Kaspersky Research Sandbox

Kaspersky Threat Attribution Engine

Kaspersky Similarity

Kaspersky Threat Analysis

kaspersky bring on the future

Kaspersky Threat Analysis

Kaspersky Threat Analysis

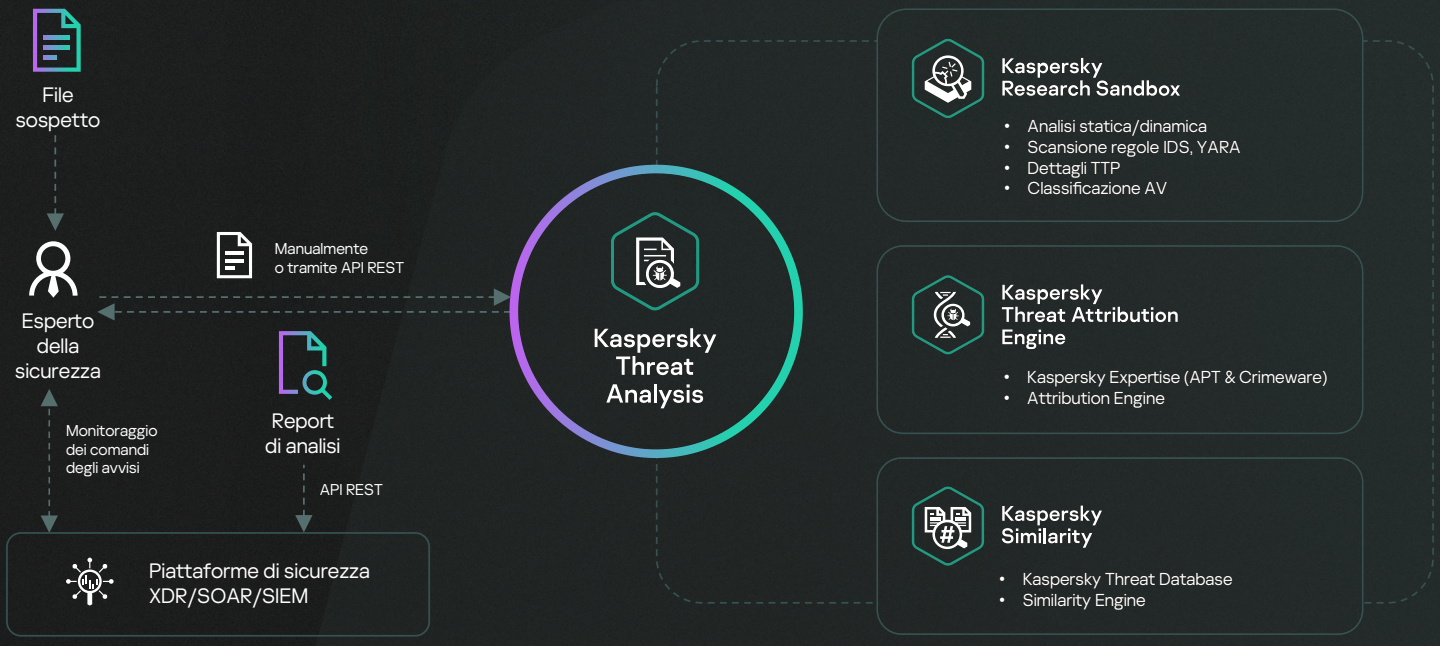
Di fronte a una potenziale minaccia informatica, le decisioni prese e la capacità di prenderle possono rivelarsi fondamentali. È impossibile prevenire gli attacchi mirati odierni esclusivamente con i tradizionali strumenti anti-virus. I motori anti-virus sono in grado di bloccare solo le minacce conosciute e le loro varianti, mentre i sofisticati threat actor fanno uso di tutti i mezzi a loro disposizione per eludere il rilevamento automatico. Il numero degli avvisi elaborati ogni giorno dai SOC sta crescendo in modo esponenziale. Con la quantità di campioni di malware generati ogni giorno, una gestione efficace delle priorità, del triage e della convalida degli avvisi diventa quasi impossibile.

La combinazione di threat intelligence, analisi dinamica, attribuzione delle minacce e tecnologie di similarity offre un potente strumento per il rilevamento degli oggetti dannosi ancora sconosciuti. Per aiutare i ricercatori nel campo della sicurezza a rimanere informati sulle minacce esistenti ed emergenti, Kaspersky fornisce un unico framework resiliente per automatizzare l'analisi di routine dei file sospetti.

Oltre alle tecnologie di analisi delle minacce tradizionali come la sandbox, Kaspersky Threat Analysis fornisce tecnologie di attribuzione e similarity all'avanguardia, attraverso un approccio ibrido che fornisce un'analisi efficiente delle minacce. In tal modo, potete prendere decisioni pienamente informate e mantenere al sicuro la vostra infrastruttura.

