Kaspersky Research Sandbox

Kaspersky Threat Attribution Engine

Kaspersky Similarity

Kaspersky Threat Analysis

kaspersky BRING ON THE FUTURE

Kaspersky Threat Analysis

Kaspersky Threat Analysis

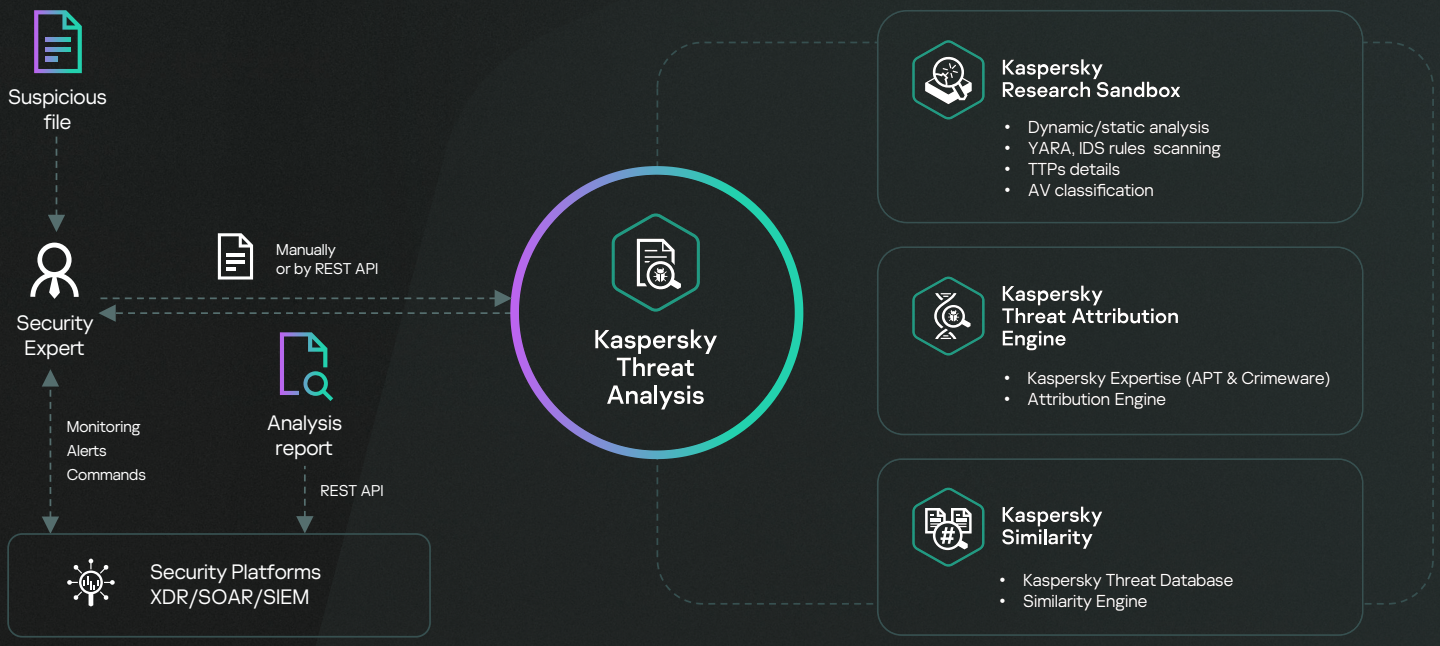
Faced with a potential cyberthreat, the decisions you make, and how well you can make them, can both prove critical. It is impossible to prevent today's targeted attacks solely with traditional anti-virus tools. Anti-virus engines are capable of stopping only known threats and their variations, while sophisticated threat actors use all means at their disposal to evade automatic detection. The number of security alerts processed by SOCs every day is growing exponentially. With the amount of malware samples generated every day, effective alert prioritization, triage, and validation becomes nearly unfeasible.

Combining threat intelligence, dynamic analysis, threat attribution and similarity technologies gives a powerful tool for the detection of malicious objects not previously seen. To help security researchers stay informed about existing and emerging threats, Kaspersky provides a single resilient framework to automate routine analysis of suspicious files.

In addition to traditional threat analysis technologies like sandboxing, Kaspersky Threat Analysis arms you with state-of-the-art attribution and related similarity technologies — a hybrid approach that delivers efficient threat analysis, so you can make fully informed decisions and keep your infrastructure secure.

