



# Kaspersky Threat Lookup



# Kaspersky Threat Lookup


Cyberkriminalität entwickelt sich mit dem technologischen Fortschritt und kennt kaum noch Grenzen. Wir beobachten Cyberangriffe, die immer raffinierter werden, und Cyberkriminelle, die für ihre Angriffe zunehmend Ressourcen aus dem Dark Web einsetzen. Cyberbedrohungen werden immer häufiger, komplexer und schwerer erkennbar. Zuverlässige Abwehrmaßnahmen zu finden, wird deshalb auch zunehmend schwieriger. Die Angreifer nutzen dabei komplizierte „Kill Chains“ und individuelle Taktiken, Techniken und Abläufe (Tactics, Techniques and Procedures, TTPs), um Ihre Geschäftsabläufe zu stören, Ihre Vermögenswerte zu entwenden oder Ihren Kunden zu schaden.

Kaspersky Threat Lookup bietet das gesamte Wissen von Kaspersky über Cyberbedrohungen und ihre Interdependenzen in einem einzigen, leistungsstarken Webservice. Das Ziel ist es, Sie und Ihre Sicherheitsteams mit so vielen Informationen wie möglich zu versorgen, damit Cyberangriffe schon im Vorfeld abgewendet werden können. Die Plattform ruft die neuesten detaillierten Bedrohungsdaten ab zu URLs, Domänen, IP-Adressen, Hash-Werten, Namen von Bedrohungen, statistische/Verhaltensdaten, WHOIS/DNS-Daten, Dateiattribute, geographische Standortdaten, Downloadketten, Zeitstempel etc. Im Ergebnis erhalten Sie eine weltweite Übersicht über neue und sich entwickelnde Bedrohungen, damit Sie Ihre Organisation schützen und die Vorfallsreaktion beschleunigen können.







## Wichtigste Vorteile




**Vertrauenswürdige Informationen:** Ein zentraler Bestandteil von Kaspersky Threat Lookup ist die Zuverlässigkeit unserer Bedrohungsinformationen, die durch einen praktisch umsetzbaren Kontext ergänzt werden. Kaspersky-Produkte zählen zu den führenden bei Anti-Malware-Tests<sup>1</sup>. Die hohen Erkennungsraten in Kombination mit False Positives, die praktisch gegen Null gehen, zeigen die Zuverlässigkeit unserer Sicherheitsinformationen.




**Threat Hunting:** Gehen Sie bei der Prävention, Erkennung und Reaktion auf Angriffe proaktiv vor, um deren Auswirkung und Häufigkeit zu minimieren. Erkennen und beenden Sie Angriffe so früh wie möglich. Je früher Sie eine Bedrohung entdecken, umso weniger Schaden entsteht, umso schneller können Korrekturmaßnahmen stattfinden und umso eher kann sich der Netzwerkbetrieb normalisieren.



**Vorfallsuntersuchung:** Ein Research Graph sorgt für eine effektivere Vorfallsuntersuchung, da sie Daten und erkannte Ereignisse visuell in Threat Lookup untersuchen können. Er bietet eine grafische Darstellung der Interdependenzen zwischen URLs, Domänen, IPs, Dateien und anderen Kontexten, damit Sie den Umfang eines Vorfalls besser verstehen und die Ursache identifizieren können.



**Master-Suche:** Suchen Sie nach Informationen in allen aktiven Threat Intelligence-Produkten und externen Quellen (einschließlich OSINT IoCs, Dark Web und öffentliches Internet) über eine einzige, leistungsstarke Oberfläche.




**Benutzerfreundliche Weboberfläche oder RESTful API:** Sie können auf diesen Service manuell über eine Web-Oberfläche (über einen Browser) oder über eine einfache RESTful-API zugreifen.




**Breite Palette an Exportformaten:** Exportieren Sie die Gefährdungsindikatoren (Indicators of Compromise, IOCs) oder den praktisch umsetzbaren Kontext in gängige, strukturierte und computerlesbare Formate, z. B. STIX, OpenIOC, JSON, Yara, Snort oder sogar CSV. So können Sie alle Vorteile von Threat Intelligence nutzen, betriebliche Abläufe automatisieren oder eine Integration in bestehende Sicherheitskontrollen, z. B. SIEMs ermöglichen.