Kaspersky Threat Analysis viene fornito tramite interfacce Web e RESTful unificate e consente agli utenti di impostare parametri specifici per analizzare oggetti sospetti in modo altamente efficiente. Diversi strumenti di analisi delle minacce si combinano per consentire a voi e al vostro team di analizzare la situazione da tutte le prospettive, grazie a report completi e dettagliati, e di rispondere in modo rapido ed efficace.

Come funziona



Kaspersky
Threat Analysis

Kaspersky
Research
Sandbox

Tecnologie di sandboxing

sono potenti strumenti di analisi dinamica che consentono di indagare sulle origini dei campioni di file, raccogliere IOC in base all'analisi comportamentale e identificare oggetti dannosi non rilevati dai tradizionali strumenti anti-virus.

Sono disponibili versioni cloud e on-premises.

Sandbox

Kaspersky Research Sandbox è stato sviluppato direttamente dal nostro laboratorio dedicato al sandboxing: si tratta di un'avanzata tecnologia, in costante evoluzione da oltre vent'anni. Integra tutte le conoscenze sul comportamento del malware acquisite nel corso degli anni di costante ricerca sulle minacce e ci permette di rilevare ogni giorno più di 420.000 nuovi oggetti dannosi. Fornisce un innovativo approccio ibrido, capace di combinare perfettamente l'analisi comportamentale e sofisticate tecniche anti-elusione con tecnologie in grado di simulare il fattore umano.

Questa tecnologia, distribuita on-premises, previene l'esposizione dei dati aziendali all'esterno dell'organizzazione. Kaspersky Research Sandbox on-premises consente inoltre la creazione di ambienti di esecuzione personalizzati per l'analisi, adattandoli agli ambienti reali: ciò aumenta l'accuratezza del rilevamento delle minacce e la velocità delle indagini.

Perché usarlo?

I file sospetti, non rilevati dagli strumenti anti-virus, possono rivelare le loro caratteristiche dannose solo attraverso il loro comportamento. Kaspersky Research Sandbox consente di emulare il comportamento ed evidenziare le azioni pericolose.

Principali caratteristiche del prodotto

Analisi automatica degli oggetti negli ambienti Windows, Linux e Android

Le immagini personalizzate consentono l'analisi delle minacce tra i sistemi operativi e le applicazioni Windows (solo quelle che si applicano agli ambienti reali)

La percentuale di minacce basata su metriche e dati ottenuti durante l'esecuzione del file mostra il livello di pericolosità dell'oggetto analizzato

Avanzate tecniche anti-elusione e tecnologie di simulazione del fattore umano

Caricamento manuale dei campioni e API REST ottimizzata per l'integrazione con flussi di lavoro automatizzati

Supporto per l'analisi di oltre 200 tipi di file con report di analisi dettagliati

È possibile aggiungere regole Suricata personalizzate per esaminare il traffico di rete e utilizzarle insieme alle regole Suricata

Oltre 1.000 ricerche univoche per estrarre TTP tramite MITRE ATT&CK

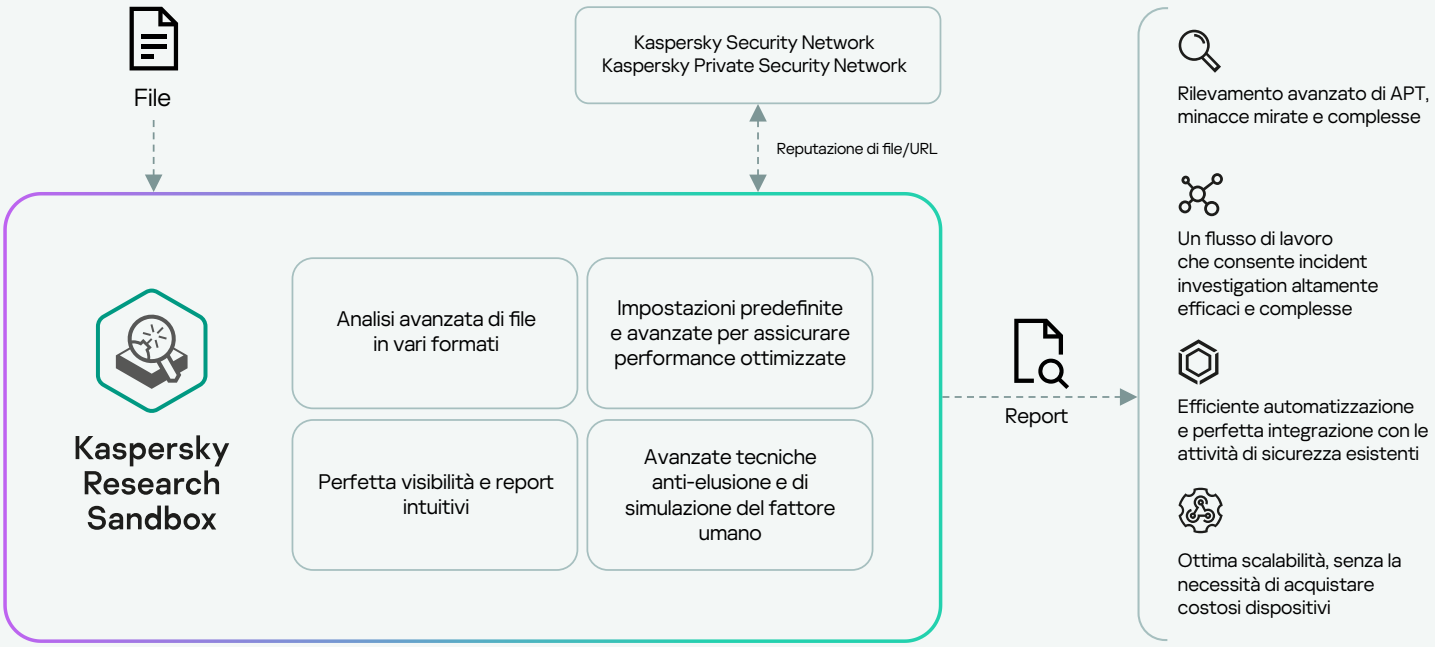
Supporto per la modalità interattiva (previsto nel primo trimestre del 2024)