Kaspersky Threat Analysis is provided via both a united web and RESTful interfaces and allows users to set specific parameters to analyze suspicious objects with high efficiency. Multiple threat analysis tools combine to let you and your team analyze the situation from all angles, equipped with a complete and detailed reports to respond swiftly and effectively.

How it works



Kaspersky
Threat Analysis

Kaspersky
Research
Sandbox

Sandboxing technologies

are powerful dynamic analysis tools that allow to investigate file sample origins, to collect IOCs based on behavioral analysis and identify malicious objects not detected by traditional antivirus tools.

Cloud and on-prem versions are available.

Sandbox

Kaspersky Research Sandbox has been developed directly out of our in-lab sandboxing complex, a technology that's been evolving for over two decades. It incorporates all the knowledge about malware behaviors we have acquired throughout our continuous threat research, allowing us to detect 420 000+ new malicious objects every day. It offers a hybrid approach, combining behavioral analysis and rock-solid anti-evasion techniques, with human-simulating technologies.

Deployed on-premise, the technology prevents exposure of data outside the organization. Kaspersky Research Sandbox on-premise also allows to create custom execution environments for analysis tailoring them to real environments, which increases the accuracy of threat detection and the speed of investigation.

Why to use?

Suspicious files, not detected by anti-virus tools, can reveal their malicious traits only during their behavior. Kaspersky Research Sandbox allows to emulate the behavior and highlight dangerous actions.

Product highlights

Automated object analysis in Windows, Linux and Android environments

Custom images allow threat analysis across Windows operating systems and applications (only those that apply to real environments)

The threat score based on metrics and data obtained during file execution shows the danger level of analyzed object

Advanced anti-evasion techniques and human-simulating technologies

Manual sample upload and an enhanced REST API for integration with automated workflows

Support for analysis of over 200 file types with detailed analysis reports

Custom Suricata rules to scan network traffic can be added and used together with the Suricata rules

1000+ unique hunts for extracting TTPs by MITRE ATT&CK

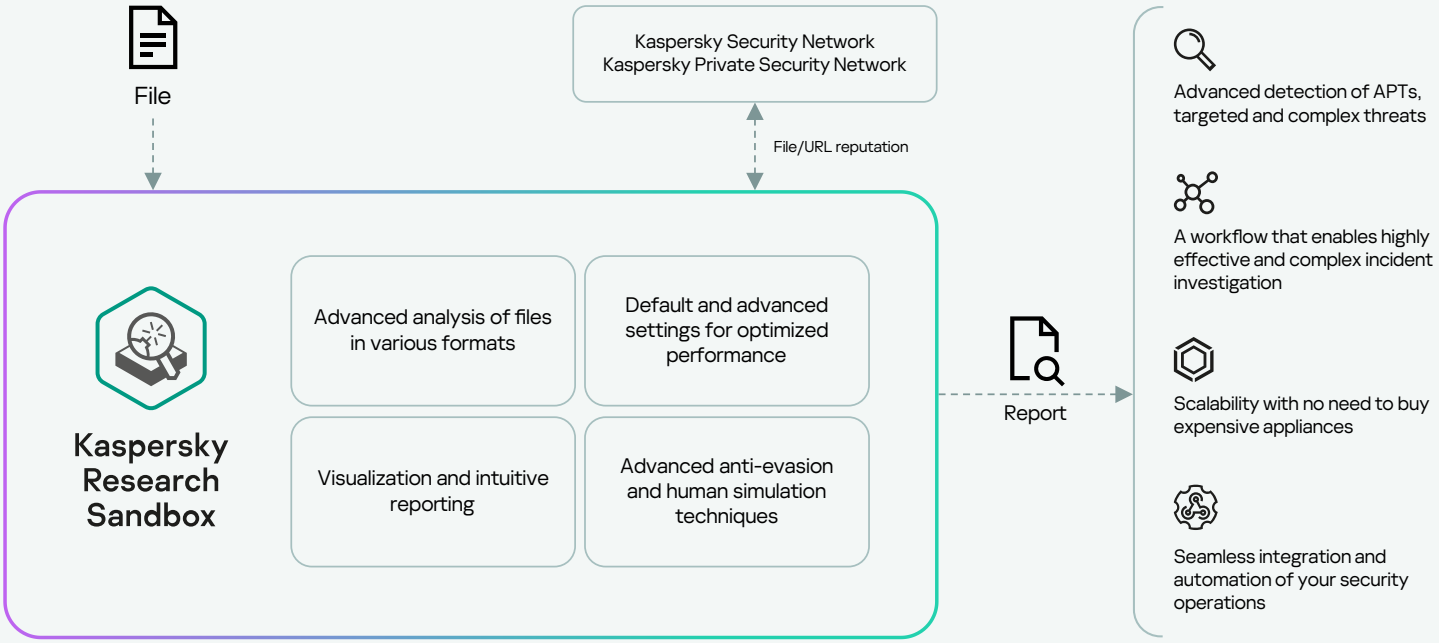
Interactive mode support (expected in Q1 2024)

