kaspersky BRING ON THE FUTURE

Kaspersky Threat Attribution Engine

Monitorare, analizzare, interpretare e mitigare le minacce alla sicurezza IT in continua evoluzione è un impegno di enorme portata. La Threat Intelligence ha un valore reale al di là dell'attuale entusiasmo generato per l'apertura di una nuova strada nel settore della sicurezza informatica e l'attribuzione delle minacce è probabilmente il punto di interesse e di conflitto più evidente quando si tratta di Threat Intelligence.

Principali caratteristiche del prodotto:

- Fornisce accesso immediato a un archivio di dati selezionati su centinaia di attori e campioni APT
- 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 aperta per l'integrazione con flussi di lavoro automatizzati
- Questa soluzione può essere distribuita in ambienti air-gap sicuri per proteggere i sistemi e i dati, soddisfacendo al contempo eventuali requisiti di compliance
- Mantiene la privacy e la riservatezza assolute di tutte le trasmissioni per evitare l'esposizione di informazioni sensibili

E c'è una chiara ragione. Il tempo trascorso tra il rilevamento di una minaccia altamente sofisticata e la corretta risposta è in media troppo lungo, a causa dei complessi processi di investigation e reverse engineering. In molti casi è sufficiente per consentire agli autori degli attacchi di raggiungere i propri obiettivi. L'attribuzione corretta e tempestiva non solo consente di ridurre i tempi di incident response da ore a minuti, ma anche di diminuire il numero di falsi positivi.

Identificare un attacco mirato, tracciare un profilo degli autori e creare fattori di attribuzione per i diversi threat actor è un lavoro lungo e meticoloso, che può richiedere anni. L'attribuzione del lavoro richiede inoltre la grande quantità di dati accumulati negli anni e un team di ricercatori altamente qualificati con esperienza nel campo dell'investigation. Insieme, i ricercatori seguono l'attività di diversi gruppi e popolano il database con i dati. A questo punto il database diventa una risorsa preziosa da condividere sotto forma di soluzione di sicurezza.

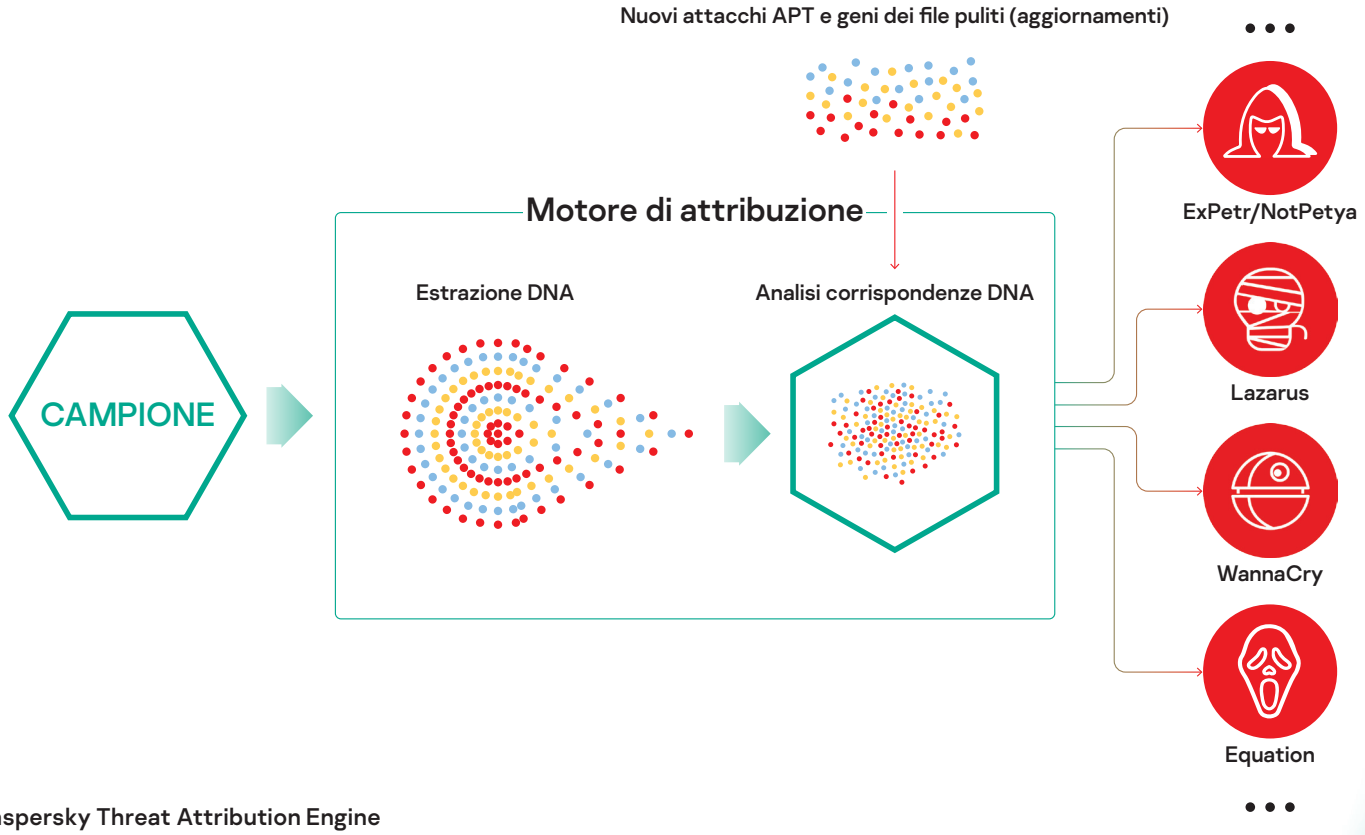
Kaspersky Threat Attribution Engine incorpora un database con campioni di malware APT e file raccolti dagli esperti di Kaspersky negli ultimi 22 anni di lavoro. Monitoriamo oltre 600 campagne e threat actor rilasciando oltre 120 APT Intelligence Report all'anno. La nostra ricerca continua supporta l'aggiornamento dell'ampia raccolta APT contenente oltre 60.000 file. Migliora il rilevamento dei falsi positivi e rende l'attribuzione il più accurata possibile attraverso strumenti automatizzati.