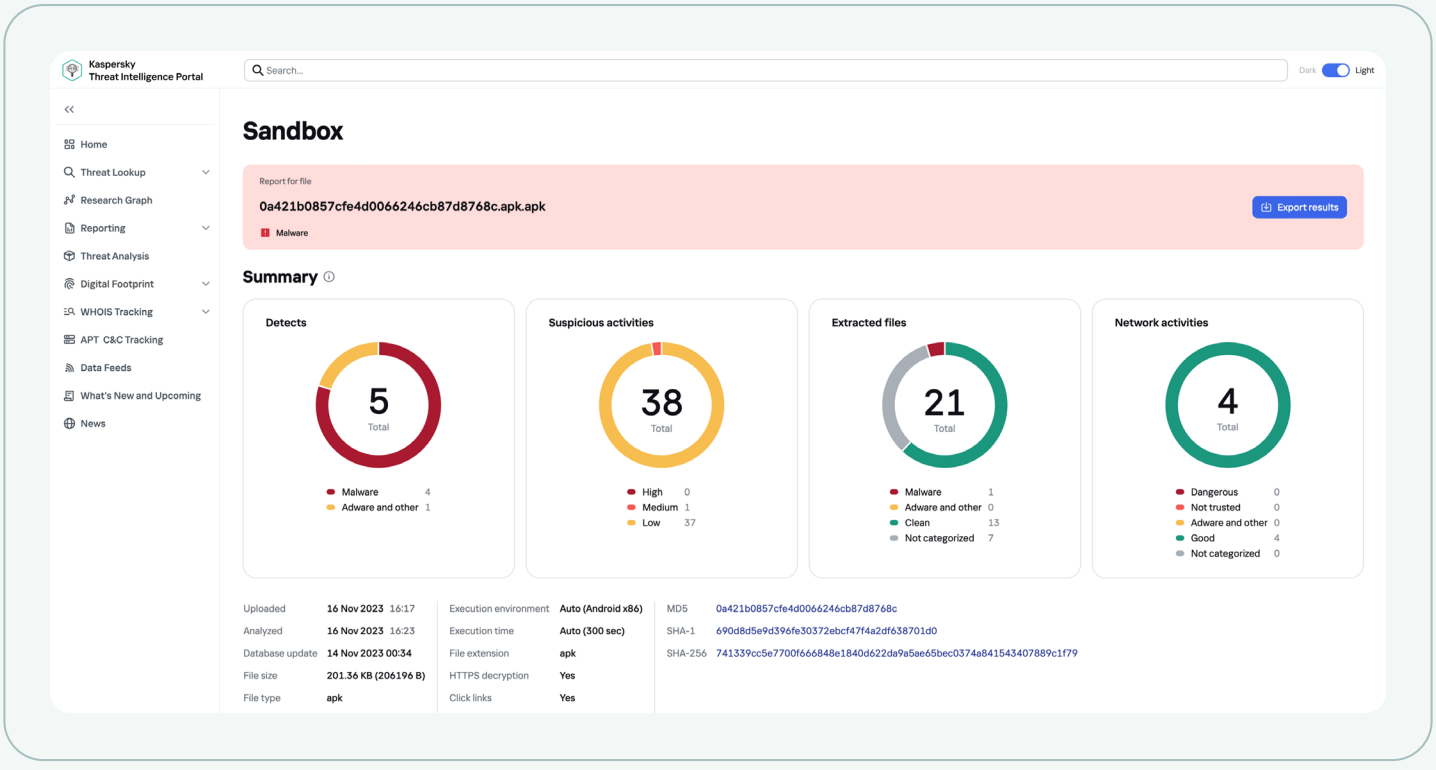
Il prodotto supporta la distribuzione bare metal. La configurazione hardware dipende dalle prestazioni desiderate ed è facilmente scalabile. Richiede almeno una connessione ISP indipendente (due o più sono consigliate per la tolleranza di errore), 100 Mbps per ciascun canale.

