kaspersky bring on the future

Kaspersky
Threat Intelligence

Kaspersky Threat Data Feeds

Overview

What's in the feeds

Entries in feeds provided by Kaspersky contain contextual data that allows you to quickly confirm and prioritize threats:

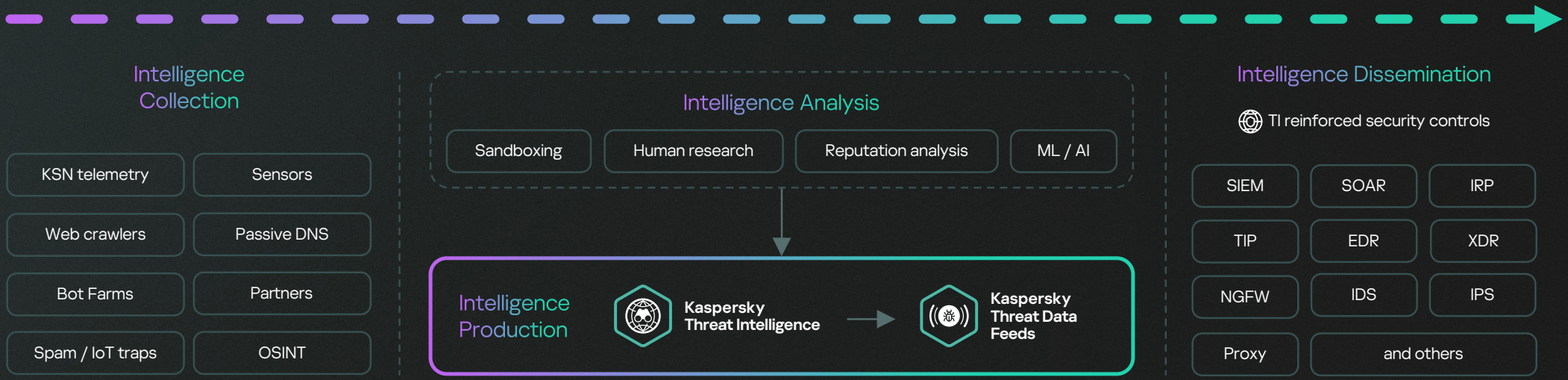
- threat names
- established IP addresses and domain names of malicious web resources
- hashes of malicious files
- identifiers of vulnerable and compromised objects
- tactics, techniques and procedures of attacks according to MITRE ATT&CK classification
- timestamps
- geographical position
- popularity, and so on.

Kaspersky Threat Data Feed service delivers real-time threat intelligence information to help organizations protect their networks and systems from cyberthreats. The data feeds include information on known malware, phishing websites, latest vulnerabilities and exploits, and other types of cyberthreats. Organizations can use this information to block malicious traffic, update their security software, and take other measures to protect themselves from cyberattacks.

Data is collected from a wide variety of trusted sources, including the Kaspersky Security Network and our own crawlers, botnet threat monitoring service (24/7 botnet monitoring, their targets and activities), spam traps, data from research groups and partners.

All collected information is carefully checked and cleaned in real time using various pre-processing methods: sandboxing, statistical and heuristic analysis, similarity tools, behavioral profiling and expert analysis.

Data Feeds help to collect general information about an event, and help to dig into details. It also helps to answer the questions 'Who? What? Where? Why?' and to identify the source of an attack, enabling quick decision-making and protecting the company from threats of any complexity.



How to use data feeds

Feed name	Prevention	Detection	Investigation
Malicious URL Data Feed	•	•	•
Ransomware URL Data Feed	•	•	•
Phishing URL Data Feed	•	•	•
Botnet C&C URL Data Feed	•	•	•
Mobile Botnet C&C URL Data Feed	•	•	•
Malicious Hash Data Feed	•	•	•
Mobile Malicious Hash Data Feed	•	•	•
IP Reputation Data Feed	•	•	•
IoT URL Data Feed	•	•	•
Vulnerability Data Feed	•	•	•
ICS Vulnerability Data Feed	•	•	•
ICS Vulnerability Data Feed in OVAL format		•	
ICS Hash Data Feed	•	•	•
pDNS Data Feed			•

Feed name	Prevention	Detection	Investigation
Suricata Rules Data Feed		•	
Cloud Access Security Broker (CASB) Data Feed		•	
APT Hash Data Feed		•	•
APT IP Data Feed		•	•
APT URL Data Feed		•	•
APT Yara Data Feed		•	•
Open Source Software Threats Data Feed	•	•	•
Crimeware Hash Data Feed		•	•
Crimeware URL Data Feed			•
Crimeware Yara Data Feed			•
Sigma Rules Data Feed	•		
Network Security IP Data Feed	•	•	
Network Security URL Data Feed	•	•	
Network Security Web Filtering Data Feed	•	•	

The list of Kaspersky Threat Data Feeds is constantly expanding.

