Kaspersky Threat Lookup

kaspersky BRING ON THE FUTURE

Kaspersky Threat Lookup

Il cybercrime non conosce confini e le capacità tecniche mostrano un rapido miglioramento: gli attacchi diventano sempre più sofisticati e i criminali informatici utilizzano le risorse del Dark Web per raggiungere i propri obiettivi. Le minacce informatiche registrano una costante crescita in termini di frequenza, complessità e tecniche di offuscamento, con un numero sempre maggiore di tentativi di compromissione delle soluzioni di protezione. I cybercriminali, nelle loro campagne, utilizzano complessi attacchi a catena, tattiche, tecniche e procedure personalizzate (TTP) mirate a interrompere le attività aziendali, carpire le risorse o danneggiare i clienti dell'impresa.

Kaspersky Threat Lookup fornisce tutte le conoscenze acquisite da Kaspersky sulle minacce informatiche e sulle relazioni tra di esse, riunite in un unico e potente servizio Web. L'obiettivo è fornire ai team di sicurezza la maggior quantità possibile di dati, per prevenire gli attacchi informatici prima che compromettano l'organizzazione. La piattaforma recupera le informazioni dettagliate più recenti in termini di Threat Intelligence riguardo a URL, domini, indirizzi IP, hash di file, denominazioni delle minacce, dati statistici/comportamentali, dati WHOIS/DNS, attributi di file, dati di geolocalizzazione, catene di download, timestamp. Il risultato è una visibilità globale delle minacce nuove ed emergenti: ciò consente di proteggere al meglio la propria azienda, migliorando sensibilmente qualità ed efficienza delle attività di incident response.

Caratteristiche principali

Intelligence altamente affidabile: un elemento chiave di Kaspersky Threat Lookup è l'elevata affidabilità dei nostri dati di Threat Intelligence. Kaspersky si colloca in testa rispetto ai test condotti sulle soluzioni anti-malware[1], grazie all'impareggiabile qualità della nostra security intelligence e ai tassi di rilevamento estremamente elevati, con falsi positivi vicini allo zero

Ricerca delle minacce: massima proattività nella prevenzione, nel rilevamento e nella risposta agli attacchi, al fine di ridurne al minimo l'impatto e la frequenza. Monitoraggio e tempestiva eliminazione degli attacchi nel minor tempo possibile. Quanto prima viene rilevata la minaccia, tanto minore sarà il danno causato. Quanto più rapidamente vengono prese misure correttive, tanto prima potranno tornare al loro normale funzionamento le attività di rete

Indagini sugli incidenti: un grafico di ricerca ottimizza le indagini sugli incidenti consentendo di esplorare visivamente i dati e i rilevamenti archiviati in Threat Lookup. Offre una visualizzazione grafica della relazione tra URL, domini, file e altri contesti per comprendere meglio l'ambito completo di un incidente e identificarne le cause principali

Ricerca master: consente la ricerca di informazioni in tutte le fonti esterne e i prodotti di Threat Intelligence attivi (inclusi IoC OSINT, Dark Web e Surface Web) in un'interfaccia unica e potente

Interfaccia Web o API RESTful facili da usare: si può utilizzare il servizio in modalità manuale attraverso un'apposita interfaccia Web (tramite browser Web) o accedervi tramite API RESTful, a seconda delle preferenze.

Ampia gamma di formati di esportazione: è possibile esportare gli IoC (indicatori di compromissione) o i dati relativi al contesto finalizzato all'azione nei formati di condivisione machine-readable maggiormente utilizzati e organizzati, come STIX, OpenIOC, JSON, Yara, Snort o addirittura CSV, per ottenere tutti i vantaggi offerti dalla Threat Intelligence, automatizzare il flusso di lavoro operativo o effettuare la relativa integrazione con controlli di sicurezza come SIEM

