THREAT DATA FEEDS

www.kaspersky.com

THREAT DATA FEEDS

Kaspersky security intelligence. Threat data feeds description. Version: v1.0

EXECUTIVE SUMMARY

Malware families and variations have grown exponentially in recent years. Kaspersky Lab currently detects about 325,000 unique malware samples daily, and these malicious samples are growing in complexity as well as in volume.

To protect their IT-infrastructure from all these new threats, most enterprises already deploy protection measures including anti-malware solutions, intrusion prevention and threat detection systems. Kaspersky Lab Intelligence Data Feeds have a crucial role in a comprehensive multi-layered defense strategy, continuously providing essential security information to in-house SIEM (Security Information and Event Management) systems.

This service is designed for use by any enterprise organization planning to control the presence of malware at infrastructure level leveraging existing SIEM solution via integration with KL Threat Data Feeds. Using superior global intelligence, security operation centers are armed to combat the latest cybercrime techniques, which are designed to bypass even the most sophisticated protection. Combined with local intelligence data, this global information can help protect the enterprise IT-infrastructure.

Kaspersky Lab's Intelligence Data Feeds are highly flexible and can be provided in different formats, allowing easy integration into different third party cybersecurity solutions, including HP ArcSight, IBM QRadar and Splunk SIEMs.

TARGET AUDIENCE:

- Large enterprises (banks, Telco's, airlines, hotel chains, etc.) and any other organization with deployed SIEM
- MSSPs (Managed Security Services Providers). These organizations can add a value to own Security services leveraging Intelligence gained from KL Threat Data Feeds
- Law enforcement agencies (LEA)

CUSTOMER BENEFITS

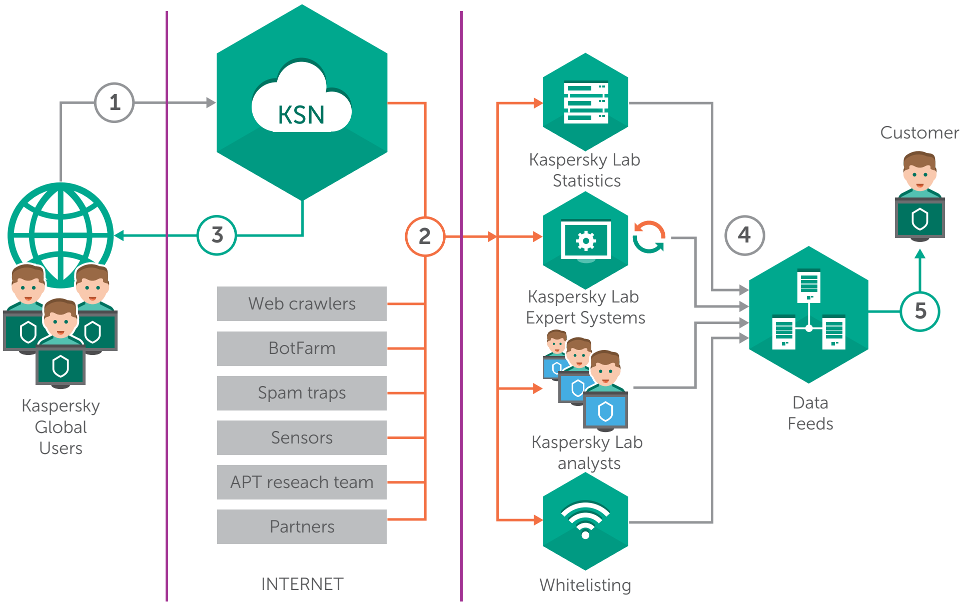
Intelligence Feed databases are updated regularly with the latest findings from the Kaspersky Security Network. In its turn, this global cloud database is fed in real time by data from over 80 million participating Kaspersky Lab software users worldwide, as well as the organization's own experts.

Kaspersky Lab's Intelligence Data Feeds give customers an addition level of malware defense. The distribution of malicious objects can be controlled at infrastructure level by comparing data from the log files coming from the SIEM systems with the data from KL Threat Data Feeds. In case of detection, the SIEM admin is notified about this incident that helps additionally prevent malware infection within the organization.

THREAT DATA FEEDS

TECHNICAL DESCRIPTION

THREAT DATA FEEDS: INTELLIGENCE SOURCES



THE DATA THAT INTELLIGENCE DATA FEEDS PROVIDE

Three URL Feeds provide comprehensive information about every URL that the organization should block:

FEED DESCRIPTION
Malicious URLs – a set of URLs covering the most harmful links and websites. Masked and non-masked records are available.
Phishing URLs – a set of URLs identified by Kaspersky Lab as phishing sites. Masked and non-masked records are available.
Botnet C&C URLs – a set of URLs of botnet command and control (C&C) servers and related malicious objects.

