Kaspersky Threat Data Feeds

First-tier security vendors and enterprises use time-honored and authoritative Kaspersky Threat Data Feeds to **produce premium security solutions or to protect their business**.

Cyber attacks happen every day. Cyber threats are constantly growing in frequency, complexity and obfuscation, as they try to **compromise your defenses**. Adversaries currently use complicated intrusion **kill chains**, campaigns and customized **Tactics, Techniques and Procedures (TTPs) to disrupt your business or damage your clients**.

Kaspersky Lab offers **continuously updated** Threat Data Feeds to **inform your business or clients about risks** and implications associated with cyber threats, helping you to **mitigate threats more effectively** and **defend against attacks** even before they are launched.

Intelligence Cycle

The Data Feeds

Contextual Data

Every record in each Data Feed is enriched with **actionable context** (threat names, timestamps, geolocation, resolved IPs addresses of infected web resources, hashes, popularity etc). Contextual data helps reveal the 'bigger picture', further validating and supporting the wide-ranging use of the data. Set in context, the data can more readily be used to answer the **who, what, where, when questions** which lead to identifying your adversaries, helping you make timely decisions and actions **specific to your organization.**

Feeds comprise sets of:

- **IP Reputation Feed** – a set of IP addresses with context covering suspicious and malicious hosts;
- **Malicious and Phishing URL Feed** – covering malicious and phishing links and websites;
- **Botnet C&C URL Feed** – covering desktop botnet C&C servers and related malicious objects;
- **Mobile Botnet C&C URL Feed** – covering mobile botnet C&C servers. Identify infected machines that communicates with C&Cs;
- **Ransomware URL Feed** – covering links that host ransomware objects or that are accessed by them.
- **APT IoC Feeds** – covering malicious domains, hosts, malicious IP addresses, malicious files used by adversaries to commit APT attacks.
- **Passive DNS (pDNS) Feed** – a set of records that contain the results of DNS resolutions for domains into corresponding IP addresses

Service Highlights

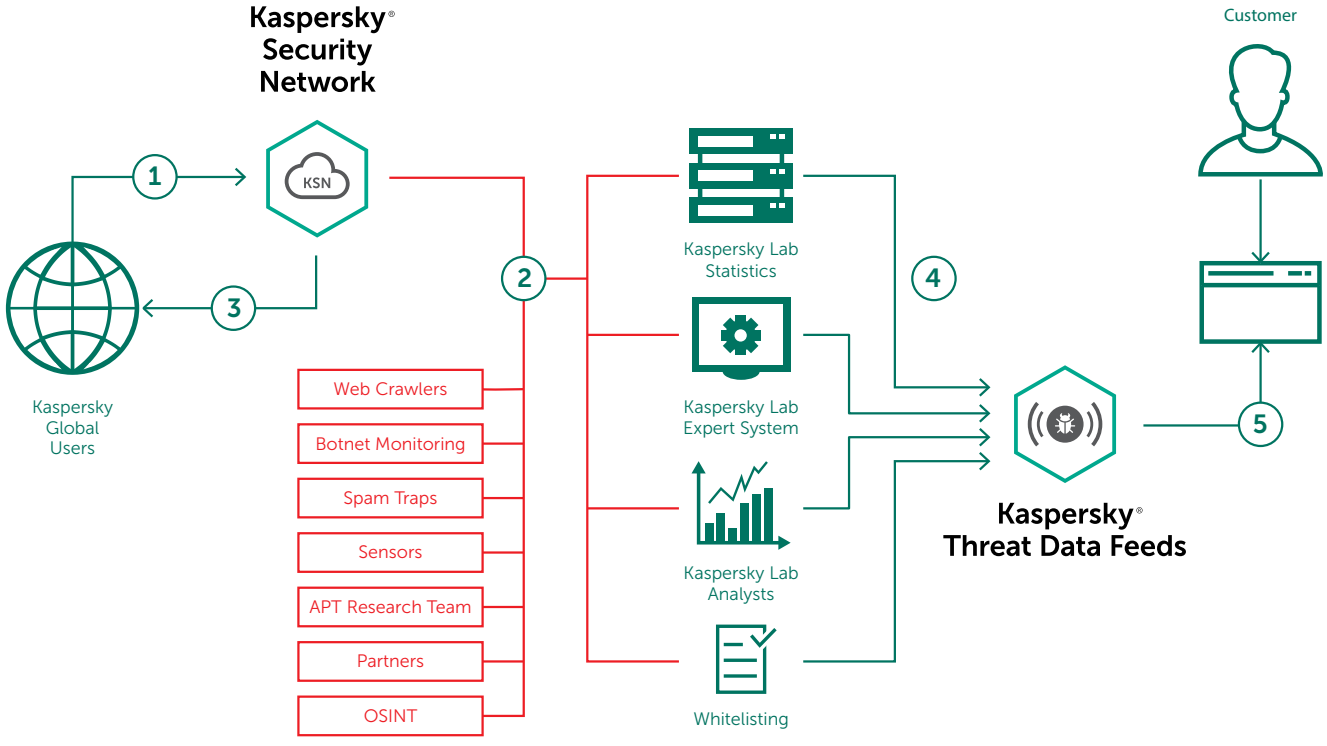
- Data Feeds littered with **False Positives** are valueless, so very extensive tests and filters are applied before releasing feeds, to ensure that 100% vetted data is delivered;
- Data Feeds are automatically generated in real time, based on findings across the globe (Kaspersky Security Network provides visibility to a significant percentage of all internet traffic, covering tens of millions of end-users in more than 213 countries) providing high **detection rates** and accuracy;
- All feeds are generated and monitored by a highly fault-tolerant infrastructure, ensuring **continuous availability**;
- The Data Feeds allow **immediate detection of URLs** used to host phishing, malware, exploits, botnet C&C URLs and other malicious content;
- **Malware** in all types of traffic (web, email, P2P, IM,...) and targeted at mobile platforms can also be **instantly detected** and identified;
- Simple lightweight **dissemination** formats (**JSON, CSV, OpenIoC, STIX**) via **HTTPS** or ad-hoc delivery mechanisms support easy integration of feeds into security solutions;
- Hundreds of experts, including **security analysts** from across the globe, world-famous **security experts from GReAT team and leading-edge R&D teams**, contribute to generating these feeds. Security officers receive critical information and alerts generated from the highest quality data, with no risk of being deluged by superfluous indicators and warnings;
- **Ease of implementation**. Supplementary documentation, samples, a dedicated technical account manager and technical support from Kaspersky Lab all combine to enable straightforward integration.