Description of Kaspersky Threat Data Feeds

Commercial feeds

Commercial feeds provide access to the most comprehensive collection of information available by subscription. Information is updated on a regular basis. Depending on the type of feed, the regularity of updates can vary from several minutes to several hours. In addition to the listed data feeds, you can request to create a custom feed tailored to your needs.

Feed name	Feed description	Indicator type	Use cases
Malicious URL Data Feed	Web resources from which malware is distributed	Mask	• Information security management systems are opened for enrichment with external sources of information. Connecting these streams to SIEM / SOAR / IRP allows users to respond to current threats in a timely manner, and create additional context when investigating an incident. • Integration with network and email security systems (for example, NGFW / IDS / IPS / Mail / Web Security) helps prevent cyber incidents by enrichment of native security control capabilities with IOCs from data feed.
Ransomware URL Data Feed	Web resources from which ransomware is distributed		
Phishing URL Data Feed	Phishing web resources		
Botnet C&C URL Data Feed	Botnet C&C servers and related malicious objects (bots)		
Mobile Botnet C&C URL Data Feed	C&C mobile botnet servers with associated malicious objects (bots)		

#Prevention

#Detection

#Investigation

Feed name	Feed description	Indicator type	Use cases
Malicious Hash Data Feed	Hashes of common malicious files	Hash	• Integration with infrastructure security systems (Endpoint Security, Server Security, Mail/Web Security) to prevent malware from downloading and running, as well as detecting already running malware. • Integration with SIEM / SOAR / IRP systems allows users to respond to current threats quickly, and create additional context when investigating an incident.
Mobile Malicious Hash Data Feed	Hashes of common malicious files for mobile operating systems (Android and iOS)		
IP Reputation Data Feed	Various categories of suspicious and malicious IP addresses	IP	• Integration with network and mail security systems (NGFW / Mail Security) helps prevent cyber incidents by supplementing the native database of indicators of compromise with data on current threats. • Integration with SIEM/SOAR/IRP class systems allows users to respond to current threats quickly, and create additional context when investigating an incident.
IoT URL Data Feed	Web resources that distribute malicious software for IoT devices (IP cameras, smart vacuum cleaners, teapots, coffee makers, etc.)	Mask	
Vulnerability Data Feed	Enterprise software vulnerabilities	CVE	• Identification of vulnerable infrastructure elements through integration with vulnerability scanners and Asset Management systems. • Integration with Endpoint Protection systems to prevent the launch of software containing critical vulnerabilities. • Detection of the launch of vulnerable software. • Assistance with investigations. • Recommendations for vulnerabilities mitigations.
ICS Vulnerability Data Feed	Vulnerabilities in ICS software and hardware, as well as corporate software used in the process control infrastructure		

#Prevention

#Detection

#Investigation

Feed name	Feed description	Indicator type	Use cases	
ICS Vulnerability Data Feed in OVAL format	Rules for automated searches for ICS software vulnerabilities	OVAL check	· Enrichment of popular software vulnerability scanners to detect vulnerable ICS software.	#Detection
ICS Hash Data Feed	Common malicious files that pose a threat to ICS	Hash	· At the perimeter of OT networks, similar to the scenarios for using Malicious Hash Data Feed. · Inside OT networks to detect potentially dangerous files.	#Prevention #Detection #Investigation
pDNS Data Feed	Records of DNS lookups for domains to corresponding IP addresses over a period of time	IP, FQDN	· Providing context when investigating cyber incidents	#Investigation
Suricata Rules Data Feed	Rules for detecting various categories of threats in network traffic, such as APT, Botnet C&C, Ransomware, etc.	Suricata-rule	· Integration with NGFW/IDS/IPS/NTA/NDR systems to enrich the rules for detecting malicious activity.	#Detection
Cloud Access Security Broker (CASB) Data Feed	Domains and hosts related to popular cloud services	Mask	· Building a CASB solution, in particular, for setting up access policies for cloud services.	#Detection

