Kaspersky Threat Feed App for MISP

Product version: 1.0
Dear User,

Thank you for choosing Kaspersky Lab 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 Lab). 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 Lab.

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

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

Kaspersky Lab 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: 27.07.2018

© 2018 AO Kaspersky Lab. All Rights Reserved.

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

About this document ........................................................................................................................................ 4

About MISP ...................................................................................................................................................... 5

About Kaspersky Threat Feed App for MISP ................................................................................................. 6
  Distribution kit ........................................................................................................................................... 6
  Hardware and software requirements .......................................................................................................... 7
  Feeds from Kaspersky Lab .......................................................................................................................... 8

Using Kaspersky Threat Feed App for MISP ................................................................................................. 10
  Installing Kaspersky Threat Feed App for MISP ...................................................................................... 10
  Configuring Kaspersky Threat Feed App for MISP .................................................................................. 11
  Removing Kaspersky Threat Feed App for MISP ..................................................................................... 13
  Command-line options ............................................................................................................................... 13
  Kaspersky Threat Feed App for MISP features ....................................................................................... 15

AO Kaspersky Lab ........................................................................................................................................... 17

Trademark notices .......................................................................................................................................... 19
About this document

This document describes Kaspersky Threat Feed App for MISP, a utility developed by Kaspersky Lab that imports Kaspersky Threat Data Feeds to a Malware Information Sharing Platform (MISP) instance.
About MISP

Malware Information Sharing Platform (MISP) is an open-source software solution for collecting, storing, distributing, sharing, and correlating Indicators of Compromise. There can be Indicators of Compromise of targeted attacks, threat intelligence, financial fraud information, vulnerability information, or even counter-terrorism information. The objective of MISP is to foster the sharing of structured information within the security community and abroad. MISP provides functionalities to support exchange of information but also consumption of the information by Intrusion Detection Systems (IDS), log analysis tools, and SIEM software.

The MISP features include the following:

- Importing indicators from MISP, STIX™, OpenIOC, text, and CSV data
- Automatic information sharing about threats among various participants
- Automatic generating rules for IDS Bro, Snort®, and Suricata, and for various SIEM software programs

MISP includes many Python® modules for integration with various software programs:

- Expansion modules—Modules that enrich events with some data.

  Expansion modules can be of two types:

  - Hover type
    
    Modules that display enriched events without modifying the events.
  
  - Expansion type
    
    Modules that modify events by enriching them with data and displaying the result.

- Import modules—Modules that import indicators to MISP.

- Export modules—Modules that export data from MISP (for example, to SIEM software).
About Kaspersky Threat Feed App for MISP

Kaspersky Threat Feed App for MISP imports and updates Kaspersky Threat Data Feeds in a MISP instance. Every feed is imported as a MISP event. Indicators from the feeds are added to events as attributes. The supported feeds are described in section "Feeds from Kaspersky Lab (on page 8)".

In this chapter

| Distribution kit | ................................................................. 6 |
| Hardware and software requirements | ........................................................................... 7 |
| Feeds from Kaspersky Lab | ........................................................................... 8 |

Distribution kit

Kaspersky Threat Feed App for MISP is shipped as an archive named Kaspersky_Threat_Feed_App_for_MISP.tar.gz. The contents of the archive are described in the following table.

<table>
<thead>
<tr>
<th>Item</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>feed_util/*</td>
<td>Directory that contains Kaspersky Feed Utility.</td>
</tr>
<tr>
<td>import_to_misp.py</td>
<td>Script that imports feeds to a MISP instance.</td>
</tr>
<tr>
<td>Kaspersky Threat Feed App for MISP.pdf</td>
<td>Kaspersky Threat Feed App for MISP documentation.</td>
</tr>
<tr>
<td>Item</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------------</td>
<td>--------------------------------------------------</td>
</tr>
<tr>
<td>kl_feeds_converter.py</td>
<td>Service file for the importing utility.</td>
</tr>
<tr>
<td>legal_notices.txt</td>
<td>Legal notices for the product.</td>
</tr>
<tr>
<td>license.txt</td>
<td>End User License Agreement (EULA).</td>
</tr>
<tr>
<td>misp_api.py</td>
<td>Service file for the importing utility.</td>
</tr>
<tr>
<td>process_feed.py</td>
<td>Service file for the importing utility.</td>
</tr>
<tr>
<td>rollback.py</td>
<td>Service file for the script run.py.</td>
</tr>
<tr>
<td>run.py</td>
<td>Script that runs successively Feed Utility and the importing script.</td>
</tr>
<tr>
<td>settings.py</td>
<td>Script with settings for the script run.py.</td>
</tr>
<tr>
<td>utils.py</td>
<td>Service file for the importing utility.</td>
</tr>
</tbody>
</table>

**Hardware and software requirements**

Kaspersky Threat Feed App for MISP has the following system requirements.

