Kaspersky Data Feeds for QRadar importing utility

Product version: 2.0
Dear User,

Thank you for choosing Kaspersky as your security software provider. We hope that this document helps you to use our product.

Attention! This document is the property of AO Kaspersky Lab (herein also referred to as Kaspersky). All rights to this document are reserved by the copyright laws of the Russian Federation and by international treaties. Illegal reproduction and distribution of this document or parts hereof incur civil, administrative, or criminal liability under applicable law.

Any type of reproduction or distribution of any materials, including translations, is allowed only with the written permission of Kaspersky.

This document, and graphic images related to it, may be used for informational, non-commercial, and personal purposes only.

Kaspersky reserves the right to amend this document without additional notification.

Kaspersky assumes no liability for the content, quality, relevance, or accuracy of any materials used in this document to which rights are held by third parties, or for any potential harms associated with use of the document.

Registered trademarks and service marks used in this document are the property of their respective owners.

Document revision date: 2/26/2021

© 2021 AO Kaspersky Lab

https://www.kaspersky.com
https://help.kaspersky.com
https://support.kaspersky.com

About Kaspersky: (https://www.kaspersky.com/about/company)
# Contents

About this document ........................................................................................................... 4
About Kaspersky Data Feeds for QRadar importing utility .................................................. 5
Distribution kit .................................................................................................................. 5
Hardware and software requirements ................................................................................. 6
Kaspersky Threat Data Feeds ............................................................................................. 6
Installing and configuring Kaspersky Data Feeds for QRadar importing utility .................... 8
Custom event properties ................................................................................................... 8
Authorized services .......................................................................................................... 12
Preparing Kaspersky Data Feeds for QRadar importing utility for use ................................. 13
Reference sets .................................................................................................................. 14
Command-line options ...................................................................................................... 14
Custom rules ..................................................................................................................... 15
Running Kaspersky Data Feeds for QRadar importing utility on a regular basis .................. 19
Additional information about Kaspersky Data Feeds for QRadar importing utility ................. 20
Workflow .......................................................................................................................... 20
Splitting reference sets by popularity .............................................................................. 22
Logging ............................................................................................................................ 22
Removing Kaspersky Data Feeds for QRadar importing utility ............................................ 23
Alternative ways of checking events .................................................................................. 25
AO Kaspersky Lab ............................................................................................................. 26
Information about third-party code .................................................................................... 27
Trademark notices ............................................................................................................ 28
About this document

This document describes Kaspersky Data Feeds for QRadar® importing utility.
About Kaspersky Data Feeds for QRadar importing utility

Kaspersky Data Feeds for QRadar importing utility is a utility provided by Kaspersky that imports indicators from Kaspersky Threat Data Feeds to IBM® QRadar reference sets.

After the indicators are imported from the feed to QRadar, you can check incoming events in QRadar against them. The Custom Rules Engine (CRE) module of QRadar can check whether incoming events contain records stored in the reference sets. You can configure QRadar to respond in a specific way when an incoming event contains a record from one of the reference sets that have been created.

Kaspersky Data Feeds for QRadar importing utility is a Python® application; it contains no binary files.

In this chapter

Distribution kit .......................................................... 5
Hardware and software requirements ........................................... 6
Kaspersky Threat Data Feeds ................................................... 6

Distribution kit

Kaspersky Data Feeds for QRadar importing utility is shipped as an archive. The following table describes the contents of the archive.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>modules/apiclient.py</td>
<td>Auxiliary file.</td>
</tr>
<tr>
<td>modules/RestApiClient.py</td>
<td>Auxiliary file.</td>
</tr>
<tr>
<td>modules/<strong>init</strong>.py</td>
<td>Auxiliary file.</td>
</tr>
<tr>
<td>download_feeds.py</td>
<td>Auxiliary file.</td>
</tr>
<tr>
<td>feed_downloader_for_qradar.py</td>
<td>Main file to run.</td>
</tr>
<tr>
<td>parse_feeds.py</td>
<td>Auxiliary file.</td>
</tr>
<tr>
<td>utils.py</td>
<td>Auxiliary file.</td>
</tr>
<tr>
<td>legal_notices.txt</td>
<td>Legal notices for the product and information about third-party code.</td>
</tr>
<tr>
<td>license.txt</td>
<td>End User License Agreement (EULA).</td>
</tr>
<tr>
<td>requirements.txt</td>
<td>File with dependencies for Python 2.</td>
</tr>
<tr>
<td>requirements3.txt</td>
<td>File with dependencies for Python 3.</td>
</tr>
</tbody>
</table>
Hardware and software requirements

Kaspersky Data Feeds for QRadar importing utility has the following system requirements.

