KASPERSKY lab

How to import Kaspersky Threat Data Feeds to AlienVault OTX

Document version: 1.0

Dear User,

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

Document revision date: 03.10.2017

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

How to import Kaspersky Threat Data Feeds to AlienVault OTX

This document describes how to import Kaspersky Threat Data Feeds to AlienVault OTX.

In this chapter

Kaspersky Threat Data Feeds fit for AlienVault OTX

The following Kaspersky Threat Data Feeds can be easily integrated with AlienVault OTX:

- Malicious URL Data Feed
- Malicious Hash Data Feed
- IP Reputation Data Feed
- Phishing URL Data Feed
- Botnet C&C URL Data Feed

- Mobile Malicious Hash Data Feed
- Mobile Botnet Data Feed
- P-SMS Trojan Data Feed

For more information about Kaspersky Threat Data Feeds, see section "Data feeds from Kaspersky Lab (on page 4)".

Data feeds from Kaspersky Lab

This section describes Kaspersky Threat Data Feeds.

The following data feeds are available:

- Malicious URL Data Feed—A set of URLs with context covering malicious websites and web pages. Masked and non-masked records are available.

  This feed is updated every 10 minutes.

- Phishing URL Data Feed—A set of URLs with context covering phishing websites and web pages. Masked and non-masked records are available.

  This feed is updated every 10 minutes.

- Botnet CnC URL Data Feed—A set of URLs and hashes with context covering desktop botnet C&C servers and related malicious objects.

  This feed is updated once every hour.

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

  This feed is updated every 20 minutes.

- 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.

  This feed is updated every 20 minutes.

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

  This feed is updated every eight hours.

- IP Reputation Data Feed—A set of IP addresses with context covering malicious hosts.

  This feed is updated every 10 minutes.

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

  This feed is updated every eight hours.

Demo (free) data feeds are also available. Demo feeds provide lower detection rate in comparison with their corresponding commercial versions. The following demo data 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.

The demo data feeds are updated every 24 hours.

All records in the feeds are sorted in descending order of popularity.

Fields from Kaspersky Threat Data Feeds that can be ingested by AlienVault OTX

The following fields from Kaspersky Threat Data Feeds can be ingested by AlienVault OTX:

- Malicious URL Data Feed

Field	Indicator type in AlienVault OTX
mask	domain hostname URL
MD5	FileHash-MD5
SHA1	FileHash-SHA1
SHA256	FileHash-SHA256

- Malicious Hash Data Feed

Field	Indicator type in AlienVault OTX
MD5	FileHash-MD5
SHA1	FileHash-SHA1
SHA256	FileHash-SHA256

- IP Reputation Data Feed

Field	Indicator type in AlienVault OTX
ip	IPv4

- Phishing URL Data Feed

Field	Indicator type in AlienVault OTX
mask	domain hostname URL

- Botnet C&C URL Data Feed

Field	Indicator type in AlienVault OTX
mask	domain hostname URL
MD5	FileHash-MD5
SHA1	FileHash-SHA1
SHA256	FileHash-SHA256

- Mobile Malicious Hash Data Feed

Field	Indicator type in AlienVault OTX
MD5	FileHash-MD5
SHA1	FileHash-SHA1
SHA256	FileHash-SHA256

- Mobile Botnet Data Feed

Field	Indicator type in AlienVault OTX
MD5	FileHash-MD5
mask	URL

- P-SMS Trojan Data Feed

Field	Indicator type in AlienVault OTX
MD5	FileHash-MD5

Integration of URL masks from Kaspersky Threat Data Feed to AlienVault OTX

When you integrate the URL masks from Kaspersky Threat Data Feeds to AlienVault OTX, transform them according to the table below.