Kaspersky Research Sandbox si basa su una tecnologia proprietaria brevettata (brevetto n. US10339301). Creando le esatte condizioni che attivano l'esecuzione del malware, consente ai ricercatori di analizzare file e URL sospetti con un unico tentativo.

Per evitare il rilevamento, un file dannoso può dapprima verificare se si trova in una macchina virtuale, o può rimanere inattivo fin quando la sandbox non risulta più operativa. In simili casi, la nostra tecnologia brevettata accelera il flusso temporale all'interno della macchina virtuale, in modo da forzare l'esecuzione anticipata del codice dannoso.

Schema operativo generale della soluzione Kaspersky Research Sandbox





Report di analisi dettagliati

Una volta completata l'analisi, Research Sandbox fornisce un report dettagliato sul comportamento e sulle specifiche funzionalità del campione esaminato, consentendo di definire le procedure di risposta più appropriate:

Riepilogo	Informazioni generali sui risultati di esecuzione di un file/esplorazione delle URL.
Nomi di rilevamento	Un elenco dei rilevamenti (sia anti-virus che comportamentali) registrati durante l'esecuzione del file.
Regole di rete attivate	Un elenco delle regole di rete Suricata attivate dall'oggetto eseguito durante l'analisi del traffico.
Mappa dell'esecuzione	Una sequenza di attività degli oggetti rappresentata graficamente e la relazione tra essi.
Attività sospette	Attività sospette: elenco delle attività sospette registrate.
Schermate	Una serie di schermate acquisite durante l'esecuzione del file/l'esplorazione dell'URL.
Immagini PE caricate	Un elenco delle immagini PE caricate, rilevate durante l'esecuzione del file o l'esplorazione dell'URL.
Operazioni sui file	Un elenco delle operazioni sui file registrate durante l'esecuzione del file/l'esplorazione dell'URL.
Operazioni sul registro	Un elenco delle operazioni eseguite sul registro del sistema operativo, rilevate durante l'esecuzione del file/l'esplorazione delle URL.
Operazioni sui processi	Un elenco delle interazioni del file con i vari processi, registrate durante l'esecuzione del file.
Operazioni di sincronizzazione	Un elenco delle operazioni relative agli oggetti di sincronizzazione creati (mutex, evento, semaphore), registrate durante l'esecuzione del file/l'esplorazione delle URL.
File scaricati	Un elenco di file estratti dal traffico di rete durante l'esecuzione del file/l'esplorazione dell'URL.
File creati	Un elenco dei file salvati (creati o modificati) dal file eseguito.
HTTPS/HTTP/DNS/IP/TCP/UDP e così via.	Dettagli di richieste/sessioni di rete registrati durante l'esecuzione del file/l'esplorazione dell'URL
Dump del traffico di rete (PCAP)	È possibile esportare l'attività di rete in formato PCAP.
Matrice MITRE ATT&CK	Tutte le attività dei processi identificate e registrate durante l'emulazione sono presentate sotto forma di matrice MITRE ATT&CK.

Kaspersky
Threat Analysis

Kaspersky
Threat Attribution
Engine

Attribuzione delle minacce

Monitorare, analizzare, interpretare e ridurre le minacce alla sicurezza IT in continua evoluzione è un impegno di enorme portata. Mettendo da parte tutto il clamore, la threat intelligence ha un valore reale e l'attribuzione delle minacce è un elemento critico.

Sono disponibili versioni cloud e on-premises.

Attribuzione

Kaspersky Threat Attribution Engine è uno strumento unico di analisi delle minacce che fornisce informazioni sull'origine del malware di alto profilo e sui suoi possibili autori. Connette rapidamente un file sospetto a minacce APT note, autori degli attacchi e campagne, utilizzando un algoritmo unico e uno speciale database che comprende campioni di malware APT e la più vasta raccolta del settore di file puliti, raccolti dagli esperti Kaspersky nel corso di oltre 25 anni.