Supported operating systems
Kaspersky Data Feeds for QRadar importing utility can run on the following operating systems:

- Linux® x64

Software requirements
Kaspersky Data Feeds for QRadar importing utility works with the following versions of Python:

- Python 2.7.18
- Python 3.7.0 or later

The dependencies for both versions are listed in requirements.txt and requirements3.txt, respectively.

RAM requirements
Kaspersky Data Feeds for QRadar importing utility requires at least 700 MB of RAM.

Kaspersky Threat Data Feeds

This section describes Kaspersky Threat Data Feeds that are processed by the Kaspersky Data Feeds for QRadar importing utility.

The following feeds are processed:

- IP Reputation Data Feed—A set of IP addresses with context covering malicious hosts.
- APT Hash Data Feed—A set of hashes that cover malicious artifacts used by APT actors to conduct APT campaigns.
- APT IP Data Feed—A set of IP addresses that belong to the infrastructure used in APT campaigns.
- APT URL Data Feed—A set of domains that belong to the infrastructure used in APT campaigns.
- Botnet CnC URL Data Feed (exact)—A set of URLs and hashes with context that cover desktop botnet C&C servers and related malicious objects.
- Malicious Hash Data Feed—A set of file hashes with context that cover the most dangerous, prevalent, or emerging malware.
- Malicious URL Data Feed (exact)—A set of URLs with context that cover malicious websites and web pages.
- Mobile Botnet CnC URL Data Feed—A set of URLs with context that cover mobile botnet C&C servers.
• Mobile Malicious Hash Data Feed—a set of file hashes with context for detecting malicious objects that infect mobile Google™ Android™ and Apple® iPhone® devices.

• Phishing URL Data Feed (exact)—A set of URLs with context that cover phishing websites and web pages.

• Ransomware URL Data Feed—A set of URLs, domains, and hosts with context that cover ransomware links and websites.

• Vulnerability Data Feed—A set of file hashes with context that cover vulnerabilities in applications and cover exploits that use those vulnerabilities.

• IoT URL Data Feed—A set of URLs with context that cover malicious links used to download malware targeting Internet of Things-enabled devices.

• ICS Hash Data Feed—A set of hashes of malicious applications that are used to attack the ICS (Industrial Control Systems) infrastructure.

Demo feeds are also available. Demo feeds provide lower detection rates in comparison with their corresponding commercial versions. The following demo feeds are available:

• Demo Botnet CnC URL Data Feed—a demo version of Botnet CnC URL Data Feed.

• Demo IP Reputation Data Feed—a demo version of IP Reputation Data Feed.

• Demo Malicious Hash Data Feed—a demo version of Malicious Hash Data Feed.

• Demo APT Hash—a demo version of APT Hash Data Feed.

• Demo APT URL—a demo version of APT URL Data Feed.

• Demo APT IP—a demo version of APT IP Data Feed.
Installing and configuring Kaspersky Data Feeds for QRadar importing utility

This section describes QRadar entities used by Kaspersky Data Feeds for QRadar importing utility and provides the steps to be performed before you use Kaspersky Data Feeds for QRadar importing utility.

In this chapter

<table>
<thead>
<tr>
<th>Custom event properties</th>
<th>8</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authorized services</td>
<td>12</td>
</tr>
<tr>
<td>Preparing Kaspersky Data Feeds for QRadar importing utility for use</td>
<td>13</td>
</tr>
<tr>
<td>Reference sets</td>
<td>14</td>
</tr>
<tr>
<td>Command-line options</td>
<td>14</td>
</tr>
<tr>
<td>Custom rules</td>
<td>15</td>
</tr>
<tr>
<td>Running Kaspersky Data Feeds for QRadar importing utility on a regular basis</td>
<td>19</td>
</tr>
</tbody>
</table>

Custom event properties

QRadar provides various event properties, based on regular expressions, for extracting information from events and checking the information against reference sets. Make sure that you have event properties for all indicators that you want to match against Kaspersky Data Feeds. If event properties for some indicators do not exist, create your own custom event properties.

To create a custom event property:

1. In QRadar, select the Admin tab, go to the Data sources section, and under Events, click Custom Event Properties.

   The Custom Event Properties dialog box opens.

2. Click the Add button.

   The Custom Event Property Definition dialog box opens.