Mask type	Type in AlienVault OTX	Transformation method
1	domain	As is
2	hostname	As is
3	URL	As is
4	URL	As is
19	hostname	Symbols `*.` are removed from the masks
20	URL	Symbols `/*` are removed from the masks

Mask type	Type in AlienVault OTX	Transformation method
21	URL	Asterisks (*) are removed from the masks
22	-	Ignored

The masks in Kaspersky Threat Data Feeds can contain space symbols. It is not necessary to replace space symbols with symbols `%20` before loading the masks in AlienVault OTX. However we recommend that you normalize masks and replace space symbols with symbols `%20` if the users will use AlienVault OTX for automatic checking of indicators (for example, by using AlienVault USM).

Downloading Kaspersky Threat Data Feeds

To download Kaspersky Threat Data Feeds, use Feed Utility. This utility has the following features:

- Downloading data feeds
- Creating DIFF files
- Filtering feed records
- Converting data feeds to JSON, STIX, CSV, or OpenIoC format
- Reducing the size of data feeds by specifying the maximum number of indicators stored in them

To get more information about Feed Utility, refer to the Feed Utility documentation.

Feed Utility requires a Kaspersky Lab certificate. To order the certificate and the Feed Utility distribution kit, send a request to intelligence@kaspersky.com mailto:intelligence@kaspersky.com.

Loading indicators from Kaspersky Threat Data Feeds to AlienVault OTX

You can load indicators from Kaspersky Threat Data Feeds to AlienVault OTX either by using the web interface, or by using the RESTful API of AlienVault.

When downloading a feed, you will get its full version. So you will have to completely remove from AlienVault the indicators of the data feed you are going to update and load the indicators from the downloaded feed. In this case it is guaranteed you use the latest version of the data feed.

Alternatively, you can set the expiry time for every imported indicator by using the RESTful API of AlienVault: we recommend that you set it to one hour beyond the time of the upcoming update of the feed. When loading a new set of indicators, check whether the indicators already exist. For every existing indicator, merely update its expiry time.

Use the procedure provided below for every feed you want to update.

► *To load indicators from a data feed to AlienVault OTX:*

1. By using Feed Utility, convert the data feed to CSV format. When converting, select only those indicators that are mentioned in section "Fields from Kaspersky Threat Data Feeds that can be ingested by AlienVault OTX (on page 6)".

   A CSV file will be created that contains from one to four columns.

2. In the CSV file, process the values in the `mask` column as specified in section "Integration of URL masks from Kaspersky Threat Data Feed to AlienVault OTX (on page 8)".