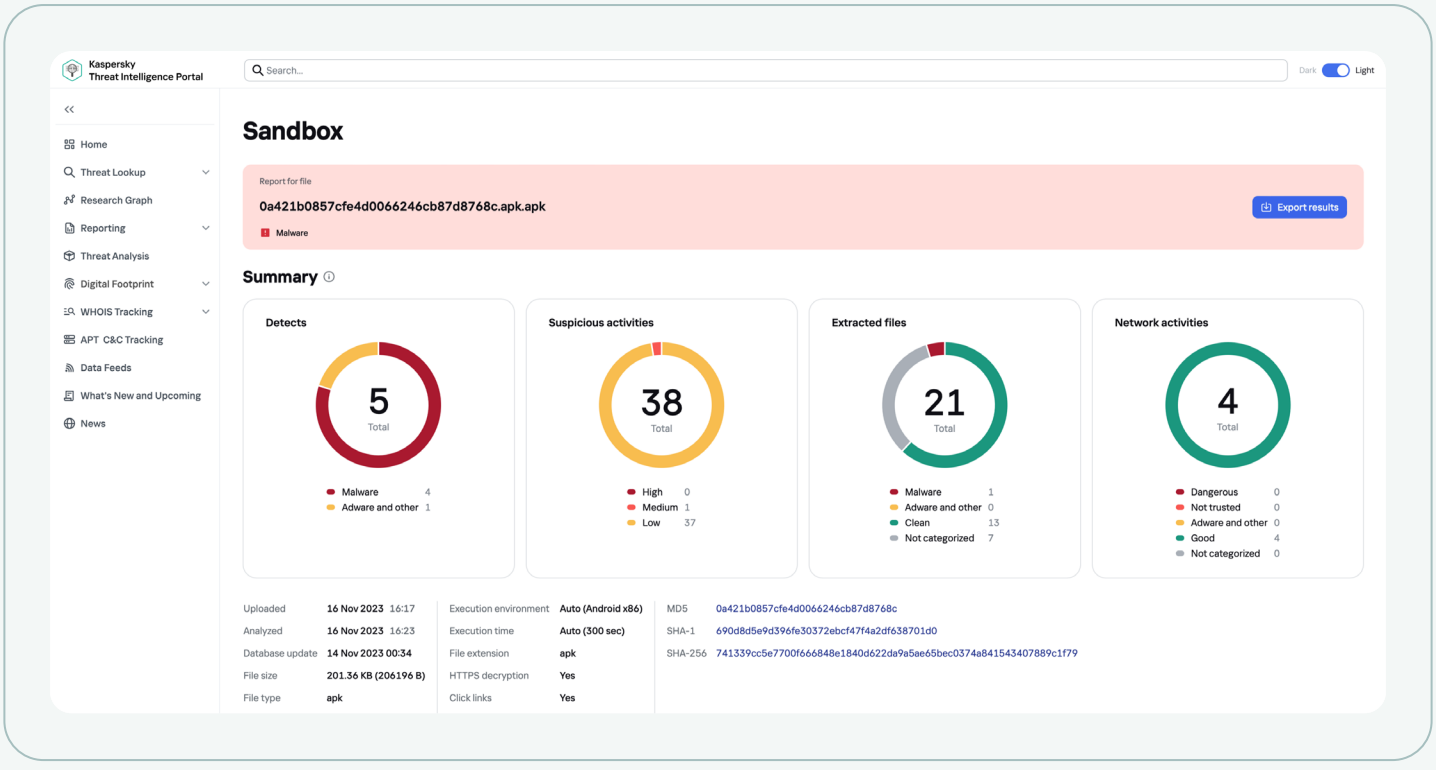
The product supports bare metal deployment. Hardware configuration depends on the required performance and can be scaled. It requires at least one independent ISP connection (two or more are recommended for fault-tolerance), 100 Mbps for each channel.

