Kaspersky Threat Lookup

kaspersky PREPARADOS PARA O FUTURO

Kaspersky Threat Lookup

O crime virtual não tem fronteiras e as capacidades técnicas estão melhorando rapidamente: os ataques estão cada vez mais sofisticados, pois os criminosos virtuais utilizam recursos da Dark Web para ameaçar seus alvos. As ameaças virtuais estão em constante crescimento em termos de frequência, complexidade e ofuscação, à medida que novas tentativas são realizadas para comprometer suas defesas. Os invasores utilizam cadeias de destruição complicadas, e táticas, técnicas e procedimentos (TTP) personalizados nas campanhas para perturbar as suas operações, roubar os seus ativos ou causar danos aos seus clientes.

O Kaspersky Threat Lookup oferece todo o conhecimento adquirido pela Kaspersky sobre ameaças virtuais e respectivas relações, reunindo tudo em um serviço da Web único e poderoso. O objetivo é fornecer às suas equipes de segurança o maior número de dados possível, prevenindo os ataques virtuais antes que afetem sua organização. A plataforma obtém a inteligência de ameaças detalhada mais recente sobre URL, domínios, endereços IP, hashes de arquivos, nomes de ameaças, dados estatísticos/comportamentais, dados de WHOIS/DNS, atributos de arquivos, dados de geolocalização, cadeias de download, carimbos de data/hora, etc. O resultado é a visibilidade global de ameaças novas e emergentes, ajudando você a proteger a sua organização e a melhorar a resposta a incidentes.

Destaques

Inteligência confiável: um atributo fundamental do Kaspersky Threat Lookup é a confiabilidade dos nossos dados de inteligência de ameaças, enriquecidos com contexto acionável. A Kaspersky é líder no campo dos testes antimalware[1], demonstrando a qualidade inigualável da nossa inteligência de segurança ao fornecer as mais altas taxas de detecção, com quase zero falsos positivos

Busca de ameaças: seja proativo na prevenção, detecção e resposta a ataques, para minimizar o seu impacto e frequência. Rastreie e elimine severamente os ataques o mais cedo possível. Quanto antes conseguir descobrir uma ameaça, menos danos são causados, mais rapidamente são efetuadas reparações, e mais cedo as operações de rede podem voltar ao normal

Investigações de incidentes: um gráfico de pesquisas impulsiona as investigações de incidentes permitindo que você explore visualmente dados e detecções armazenadas no Threat Lookup. Ele fornece uma visualização gráfica da relação entre URLs, domínios, IPs, arquivos e outros contextos para que você possa compreender melhor o escopo total de um incidente, além de identificar a causa-raiz dele.

Pesquisa principal: busque informações em todos os produtos ativos de inteligência de ameaças e fontes externas (incluindo OSINT IoCs, Dark Web e Superfície da web) em uma interface única e robusta.

Interface Web ou API RESTful fáceis de usar: Use o serviço em modo manual através de uma interface online (através de um navegador Web) ou acesse através de uma API RESTful simples, como você preferir

Vasta gama de formatos de exportação: exporte IOCs (indicadores de comprometimento) ou contexto acionável para formatos de compartilhamento de leitura por máquinas amplamente utilizadas e mais organizadas, como STIX, OpenIOC, JSON, Yara, Snort ou mesmo CSV, para desfrutar da totalidade dos benefícios da inteligência de ameaças, automatizar o fluxo de trabalho das operações ou integrar em controles de segurança como SIEMs.