3. In AlienVault OTX, select the **Create Pulse** tab.

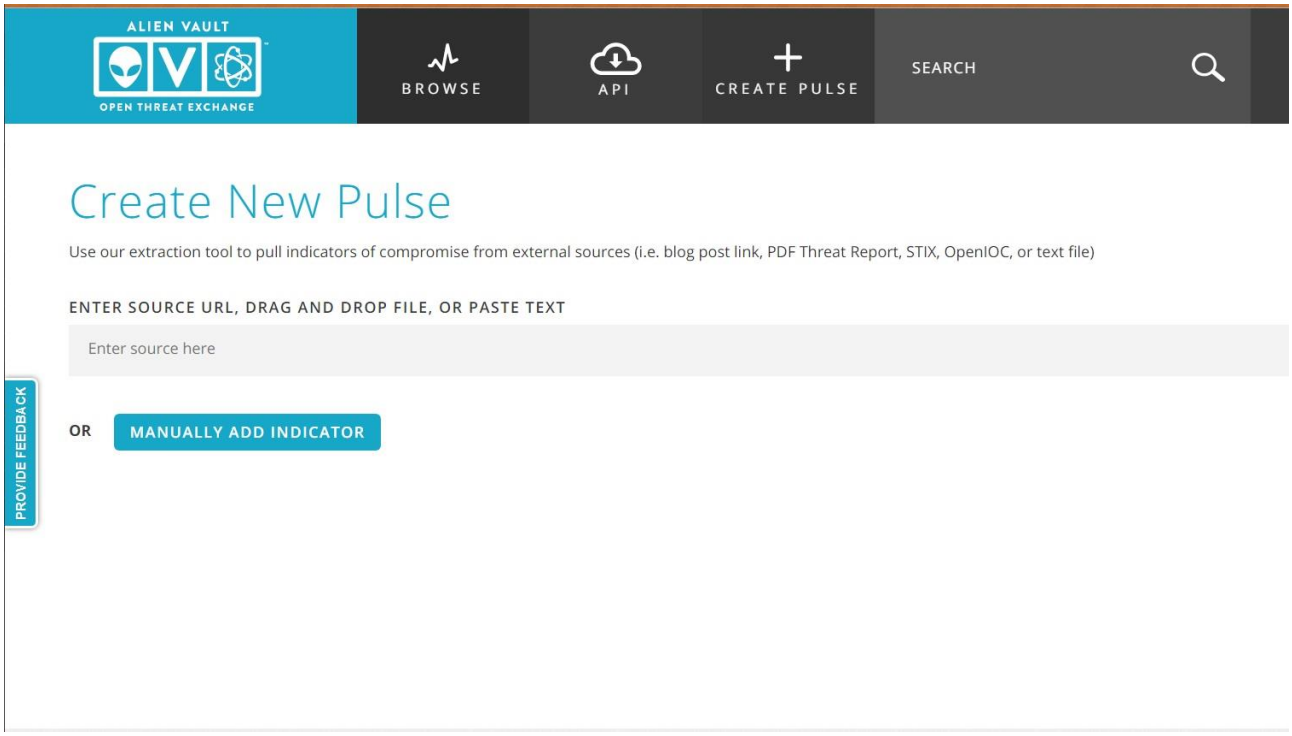

Figure 1. Create Pulse tab

4. Drag the converted CSV file, that you are going to load to AlienVault OTX, to the **Enter Source** box.

   In the figure below, the IP_Reputation_Data_Feed.csv file is loaded.