Kaspersky Research Sandbox is based on a patented proprietary technology (patent no. US10339301). By creating the exact conditions that trigger malware execution, it allows researchers to analyze a suspicious file/URL in a single attempt.

To avoid exposure, a malicious file may first investigate if it's in a virtual machine or stay inactive until the sandbox is no longer operating. In such cases, the patented technology speeds up the time flow inside the virtual machine so the malicious code is forced to execute sooner.

Kaspersky Research Sandbox high-level operation scheme





Detailed analysis reports

Once the analysis is complete, Research Sandbox provides a detailed report on the behavior and functionality of the analyzed sample, allowing you to define the appropriate response procedures:

Summary	General information about a file's execution/URL browsing results.
Detection names	A list of detects (both AV and behavioral) that were registered during the file execution.
Triggered network rules	A list of network Suricata rules that were triggered during analysis of traffic from the executed object.
Execution map	A graphically represented sequence of object activities and the relationship between them.
Suspicious activities	Suspicious activities — a list of registered suspicious activities.
Screenshots	A set of screenshots that were taken during the file execution/URL browsing.
Loaded PE images	A list of loaded PE images that were detected during the file execution/ URL browsing.
File operations	A list of file operations that were registered during the file execution/ URL browsing.
Registry operations	A list of operations performed on the OS registry that were detected during file execution/URL browsing.
Process operations	A list of interactions of the file with various processes that were registered during the file execution.
Synchronize operations	A list of operations of created synchronization objects (mutex, event, semaphore) that were registered during the file execution/URL browsing.
Downloaded files	A list of files that were extracted from network traffic during the file execution/ URL browsing.
Dropped files	A list of files that were saved (created or modified) by the executed file.
HTTPS/HTTP/DNS/IP/TCP/UDP and etc.	Network sessions/requests details that were registered during the file execution/ URL browsing.
Network traffic dump (PCAP)	Network activity can be exported in PCAP format.
MITRE ATT&CK matrix	All identified process activities recorded during emulation are presented in the form of a MITRE ATT&CK matrix.

Kaspersky
Threat Analysis

Kaspersky Threat Attribution Engine

Threat attribution

Tracking, analyzing, interpreting and mitigating constantly evolving IT security threats is a massive undertaking. Setting aside all the hype, threat intelligence is of true value, and threat attribution is a critical element here.

Cloud and on-prem versions are available.

Attribution

Kaspersky Threat Attribution Engine is a unique threat analysis tool providing insights into the origin of high-profile malware and its possible authors. It quickly connects a suspicious file to known APT threats, actors, campaigns, using a unique algorithm and a special database comprising APT malware samples and the industry's largest collection of clean files gathered by Kaspersky experts over the last 25 years and more.