- **IoT URL Feed** – covering websites that were used to download malware that infects IoT devices
- **Malicious Hash Feed** – covering the most dangerous, prevalent and emerging malware;
- **Mobile Malicious Hash Feed** – supporting the detection of malicious objects that infect mobile Android and iPhone platforms;
- **P-SMS Trojan Feed** – supporting the detection of SMS Trojans enabling attackers to steal, delete and respond to SMS messages, as well as ringing up premium charges for mobile users;
- **Whitelisting Data Feed** – providing third-party solutions and services with a systematic knowledge of legitimate software.
- **Kaspersky Transforms for Maltego** – providing Maltego users with a set of transforms that give access to Kaspersky Lab Threat Data Feeds. Kaspersky Transforms for Maltego allows you to check URLs, hashes, and IP addresses against the feeds from Kaspersky Lab. The transforms can determine the category of an object as well as provide actionable context about it.

Collection and processing

Data Feeds are aggregated from fused, heterogeneous and highly reliable sources, such as Kaspersky Security Network and our own web crawlers, Botnet Monitoring service (24/7/365 monitoring of botnets and their targets and activities), spam traps, research teams and partners.

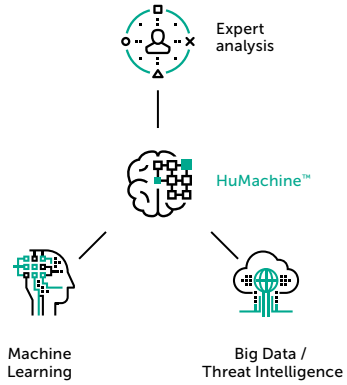
Then, in real-time, all the aggregated data is carefully inspected and refined using multiple preprocessing techniques, such as statistical criteria, Kaspersky Lab Expert Systems (sandboxes, heuristics engines, multi-scanners, similarity tools, behavior profiling etc.), analysts validation and whitelisting verification:



Kaspersky Threat Data Feeds contain thoroughly vetted threat indicator data sourced from the real world in real time.

Benefits

- **Reinforce your network defense solutions**, including SIEMs, Firewalls, IPS/IDS, Security Proxy, DNS solutions, Anti-APT, with continuously updated Indicators of Compromise (IOCs) and actionable context, delivering insight into cyber-attacks and a greater understanding of the intent, capabilities and targets of your adversaries. Leading SIEMs (including HP ArcSight, IBM QRadar, Splunk etc.) are fully supported;
- Develop or enhance **anti-malware protection for perimeter and edge network devices** (such as routers, gateways, UTM appliances).
- **Improve and accelerate your incident response and forensic capabilities** by providing security/SOC teams with meaningful information about threats and global insights into what lies behind targeted attacks. Diagnose and analyze security incidents on hosts and the network more efficiently and effectively, and prioritize signals from internal systems against unknown threats to minimize incident response time and disrupt the kill chain before critical systems and data are compromised;
- **Provide threat intelligence to enterprise subscribers**. Leverage the first-hand information about emerging malware and other malicious threats to **preemptively strengthen your defensive posture and prevent compromises**;
- **Help to mitigate targeted attacks**. Enhance your security posture with tactical and strategic threat intelligence by adapting defensive strategies to counter the specific threats your organization faces;
- Use threat intelligence to **detect malicious content hosted on your networks and data centers**;
- **Prevent the exfiltration of sensitive assets and intellectual property** from infected machines to outside the organization, detecting infected assets fast, preventing competitive advantage and business opportunities loss and protecting the reputation of your brand;
- Conduct deep searches into threat indicators such as command-and-control protocols, IP addresses, malicious URLs or file hashes, with human-validated threat context that allows the prioritization of attacks, improves IT expenditure and resource allocation decisions and **supports you in focusing on mitigating those threats that pose the most risk to your business**;
- Use our expertise and actionable contextual intelligence to **enhance the protection delivered by your products and services** such as web content filtering, spam/phishing blocking and etc;
- **As an MSSP**, grow your business through providing industry-leading threat intelligence as a premium service to your customers. **As a CERT**, enhance and extend your cyber threat detection and identification capabilities.



Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Cyber Threats News: **www.securelist.com**
IT Security News: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.com