3. Specify the parameters of the new property.
   
   a. Select the Regex Based option or make sure that the Regex Based option is selected. In the some versions of QRadar, this option is called Extraction Based.
   
   b. In the Property Definition group box, select the New Property radio button.
   
   c. Enter the name of the new property in the text field next to the New Property radio button. Examples of property names are listed in the table below.
   
   d. In the Field Type drop-down list, select the field type for the property. Example property names that correspond to different field types are listed in the table below.
   
   e. Select the Parse in advance for rules, reports and searches checkbox.
f. If needed, enter the description of the property in the **Description** text field.

![Image](image.png)

4. In the **Property Expression Definition** group box, specify the definition of the new property.
   a. Select the **Enabled** checkbox.
   b. In the **Log Source Type** and **Log Source** fields select the event source that the new event property will be applied to.
   c. Do one of the following:
      * Select the **Event Name** radio button and enter the name of the event that must be parsed into the field next to it
      * Select the **Category** radio button and select the category of the event in the drop-down list next to it
   d. In the **Extraction using** drop-down list, select **Regex**. Some versions of QRadar might not have this list. In this case, proceed to the next step.
   e. In the **Regex** text field, specify the regular expression for extracting the corresponding indicator. Examples of regular expressions are listed in the table below.
   f. In the **Capture Group** field, enter 1.
   g. In the text field **Test Field** above the **Property Definition** group box, specify an example event for verification of the regular expression.
h. Verify the correctness of the regular expression by clicking the Test button.

5. Click Save.

The regular expressions specified below apply to events in the LEEF format that contain the fields `url`, `ip`, `md5`, `sha1`, and `sha256` (see the example event below). If you use a different event format, you need to edit these regular expressions to match it.

Table 2. Property names, field types, and regular expressions

<table>
<thead>
<tr>
<th>Property name</th>
<th>Field type</th>
<th>Regular expressions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hash</td>
<td>AlphaNumeric</td>
<td>(?md5</td>
</tr>
<tr>
<td>URL</td>
<td>AlphaNumeric</td>
<td>url=([^\n]+)</td>
</tr>
</tbody>
</table>
| IP            | IP            | ip=((([0-5][0-9]|1[0-9][0-9]|2[0-4][0-9]|25[0-5]).)([0-9]){0,2})
| Domain        | AlphaNumeric  | url=(?:https?:\/\/[^\:\/\n]+@)?(\/[\^\:\/\n\t+]+)?(\^[^\:\/\n\t]+)\^[^\:\/\n\t]+)\^[^\:\/\n\t]+) |
| Host          | AlphaNumeric  | url=(?:https?:\/\/[^\:\/\n]+@)?(\/[\^\:\/\n\t+]+)?(\^[^\:\/\n\t]+)\^[^\:\/\n\t]+) |

Example event

Fields from this example event in the LEEF format can be matched by the regular expressions from the table above. The fields are separated by the TAB characters.
Authorized services

Kaspersky Data Feeds for QRadar importing utility uses the QRadar RESTful API to interact with QRadar. To authenticate API calls to QRadar Console, the QRadar RESTful API uses either authorized services or QRadar users. This section describes how to add an authorized service and receive an authorization token associated with it.

The main difference between using a QRadar user login and password and using a token is the following: when you create a new user, it exists until you explicitly remove it, while a token is usually assigned a period during which it is valid.

► To add an authorized service:

1. In QRadar Console, select the Admin tab.
2. In the left navigation pane, click System Configuration.
3. In the right pane, under User Management click Authorized Services.
   The Manage Authorized Services dialog box opens.
4. Click the Add Authorized Service button.
5. In the Service Name field, type a name for this authorized service (for example, Kaspersky Data Feeds App).
   The name can be up to 255 characters in length.
6. In the User Role column, select the Admin user role to assign to this authorized service.
   The user roles that are assigned to an authorized service determine the functions to which this service can gain access through the QRadar user interface.
7. In the Security Profile column, select the Admin security profile to assign to this authorized service.
   The security profile determines the networks and log sources that this service can access through the QRadar user interface.
8. In the Expiry Date column, type or select a date when you want this service to expire. If a date of expiration is not required, select No Expiry.
9. Click Create Service.
   A confirmation message appears containing a token field that you must copy into your vendor software to authenticate with QRadar.

The actual information about authorized service is available at https://www.ibm.com/support/knowledgecenter/SS42VS_7.3.0/com.ibm.qradar.doc/t_qradar_adm_add_auth_serv.html.
After you add an authorized service, QRadar notifies you whether the changes must be deployed.

► To deploy the changes:

1. In QRadar Console, select the **Admin** tab.
2. Click **Deploy Changes**.

### Preparing Kaspersky Data Feeds for QRadar importing utility for use

Kaspersky Data Feeds for QRadar importing utility is shipped as an archive that contains several files (see section "Distribution kit" on page 5).