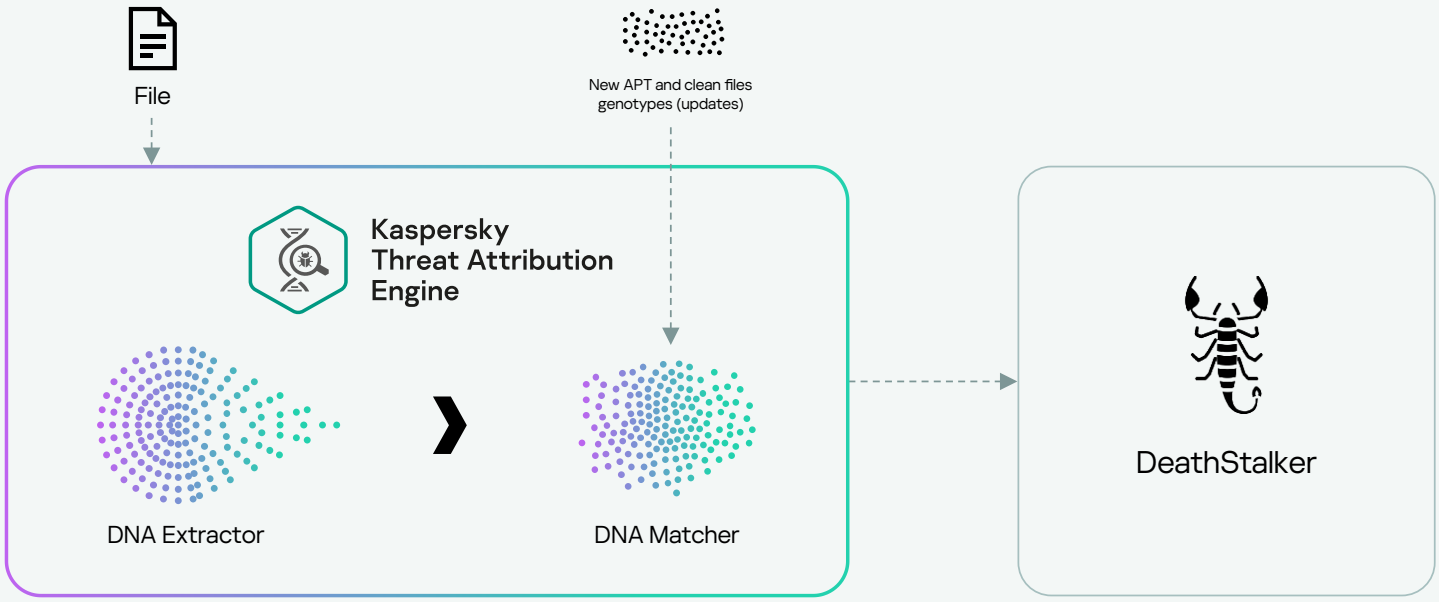
We track 1100+ threat actors and campaigns and release 200+ threat intelligence reports a year. Our ongoing research supports an APT collection which contains more than 80 000 files that, in conjunction with the use of automated tools, results in outstandingly accurate levels of attribution.

The product offers a unique approach to comparing similar samples while ensuring near-zero false positive rates. Any new attack can quickly be linked to known APT malware, previous targeted attacks and hacker groups, helping you to distinguish high-risk threats from less serious incidents, so you can take timely protective measures to prevent an attacker from gaining a foothold in your system. Kaspersky Threat Attribution Engine can be deployed in secure, air-gapped environments, restricting any 3rd party from accessing the processed information and submitted objects.

Why to use?

Attribution of a file to a certain threat actor, along with the knowledge of this threat actor, allows to know the place of this sample in overall cyber kill chain, specific for this adversary. In its turn it gives the knowledge where to look for other IoCs/IoAs and not to miss the whole attack by blocking only one particular file.

Kaspersky Threat Attribution Engine high-level operation scheme



Product highlights

Provides instant access to a repository of curated data about thousands of APT actors, samples and broader threats (via the anti-virus engine)

Unique insights into high-profile campaigns (400+) investigated by Kaspersky experts

Allows efficient automated or manual threat prioritization and alert triage

Functionality to add private actors and samples, educating the product to detect samples that are similar to files in your private collection

