kaspersky BRING ON THE FUTURE

Kaspersky Research Sandbox

Prendere decisioni sulla base del comportamento di un file, analizzando contemporaneamente la memoria di processo, l'attività di rete e così via, rappresenta di sicuro l'approccio ottimale per comprendere al meglio le attuali sofisticate minacce mirate e personalizzate. Le tecnologie di sandboxing, efficaci strumenti avanzati, consentono di condurre risolutive investigation sulle origini dei sample di file, eseguire la raccolta di preziosi IoC in base all'analisi comportamentale ed effettuare il rilevamento di oggetti dannosi non individuati in precedenza.

Principali caratteristiche del prodotto:

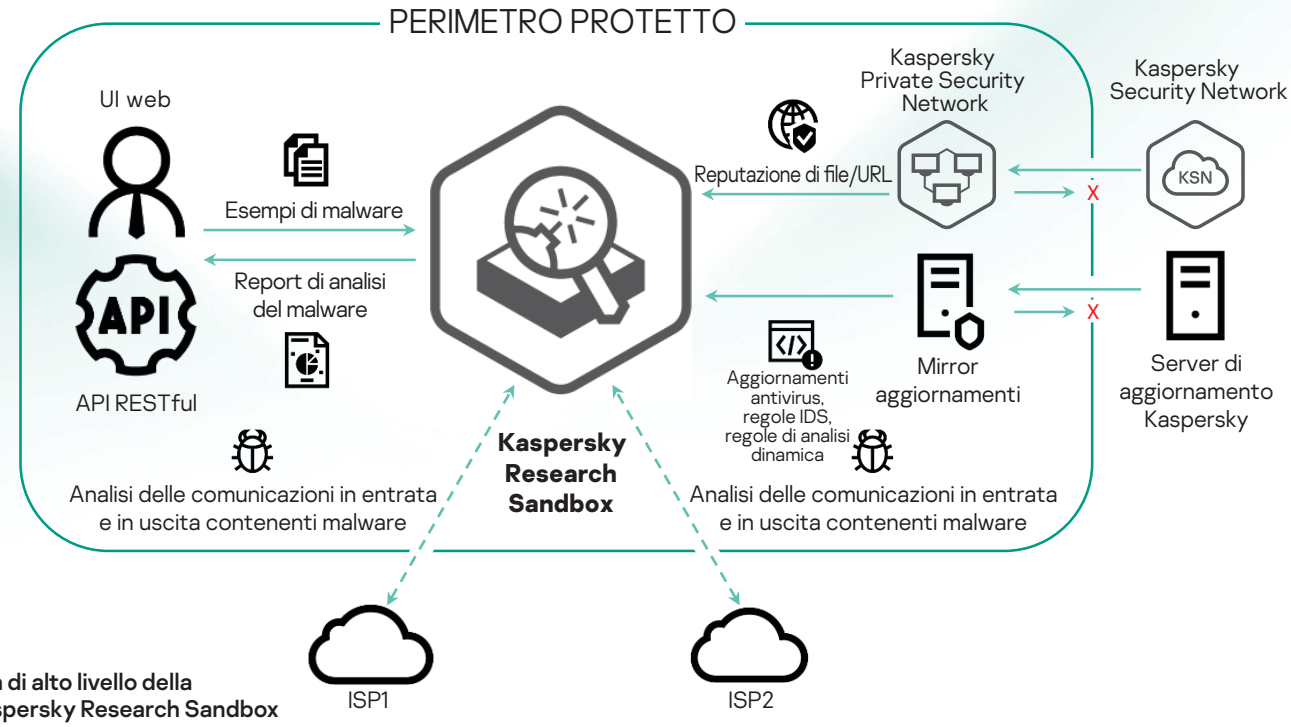
- Il deployment effettuato on-premise fa sì che nessun dato aziendale risulti esposto all'esterno dell'organizzazione
- Supporta l'analisi di oltre cento tipi di file
- Avanzate tecniche antievasione
- Emulazione delle attività dell'utente
- Le immagini personalizzate consentono di analizzare le minacce IT su un'ampia gamma di sistemi operativi e applicazioni; vengono inoltre esaminate esclusivamente le minacce che riguardano gli ambienti reali
- Analisi separata di ogni processo, per rilevare le attività sospette con connessioni di rete associate
- Dettagliati report di analisi, comprendenti tutte le attività di sistema, file estratti, attività di rete (PCAP) e grafiche visive
- Supporta l'integrazione con Kaspersky Private Security Network
- Inserimento manuale dei file; API RESTful per un'efficiente automatizzazione e una perfetta integrazione con le attività di sicurezza già esistenti

Il malware di oggi si avvale di un'ampia varietà di metodi per evitare l'esecuzione del proprio codice, visto che tale operazione ne potrebbe immediatamente rivelare gli intenti dannosi. Se il sistema non soddisfa i parametri richiesti, il programma dannoso quasi sicuramente si distruggerà da solo, senza lasciare alcuna traccia. Affinché il codice dannoso venga eseguito, l'ambiente di sandboxing dovrà quindi essere in grado di imitare accuratamente il normale comportamento dell'utente finale.