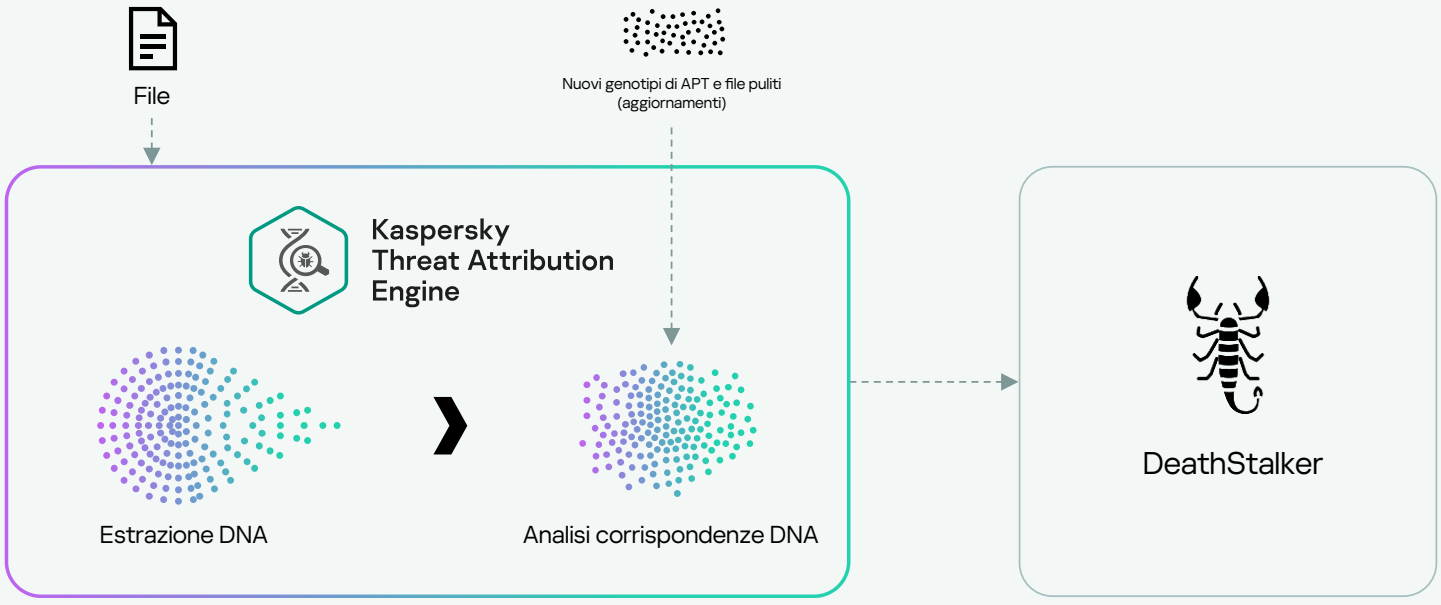
Monitoriamo oltre 1.100 threat actor e campagne e pubblichiamo oltre 200 report di threat intelligence all'anno. Le nostre continue attività di ricerca supportano una raccolta APT che contiene più di 80.000 file che, insieme all'uso di strumenti automatizzati, si traducono in livelli di attribuzione eccezionalmente accurati.

Il prodotto offre un approccio unico per il confronto di campioni simili, garantendo al tempo stesso tassi di falsi positivi prossimi allo zero. Qualsiasi nuovo attacco può essere rapidamente collegato a malware APT noto, attacchi mirati precedenti e gruppi di hacker, aiutandovi a distinguere le minacce ad alto rischio dagli incidenti meno gravi, in modo da poter adottare misure di protezione tempestive per impedire all'autore dell'attacco di penetrare nel sistema. Kaspersky Threat Attribution Engine si può implementare in ambienti air-gap sicuri, atti a limitare l'accesso di terze parti alle informazioni elaborate e agli oggetti analizzati.

Perché usarlo?

L'attribuzione di un file a un certo threat actor, insieme alla conoscenza di questo threat actor, consente di posizionare l'esempio nella kill chain complessiva specifica per questo avversario. A sua volta, fornisce informazioni su dove cercare altri IoC/IoA, per evitare il rischio di perdere l'intero attacco bloccando solo un particolare file.

Schema operativo generale della soluzione Kaspersky Threat Attribution Engine



Principali caratteristiche del prodotto

Fornisce un accesso istantaneo a un archivio di dati selezionati su migliaia di gruppi APT, campioni e minacce più ampie (tramite il motore anti-virus)

Approfondimenti unici su campagne di alto profilo (oltre 400) su cui hanno svolto indagini gli esperti Kaspersky

Consente di assegnare in modo efficiente la priorità delle minacce, in modo automatico o manuale, e di attivare il processo di triage

Possibilità di aggiungere campioni e attori privati, configurando il prodotto per identificare campioni simili ai file presenti nella raccolta privata