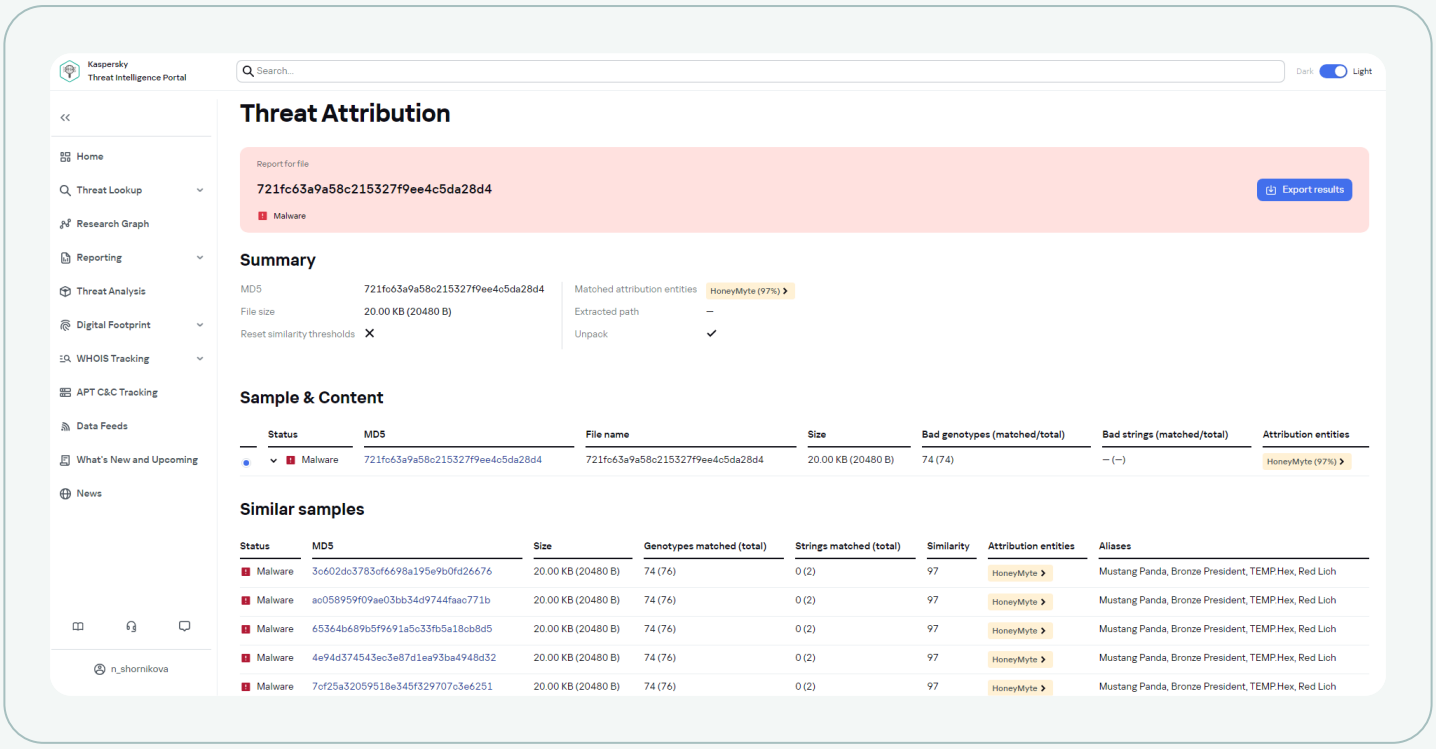
Manual sample upload and an enhanced REST API for integration with automated workflows

Supports deployment on cloud infrastructures such as Amazon Web Services (AWS) enabling quick product setup and saving costs as no need to invest in hardware upfront

Export to YARA rules for further automated search/scanning for similar files or integration with third-party solutions

Export to STIX 2.1 format (TXT and JSON formats are also supported) for further automated analysis of security logs or integration with third-party solutions/security controls

Functionality for unpacking password protected archives with custom passwords



Proprietary searching method

To link malware to attribution entities, Kaspersky Threat Attribution Engine uses a unique proprietary method of searching for similar genotypes and strings between files. This method involves:

Analyzing the genetics of a sample

by extracting the following elements from its code:

- Genotypes — distinctive pieces of binary code
- Strings — distinctive strings of characters

Automatically searching the analyzed files

for genotypes and strings which are similar to genotypes and strings of APT samples previously analyzed, or already linked to attribution entities

Based on similar genotypes and strings

found in APT samples, providing a report on the origin of the analyzed sample, related attribution entities, and any similarities between this sample and known APT samples

Kaspersky
Threat Analysis

Kaspersky
Similarity

Files similarity

To build an effective defense line, it's not always necessary to know your enemy by sight. Kaspersky Similarity allows to Identify file samples with similar functions, to protect against unknown and evasive threats.

Cloud version is available via Kaspersky Threat Intelligence Portal.

