Kaspersky Research Sandbox

kaspersky BRING ON THE FUTURE

Tecnologie di sandboxing

Le tecnologie di sandboxing sono efficaci strumenti che permettono di indagare le origini dei campioni di file, di eseguire la raccolta di IOC in base all'analisi comportamentale e il rilevamento di oggetti dannosi non individuati in precedenza.

Kaspersky Research Sandbox

Prendere decisioni sulla base del comportamento di un file o di una URL, 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.

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 sviluppato direttamente 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 nel corso degli anni di costante ricerca sulle minacce, e ci permette di rilevare ogni giorno più di 380.000 nuovi oggetti dannosi. Questa potente tecnologia, distribuita on-premises, 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 anti-elusione con tecnologie in grado di simulare il fattore umano. Kaspersky Research Sandbox consente inoltre la personalizzazione delle immagini di sistema per l'analisi, adattandole agli ambienti reali: ciò aumenta l'accuratezza del rilevamento delle minacce e la velocità delle indagini.

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
- La distribuzione on-premises fa sì che nessun dato aziendale risulti esposto all'esterno dell'organizzazione
- Avanzate tecniche anti-elusione e tecnologie di simulazione del fattore umano
- Invio manuale di file/URL e API RESTful
- Supporto per l'analisi di oltre 100 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 preconfigurate
- Il prodotto supporta la distribuzione "bare metal" e può essere facilmente adattato in base alle prestazioni desiderate

L'architettura di alto livello della soluzione Kaspersky Research Sandbox

Il prodotto supporta la distribuzione bare metal. La configurazione hardware dipende dalle prestazioni desiderate 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 per la tolleranza d'errore). Da parte sua, l'ISP dovrebbe essere consapevole della presenza di traffico nocivo ed essere quindi pronto ad affrontarlo.

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/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.

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. 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.

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 delle URL.

Immagini PE caricate

Un elenco delle immagini PE caricate, rilevate durante l'esecuzione del file o l'esplorazione delle URL.

Operazioni sui file

Un elenco delle operazioni sui file registrate durante l'esecuzione del file/l'esplorazione delle 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 delle 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 delle 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 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.

www.kaspersky.it