Malware Hash Feeds provide all needed data about malicious files, which should not be executed in enterprises' security perimeter:

FEED DESCRIPTION
Malware Hashes ITW (In The Wild) - the set of file hashes (and Kaspersky Lab's verdicts for each object) covering malware encountered by Kaspersky Lab's software users. Hashes of all files that were blocked using local security technologies are given.
Malware Hashes UDS (Urgent Detection System) - can be described as "recently identified malware hashes". The malware samples in this set were detected by Kaspersky Lab's cloud technologies after receiving a request about file reputation from a PC with Kaspersky Lab's software installed.
Android and iOS Malware Hashes - suitable for customers allowing corporate or private (BYOD) smartphones within their security perimeter. This set of file hashes is designed to detect malicious objects aimed at mobile Android and iOS platforms.

THREAT DATA FEEDS

Mobile Threat Feeds provide all needed data to detect SMS Trojans and communications with mobile botnets command servers:

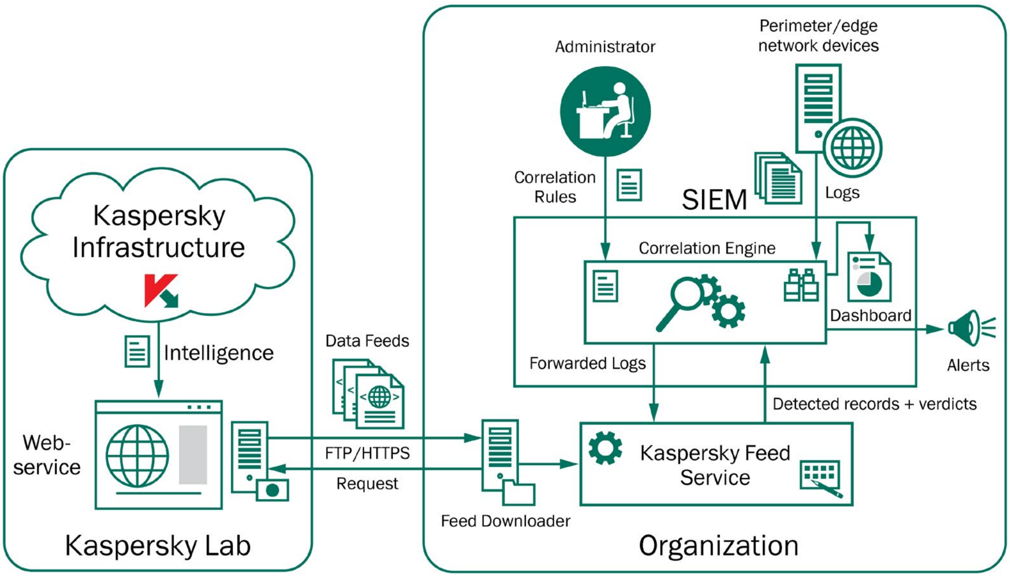
FEED DESCRIPTION
P-SMS Trojan Feed — a set of Trojan hashes with corresponding context for detecting SMS Trojans ringing up premium charges for mobile users as well as enabling an attacker to steal, delete and respond to SMS messages.
Mobile Botnet C&C URLs — a set of URLs with context covering mobile botnet C&C servers.

All this data can be provided as delimited text or JavaScript Object Notation (JSON) with all corresponding information.

INTEGRATION WITH THIRD-PARTY SOLUTIONS

Kaspersky Lab's Intelligence Data Feeds are designed to integrate with third-party SIEM systems including HP ArcSight, IBM QRadar and Splunk. Integration is quite simple, as illustrated below. An alarm is issued to the System administrator if content monitored by the SIEM system, matches data in the malicious URL-feeds.

INTEGRATION WITH SIEM SOLUTIONS



WHY CHOOSE KASPERSKY LAB'S INTELLIGENCE DATA FEEDS

Kaspersky Lab gains comprehensive information about threat landscapes from a multitude of sources right across the globe. Our cloud-based tools monitor millions of cyberthreats worldwide in real time, and we work in partnership with global law enforcement agencies including Interpol and CERTs. Besides automated tools, Antimalware Research (AMR) department and Kaspersky Lab's Global Research & Analysis Team (GReAT) provides a unique analytical insight into the most advanced threats, right across the board, on a daily basis. Gartner, Forrester and IDC identify Kaspersky Lab as a leader in different information security areas.