Kaspersky Research Sandbox è stato sviluppatodirettamente attraverso il nostro laboratorio dedicato al sandboxing: si tratta di un'avanzata tecnologia, in rapida e costante evoluzione da oltre un decennio. Integra tutte le conoscenze sul comportamento del malware acquisite da Kasperskynel corso di oltre 20 anni di costante ricerca sulle minacce, e ci permette di rilevare ogni giorno più di 350.000 nuovi oggettidannosi. Questa potente tecnologia, distribuita on-premise, previene ugualmente l'esposizione dei dati aziendali all'esterno dell'organizzazione.

Fornisce un innovativo approccio ibrido, capace di combinare perfettamente l'analisi comportamentale e sofisticate tecniche antievasione con tecnologie in grado di simulare il fattore umano. Kaspersky Research Sandbox consente inoltre di personalizzare le immagini del sistema operativo ospite, adattandole agli ambienti reali: ciò aumenta l'accuratezza dei risultati inerenti al rilevamento delle minacce e accelera sensibilmente il processo di incident investigation.

La figura qui sotto illustra in maniera schematica l'architettura di Kaspersky Research Sandbox.



L'architettura di alto livello della soluzione Kaspersky Research Sandbox

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

Se prende di mira un'applicazione specifica non presente nella sandbox, il malware può di fatto non mostrare il proprio comportamento dannoso. Per risolvere questa sfida, i ricercatori devono esaminare i registri, comprendere cosa manca e aggiungere tale elemento a una macchina virtuale, per poi eseguire nuovamente il processo. In questo modo, nel momento in cui il malware tenta di accedere a un'applicazione, il sistema brevettato intercetta il tentativo in opera. Non attende quindi il completamento dell'esecuzione del file: sospende invece il processo, per creare l'applicazione richiesta e il relativo contenuto.

Le regole di rilevamento che descrivono il modo in cui occorre reagire a un evento specifico non sono preinstallate, né implementate all'interno del motore: si possono tuttavia aggiornare e aggiungere facilmente.

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 un file sospetto con un unico tentativo.

Il prodotto supporta il deployment di tipo "bare metal". La configurazione hardware dipende dal genere di performance richiesta ed è facilmente scalabile. Richiede una connessione di rete a 100 Mbps per ogni canale e almeno una connessione ISP indipendente (due o più sono tuttavia consigliate in ragione della tolleranza d'errore). Da parte sua, l'ISP dovrebbe essere consapevole della presenza di traffico nocivo ed essere quindi pronto ad affrontarlo.

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

- **Riepilogo**: informazioni generali sui risultati dell'esecuzione di un file.
- **Nomi di rilevamento sandbox**: elenco dei rilevamenti (sia antivirus che comportamentali) registrati durante l'esecuzione del file.
- **Regole di rete attivate**: elenco delle regole di rete SNORT attivate dall'oggetto eseguito durante l'analisi del traffico.
- **Mappa di esecuzione**: rappresentazione grafica delle attività eseguite in sequenza dall'oggetto (azioni avviate su file, processi, registro e attività di rete) e delle relative relazioni intercorrenti. Nella vista ad albero il nodo alla radice rappresenta l'oggetto eseguito.
- **Attività sospette**: elenco delle attività sospette registrate.
- **Screenshot**: serie di screenshot acquisiti durante l'esecuzione del file.
- **Immagini PE caricate**: elenco delle immagini PE caricate, rilevate durante l'esecuzione del file.
- **Operazioni sui file**: elenco delle operazioni sui file registrate durante l'esecuzione del file.
- **Operazioni sul registro**: elenco delle operazioni eseguite sul registro del sistema operativo, rilevate durante l'esecuzione del file.
- **Operazioni sui processi**: elenco delle interazioni del file con i vari processi, registrate durante l'esecuzione del file.
- **Operazioni di sincronizzazione**: elenco delle operazioni relative agli oggetti di sincronizzazione creati (mutex, evento, semaphore), registrate durante l'esecuzione del file.
- **File scaricati**: elenco dei file estratti dal traffico di rete durante l'esecuzione del file.
- **File inseriti**: elenco dei file salvati (creati o modificati) dal file eseguito.
- **Richieste HTTPS/HTTP/DNS**: elenchi relativi alle richieste HTTPS/HTTP/DNS registrate durante l'esecuzione del file.
- **Dump del traffico di rete (PCAP)**: l'attività di rete si può esportare in formato PCAP.

Kaspersky Research Sandbox è lo strumento ideale per il rilevamento delle minacce sconosciute. Presenta un elevato livello di maturità tecnologica e risulta molto più focalizzato sulle minacce avanzate rispetto a qualsiasi altra soluzione del genere.

Notizie sulle cyberminacce: www.securelist.com
Notizie sulla sicurezza IT:
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

We are proven. Siamo indipendenti. Siamo trasparenti. Siamo pronti a costruire un mondo sicuro, dove le tecnologie migliorano le nostre vite. È per questo che lo proteggiamo, così che chiunque, in ogni luogo possa godere delle infinite opportunità che offre. Bring on cybersecurity for a safer tommorow.

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

Proven.
Transparent.
Independent.