## Vorteile



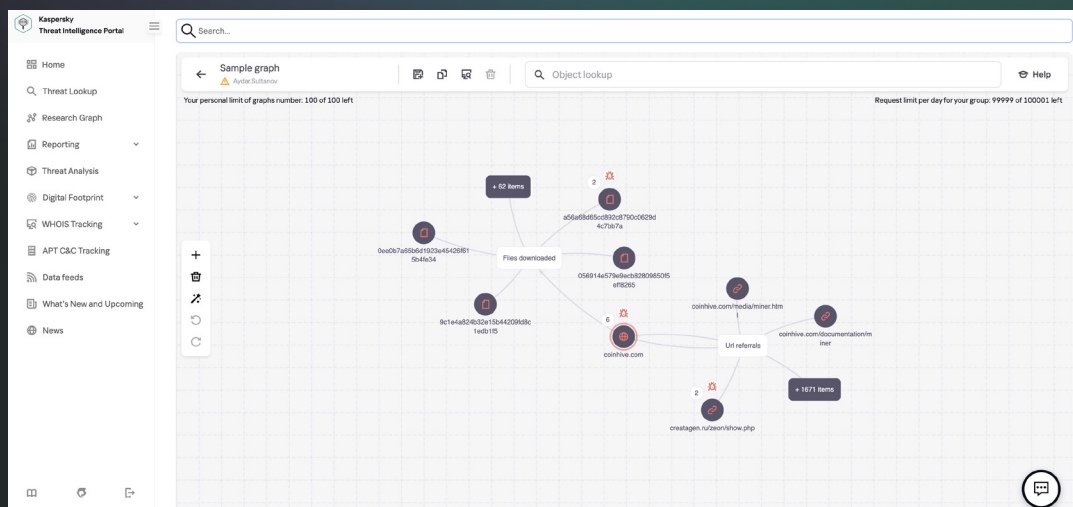
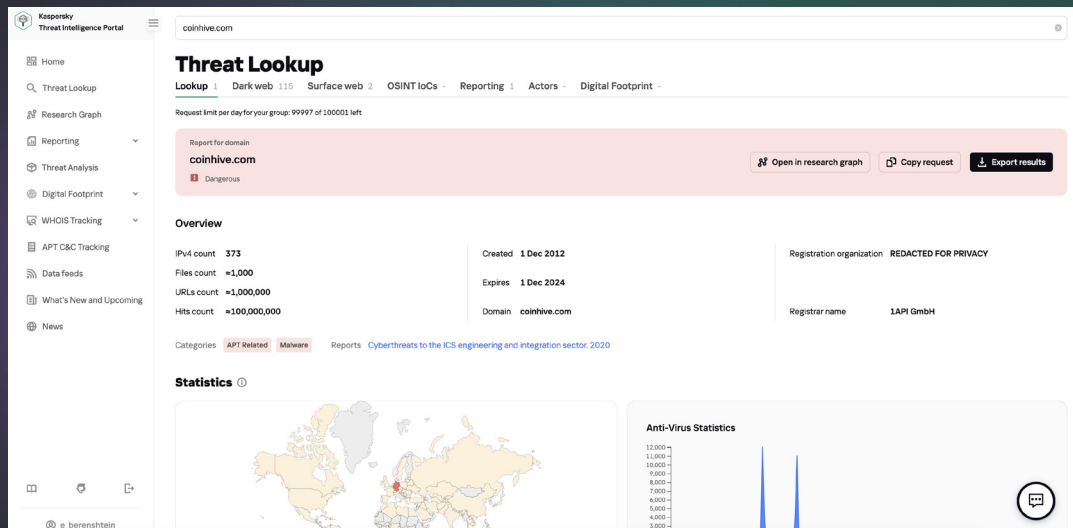
Führen Sie detaillierte Suchen innerhalb der Bedrohungsindikatoren anhand hochzuverlässiger Bedrohungskontexte durch, um Angriffe zu priorisieren und sich auf die Abwehr derjenigen Bedrohungen zu konzentrieren, die das größte Risiko für Ihr Unternehmen darstellen.



Diagnostizieren und analysieren Sie Sicherheitsvorfälle auf Hosts und im Netzwerk effizienter und wirkungsvoller. Priorisieren Sie Signale von internen Systemen gegenüber unbekannten Bedrohungen.



Beschleunigen Sie Ihre Vorfallsreaktion sowie Ihre Threat Hunting-Funktionen, um die „Kill Chains“ zu durchbrechen, bevor kritische System und Daten in Mitleidenschaft gezogen werden.



## Jetzt können Sie

Suchen Sie über eine webbasierte Benutzeroberfläche oder die RESTful-API nach Bedrohungsindikatoren.

Überprüfen Sie zusätzliche Details, darunter Zertifikate, häufig genutzte Bezeichnungen, Dateipfade oder zugehörige URLs, um neue verdächtige Objekte zu ermitteln.

Überprüfen Sie, ob ein entdecktes Objekt weit verbreitet ist oder nur vereinzelt vorkommt.

Verstehen Sie, warum ein Objekt als schädlich eingestuft wird.



# Kaspersky Threat Lookup

Weitere  
informationen

[www.kaspersky.de](https://www.kaspersky.de)

© 2022 AO Kaspersky Lab.  
Eingetragene Marken und Servicemarken sind Eigentum  
ihrer jeweiligen Rechtsinhaber.