
# Kaspersky Threat Lookup

kaspersky PREPARADOS PARA EL FUTURO

# Kaspersky Threat Lookup

La ciberdelincuencia no tiene límites y sus capacidades técnicas mejoran rápidamente. Los ciberdelincuentes utilizan recursos de la Web oculta para amenazar a sus objetivos, por lo que los ataques son cada vez más sofisticados. La frecuencia, la complejidad y la confusión en torno a las ciberamenazas crecen de forma sostenida a medida que se producen nuevos intentos de poner en peligro sus defensas. Los atacantes utilizan complicadas cadenas de ataques, así como tácticas, técnicas y procedimientos (TTP) personalizados en sus campañas para interrumpir las actividades de su negocio, robar sus activos y dañar a sus clientes.

Kaspersky Threat Lookup ofrece todos los conocimientos de Kaspersky sobre las ciberamenazas y sus relaciones reunidos en un único y potente servicio web. El objetivo es proporcionar a los equipos de seguridad la mayor cantidad de datos posible, evitando los ciberataques antes de que afecten a su organización. La plataforma recupera la inteligencia de amenazas más reciente y detallada sobre URL, dominios, direcciones IP, hash de archivos, nombres de amenazas, datos estadísticos y de comportamiento, datos de WHOIS y DNS, atributos de archivos, datos de geolocalización, cadenas de descargas, marcas de tiempo, etc. El resultado es una visibilidad global de las amenazas nuevas y emergentes, que le ayuda a proteger su organización y mejorar sus índices de respuesta ante incidentes.

## Aspectos destacados

Inteligencia de confianza: un atributo clave de Kaspersky Threat Lookup es la fiabilidad de nuestros datos de inteligencia de amenazas, que se mejoran con contexto útil. Kaspersky está a la vanguardia de las pruebas antimalware[1], demostrando la calidad inigualable de nuestra inteligencia de seguridad al proporcionar los más altos índices de detección, sin apenas falsos positivos.

Búsqueda de amenazas: sea proactivo en la prevención, detección y respuesta frente a los ataques para minimizar su impacto y frecuencia. Se debe realizar un seguimiento y eliminar drásticamente los ataques lo antes posible. Cuanto antes se detecte una amenaza, menos daños provocará, más rápido se harán las correcciones y antes podrán volver a la normalidad las operaciones de red.

Investigaciones de incidentes: un gráfico de investigación potencia las investigaciones de incidentes al permitirle explorar visualmente los datos y las detecciones almacenados en Threat Lookup. Proporciona una visualización gráfica de la relación entre las URL, los dominios, las IP, los archivos y otros contextos para que se entienda mejor el alcance completo de un incidente y se identifique su causa raíz.

Búsqueda maestra: busque información en todos los productos de inteligencia de amenazas activas y fuentes externas (incluye los IoC de OSINT, la Web oculta y la Web visible) en una interfaz única y potente.

Interfaz web o API RESTful fáciles de usar: use el servicio en modo manual mediante una interfaz web (a través de un navegador web) o acceso a través de una sencilla API RESTful, según las preferencias.

Amplia gama de formatos de exportación: exporte IOC (Indicadores de compromiso) o contexto útil sobre los formatos de uso compartido legibles por máquina más ampliamente utilizados y más organizados, como STIX, OpenIOC, JSON, Yara, Snort o incluso CSV, para disfrutar de todas las ventajas de la inteligencia de amenazas, automatizar el flujo de trabajo de operaciones o integrarlos en los controles de seguridad como SIEM.