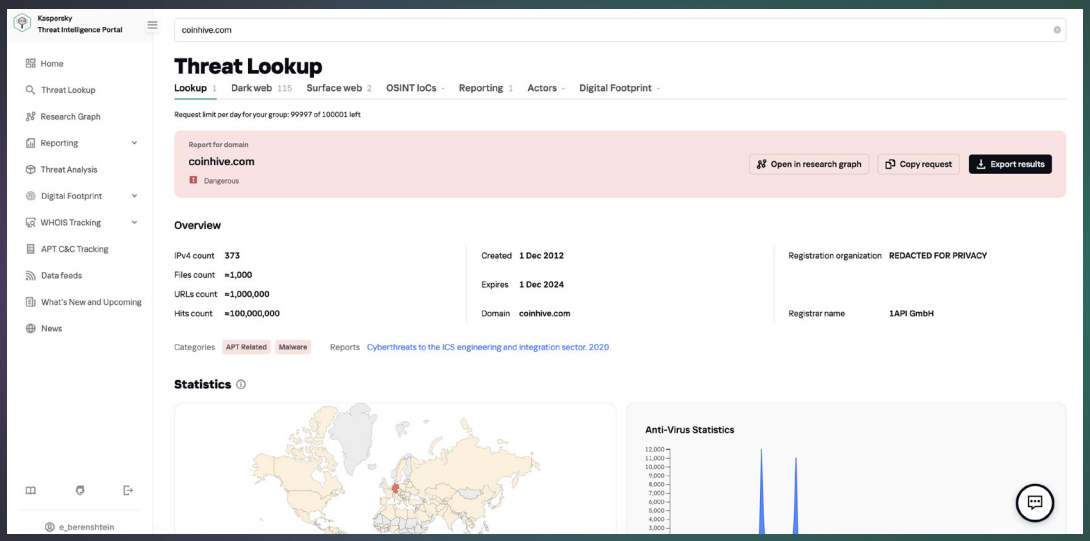
Vantaggi

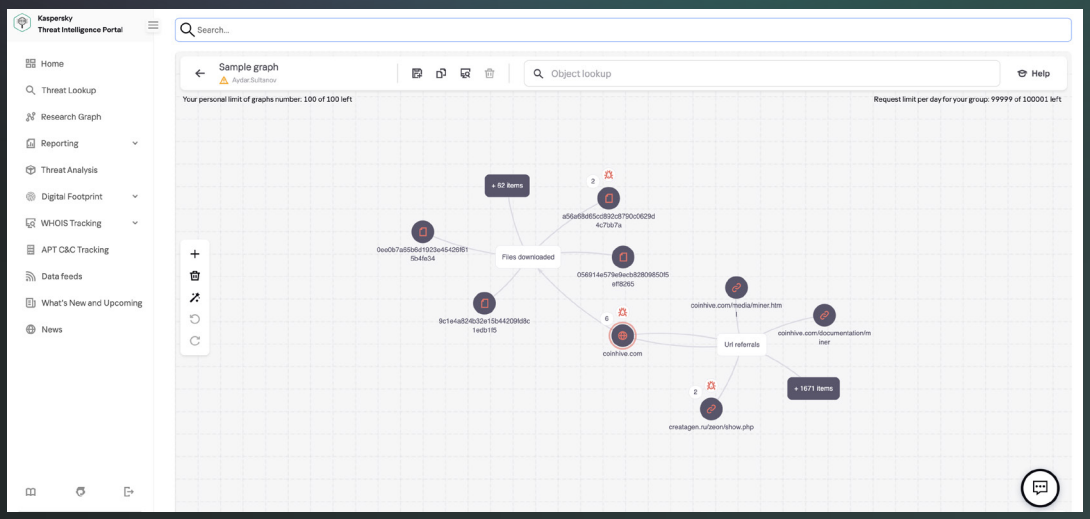
Ricerche approfondite sugli indicatori delle minacce con un contesto comprovato che consenta di assegnare la priorità agli attacchi e concentrarsi sulla mitigazione delle minacce più rischiose per l'azienda

Diagnosi e analisi degli incidenti di sicurezza negli host e nella rete in modo più efficace ed efficiente e assegnazione delle priorità ai segnali dei sistemi interni contro le minacce sconosciute