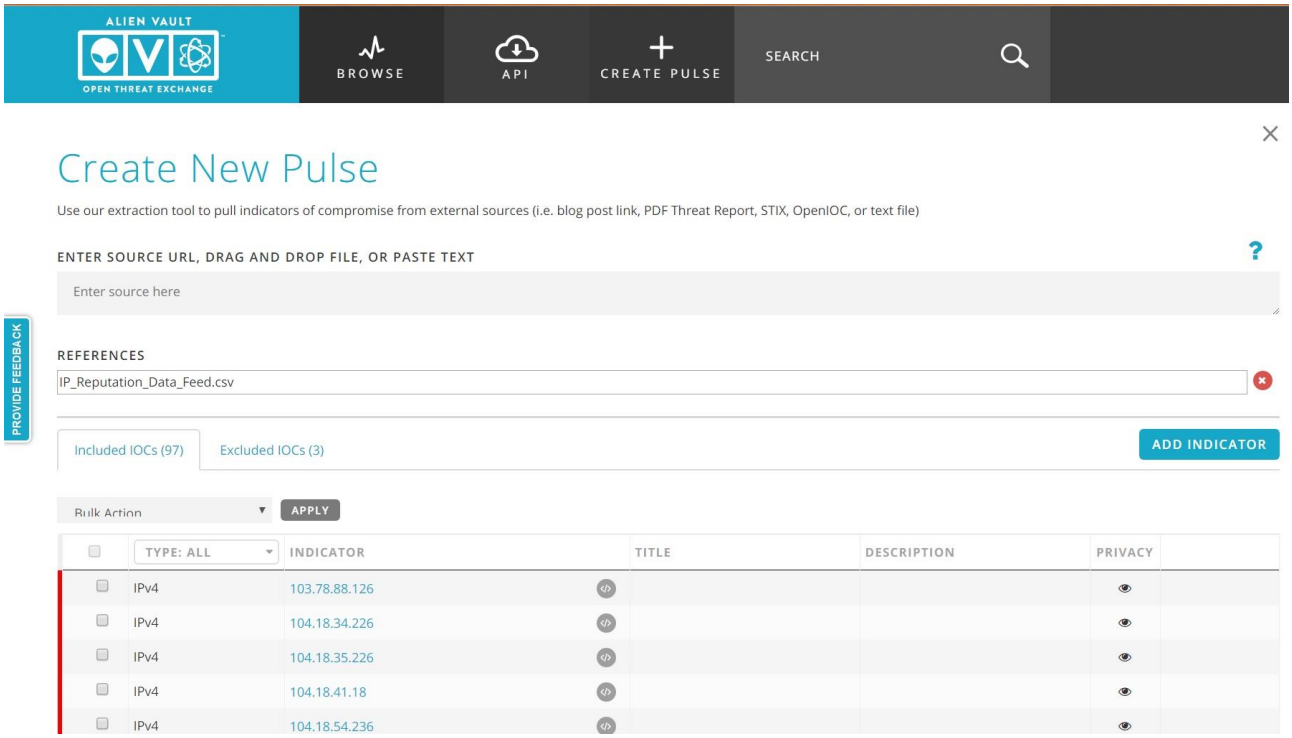

Figure 2. Feed loaded

5. Select the **Excluded IOCs** tab.

   This tab displays indicators that are for some reason excluded from loading to AlienVault OTX. We recommend that you include these indicators also if there is no reason in filtering them out. To do this, select the check boxes of the excluded indicators, select `Include Indicators` in the drop-down box, and click **Apply**.

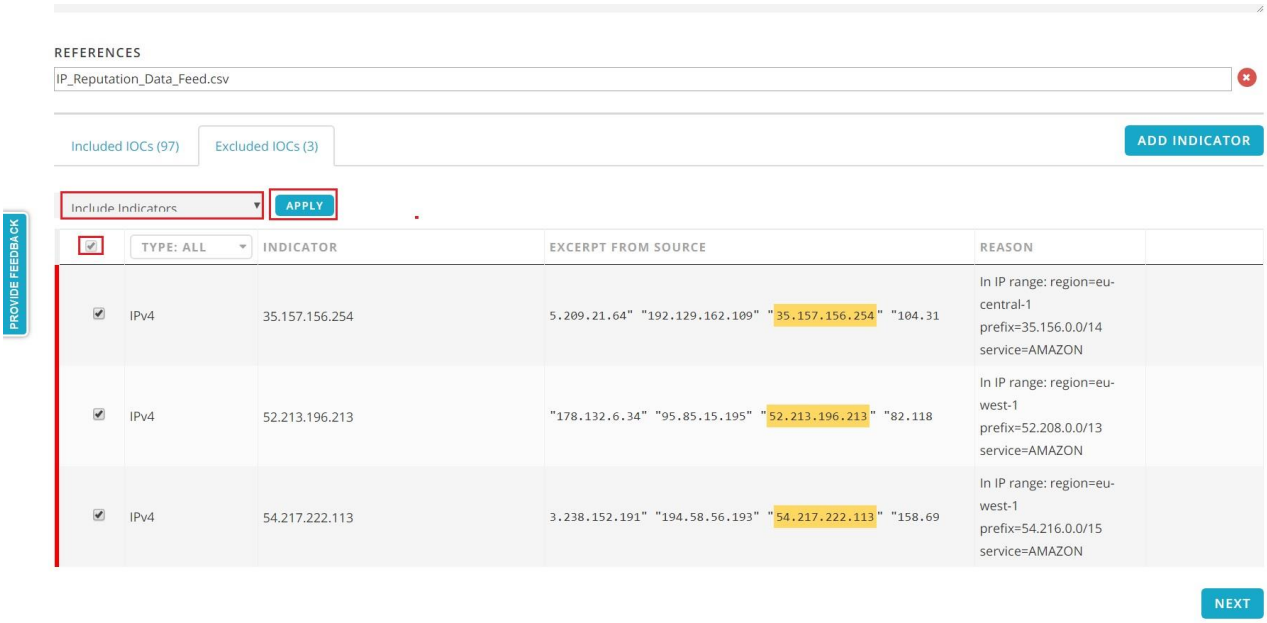

Figure 3. Excluded indicators

6. Click **Next**.

7. Specify the pulse settings.

   In the **Name** box, specify the pulse name. Select `Red` in the **TLP** box and select **Private**. Set other settings as you wish: for example, we recommend that you add a `Kaspersky` tag.