► To prepare Kaspersky Data Feeds for QRadar importing utility for use:

1. Unpack the Kaspersky Data Feeds for QRadar importing utility archive to any directory on your system. This directory is referred to as `%utility_dir%` in this document.
2. Install the dependencies:
   - For Python 2.X.X, run:
     ```bash
     pip install -r requirements.txt
     ```
   - For Python 3.X.X, run:
     ```bash
     pip install -r requirements3.txt
     ```
3. Open the file `settings.py` for editing.
4. In the `FEEDS` dictionary, comment out Kaspersky Threat Data Feeds that you do not want to use.

   The list of feeds that you can use is defined by your PEM certificate.

5. Specify the time period (in hours) for storing indicators in QRadar by using the `UPDATE_PERIOD_HOURS` variable.

   It is recommended to specify a value close to the period for running Kaspersky Data Feeds for QRadar importing utility (see section "Running Kaspersky Data Feeds for QRadar importing utility on a regular basis" on page 19).

   If you want to change the value of `UPDATE_PERIOD_HOURS` after you have already imported indicators to QRadar reference sets, delete the reference sets by using the QRadar GUI, change the `UPDATE_PERIOD_HOURS` value, and then launch Kaspersky Data Feeds for QRadar importing utility.
6. Save and close settings.py.

7. Run (see section "Command-line options" on page 14) Kaspersky Data Feeds for QRadar importing utility manually.

   The necessary reference sets will be created in QRadar. You will also be able to check whether the utility works properly.

Reference sets

QRadar uses reference sets to store data in a simple list format.

A reference set contains unique values that you can use in searches, filters, rule test conditions, and rule responses. Thus, you can use reference sets for storing indicators of compromise (IOCs). To determine whether a reference set contains a data element, use a rule (see section "Custom rules" on page 15). For example, you can create a rule that detects that an IP address takes the user to a dangerous website.

URLs that contain colons (:), commas (,), or quotation marks (") are converted to percent encoding before being loaded to QRadar.


Command-line options

Kaspersky Data Feeds for QRadar importing utility is launched from the command line as follows:

```python
```

The following table explains the command-line options.

<table>
<thead>
<tr>
<th>Option (full / short)</th>
<th>Description</th>
<th>Mandatory, default value</th>
</tr>
</thead>
<tbody>
<tr>
<td>qradar / q</td>
<td>IP address or host name where QRadar Console is available.</td>
<td>Mandatory.</td>
</tr>
<tr>
<td>proxy / x</td>
<td>Proxy server connection string in the format http[s]://user:password@host:port. This proxy server will be used for downloading Kaspersky feeds from the WlInfo server (<a href="https://wlinfo.kaspersky.com/">https://wlinfo.kaspersky.com/</a>).</td>
<td>Optional. If this option is not specified, no proxy is used.</td>
</tr>
</tbody>
</table>
Installing and configuring Kaspersky Data Feeds for QRadar importing utility

<table>
<thead>
<tr>
<th>Option</th>
<th>Description</th>
<th>Required/Optional</th>
</tr>
</thead>
<tbody>
<tr>
<td>user / u</td>
<td>Name of the user that has administrator privileges for access to the QRadar RESTful API.</td>
<td>You must specify either a user name and password or a token.</td>
</tr>
<tr>
<td>password / p</td>
<td>Password for access to the QRadar RESTful API.</td>
<td>You must specify either a user name and password or a token.</td>
</tr>
<tr>
<td>token / t</td>
<td>Authentication token for access to the QRadar RESTful API.</td>
<td>You must specify either a user name and password or a token.</td>
</tr>
<tr>
<td>pem_file / f</td>
<td>Path to the PEM-formatted certificate that will be used for downloading Kaspersky feeds.</td>
<td>Optional. By default, it is %utility_dir%/feeds.pem.</td>
</tr>
<tr>
<td>verbose / v</td>
<td>If specified, verbose logging is performed.</td>
<td>Optional.</td>
</tr>
<tr>
<td>help / h</td>
<td>If specified, a short description of Kaspersky Data Feeds for QRadar importing utility and how to use it is printed to the console.</td>
<td>Optional.</td>
</tr>
<tr>
<td>split-by-popularity / s</td>
<td>If specified, divides reference sets, created by Kaspersky Data Feeds for QRadar importing utility, by the value of the popularity field. For more information, see section &quot;Splitting reference sets by popularity (on page 22)&quot;.</td>
<td>Optional.</td>
</tr>
</tbody>
</table>

If Kaspersky Data Feeds for QRadar importing utility has successfully finished its work, it returns 0; otherwise, the return code is greater than 0. Therefore, you can check the return code and write a proper message to the console whether the work of Kaspersky Data Feeds for QRadar importing utility succeeded or failed.