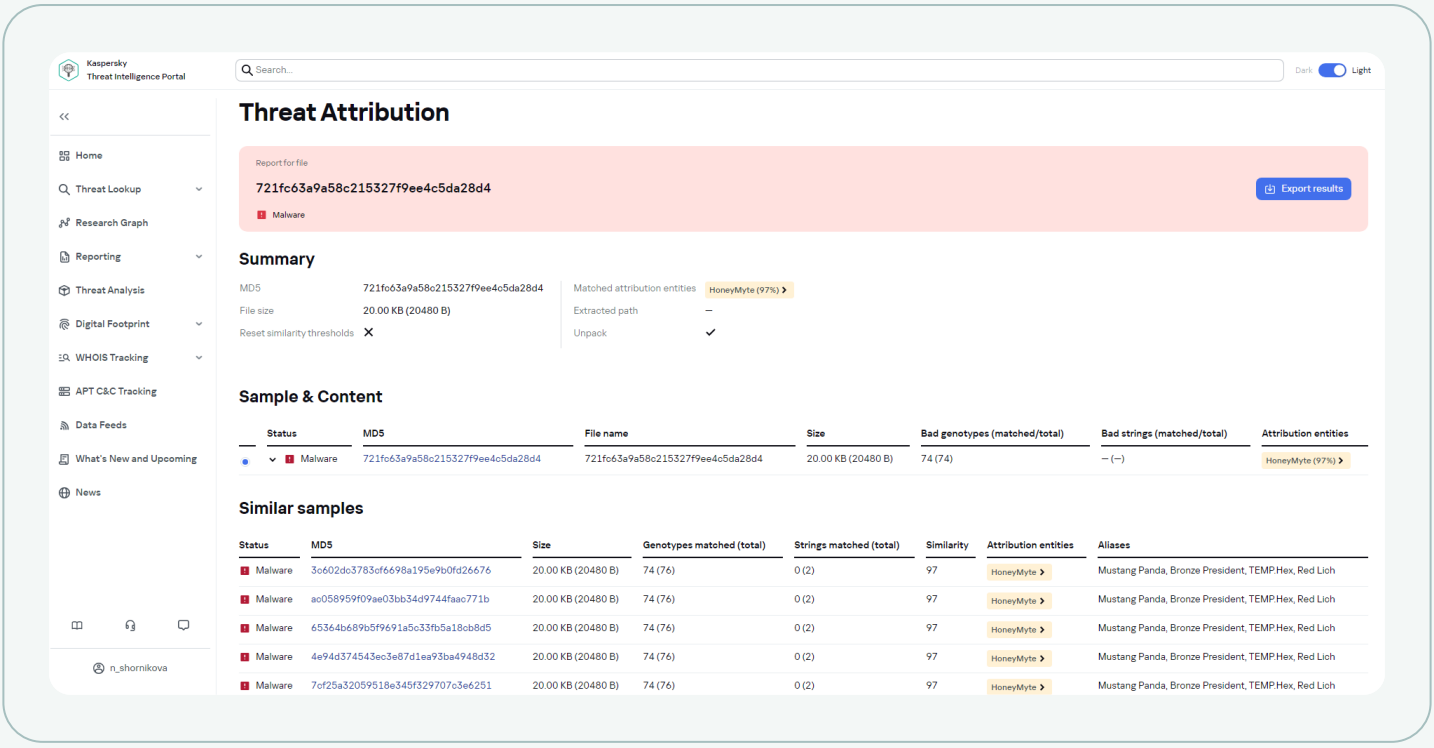
Caricamento manuale dei campioni e API REST ottimizzata per l'integrazione con flussi di lavoro automatizzati

Supporta la distribuzione in infrastrutture cloud come Amazon Web Services (AWS), consentendo una rapida configurazione del prodotto e assicurando un risparmio sui costi, in quanto non richiede investimenti hardware in anticipo

Esportazione in regole YARA per ulteriori attività di ricerca/scansione automatizzata di file simili o integrazione con soluzioni di terze parti

Esportazione in formato STIX 2.1 (sono supportati anche i formati TXT e JSON) per ulteriori attività di analisi automatizzata dei log di sicurezza o l'integrazione con soluzioni/controlli di sicurezza di terze parti

Funzionalità per la decompressione degli archivi protetti da password con password personalizzate



Metodo di ricerca proprietario

Per collegare il malware alle entità di attribuzione, Kaspersky Threat Attribution Engine utilizza un metodo esclusivo e proprietario per la ricerca dei genotipi simili e delle stringhe tra i file. Questo metodo comprende:

Analisi della genetica di un campione

con l'estrazione dei seguenti elementi dal codice:

- Genotipi: pezzi distintivi di codice binario
- Stringhe: stringhe distintive di caratteri

Ricerca automatica nei file analizzati

di genotipi, stringhe simili a genotipi e stringhe di campioni APT precedentemente analizzati o già collegati a entità di attribuzione

Sulla base dei genotipi e delle stringhe simili

rilevati nei campioni APT, viene generato un rapporto sull'origine del campione analizzato, le entità di attribuzione correlate e le eventuali somiglianze con campioni APT noti

Kaspersky
Threat Analysis

Kaspersky
Similarity

Somiglianza dei file

Per costruire una linea di difesa efficace, non è sempre necessario conoscere il nemico. Kaspersky Similarity consente di identificare esempi di file con funzioni simili, per proteggervi da minacce sconosciute ed elusive.

La versione cloud è disponibile tramite Kaspersky Threat Intelligence Portal.