Ottimizzazione della risposta agli incidenti e delle funzionalità di ricerca delle minacce per interrompere la kill chain prima che vengano compromessi dati e sistemi critici

[1] kaspersky.com/top3





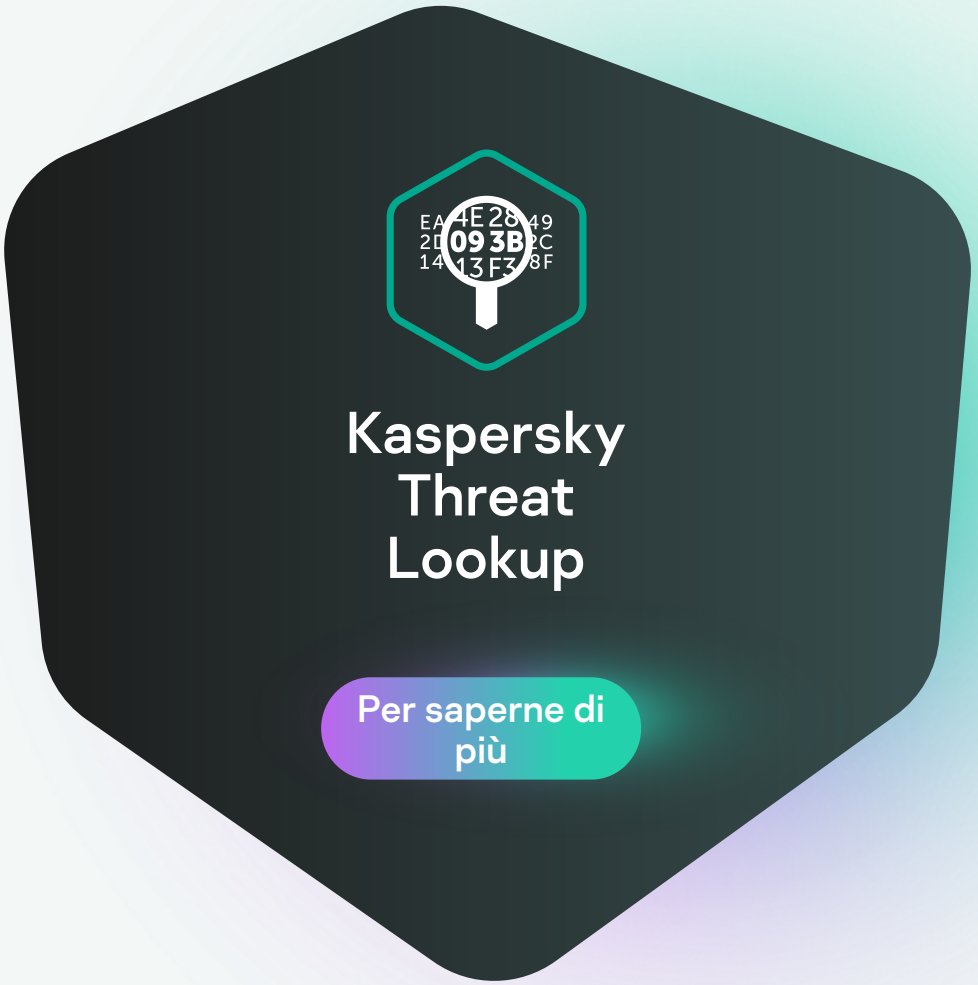
Adesso è possibile

Cercare gli indicatori delle minacce attraverso un'interfaccia basata sul Web o tramite l'API RESTful

Analizzare dettagli avanzati tra cui certificati, nomi comunemente utilizzati, percorsi di file o URL correlati per scoprire nuovi oggetti sospetti

Controllare se l'oggetto rilevato è unico o ampiamente diffuso

Comprendere il motivo per cui un oggetto si deve considerare dannoso



www.kaspersky.it

© 2022 AO Kaspersky Lab.
I marchi registrati e i marchi di servizio appartengono ai rispettivi proprietari.