**Custom rules**

This section describes how to configure QRadar so that it will respond to incoming events. You configure QRadar by creating event rules after Kaspersky Data Feeds for QRadar importing utility successfully finishes its work for the first time.
To create QRadar event rules:

1. In QRadar Console, select the **Offenses** tab, and then click **Rules** in the left navigation pane.

![QRadar Offenses Tab](image)

2. Click the **Actions** drop-down list, and then select **New Event Rule**.

The **Rule Wizard** starts.

3. Select the **Events** radio button, and then click **Next**.

![QRadar Rule Wizard](image)
4. In the list, select the **when any of these event properties are contained in any of these reference set(s)** item, and then click the **Add test to rule** button (⊕) next to the item.

5. Specify the following parameters of the rule:
   - **Rule name**, in the **Apply** field.
     For example, **KL_IP_Reputation_Danger**.
   - **Detection system**, in the system drop-down list.
     You can select either the local or the global detection system.
     - If you select **Local**, all rules are processed by the event processor in which they were received and offenses are created only for the events that are processed locally.
     - If you select **Global**, all matching events are sent to QRadar Console for processing and, therefore, QRadar Console uses more bandwidth and processing resources.
   - **Fields containing indicators that must be checked against Kaspersky Data Feeds**.
     You can specify these fields by clicking **these event properties**. You can add necessary fields to QRadar beforehand (see section "Custom event properties" on page 8) if they are not already present there.
   - **Reference set**.
     You can specify the reference set (see section "Reference sets" on page 14) by clicking **these reference set(s)**.

Click **Next**.
6. Create the rule response by using the Wizard, as shown in the figure below.

7. Click Finish to save the rule.

8. Repeat the above steps for each reference set.
   You can specify different responses for different reference sets.
Running Kaspersky Data Feeds for QRadar importing utility on a regular basis

Typically Kaspersky Data Feeds for QRadar importing utility is run on a regular basis. This section describes how to use the cron utility for this purpose.

► To configure periodic running of Kaspersky Data Feeds for QRadar importing utility:

2. Redirect log messages to /tmp/kaspersky_feeds_for_qradar.log, as described in Logging (on page 22).
3. Run the following command for editing the crontab file:
   
crontab -e
4. Add the following string to the crontab file:
   
   */30 * * * * python %utility_dir%/feed_downloader_for_qradar.py
   <command-line-options> || mail -s "KL feeds update failed"
   email@example.com
   
   (Substitute %utility_dir% with its real value and use a real email address for receiving failure notifications instead of email@example.com.)

Kaspersky Data Feeds for QRadar importing utility will run every 30 minutes and write its log messages to the /tmp/kaspersky_feeds_for_qradar.log file. If the work of Kaspersky Data Feeds for QRadar importing utility fails, an email with the subject KL feeds update failed will be sent to the specified email address.

Recommended intervals

The period for running Kaspersky Data Feeds for QRadar, which is specified in crontab, must have the following properties:

- Less than the value of the UPDATE_PERIOD_HOURS parameter in feed_downloader_for_qradar.py. The UPDATE_PERIOD_HOURS parameter means the lifetime of records in the reference sets created by Kaspersky Data Feeds for QRadar.
- Greater than the time needed by Kaspersky Data Feeds for QRadar to process all of the selected feeds. Kaspersky Data Feeds for QRadar needs up to three hours to processes all the feeds listed above. Kaspersky Data Feeds for QRadar needs about five minutes to process all the demo feeds.

We recommend that you update the reference sets as often as possible.
Additional information about Kaspersky Data Feeds for QRadar importing utility

This section explains how to use Kaspersky Data Feeds for QRadar importing utility.

In this chapter
- Workflow ................................................................. 20
- Splitting reference sets by popularity ................................ 22
- Logging ................................................................. 22
- Removing Kaspersky Data Feeds for QRadar importing utility ........................................ 23
- Alternative ways of checking events ............................................................. 25

Workflow

When you launch Kaspersky Data Feeds for QRadar importing utility from the command line and specify the correct parameters, the utility downloads Kaspersky Threat Data Feeds from a Kaspersky server. Then it imports indicators from the feed to reference sets that are described in the table below.