Similarity

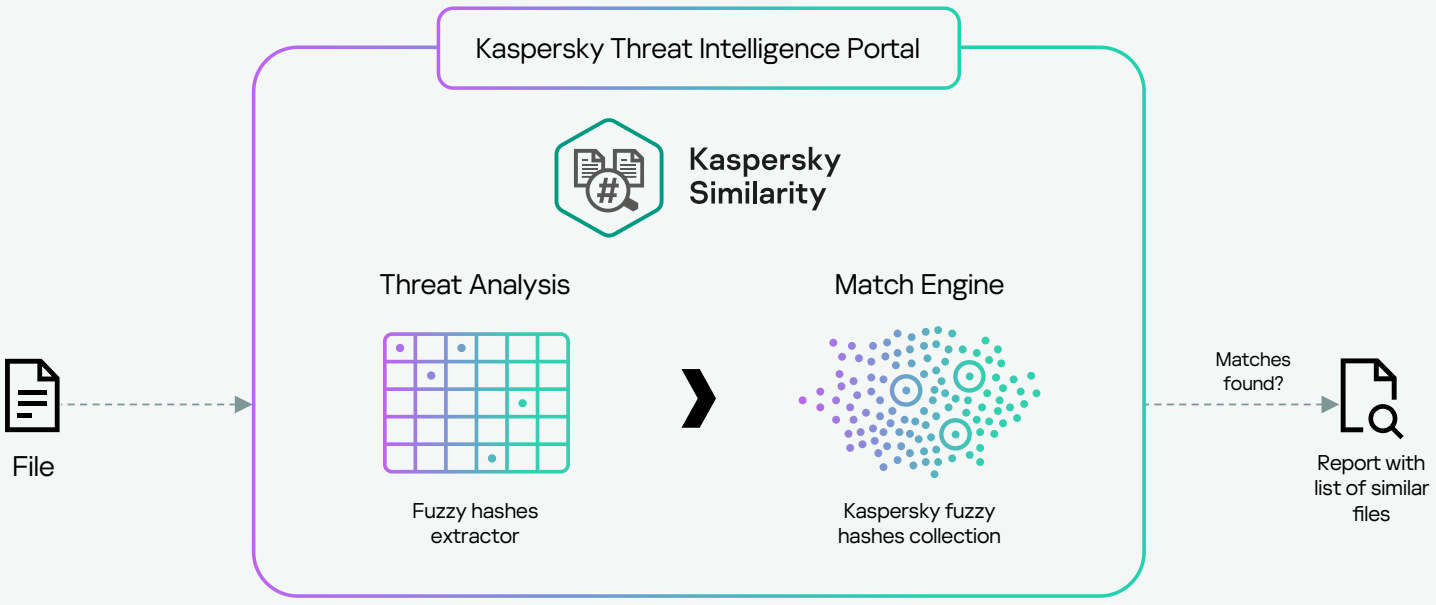
Kaspersky Similarity is an additional feature available via Threat Intelligence Portal both for Kaspersky Research Sandbox and Kaspersky Threat Attribution Engine users helping to identify files that look and behave in similar ways.

Similar files are being searched and calculated for the original file using the cutting-edge technology invented by Kaspersky experts leveraging more than 50 unique similarity hash types. This allows to ensure accurate and high confident similarity results.

Why to use?

Find similar (e.g. evasive) malware and look for it in your infrastructure to be confident that a slight change of the sample, made by the adversary, is still on your security radar. The technology is distinguished from attribution: even not attributed similar malware files can be found.

Kaspersky Similarity high-level work scheme



Similarity reports

Each file has specific format, used packers, sections, strings, import tables etc. Kaspersky experts have created a set of hashes to determine the similarity between different files based on these attributes. Kaspersky Similarity allows users to submit a suspicious file, extract its fuzzy hashes and compare them with fuzzy hashes of files existing in Kaspersky threat database. In case the matches are found it generates the list of hashes for TOP similar malicious files, already known to Kaspersky and sorted by similarity score. The report contains the additional context with metadata for each similar file:

- Similarity confidence
- File status (malware, adware or other)
- Threat name
- Timestamps of first and last detection
- Quantity of hits (detections)
- File hash
- File type
- File size

