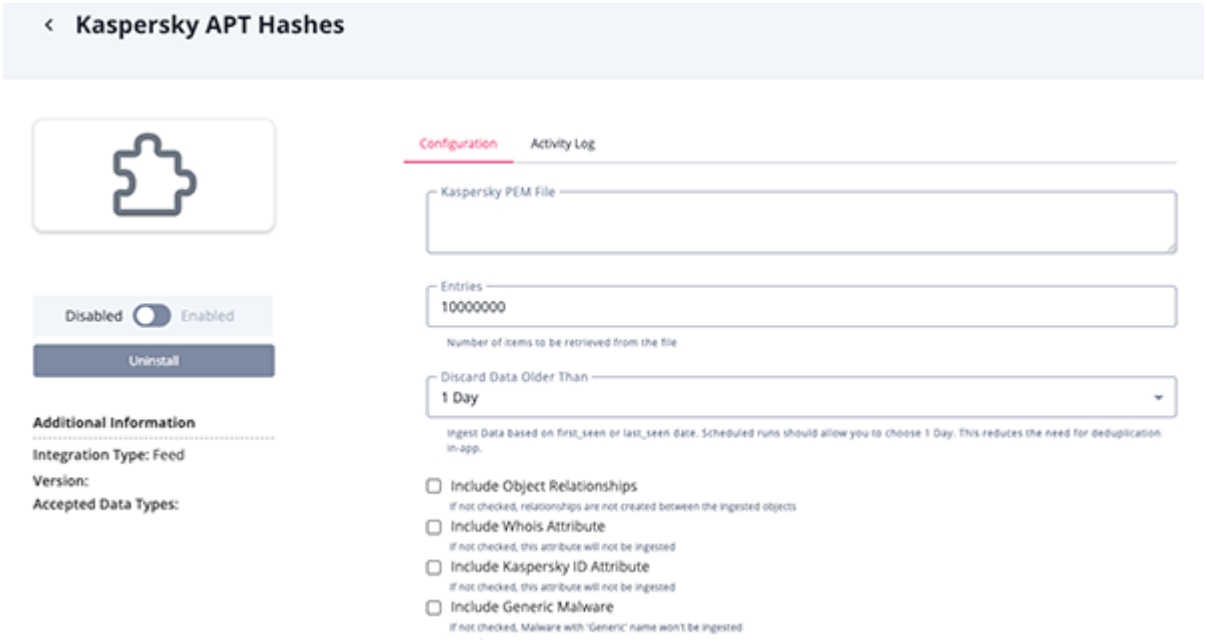
   > If you are installing the integration for the first time, it will be located under the **Disabled** tab.