<table>
<thead>
<tr>
<th>Reference set name</th>
<th>Custom event property</th>
</tr>
</thead>
<tbody>
<tr>
<td>Kaspersky Malicious Hash [POPULARITY_EN]</td>
<td>Hash</td>
</tr>
<tr>
<td>Kaspersky Demo Malicious Hash [POPULARITY_EN]</td>
<td>Hash</td>
</tr>
<tr>
<td>Kaspersky ICS Hash [POPULARITY_EN]</td>
<td>Hash</td>
</tr>
<tr>
<td>Kaspersky Vulnerability Vulnerable Hash [SEVERITY]</td>
<td>Hash</td>
</tr>
<tr>
<td>Kaspersky Vulnerability Exploit Hash [SEVERITY]</td>
<td>Hash</td>
</tr>
<tr>
<td>Kaspersky APT Hash</td>
<td>Hash</td>
</tr>
<tr>
<td>Kaspersky Demo APT Hash</td>
<td>Hash</td>
</tr>
<tr>
<td>Kaspersky Mobile Malicious Hash [POPULARITY_EN]</td>
<td>Hash</td>
</tr>
<tr>
<td>Kaspersky IP Reputation [IPCATEGORY] [THREAT_LEVEL]</td>
<td>IP</td>
</tr>
<tr>
<td>Kaspersky Demo IP Reputation [IPCATEGORY] [THREAT_LEVEL]</td>
<td>IP</td>
</tr>
<tr>
<td>Kaspersky APT IP</td>
<td>IP</td>
</tr>
<tr>
<td>Kaspersky Demo APT IP</td>
<td>IP</td>
</tr>
</tbody>
</table>

Table 4. Reference sets and custom event properties
<table>
<thead>
<tr>
<th>Kaspersky Data Feeds for QRadar importing utility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Additional information about Kaspersky Data Feeds for QRadar importing utility</td>
</tr>
</tbody>
</table>

| Kaspersky Botnet CnC URL [POPULARITY_EN] | URL |
| Kaspersky Botnet CnC Host [POPULARITY_EN] | Host |
| Kaspersky Botnet CnC Domain [POPULARITY_EN] | Domain |
| Kaspersky Malicious URL [MASK_CATEGORY] [POPULARITY_EN] | URL |
| Kaspersky Malicious Host [MASK_CATEGORY] [POPULARITY_EN] | Host |
| Kaspersky Malicious Domain [MASK_CATEGORY] [POPULARITY_EN] | Domain |
| Kaspersky Phishing URL | URL |
| Kaspersky Phishing Host | Host |
| Kaspersky Phishing Domain | Domain |
| Kaspersky IoT URL | URL |
| Kaspersky Ransomware URL | URL |
| Kaspersky Ransomware Host | Host |
| Kaspersky Ransomware Domain | Domain |
| Kaspersky Mobile Botnet CnC URL [POPULARITY_EN] | URL |
| Kaspersky Mobile Botnet CnC Host [POPULARITY_EN] | Host |
| Kaspersky Mobile Botnet CnC Domain [POPULARITY_EN] | Domain |
| Kaspersky APT URL | URL |
| Kaspersky APT Host | Host |
| Kaspersky APT Domain | Domain |
| Kaspersky Demo APT URL | URL |
| Kaspersky Demo APT Host | Host |
| Kaspersky Demo APT Domain | Domain |
| Kaspersky Demo Botnet CnC URL | URL |
| Kaspersky Demo Botnet CnC Host | Host |
| Kaspersky Demo Botnet CnC Domain | Domain |

Here, variables in brackets can have the following values:

- **IP_CATEGORY**—Malware, Spam, Tor Exit Node, Proxy, Phishing, Botnet CnC, Tor Node, Vpn, Test.

The list of possible values may change in further feed updates.
• **MASKCATEGORY**—Malicious Redirect, Bot CnC, Exploit, Fraud, Malware, Mobile Malware. The list of possible values may change in further feed updates.

• **SEVERITY**—Warning, Low, Medium, High, Critical.

• **THREATLEVEL**—Danger, Suspicious. These values are determined depending on the threat_score field of the feed. If threat_score is less than 75, then the value is Suspicious, otherwise Danger.

• **POPULARITYEN**—Rare, Very Rare, Average, Common, Very Common (present only if Kaspersky Data Feeds for QRadar importing utility is launched with the --split-by-popularity flag). These values are determined depending on the popularity field of the feed. If popularity = 1, the value is Very Rare; 2—Rare; 3—Average; 4—Common; 5—Very Common.