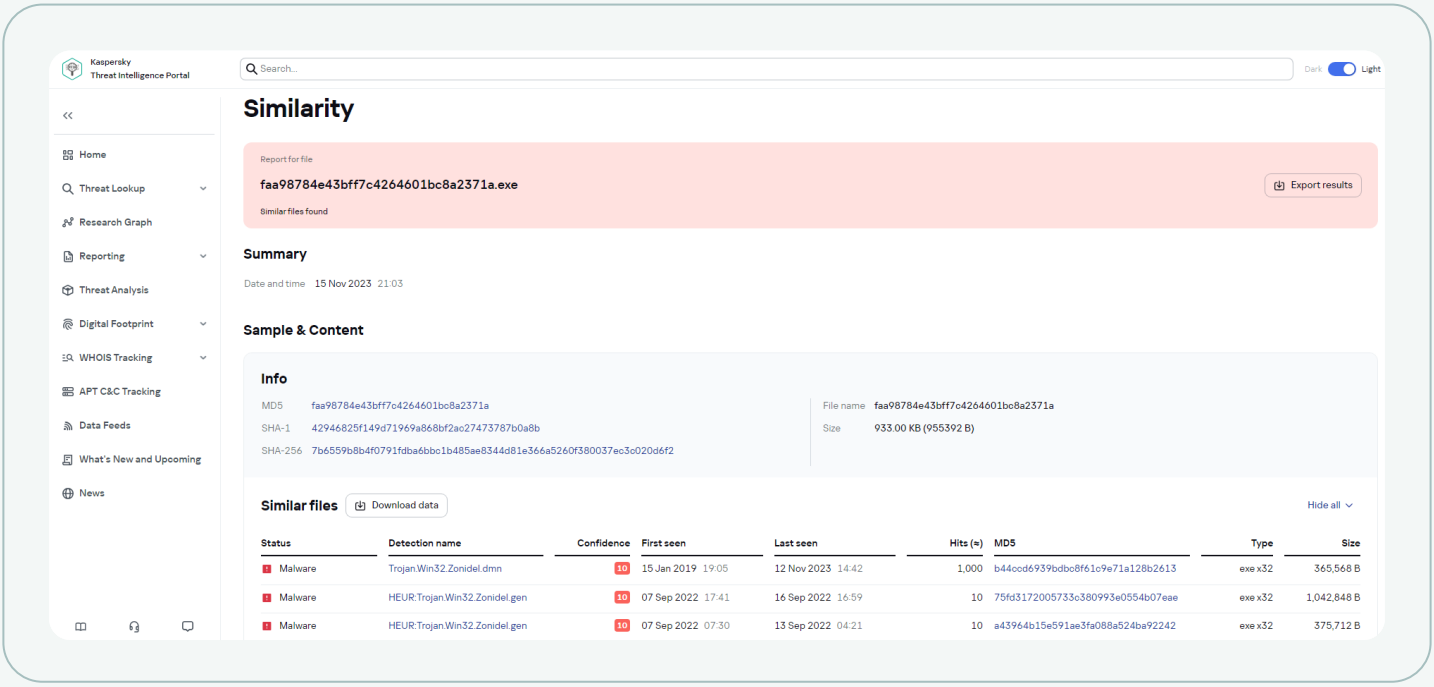
Feature highlights

Leverages one of the largest in the industry database of malicious and clean files, collected by latest 25+ years, enabling maximum coverage for highest comparison accuracy

Manual sample upload and an enhanced REST API for integration with automated workflows

Is provided to Kaspersky Research Sandbox and Kaspersky Threat Attribution users for free to enhance the effectiveness of both technologies and provide comprehensive information on the analyzed file

Is already used extensively by Kaspersky experts for exploring new threats to deliver even higher threat protection in our products which is regularly confirmed by regular top rates according to independent tests:



Kaspersky Threat Analysis use cases

Kaspersky Threat Analysis provides mature instruments of choice for detecting unknown threats that can be widely applied in the following scenarios:

Incident Response

Reveal evasive threats

Static/dynamic analysis of suspicious files

Reveal the relation of a new malware to certain Threat Actor to know possible further steps of attack

Threat Hunting

Infrastructure scanning for IoCs received through report

Find potential malicious modifications of popular clean files

Identify shared IoCs between unknown and known malicious files

Malware Analysis

Unknown threat analysis

Find related malware to help with reverse engineering of obfuscated files

Kaspersky Threat Analysis is a flexible research tool with interconnected components that enables comprehensive and multilayered assessment of suspicious objects for identification and classification of advanced attacks. It helps SOC teams, security researchers, and malware analysts to stay informed about existing and emerging malware-related threats, allowing them to quickly prioritize and address critical threats and remediate them more effectively.

Kaspersky Threat Analysis

Learn more

www.kaspersky.com

#kaspersky
#bringonthefuture