**Supported operating systems**

Kaspersky Threat Feed App for MISP can run on Linux® x64.

**Software requirements**

Kaspersky Threat Feed App for MISP requires Python 3.

**RAM requirements**

Kaspersky Threat Feed App for MISP uses up to 2 gigabytes (GB) of RAM when importing feeds to MISP. RAM requirements of Kaspersky Feed Utility are described in the Kaspersky Feed Utility documentation placed in the `%utility_dir%/feed_util/doc` directory.
Feeds from Kaspersky Lab

This section describes Kaspersky Threat Data Feeds that can be imported to a MISP instance.

The following feeds are available:

- **Malicious URL Exact Data Feed**—A set of exact URLs and FQDNs with context that refer to malicious websites and web pages.

- **Phishing URL Exact Data Feed**—A set of exact URLs and FQDNs with context that refer to phishing websites and web pages.

- **Botnet CnC URL Exact Data Feed**—A set of exact URLs, exact FQDNs, and hashes with context that refer to desktop botnet C&C servers and related malicious objects.

- **Malicious Hash Data Feed**—A set of file hashes with corresponding context covering the most dangerous, prevalent, or emerging malware.

- **Mobile Malicious Hash Data Feed**—A set of file hashes with corresponding context for detecting malicious objects that infect mobile Google Android and Apple iPhone devices.

- **P-SMS Trojan Data Feed**—A set of Trojan hashes with corresponding context for detecting SMS Trojans that send premium-rate SMS messages to mobile users as well as enable attackers to steal, delete, and respond to SMS messages.

- **IP Reputation Data Feed**—A set of IP addresses with context covering spam hosts, malicious hosts, phishing hosts, Tor exit nodes, proxies, and botnet C&C servers.

- **Mobile Botnet Data Feed**—A set of URLs and hashes with context covering mobile botnet C&C servers.

- **Ransomware URL Feed**—A set of URLs with corresponding context for detecting links and websites that host ransomware.
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**
  
  This is a demo version of Botnet CnC URL Data Feed.

- **Demo Malicious Hash Data Feed**
  
  This is a demo version of Malicious Hash Data Feed.

- **Demo IP Reputation Data Feed**
  
  This is a demo version of IP Reputation Data Feed.
Using Kaspersky Threat Feed App for MISP

This section describes how to use Kaspersky Threat Feed App for MISP.

In this chapter

- Installing Kaspersky Threat Feed App for MISP .......................................................... 10
- Configuring Kaspersky Threat Feed App for MISP ......................................................... 11
- Removing Kaspersky Threat Feed App for MISP ............................................................. 13
- Command-line options ........................................................................................................ 13
- Kaspersky Threat Feed App for MISP features ................................................................ 15

Installing Kaspersky Threat Feed App for MISP

This section describes how to install Kaspersky Threat Feed App for MISP.

► To install Kaspersky Threat Feed App for MISP:

1. Add the following Python modules to the Python installation (if they were not yet added):
   - pymisp
   - ijson
   - psutil

2. Create a directory for the files of Kaspersky Threat Feed App for MISP.

   Hereinafter, this directory is referred to as %utility_dir%. 
3. Unpack the distribution archive.

4. Configure Kaspersky Threat Feed App for MISP (see Section "Configuring Kaspersky Threat Feed App for MISP" on page 11).

5. Add the following line to the crontab file:

```
0 0 * * * %utility_dir%/run.py
```

Subsequently, the master script run.py will be run regularly (every 24 hours): Feed Utility will download the feeds from the Kaspersky Lab servers and then the importing script import_to_misp.py will import the feeds to a MISP instance.

---

## Configuring Kaspersky Threat Feed App for MISP

You can configure or reconfigure Kaspersky Threat Feed App for MISP mainly by editing the settings script file settings.py.