Similarity

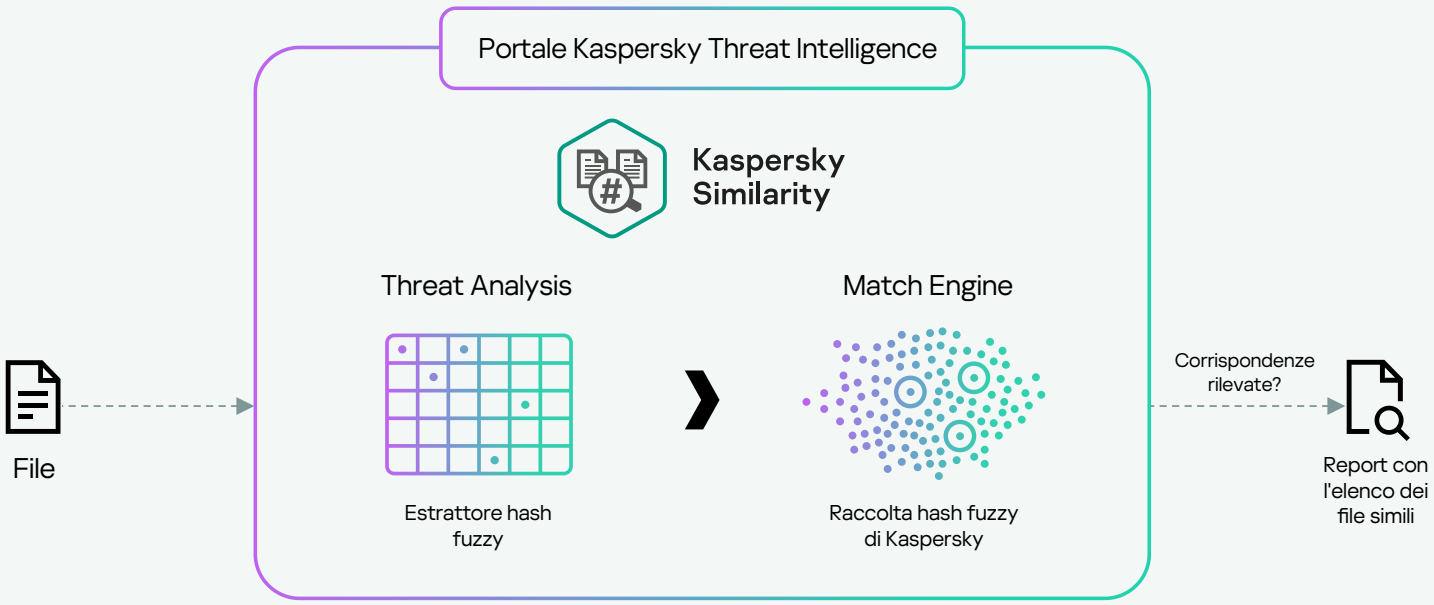
Kaspersky Similarity è una funzionalità aggiuntiva disponibile tramite Threat Intelligence Portal, sia per gli utenti di Kaspersky Research Sandbox che di Kaspersky Threat Attribution Engine, che aiuta a identificare i file che si presentano e si comportano in modo simile.

I file simili vengono cercati e calcolati per il file originale utilizzando la tecnologia all'avanguardia inventata dagli esperti di Kaspersky, che sfrutta più di 50 tipi di hash di somiglianza univoci. Ciò consente di garantire risultati di somiglianza accurati e altamente sicuri.

Perché usarlo?

Trovate i malware simili (ad esempio, elusivi) e cercateli nella vostra infrastruttura per essere sicuri che una leggera modifica del campione, apportata dall'avversario, venga comunque rilevata dagli strumenti di sicurezza. La tecnologia si distingue dall'attribuzione: è possibile trovare file malware simili anche se non attribuiti.

Schema operativo generale di Kaspersky Similarity



Report di somiglianza

Ogni file ha specifici formati, packer, sezioni, stringhe, tabelle di importazione e così via. Gli esperti di Kaspersky hanno creato una serie di hash per determinare la somiglianza tra diversi file in base a questi attributi. Kaspersky Similarity consente agli utenti di inviare un file sospetto, estrarne gli hash fuzzy e confrontarli con gli hash fuzzy dei file esistenti nel database delle minacce Kaspersky. Nel caso vengano trovate corrispondenze, genera l'elenco degli hash per i principali file dannosi simili, già noti a Kaspersky e ordinati per punteggio di somiglianza. Il report contiene il contesto aggiuntivo con metadati per ogni file simile:

- Attendibilità della somiglianza
- Stato del file (malware, adware o altro)
- Nome della minaccia
- Timestamp del primo e dell'ultimo rilevamento
- Quantità di riscontri (rilevamenti)
- Hash dei file
- Tipo di file
- Dimensione file