3. Click on the integration entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

All Feed Parameter Except Malicious Hash

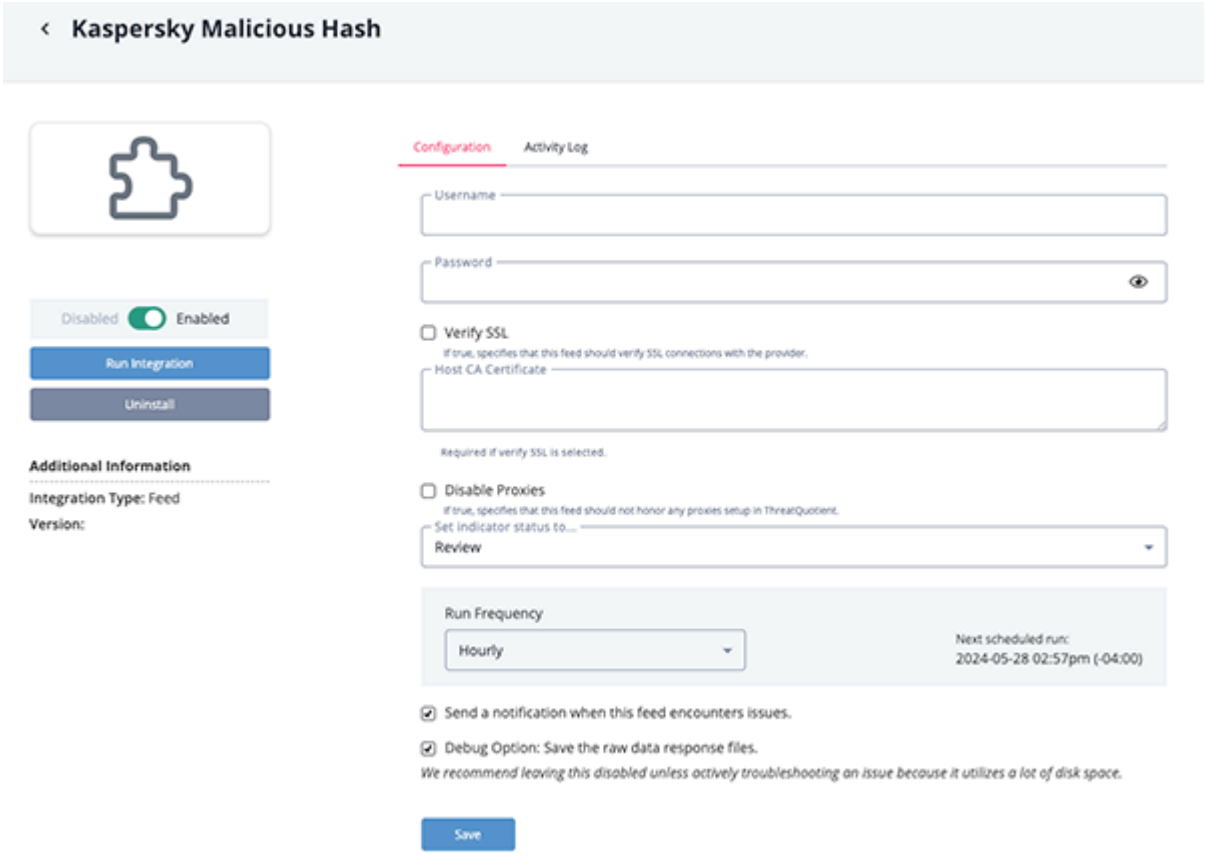
PARAMETER	DESCRIPTION
Kaspersky PEM File	Your Kaspersky Client Certificate for authentication.
Entries	The number of entries to be retrieved. The default is set to 10,000,000.
Discard Data Older Than	Discard data based on the first_seen and last_seen fields to reduce load. Option include: ◦ 1 Day (default) ◦ 2 Days ◦ 5 Days ◦ 7 Days ◦ All Time
Include Object Relationships	When enabled, relationships will be created between ingested objects.
Include Whois Attribute	When enabled, the Whois attribute is ingested.

Include Kaspersky ID Attribute	When enabled, the Kaspersky ID attribute is ingested.
Include Generic Malware	When enabled, malware with the **Generic** name will be ingested.



Malicious Hash Parameters

PARAMETER	DESCRIPTION
Username	Your Kaspersky TAXII service username.
Password	Your Kaspersky TAXII service token.
Verify SSL	Enable or disable verification of SSL connections with the provider.
Disable Proxies	If enabled, the feed will not honor proxy settings within ThreatQ.



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. It ingests indicators and malware together with their attributes.

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 Sample Response:


```
[
    {
        "bot_urls": [
            {
                "bot_url": "one.saltapparel.club/accept.php"
            }
        ],
        "category": "Malware",
        "domains": [
            {
                "domain": "saltapparel.club"
            }
        ],
        "files": [
            {
                "MD5": "51D2B6222891CD0F444C1CF8E542A003",
                "SHA1": "E18F994827E26C2393832532142BB99D611B0B82",
                "SHA256":
"EEF0CABE42B36B9544DD8E3BB3ACE0002D82579DDD4E40060C2397D510CD5EAE",
                "threat": "Trojan.Win32.Generic.go"
            },
            {
                "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"
        }
    },
    ...
]
```

ThreatQuotient provides the following default mapping for this feed:

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
[].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
[].files[].threat	Related Malware.Value	N/A	[].first_seen	Generic.go	Having the `[Prefix:]Behaviour.Platform.Name[.Variant]` pattern, it ingest the last part (`Name[.Variant]`). Related to `[].files[]` Indicators.
[].geo	Indicator.Attribute, Malware.Attribute, Related Malware.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-