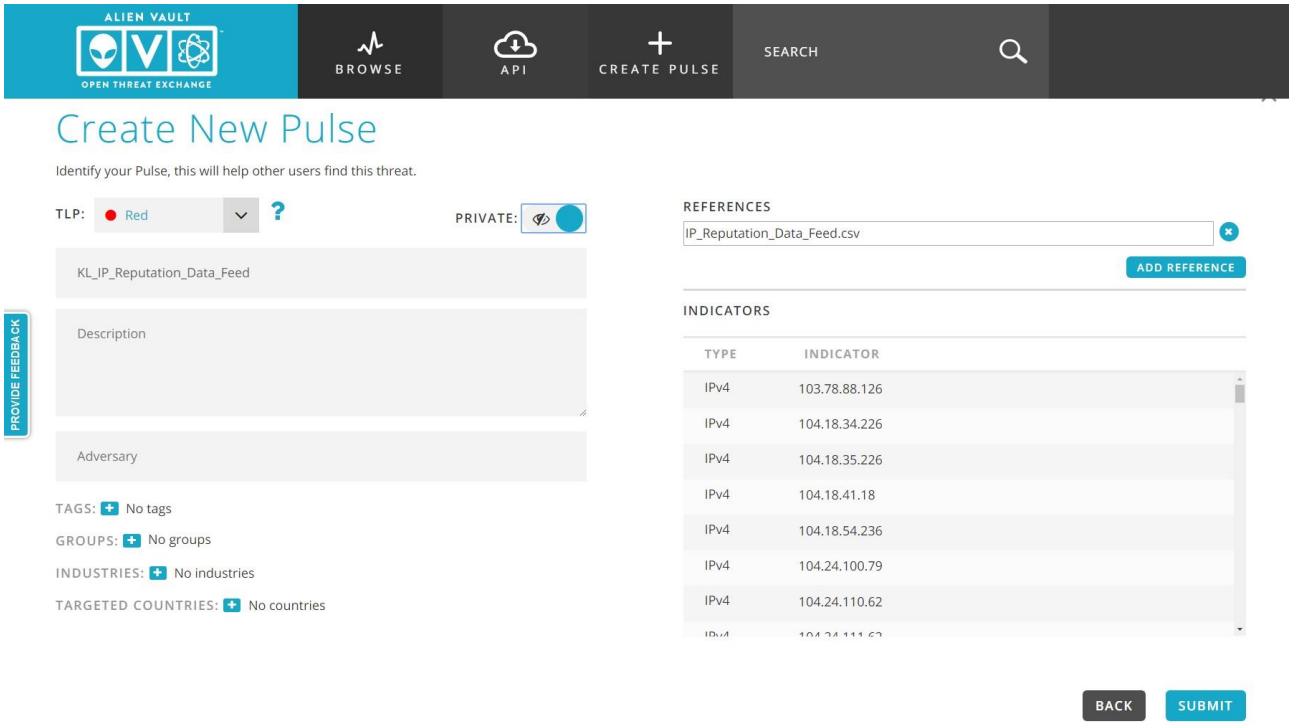

Figure 4. Pulse settings

8. Click **Submit**.

   The properties of the loaded pulse will be displayed.