*To configure Kaspersky Threat Feed App for MISP:*

1. In the settings script file settings.py, specify the following parameters:

   - **MISP_URL**
     
     This is the URL where the MISP instance is available.

   - **MISP_TOKEN**
     
     This is the key for using the MISP instance.

   - **RECORDS_COUNT**
     
     This setting specifies the maximum number of attributes that a MISP event will contain after a feed is imported to a MISP instance. It must be a non-negative integer (0 means no limit).

2. In the settings script file settings.py, uncomment the lines containing the names of the feeds that you will import to a MISP instance.
3. Copy the certificate for getting feeds to the same directory where the Feed Utility binary file resides and rename it to feeds.pem.

4. If you are going to use a proxy server to gain access to Kaspersky Lab servers to download feeds, from the Feed Utility directory run the following command once:

   `kl_feed_util --set-proxy %PROXY% -c template.conf`

   Here `%PROXY%` is the setting that specifies the proxy server parameters for gaining access to the Kaspersky Lab servers.

**Recommendations on the number of attributes kept in a MISP event**

Updating the full set of Kaspersky Threat Data Feeds in a MISP instance can take a significant amount of time. You can decrease this time by specifying the maximum number of attributes to keep in a MISP event (the `RECORDS_COUNT` parameter in the settings.py file). We recommend that you set the maximum number of attributes to 200,000 (this value is initially set in the settings.py file).

In the table below, the measurement data is provided that indicates the influence of the maximum number of attributes in a MISP event on the import time. This measurement data is got when all feeds were imported on our computers. Real data depends on the software and hardware that you use, on the period between subsequent running of the importing script, and on the feeds you import to a MISP instance.
## Table 2. Import time depending on the maximum number of attributes

<table>
<thead>
<tr>
<th>Maximum number of attributes</th>
<th>Time of the first import, hours</th>
<th>Time of a regular import, hours</th>
</tr>
</thead>
<tbody>
<tr>
<td>50,000</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>200,000</td>
<td>13</td>
<td>4</td>
</tr>
<tr>
<td>500,000</td>
<td>24</td>
<td>8</td>
</tr>
</tbody>
</table>

### Removing Kaspersky Threat Feed App for MISP

This section describes how to remove Kaspersky Threat Feed App for MISP.

**To remove Kaspersky Threat Feed App for MISP:**

1. From the crontab file, remove the line that corresponds to running the master script file run.py.

2. Wait until Kaspersky Threat Feed App for MISP finishes operating or stop execution of its process manually.

3. Remove the `%utility_dir%` directory and its contents.

### Command-line options

Kaspersky Threat Feed App for MISP is designed in such a way that the user periodically runs the master script file run.py. However you can run the importing script import_to_misp.py instead of this. The import_to_misp.py script runs from the command line as follows:

```
%utility_dir%/import_to_misp.py --misp_url <MISP_URL> --auth_key <MISP_authorization_key> --proxy <proxy_to_MISP> --feed_file <feed> --deleted_file <file_with_deleted_records> --added_file <file_with_added_records> --work_dir <working_directory>
```
The following table contains the description of the command-line parameters.