If the --split-by-popularity flag is enabled and Kaspersky Data Feeds for QRadar importing utility has exported all feeds to QRadar, up to 206 reference sets are created. Without the --split-by-popularity flag, up to 94 reference sets are created.

### Splitting reference sets by popularity

Some Kaspersky Threat Data Feeds contain the popularity field. For each indicator in a feed, this field denotes the relative number of users per day that detected it. This field can have values from 1 to 5.

Kaspersky Data Feeds for QRadar importing utility allows you to split the reference sets created from Kaspersky Threat Data Feeds by the value of this field. For an example of splitting reference sets, see the variable POPULARITYEN in section "Workflow (on page 20)".

To enable splitting by popularity, run Kaspersky Data Feeds for QRadar importing utility with the split-by-popularity option (see section "Command-line options" on page 14).

### Logging

Kaspersky Data Feeds for QRadar importing utility logs its activity to the console. It can write log messages at one of two log levels: brief or verbose. The log level is specified by the command-line option (see section "Command-line options" on page 14).

#### Writing messages to a file

► To redirect log messages to a file:

1. Open the file settings.py for editing.
2. Specify the FILE value in the LOG_OUTPUT variable:

   LOG_OUTPUT = 'STDOUT'
3. Specify a full or relative path to the log file in the LOG_FILENAME variable:
   \[ \text{LOG_FILENAME} = 'qradar_kaspersky_feeds.log' \]

4. Save and close settings.py.

**Log levels**

If the brief log level is specified, the following information is written to the log:

- Information about Kaspersky Data Feeds for QRadar importing utility and the software environment:
  - Kaspersky Data Feeds for QRadar importing utility version
  - Python version (32-bit or 64-bit, version number)
  - Operating system (OS) version and bit
- Authentication method (login and password or token)
- List of feeds to be imported to QRadar
- For each downloaded feed:
  - Time when the download of the feed began
  - Time when the download of the feed finished
  - Size of the downloaded archive
- For each created reference set:
  - Name and other parameters of the reference set
  - Message that the import of data to a reference set started
  - Message that the import of data to a reference set finished
  - Warnings and errors that occur during the use of RESTful API functions

If the verbose log level is specified, the following information is written to the log:

- Information that is written for the brief log level
- Command-line parameters used for launching Kaspersky Data Feeds for QRadar importing utility
  
  The user name, password, or token are replaced with the string `<private_data>`.
- Information about network requests made by Kaspersky Data Feeds for QRadar importing utility and the return codes of the requests

**Removing Kaspersky Data Feeds for QRadar importing utility**

This section describes how to remove Kaspersky Data Feeds for QRadar importing utility.

After you have removed the Kaspersky Data Feeds for QRadar importing utility files, you may also have to remove the following QRadar objects:

- Custom rules
- Custom event properties
• Reference sets
• Authorized services
• Users

Removing custom rules
The following procedure describes how to delete a custom rule.

► To delete a custom rule:
1. In QRadar, select the Offenses tab.
2. In the left navigation pane, click Rules.
3. Select a custom rule, click Actions, and in the drop-down list select Delete.

Removing custom event properties
The following procedure describes how to delete a custom event property.

► To delete a custom event property:
1. In QRadar, select Admin, go to the Data sources section, and under Events click Custom Event Properties.
   The Custom Event Properties dialog box opens.
2. Select a custom event property and click the Delete button.

Removing reference sets
The following procedure describes how to delete a reference set.

► To delete a reference set:
1. In QRadar, select Admin and under System configuration, select Reference Set Management.
   The Reference Set Management dialog box opens.
2. Select a reference set and click the Delete button.

Removing authorized services
The following procedure describes how to delete an authorized service.

► To delete an authorized service:
1. In QRadar, select Admin, go to the System configuration section, and under User Management click Authorized Services.
   The Manage Authorized Services dialog box opens.
2. Select an authorized service and click the Delete button.
Removing QRadar users

The following procedure describes how to delete a QRadar user.

► To delete a QRadar user:

1. In QRadar, select Admin, go to the System configuration section, and under User Management click Users. The User Management dialog box opens.
2. Select a user and click the Delete button.

Alternative ways of checking events

Kaspersky Data Feeds for QRadar importing utility is designed so that you can check events by means of QRadar only, without having to use other software. At the same time, Kaspersky offers you another software product, Kaspersky CyberTrace, which has the following advantages:

- Performance of 5000 events per second without any impact on QRadar.
- High-speed capabilities for importing and exporting third-party IoCs and Data Feeds.
- Kaspersky CyberTrace does not use the built-in capabilities of SIEM solutions for matching events against Data Feeds.
- No additional load on the SIEM solution and high-matching performance.
- The SIEM solutions are not designed for processing many IoCs. Kaspersky CyberTrace does not have such limitations.
- The SIEM solutions are not designed for processing associated context for IoCs. Kaspersky CyberTrace does not have such limitations.
- Complex matching logic with normalization of observables.
- Kaspersky CyberTrace allows searching for IoCs in large sets of logs or to review historical data.