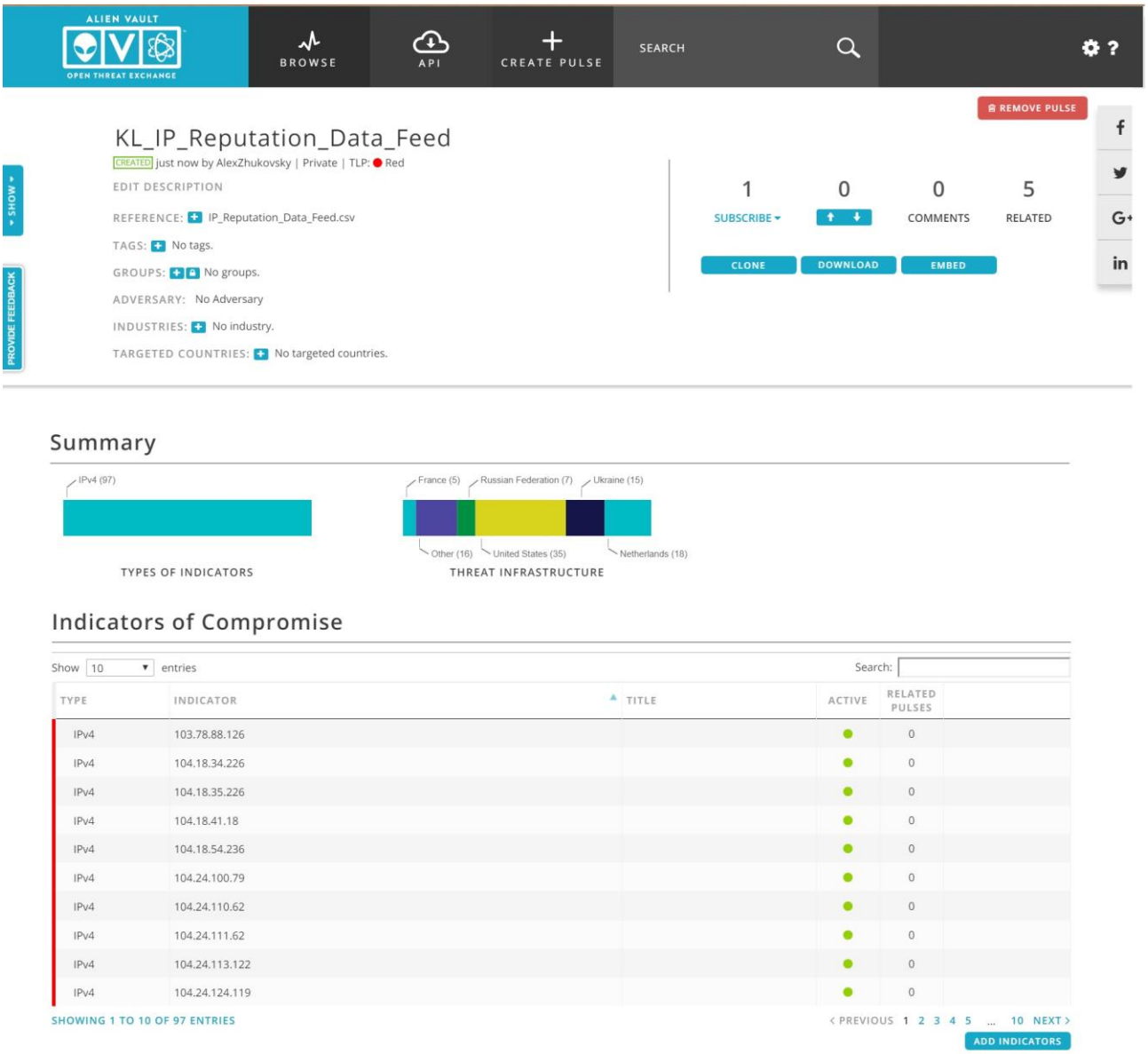

Figure 5. Pulse properties

You can make this procedure automatic by using the RESTful API of AlienVault.

AO Kaspersky Lab

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