Kaspersky Threat Data Feeds

kaspersky bring on the future

Kaspersky Threat Data Feeds

Kaspersky Threat Data Feeds

Cyberattacks happen every day. Cyberthreats are constantly growing in frequency, complexity and obfuscation, as they try to compromise your defenses. Adversaries use complicated intrusion kill chains, campaigns and customized Tactics, Techniques and Procedures (TTPs) to disrupt your business or damage your customers. It's clear that protection requires new methods, based on threat intelligence.

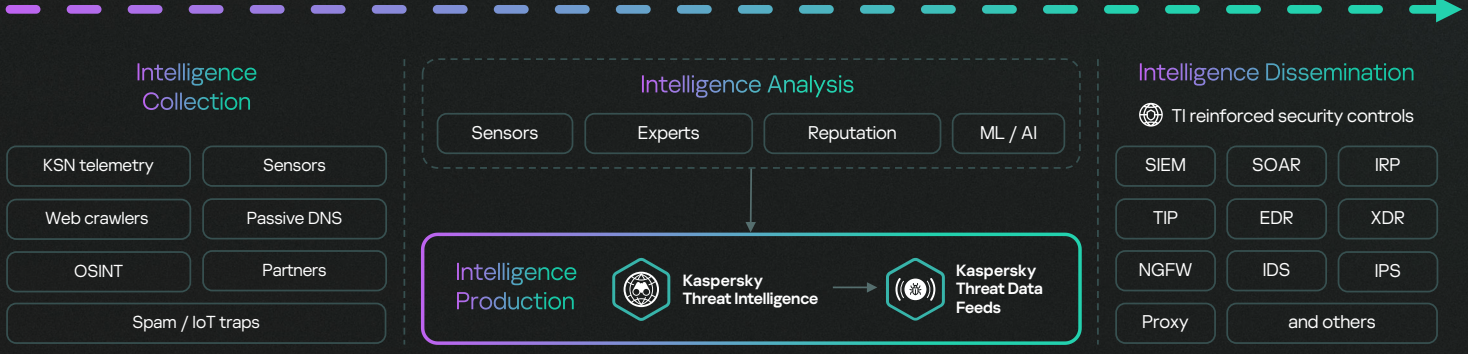
By integrating up-to-the-minute threat intelligence feeds containing information on suspicious and dangerous IPs, URLs and file hashes into existing security systems like SIEM, SOAR and Threat Intelligence Platforms, security teams can automate the initial alert triage process while providing their triage specialists with enough context to immediately identify alerts that need to be investigated or escalated to incident response teams for further investigation and response.

Contextual data

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

- Threat names
- IP addresses and domain names of malicious web resources
- Hashes of malicious files
- Vulnerable and compromised objects
- Tactics, techniques and procedures of attacks according to MITRE ATT&CK classification
- Timestamps
- Geolocation
- Popularity, and so on

How it works



Kaspersky Threat Data Feeds are aggregated from Kaspersky fused, heterogeneous and highly reliable sources:

Kaspersky Security Network

Sophisticated cloud infrastructure that collects and analyzes anonymous cyber threat data from over 400 million voluntary participants worldwide to provide the fastest response to new threats by leveraging big data analytics, machine learning and human expertise.

Web crawlers

Collect new malware and legitimate samples from a variety of sources: OSINT, research by Kaspersky analysts, and our own automatic processing and analysis systems that extract URLs from malware.

BotFarms

Dedicated botnet research team extracts bot configurations, reverse engineers their communication protocols, and monitors commands from command centers to gain valuable threat intelligence.

Spam traps

Each year our anti-phishing systems prevent more 500 million phishing link clicks and more 160 million malicious email attachments, from which we extract additional data to enrich our data streams.

Partners

We participate in partnerships to share malicious samples with other vendors and cybersecurity organizations.

Sensors

Honeypots, sinkholes, and other methods of intercepting ITW attacks. For example (including IoT devices, vulnerable systems, software, etc). Kaspersky analysts research attack attempts and methods of attackers, extract indicators of compromise, and link them to other data sources.

Passive DNS

Data is collected globally from trusted third parties such as hosting organizations and ISPs.

OSINT

Adversary data is automatically collected from publicly available sources such as news outlets, social media, public reports, dark web, etc. We use this data to search for new malicious samples exploring the adversary's infrastructure, continuously adding to our knowledge base.

Each detected indicator undergoes a multi-stage screening process in an automated processing system that uses trust and reputation technologies and machine learning models trained on samples from hundreds of millions of actual trusted and malicious files to weed out false positives. Each indicator is also analyzed in multiple sandboxes, from which dozens of additional attributes such as TTPs, network behavior, operating system behavior, and a host of other relationships are extracted.

All of this turns Kaspersky Threat Intelligence into a powerful source of tactical-level intelligence that can strengthen your threat monitoring centers and detect adversaries on the front lines of your organization.

Highlights

Data Feeds are automatically generated in real time, based on findings across the globe providing high detection rates and accuracy.

Ease of implementation is ensured by supplementary documentation, samples, a dedicated technical account manager and technical support from Kaspersky all combine to enable straightforward integration.

Simple lightweight dissemination formats (JSON, CSV, OpenIoC, STIX) via HTTPS, TAXII or ad-hoc delivery mechanisms support easy integration of feeds into security solutions. Leading SIEMs and TI Platforms are fully supported.

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.

Hundreds of experts, including security analysts from across the globe, worldrenowned security experts from GReAT and 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.

All feeds are generated and monitored by a highly fault-tolerant infrastructure, ensuring continuous availability.

Benefits

1. Reinforce your network defense solutions, including SIEMs, Firewalls, NGFW, IPS/IDS, Security Proxy, DNS solutions, Anti-APT, with continuously updated Indicators of Compromise (IOCs) and actionable context to deliver insights into cyberattacks and provide a greater understanding of the intent, capabilities and targets of your adversaries.

2. Improve and accelerate your incident response and forensic capabilities by automating the initial triage process while providing your security analysts with enough context to immediately identify alerts that need to be investigated or escalated to incident response teams for further investigation and response.

3. Prevent the exfiltration of sensitive assets and intellectual property from infected machines to outside the organization. Detect infected assets fast to protect your brand reputation, maintain your competitive advantage and secure business opportunities.

4. As an MSSP, grow your business by providing industry-leading threat intelligence as a premium service to your customers.

5. As a CERT, enhance and extend your cyberthreat detection and identification capabilities.

Kaspersky Threat Intelligence

Kaspersky Threat Intelligence provides access to a wide range of information gathered by our world-class analysts and researchers. This data will help your organization effectively counter today's cyber threats.

Our company owns deep knowledge, extensive experience in cyberthreat research and unique insights into all aspects of cybersecurity, providing up-to-date tactical, operational and strategic threat intelligence. This has made us a trusted partner of law enforcement and government organizations around the world, including Interpol and various CERT units. And all this is available to you as relevant, actionable data through the Kaspersky Threat Intelligence Portal.

Kaspersky Threat Intelligence

Learn more

www.kaspersky.com

#kaspersky
#bringonthefuture