Feed name	Feed description	Indicator type	Use cases	
APT Hash Data Feed	Hashes of files used by APT gangs to carry out targeted attacks	Hash	• Integration with infrastructure security systems (Endpoint and Server Security) to prevent malware from downloading and running, as well as detecting already running malware. • Integration with network and email security systems (for example, NGFW / IDS / IPS / Mail / Web Security) helps prevent cyber incidents by enrichment of native security control capabilities with IOCs from data feed. • Integration with SIEM / SOAR / IRP class systems allows users to create additional context when investigating an incident, as well as timely respond to current threats related to targeted attacks or related to members of APT groups.	#Detection #Investigation
APT IP Data Feed	Information about infrastructure elements relevant to conducting targeted attacks	IP		
APT URL Data Feed		Mask		
APT Yara Data Feed	YARA rules for identifying files used in targeted attacks	YARA-rule	• Proactive search for signs of targeted attacks in an organization's infrastructure. • Useful when investigating cyber incidents.	#Detection #Investigation
Open Source Software Threats Data Feed	Open source software packages containing vulnerabilities, malicious functionality, or politically motivated functionality compromises (blocking in certain regions, political slogans, etc.)	Package name and version	• Designed for component analysis of developed software as part of the secure development process (DevSecOps) in order to protect software from supply chain attacks, early detection and elimination of vulnerabilities, as well as to prevent the use of packages containing politically oriented undeclared features (NDV).	#Prevention #Detection #Investigation

Feed name	Feed description	Indicator type	Use cases	
Crimeware Hash Data Feed	Hashes of files used in fraudulent campaigns described in Kaspersky Crimeware reports	Hash	• Detection of malicious activity associated with the fraudulent actions of intruders. • Help with incident resolution by providing additional information contained in threat data feeds.	#Detection #Investigation
Crimeware URL Data Feed	Information about infrastructure elements related to fraudulent campaigns described in Kaspersky Crimeware reports	Mask		
Crimeware Yara Data Feed	YARA rules for identifying files used in fraudulent campaigns described in Kaspersky Crimeware reports	YARA-rule	• Proactively look for signs of fraudulent campaigns in the organization's infrastructure. • Useful when investigating cyber incidents.	#Investigation
Sigma Rules Data Feed	Rules in YAML format for detecting malicious activities	SIGMA-rules	• Integration with SIEM/EDR to detect malicious activities	#Detection
Network Security IP Data Feed	List of IP-addresses for NGFW alert/deny lists	IP	• Integration with network security controls (NGFWs) to increase their protection level	#Detection #Prevention

Feed name	Feed description	Indicator type	Use cases	
Network Security URL Data Feed	List of URL's for NGFW alert/deny lists	URL	• Integration with network security controls (NGFWs) to increase their protection level	#Detection #Prevention
Network Security Web Filtering Data Feed	List of categorized domains for NGFW alert/deny lists	URL	• Integration with network security controls (NGFWs) to increase their protection level	#Detection #Prevention

Demo feeds

The demo feeds are for evaluation purposes only. The data contains limited samples with significantly reduced information and less frequent updates. The structure of feeds is similar to the format of commercial feeds, but this may differ in some cases.

- Demo IP Reputation Data Feed
- Demo Botnet C&C URL Data Feed
- Demo Malicious Hash Data Feed
- Demo APT IP Data Feed
- Demo APT URL Data Feed
- Demo Sigma Rules Data Feed
- Demo APT Hash Data Feed
- Demo Suricata Rules Data Feed
- Demo Suricata Rules Data Feed
- Demo ICS Vulnerability Data Feed
- Demo ICS Vulnerability Data Feed in OVAL format
- Demo Crimeware Hash Data Feed
- Demo Crimeware URL Data Feed

Request a demo

Kaspersky Threat Intelligence

Your rich supporting context

Threat Data Feeds from Kaspersky enhance the detection capabilities of your existing security controls, including SIEM systems, intrusion detection systems, security proxies, etc.

Learn more

www.kaspersky.com

© 2024 AO Kaspersky Lab.
Registered trademarks and service marks
are the property of their respective owners.