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					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
[].mask	Indicator.Value	See Kaspersky Type Mapping table	[].first_seen	saltapparel.club	N/A
[].popularity	Indicator.Attribute, Malware.Attribute, Related Malware.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
[].threat	Malware.Value	N/A	[].first_seen	Generic	Having the `[Prefix:]Behaviour.Platform.Name[.Variant]` pattern, it ingest the last part (`Name[.Variant]`). Related 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
[].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.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					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

Kaspersky Malicious Hash

The Kaspersky Malicious Hash returns a list of STIX bundles, each of them containing Indicators related in `TAXII_Malicious_Hash_Data_Feed_Indicators` (stix2) collection. The JSON data returned is a list of qualified STIX bundles that are passed into ThreatQ's STIX Parser.

`GET https://taxii.tip.kaspersky.com/taxii2/`

Sample Response:


```
{
    "type": "bundle",
    "id": "bundle--8cb6812e-9ed2-4257-aaf9-84b3a14060d2",
    "spec_version": "2.0",
    "objects": [
        {
            "type": "indicator",
            "spec_version": "2.0",
            "id": "indicator--605539c9-8e34-439f-a5eb-419972ea46d2",
            "created": "2023-11-28T01:03:51.687Z",
            "modified": "2023-11-28T01:03:51.687Z",
            "labels": [
                "malicious-activity"
            ],
            "confidence": 100,
            "name": "Hash",
            "description":
"date_added=2023-11-28T01:03:51.687Z;file_size=4268;file_type=Eml;first_seen=20
23-11-28T00:02:00.000Z;geo=jp;last_seen=2023-11-28T00:41:00.000Z;popularity=2;t
hreat=HEUR:Hoax.Script.Scaremail.gen",
            "pattern": "[file:hashes.MD5 = '605539C98E34339FA5EB419972EA46D2'
OR file:hashes.'SHA-256' =
'16A6CF6D77CD00632C807EB739F4DAF0B8DBCDE65C5D4194FEBEE83E526F7D9F']",
            "valid_from": "2023-11-28T01:03:51.687000Z",
            "valid_until": "2100-01-01T00:00:00.000000Z"
        }
  ]
}
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
[].pattern	Indicator.Value	MD5	[].created	605539C98E34339FA5E B419972EA46D2	If `MD5` exists in parsed `patterns`. Inter-related with other hash Indicators if `Include Object Relationships` is selected
[].pattern	Indicator.Value	SHA1	[].created	N/A	If `SHA-1` exists in parsed `patterns`. Inter-related with other hash Indicators if `Include Object Relationships` is selected
[].pattern	Indicator.Value	SHA256	[].created	16A6CF6D77CD00632C8 07EB739F4DAF0B8DBCD E65C5D4194FEBEE83E526F7D9F	If `SHA-256` exists in parsed `patterns`. Inter-related with other hash Indicators if `Include Object Relationships` is selected
[].confidence	Indicator.Attribute	Confidence	[].created	100	Updates at ingestion
[].valid_from	Indicator.Attribute	Valid From	[].created	2023-11-28T01:03:51.687000Z	Timestamp value
[].valid_until	Indicator.Attribute	Valid Until	[].created	2100-01-01T00:00:00.000000Z	Timestamp value. Updates at ingestion
[].modified	Indicator.Attribute	Modified At	[].created	2023-11-28T01:03:51.687Z	Timestamp value. Updates at ingestion
[].labels	Indicator.Attribute	Label	[].created	malicious-activity	Updates at ingestion
[].name	Signature.Title	N/A	[].created	Hash	
N/A	Signature.Type	STIX INDICATOR PATTERN	[].created	N/A	
[].pattern	Signature.Source Code	N/A	[].created	`[file:hashes.MD5 = '605539 C98E34339FA5EB419972EA46D 2' OR file:hashes.'SHA-256' = '16A6CF6D77CD00632C807EB7 3 9F4DAF0B8DBCDE65C5D4194FE B EE83E526F7D9F']`	

Kaspersky Mobile Malicious and ICS Hash Feeds

The Kaspersky Mobile Malicious Hash and ICS Hash feeds ingests sets of file hashes covering the most dangerous, prevalent, or emerging malware. All three 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"
            }
        ]
    },
    ...
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	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, Malware.Attribute	Country Code	[].first_seen	br	Value is split on `', '`. Applied to hash Indicators
[].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
[].MD5	Indicator.Value	MD5	[].first_seen	82865FF17BC664C711EFA674759F9991	Inter-related with other hash Indicators
[].popularity	Indicator.Attribute, Malware.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
[].threat	Malware.Value	N/A	[].first_seen	KMSAuto.i	Having the `[Prefix:]Behaviour.Platform.Name[.Variant]` pattern, it ingest the last part (`Name[.Variant]`).
[].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

APT Feeds

Kaspersky APT IPs

The Kaspersky APT IPs feed ingests sets of IP addresses that are part of infrastructure used in malicious APT campaigns.

`GET https://wlinfo.kaspersky.com/api/v1.0/feeds/90/updates`

JSON response sample:

```
[
    {
        "id": 56226423,
        "ip": "23.106.122.148",
        "detection_date": "12.08.2022 00:00",
        "publication_name": "BluePants: a new malicious framework hits Pan-Asia – Part II",
        "geo": "Central Asia, Indonesia, Kazakhstan, Malaysia, Philippines, Southeast Asia, Taiwan,
Thailand",
        "industries": "Software development, Telecommunications",
        "api_publication_id": "c402bfac-1b7d-4525-760f-03b000baf00b-apt",
        "confidence": 25
    },
    ...
]
```

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.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
[].confidence	Indicator.Attribute	Confidence	[].detection_date	25	N/A

Kaspersky APT URLs

The Kaspersky APT URLs feed ingests set of domains that are part of an infrastructure used in malicious APT campaigns.

```
GET https://wlinfo.kaspersky.com/api/v1.0/feeds/91/updates
```

JSON response sample:

```
[
    {
        "id": 56226455,
        "mask": "login.dptuoguan.com",
        "type": 2,
        "detection_date": "12.08.2022 00:00",
        "publication_name": "BluePants: a new malicious framework hits Pan-Asia - Part II",
        "geo": "Central Asia, Indonesia, Kazakhstan, Malaysia, Philippines, Southeast Asia, Taiwan,
Thailand",
        "industries": "Software development, Telecommunications",
        "api_publication_id": "c402bfac-1b7d-4525-760f-03b000baf00b-apt",
        "confidence": 25
    },
    ...
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	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
[].confidence	Indicator.Attribute	Confidence	[].detection_date	25	N/A

Kaspersky APT Hashes

`GET https://wlinfo.kaspersky.com/api/v1.0/feeds/89/updates`

This feed ingests set of hashes covering malicious artifacts used by APT actors to conduct APT campaigns.

JSON response sample:

```
[
    {
        "id": 56226535,
        "MD5": "3E9DC9C5939DE2F0DF6F5CCF48D423BE",
        "SHA1": "D23896558706BDBA3D5A3A49B756EF0E2C563D75",
        "SHA256": "3056C9014E500C35F67EA66E9DDB605F44C9B7D45574B8328967CA03823ADC95",
        "detection_date": "12.08.2022 00:00",
        "publication_name": "BluePants: a new malicious framework hits Pan-Asia - Part II",
        "geo": "Central Asia, Indonesia, Kazakhstan, Malaysia, Philippines, Southeast Asia, Taiwan,
Thailand",
        "industries": "Software development, Telecommunications",
        "api_publication_id": "c402bfac-1b7d-4525-760f-03b000baf00b-apt",
        "confidence": 100
    },
    ...
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
].MD5	Indicator.Value	MD5	[].detection_date	F805882CC276B583D9C A7E16AD957E7B	Inter-related with other hash Indicators
[].SHA1	Indicator.Value	SHA-1	[].detection_date	2E4DB721DBD2ACEFD851 BEDF95492BF789F588FD	Inter-related with other hash Indicators
[].SHA256	Indicator.Value	SHA256	[].detection_date	D76024256AC35424EB02B 6A47565F8859B12050F5DE 49EF16DEC449A61DA1EFC	Inter-related with other hash Indicators
[].publication_name	Indicator.Attribute	Publication	[].detection_date	ShadowBrokers Lost in translation leak - SWIFT attacks analysis	N/A
[].confidence	Indicator.Attribute	Confidence	[].detection_date	100	N/A

Other Feeds

Kaspersky IP Reputation

The Kasperksy IP Reputation feed ingests IP addresses of malicious hosts.

`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"
    },
    ...
]
```