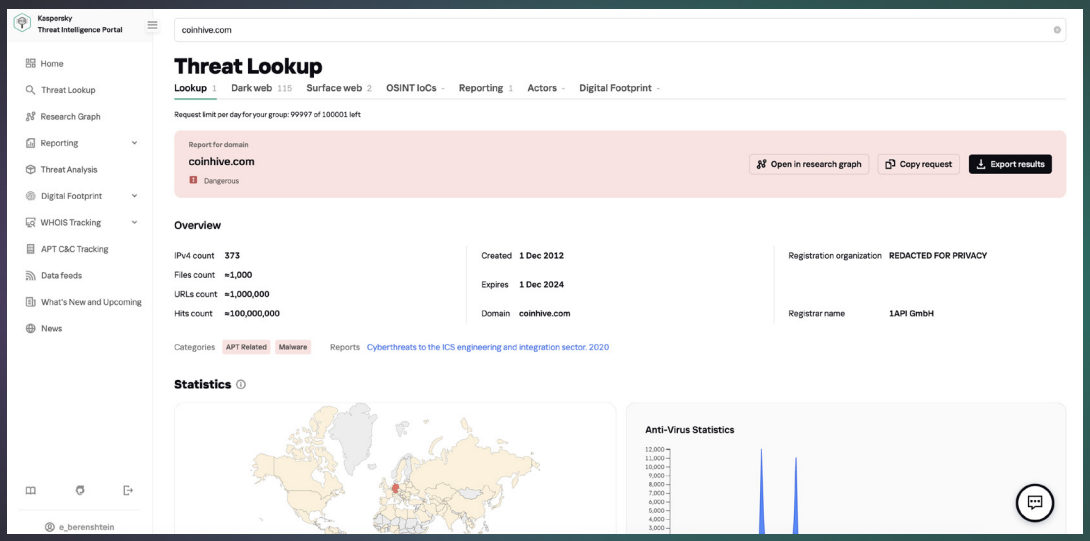
## Ventajas

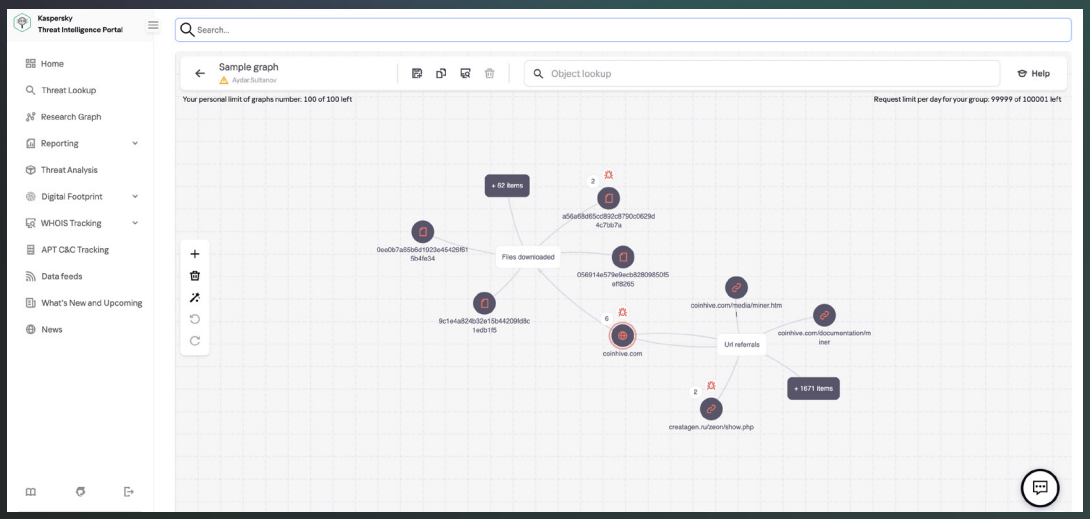
Realice búsquedas exhaustivas sobre indicadores de amenaza con un contexto de amenazas altamente validado que le permite priorizar los ataques y enfocarse en mitigar las amenazas que impliquen el mayor riesgo para su negocio.

Diagnostique y analice de forma más eficiente y efectiva los incidentes de seguridad de los hosts y la red, y priorice las señales de los sistemas internos frente a amenazas desconocidas.

Potencie sus capacidades de respuesta ante incidentes y de búsqueda de amenazas para alterar el esquema del ataque antes de que los sistemas y datos importantes se vean comprometidos.

[1] kaspersky.com/top3




## Ahora puede

- Buscar indicadores de amenaza desde una interfaz web o la API RESTful.
- Examinar datos avanzados, como certificados, nombres usados habitualmente, rutas de archivos o URL relacionadas, para detectar nuevos objetos sospechosos.
- Comprobar si el objeto detectado es común o único.
- Comprender por qué un objeto se debe tratar como malicioso.


**www.kaspersky.es**