Due to a unique integration approach with SIEM solutions, Kaspersky CyberTrace helps to detect uncovered threats, measures which streams of threat intelligence are the most relevant, and provides Security Operations Center with a powerful tool for alerts triage:

- Dashboard with statistical data about detections and a breakdown of Threat Intelligence sources, taking into account false positives to highlight the best sources.
- Native integration of Kaspersky Threat Intelligence.
- Historical correlation (retrospective scan) for finding previously uncovered threats.
- Downloading feeds to a storage on a separate computer.
- Kaspersky Threat Feed App for QRadar that displays dashboards (https://support.kaspersky.com/13854).
AO Kaspersky Lab

Kaspersky is a world-renowned vendor of systems protecting computers against digital threats, including viruses and other malware, unsolicited email (spam), and network and hacking attacks.

In 2008, Kaspersky was rated among the world’s top four leading vendors of information security software solutions for end users (IDC Worldwide Endpoint Security Revenue by Vendor). Kaspersky is the preferred vendor of computer protection systems for home users in Russia (IDC Endpoint Tracker 2014).

Kaspersky was founded in Russia in 1997. It has since grown into an international group of companies with 38 offices in 33 countries. The company employs more than 3,000 skilled professionals.

Products. Kaspersky products provide protection for all systems, from home computers to large corporate networks.

The personal product range includes security applications for desktop, laptop, and tablet computers, smartphones and other mobile devices.

The company offers protection and control solutions and technologies for workstations and mobile devices, virtual machines, file and web servers, mail gateways, and firewalls. The company’s portfolio also features specialized products providing protection against DDoS attacks, protection for industrial control systems, and prevention of financial fraud. Used in conjunction with centralized management tools, these solutions ensure effective automated protection for companies and organizations of any size against computer threats. Kaspersky products are certified by major test laboratories, compatible with software from diverse vendors, and optimized to run on many hardware platforms.

Kaspersky virus analysts work around the clock. Every day they uncover hundreds of thousands of new computer threats, create tools to detect and disinfect them, and include their signatures in databases used by Kaspersky applications.

Technologies. Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky. It is no coincidence that many other developers use the Kaspersky Anti-Virus engine in their products, including: Alcatel-Lucent, Alt-N, Asus, BAE Systems, Blue Coat, Check Point, Cisco Meraki, Clearswift, D-Link, Facebook, General Dynamics, H3C, Juniper Networks, Lenovo, Microsoft, NETGEAR, Openwave Messaging, Parallels, Qualcomm, Samsung, Stormshield, Toshiba, Trustwave, Vertu, and ZyXEL. Many of the company’s innovative technologies are patented.

Achievements. Over the years, Kaspersky has won hundreds of awards for its services in combating computer threats. Following tests and research conducted by the reputed Austrian test laboratory AV-Comparatives in 2014, Kaspersky ranked among the top two vendors by the number of Advanced+ certificates earned and was ultimately awarded the Top Rated certificate. But Kaspersky’s main achievement is the loyalty of its users worldwide. The company’s products and technologies protect more than 400 million users, and its corporate clients number more than 270,000.

Kaspersky website: https://www.kaspersky.com
Virus encyclopedia: https://securelist.com
Kaspersky VirusDesk: https://virusdesk.kaspersky.com (for analyzing suspicious files and websites)
Kaspersky Community: https://community.kaspersky.com
Information about third-party code

Information about third-party code is contained in a file named legal_notices.txt of the distribution kit.
Trademark notices

Registered trademarks and service marks are the property of their respective owners.

Android and Google are trademarks of Google, Inc.

Apple and iPhone are trademarks of Apple Inc., registered in the U.S. and other countries.

IBM, ibm.com, and QRadar are trademarks of International Business Machines Corporation, registered in many jurisdictions worldwide.

Linux is the registered trademark of Linus Torvalds in the U.S. and other countries.

Microsoft, Windows, Windows Server are registered trademarks of Microsoft Corporation in the United States and other countries.

Python is a trademark or registered trademark of the Python Software Foundation.

Tor is a trademark of The Tor Project, U.S. Registration No. 3,465,432.