ThreatQuotient provides the following default mapping for this feed:

FEED DATA PATH	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	51D2B6222891CD0F444C1CF8E542A003	Related to primary `[].ip` Indicator. Inter-related with other `[].files[]` Indicators
[].files[].SHA1	Related Indicator.Value	SHA-1	[].first_seen	E18F994827E26C2393832532142BB99D611B0B82	Related to primary `[].ip` Indicator. Inter-related with other `[].files[]` Indicators
[].files[].SHA256	Related Indicator.Value	SHA256	[].first_seen	EEF0CABE42B36B9544DD8E3BB3ACE0002D82579DDD4E40060C2397D510CD5EAE	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
[].files[].threat	Related Malware.Value	N/A	[].first_seen	Generic.go	Having the `[Prefix:]Behaviour.Platform.Name[.Variant]` pattern,

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
					it ingest the last part (`Name[.Variant]`). Only Related 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
[].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

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
[].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
[].popularity	Indicator.Attribute, Related Malware.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, Related Malware.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
Malware	812
Malware Attributes	11,663

Kaspersky Phishing URL Exact

METRIC	RESULT
Run Time	6 hours 30 minutes
Indicators	42,653
Indicator Attributes	511,333

Kaspersky Malicious URL Exact

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

Kaspersky Ransomware URL

METRIC	RESULT
Run Time	2 hours
Indicators	22,203
Indicator Attributes	164,097
Malware	424
Malware Attributes	4,014

Kaspersky IoT URL

METRIC	RESULT
Run Time	3 hours

METRIC	RESULT
Indicators	36,214
Indicator Attributes	588,846
Malware	45
Malware Attributes	5,180

Kaspersky Mobile Botnet C&C URL

METRIC	RESULT
Run Time	2 hours 15 minutes
Indicators	42,649
Indicator Attributes	180,415
Malware	68
Malware Attributes	851

Kaspersky Malicious Hash

METRIC	RESULT
Run Time	3 minutes
Indicators	3,318
Indicator Attributes	16,590

METRIC	RESULT
Signatures	1,217

Kaspersky Mobile Malicious Hash

METRIC	RESULT
Run Time	50 minutes
Indicators	14,930
Indicator Attributes	98,848
Malware	987
Malware Attributes	7,975

Kaspersky ICS Hash

METRIC	RESULT
Run Time	1 hour 50 minutes
Indicators	40,135
Indicator Attributes	268,130
Malware	1,486
Malware Attributes	19,686

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	30 minutes
Indicators	9,292
Indicator Attributes	57,202
Malware	51
Malware Attributes	170

Change Log

- **Version 2.2.6**
  - Updated the **Kaspersky Malicious Hash** feed to retrieve data via TAXII. This resolves an issue where the feed was not ingesting data on scheduled runs.
  - Updated the minimum ThreatQ version to 5.20.0
- **Version 2.2.5**
  - Added the following new configuration options:
    - **Include Object Relationships**
    - **Include Whois Attribute**
    - **Include Kaspersky ID Attribute**
    - **Include Generic Malware**
  - Removed the **Exclude Object Relationships** configuration option.
- **Version 2.2.4**
  - Added new configuration option: Exclude Object Relationships. This option allows you to control whether or not the integration will create relationships between ingested objects.
- **Version 2.2.3**
  - Added Confidence as an attribute to the following APT feeds: APT IP, APT Hash, and APT URL.
- **Version 2.2.2**
  - Updated the integration so that no records are discarded even if dates are not present when **Discard data older than** is set to **All Time**.
  - Fixed an issue that prevented APT feeds from being filtered correctly by date.
- **Version 2.2.1**
  - Updated the default setting for the Entries configuration parameter from 10,000 to 10,000,000.
  - Added configuration parameter, **Discard Data Older Than**, to discard data based on first_seen and last_seen to reduce load.
- **Version 2.2.0**
  - The integration can now ingest objects of the Malware family and relate it to indicators.
  - Removed `Last seen` attribute from indicators to avoid being duplicated with different values.
- **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