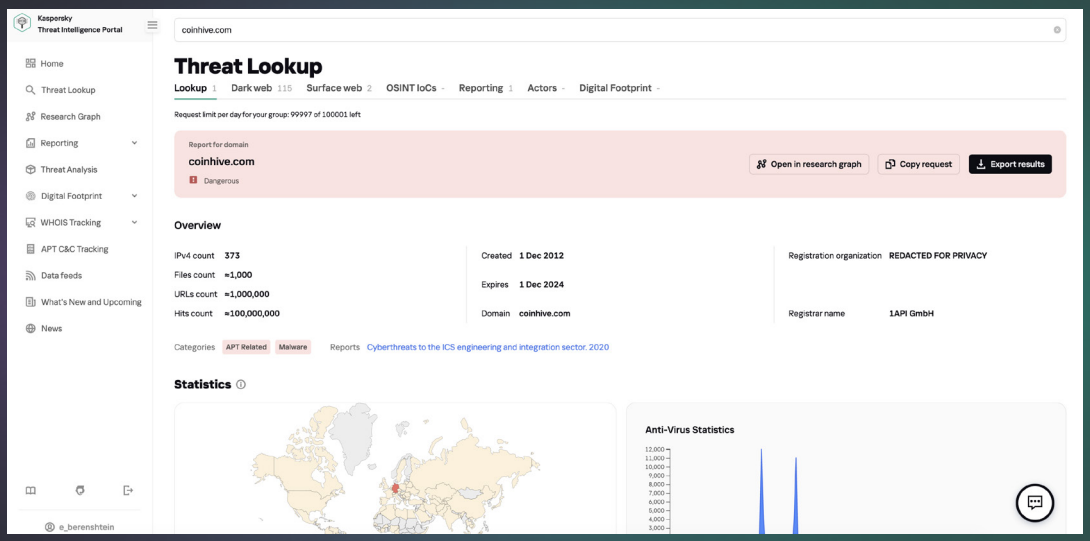
Benefícios

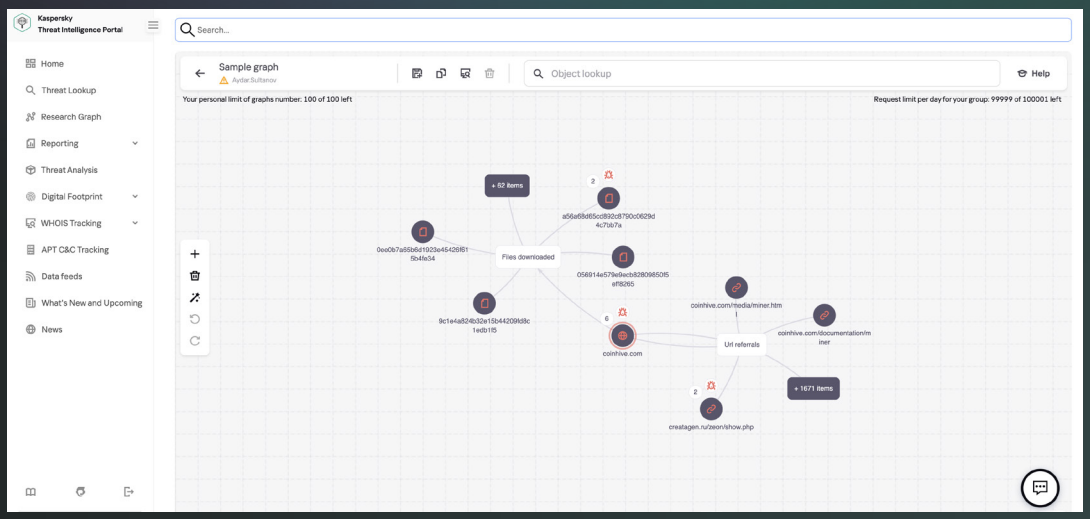
Conduza pesquisas profundas sobre indicadores de ameaças em um contexto altamente validado que permite priorizar ataques e focar na mitigação de ameaças que trazem maior risco ao seu negócio

Faça diagnósticos e análises de incidentes de segurança em hosts e na rede de maneira mais eficiente e eficaz, além de priorizar sinais de sistemas internos contra ameaças desconhecidas

Aprimore sua resposta a incidentes e funcionalidades de busca de ameaças para desfazer a cadeia perigosa antes que sistemas e dados cruciais sejam comprometidos

[1] kaspersky.com.br/top3





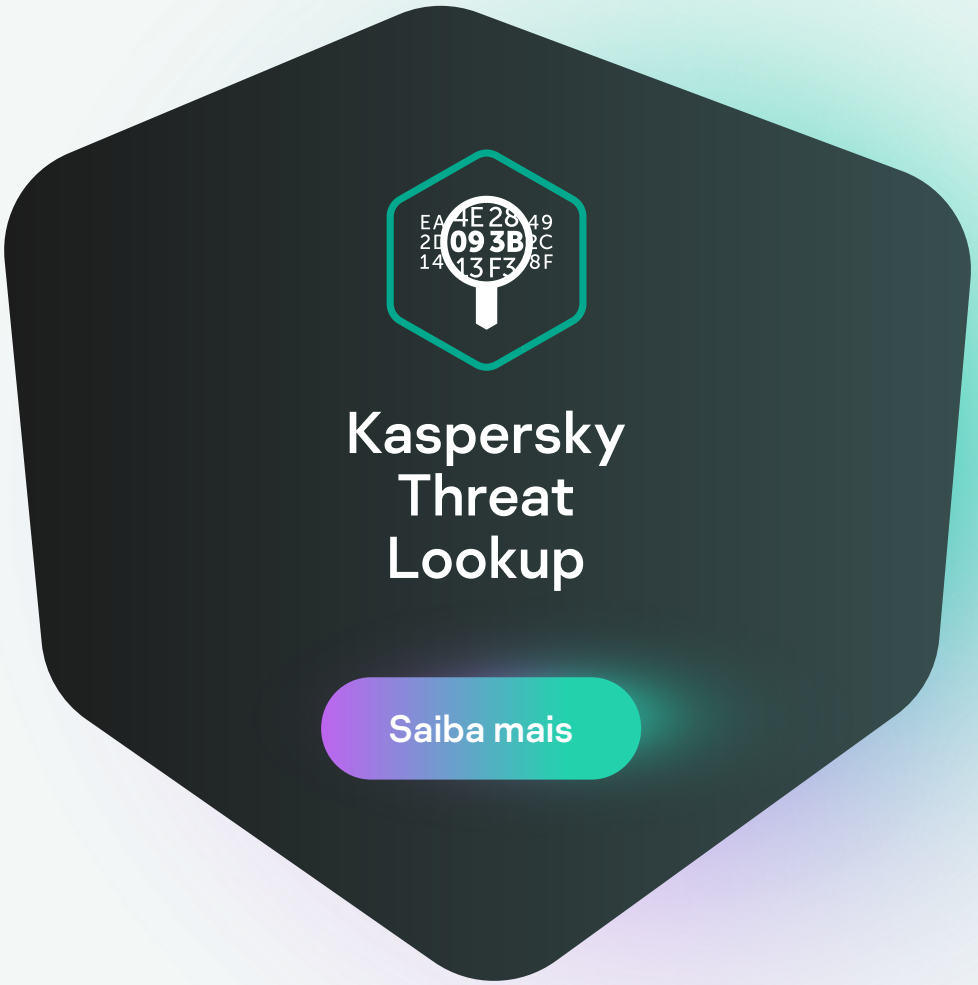
Agora você pode

Procurar indicadores de ameaças através de uma interface baseada na Web ou através da API RESTful.

Examinar detalhes avançados, incluindo certificados, nomes normalmente utilizados, caminhos de arquivo ou URLs relacionadas para descobrir novos objetos suspeitos.

Verificar se o objeto descoberto é comum ou único.

Compreender o motivo pelo qual um objeto deve ser tratado como malicioso.



www.kaspersky.com.br