



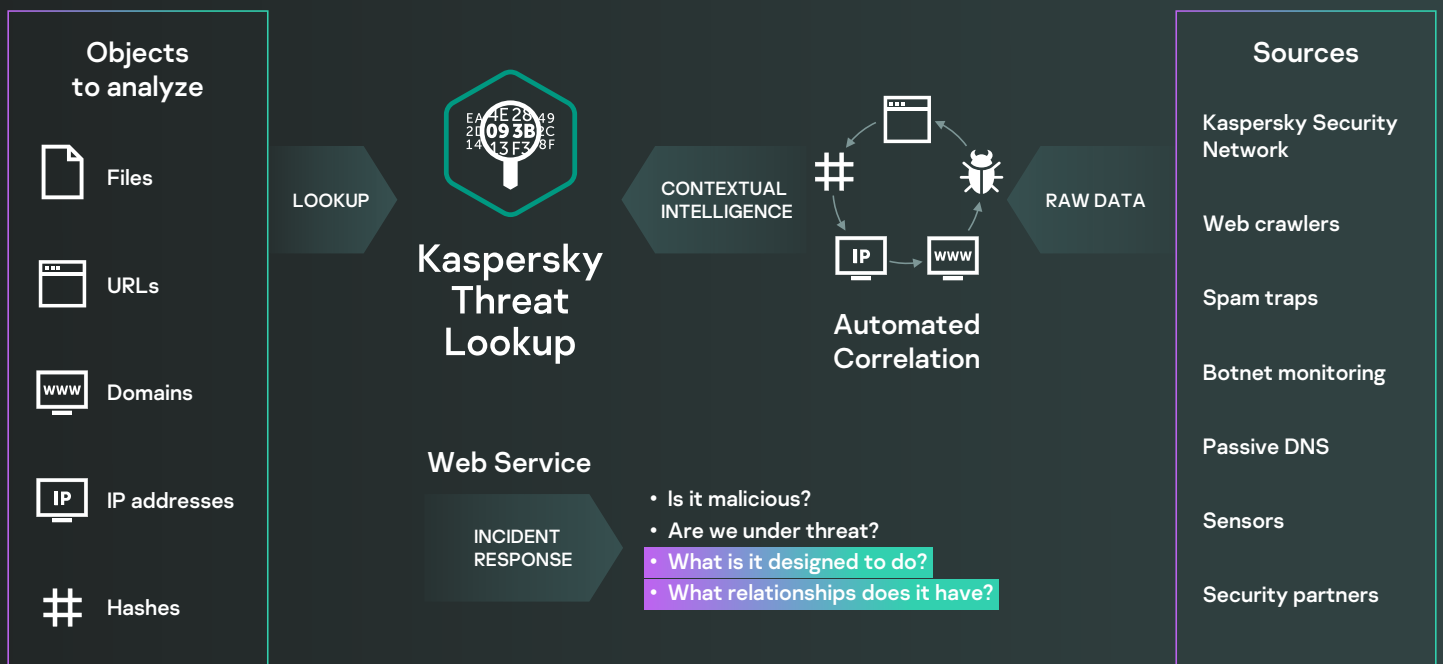
Kaspersky Threat Lookup




Kaspersky Threat Lookup

Cybercrime knows no borders, and technical capabilities are improving fast: we're seeing attacks becoming increasingly sophisticated as cybercriminals use dark web resources to threaten their targets. Cyberthreats are constantly growing in frequency, complexity and obfuscation, as new attempts are made to compromise your defenses. Attackers are using complicated kill chains, and customized Tactics, Techniques and Procedures (TTPs) in their campaigns to disrupt your business, steal your assets or damage your clients.


Kaspersky Threat Lookup delivers all the knowledge acquired by Kaspersky about cyberthreats and their relationships, brought together into a single, powerful web service. The goal is to provide your security teams with as much data as possible, preventing cyberattacks before they impact your organization. The platform retrieves the latest detailed threat intelligence about URLs, domains, IP addresses, file hashes, threat names, statistical/behavior data, WHOIS/DNS data, file attributes, geolocation data, download chains, timestamps etc. The result is global visibility of new and emerging threats, helping you secure your organization and boosting incident response.




Highlights




Trusted Intelligence: A key attribute of Kaspersky Threat Lookup is the reliability of our threat intelligence data, enriched with actionable context. Kaspersky leads the field in anti-malware tests¹, demonstrating the unequalled quality of our security intelligence by delivering the highest detection rates, with near-zero false positives




Threat hunting: Be proactive in preventing, detecting and responding to attacks, to minimize their impact and frequency. Track and aggressively eliminate attacks as early as possible. The earlier you can discover a threat, the less damage is caused, the faster repairs take place and the sooner network operations can get back to normal




Incident investigations: A Research Graph boosts incident investigations by letting you visually explore data and detections stored in Threat Lookup. It provides a graphic visualization of the relationship between URLs, domains, IPs, files and other contexts so you can better understand the full scope of an incident and identify its root cause.



Master search: Search for information across all active threat intelligence products and external sources (including OSINT IoCs, Dark Web and Surface Web) in a single and powerful interface.




Easy-to-use Web interface or RESTful API: Use the service in manual mode through a web interface (via a web browser) or access via a simple RESTful API as you prefer




Wide range of export formats: Export IOCs (Indicators of Compromise) or actionable context into widely used and more organized machine-readable sharing formats, such as STIX, OpenIOC, JSON, Yara, Snort or even CSV, to reap the full benefits of threat intelligence, automate operations workflow, or integrate with security controls such as SIEMs


Benefits



Conduct deep searches into threat indicators with highly-validated threat context that lets you prioritize attacks and focus on mitigating the threats that pose the most risk to your business



Diagnose and analyze security incidents on hosts and the network more efficiently and effectively, and prioritize signals from internal systems against unknown threats



Boost your incident response and threat hunting capabilities to disrupt the kill chain before critical systems and data are compromised

Now you can

Look up threat indicators from a web-based interface or via the RESTful API

Examine advanced details including certificates, commonly used names, file paths, or related URLs to discover new suspicious objects

Check whether the discovered object is widespread or unique

Understand why an object should be treated as malicious



Kaspersky Threat Lookup

[Learn more](#)

www.kaspersky.com

© 2022 AO Kaspersky Lab.
Registered trademarks and service marks
are the property of their respective owners.