Table 3. Parameters of the importing script

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>misp_url</strong></td>
<td>URL at which the MISP instance is available.</td>
</tr>
<tr>
<td></td>
<td>The <code>misp_url</code> parameter is mandatory.</td>
</tr>
<tr>
<td><strong>auth_key</strong></td>
<td>Key for gaining access to the MISP instance.</td>
</tr>
<tr>
<td></td>
<td>The <code>auth_key</code> parameter is mandatory.</td>
</tr>
<tr>
<td><strong>proxy</strong></td>
<td>Proxy settings in the <code>http://username:password@address:port</code> format. This is the proxy server for gaining access to the MISP instance.</td>
</tr>
<tr>
<td></td>
<td>The <code>proxy</code> parameter is optional. If the parameter is not specified, no proxy server is used.</td>
</tr>
<tr>
<td><strong>feed_file</strong></td>
<td>Path to the feed file to be initially imported. It can be an absolute or relative path. A relative path is calculated relative to the</td>
</tr>
<tr>
<td></td>
<td>import_to_misp.py file. Only local paths are supported; SMB, FTP, or HTTP paths are not supported.</td>
</tr>
<tr>
<td></td>
<td>The <code>feed_file</code> parameter must be specified if the <code>deleted_file</code> and <code>added_file</code> parameters are not specified. Otherwise, it must not be specified.</td>
</tr>
<tr>
<td><strong>deleted_file</strong></td>
<td>Path to the diff feed file that contains deleted records. It can be an absolute or relative path. A relative path is calculated relative to the</td>
</tr>
<tr>
<td></td>
<td>import_to_misp.py file. Only local paths are supported; SMB, FTP, or HTTP paths are not supported.</td>
</tr>
<tr>
<td></td>
<td>The <code>deleted_file</code> parameter must be specified if the <code>added_file</code> parameter is specified. Otherwise, it must not be specified.</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
</tr>
<tr>
<td>-----------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>added_file</td>
<td>Path to the diff file that contains added records. It can be an absolute or relative path. A relative path is calculated relative to the __init_.py file. Only local paths are supported; SMB, FTP, or HTTP paths are not supported. The <code>added_file</code> parameter must be specified if the <code>deleted_file</code> parameter is specified. Otherwise, it must not be specified.</td>
</tr>
<tr>
<td>work_dir</td>
<td>Path to the working directory. It can be an absolute or relative path. A relative path is calculated relative to the __init_.py file. Only local paths are supported; SMB, FTP, or HTTP paths are not supported. Do not specify the directory containing the feed file (see the description of the <code>feed_file</code> parameter) in the <code>work_dir</code> parameter so that the feed file will not be overwritten with a temporary file. The <code>work_dir</code> parameter is mandatory.</td>
</tr>
<tr>
<td>attributes_limit</td>
<td>Maximum number of attributes that a MISP event will contain. It must be a non-negative integer (0 means no limit). Section &quot;Configuring Kaspersky Threat Feed App for MISP (on page 11)&quot; contains recommendations on choosing the value of the <code>attributes_limit</code> parameter (by choosing the value of the <code>RECORDS_COUNT</code> parameter in the settings.py script). The <code>attributes_limit</code> parameter is optional. If it is not specified, no limit for the number of attributes is set.</td>
</tr>
</tbody>
</table>

**Kaspersky Threat Feed App for MISP features**

If Kaspersky Threat Feed App for MISP is stopped during its work (for example, its process is not executed or the operating system is restarted), it resumes work after you run the master script.
run.py. If work does not resume, contact a Kaspersky Lab representative. Alternatively, remove the imported events from the MISP instance, remove the contents of the workdir and feed_util/feeds directories, and remove the tool.pid file from the directory in which Kaspersky Threat Feed App for MISP is installed. Then run the master script run.py; the importing process will be performed from scratch.

The master script run.py and the importing script import_to_misp.py log their activities to stdout. We recommend that you save the printed messages to a file so that you can track the work performed by Kaspersky Threat Feed App for MISP.

Due to MISP restrictions, the MISP events that contain a large amount of attributes (more than 50,000) can be opened very slowly in the user interface or cannot be opened at all. This happens because MISP tries to get all attributes from a database and load the correlations between the attributes to memory. To get rid of these errors, we recommend that you increase the memory usage for the MISP instance. To do this, perform the following actions on the MISP computer:

1. Open the /etc/php/7.1/apache2/php.ini file for editing (the path may be different depending on the PHP version installed):

   vi /etc/php/7.1/apache2/php.ini

2. Specify the memory_limit parameter:

   memory_limit = 5G

3. Restart Apache:

   sudo systemctl restart apache2
Kaspersky Lab 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 Lab 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 Lab is the preferred vendor of computer protection systems for home users in Russia (IDC Endpoint Tracker 2014).

Kaspersky Lab 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 Lab 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 Lab products are certified by major test laboratories, compatible with software from diverse vendors, and optimized to run on many hardware platforms.

Kaspersky Lab 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 Lab applications.

**Technologies.** Many technologies that are now part and parcel of modern anti-virus tools were originally developed by Kaspersky Lab. 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 Lab 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 Lab ranked among the top two vendors by the number of Advanced+ certificates earned and was ultimately awarded the Top Rated certificate. But Kaspersky Lab’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 Lab website: https://www.kaspersky.com
Virus encyclopedia: https://securelist.com
Virus Lab: https://virusdesk.kaspersky.com (for analyzing suspicious files and websites)
Kaspersky Lab’s web forum: https://forum.kaspersky.com
Trademark notices

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

Apache and the Apache feather logo are trademarks of The Apache Software Foundation.

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

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

Snort is a registered trademark or trademark of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.