Il prodotto consente un approccio unico per il confronto dei campioni alla ricerca di similitudini, garantendo al contempo tassi di falsi positivi pari a zero. È in grado di collegare rapidamente un nuovo attacco a un malware APT noto, ai precedenti attacchi mirati e ai gruppi di hacker, contribuendo a evidenziare la minaccia ad alto rischio tra incidenti meno gravi e permettendo di adottare misure di protezione tempestive per impedire a un hacker di conquistare l'accesso al sistema.

Come funziona

Kaspersky Threat Attribution Engine, con un metodo automatizzato, analizza la genetica del malware, cercando la somiglianza del codice con campioni APTe attori collegati esaminati in precedenza. Confronta i genotipi, ad esempio piccole porzioni di codice binario dei file scomposti, con il database di campioni di malware APT e fornisce un report sull'origine del malware, i threat actor e la somiglianza dei file con campioni APT noti.Inoltre, il prodotto consente ai security team di aggiungere attori e oggetti privati al proprio database e di configurare il prodotto in modo da rilevare campioni simili ai file presenti nella raccolta privata. Con Threat Attribution Engine la procedura di attribuzione richiede solo pochi secondi: in passato occorrevano anni.

Il prodotto si può implementare in ambienti air-gap sicuri, atti a limitare l'accesso di terze parti alle informazioni elaborate e agli oggetti analizzati. Un'apposita interfaccia API connette il Motore ad altri framework e strumenti, al fine di implementare il processo di attribuzione nell'ambito delle infrastrutture e dei processi automatizzati già esistenti.



Kaspersky Threat Attribution Engine

Informazioni dettagliate sull'attore APT correlato sono disponibili nei Kaspersky APT Intelligence Report[1]. Agli abbonati al servizio APT Intelligence Reporting forniamo un utile e costante accesso alle nostre investigation e ai relativi risultati, che comprendono dati tecnici completi in un'ampia gamma di formati su ogni nuova APT, incluse le minacce che non saranno mai rese pubbliche.

Kaspersky Threat Attribution Engine amplia e consolida ulteriormente il portfolio Kaspersky dedicato alle agenzie di Cybersecurity nazionali e ai Security Operations Centers (SOC) di natura commerciale, fornendo un prezioso supporto nella definizione di un efficace processo di gestione degli incidenti.

Kaspersky Attribution Engine migliora notevolmente le attività di sicurezza contribuendo a:

- Attribuire rapidamente i file agli attori APT noti per rivelare motivazioni, metodi e strumenti alla base degli incidenti informatici;
- Valutare rapidamente se siete l'obiettivo dell'attacco o una vittima collaterale per configurare le corrette procedure di contenimento e risposta;
- Garantire una mitigazione delle minacce efficace e tempestiva in base a una Threat Intelligence finalizzata all'azione sulla famiglia APT fornita dai Kaspersky APT Intelligence Report.

1 Una subscription a Kaspersky APT Intelligence I report devono essere acquistati separatamente

Novità sulle minacce informatiche: www.securelist.it
IT Security News: https://www.kaspersky.it/blog/category/business/
Sicurezza IT per piccole e medie imprese: www.kaspersky.it/small-to-medium-business-security
Sicurezza IT per le aziende Enterprise: kaspersky.it/enterprise-security

www.kaspersky.it

Offriamo tecnologie di protezione comprovate. Siamo indipendenti. Siamo trasparenti. Siamo impegnati a costruire un mondo più sicuro, in cui la tecnologia migliori le nostre vite. Questo è il motivo per cui lo proteggiamo, in modo che tutti, ovunque, possano beneficiare delle infinite opportunità che offre. Bring on cybersecurity for a safer tomorrow.

Per saperne di più: www.kaspersky.it/about/transparency

Proven.
Transparent.
Independent.