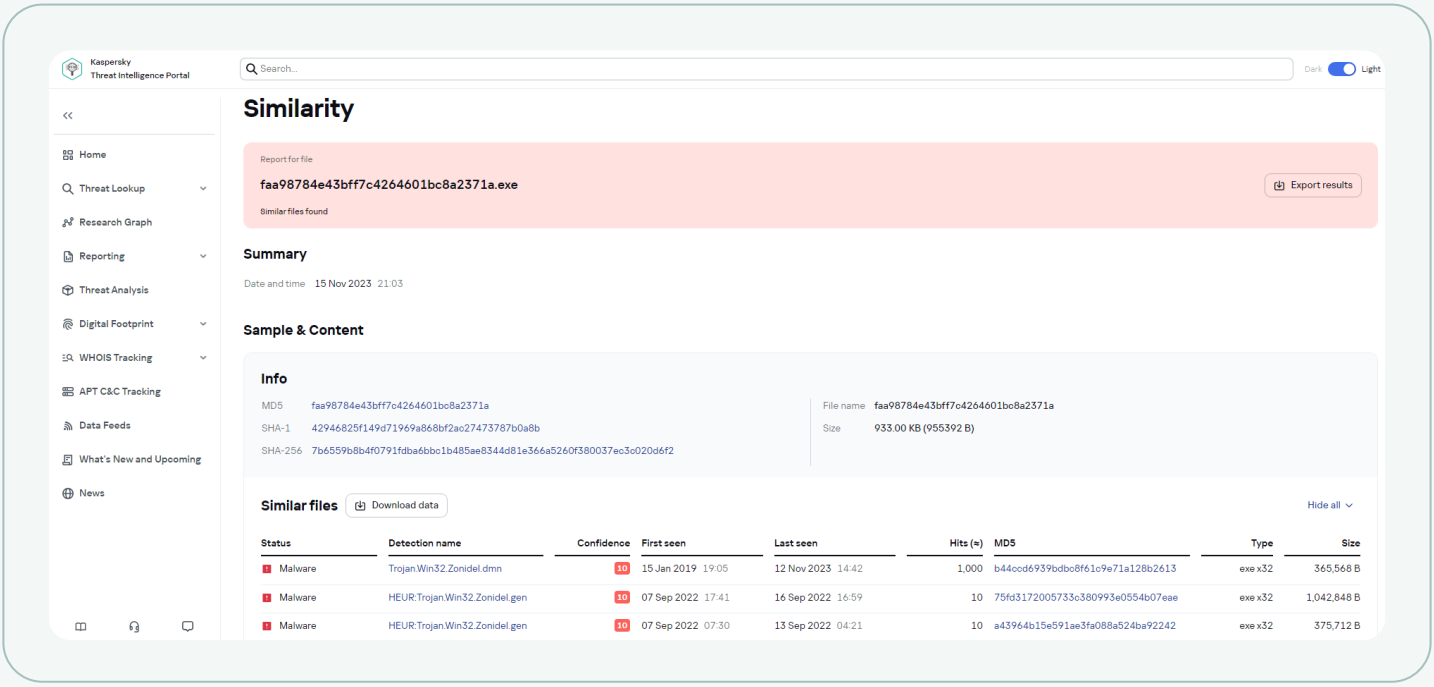
Caratteristiche della funzionalità

Sfrutta uno dei più grandi database del settore di file dannosi e puliti, raccolti in oltre 25 anni, consentendo la massima copertura per un'elevata precisione del confronto

Caricamento manuale dei campioni e API REST ottimizzata per l'integrazione con flussi di lavoro automatizzati

Viene fornito gratuitamente agli utenti di Kaspersky Research Sandbox e Kaspersky Threat Attribution per migliorare l'efficacia di entrambe le tecnologie e fornire informazioni complete sul file analizzato

È già ampiamente utilizzato dagli esperti Kaspersky per esplorare nuove minacce e fornire una protezione ancora più elevata nei nostri prodotti, come confermato regolarmente dalle migliori valutazioni secondo test indipendenti:



Use case di Kaspersky Threat Analysis

Kaspersky Threat Analysis fornisce strumenti avanzati per il rilevamento di minacce sconosciute che possono essere ampiamente applicati nei seguenti scenari:

Incident response

Rilevamento delle minacce elusive

Analisi statica/dinamica di file sospetti

Identificate la relazione di un nuovo malware con un determinato threat actor per conoscere le possibili ulteriori fasi dell'attacco

Threat Hunting

Scansione dell'infrastruttura per gli IoC ricevuti tramite report

Trovate le potenziali modifiche dannose dei file puliti più diffusi

Identificate gli IoC condivisi tra file dannosi sconosciuti e noti

Malware Analysis

Analisi delle minacce sconosciute

Trovate il malware correlato per facilitare il reverse engineering dei file offuscati

Kaspersky Threat Analysis è uno strumento flessibile di ricerca con componenti interconnessi che consente una valutazione completa e multilivello degli oggetti sospetti per l'identificazione e la classificazione degli attacchi avanzati. Aiuta i team SOC, i ricercatori di sicurezza e gli analisti di malware a rimanere informati sulle minacce esistenti ed emergenti legate al malware, consentendo loro di stabilire rapidamente la priorità, affrontare le minacce critiche e risolverle in modo più efficace.

Kaspersky Threat Analysis

Ulteriori informazioni

www.kaspersky.it

#kaspersky
#bringonthefuture