Kaspersky Cloud Sandbox

kaspersky BRING ON THE FUTURE

Kaspersky Cloud Sandbox

È di fatto impossibile prevenire gli attuali attacchi di natura mirata avvalendosi esclusivamente dei 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. Le perdite derivanti da incidenti di sicurezza informatica continuano ad aumentare in modo esponenziale, evidenziando la crescente importanza delle capacità di rilevamento immediato degli attacchi, al fine di assicurare una risposta rapida alle minacce e contrastare le stesse prima che si verifichino danni significativi.

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 sofisticate minacce mirate e personalizzate più recenti. Mentre i dati statistici possono non includere le necessarie informazioni sui malware modificati di recente, le tecnologie di sandboxing 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.

Reporting completo

- Caricamento ed esecuzione di DLL
- Connessioni esterne con nomi di dominio e indirizzi IP
- Creazione, modifica ed eliminazione di file
- Dettagliate informazioni di Threat Intelligence, corredate da contesto finalizzato all'azione, per ogni Indicatore di Compromissione (IoC) rivelato
- Dump della memoria di processo e dump del traffico di rete (PCAP)
- Richieste e risposte HTTP e DNS
- Creazione di esclusioni reciproche (mutex)
- API RESTful
- Modifica e creazione di chiavi di registro
- Creazione di processi attraverso il file eseguito
- Screenshot
- **e molto altro ancora**

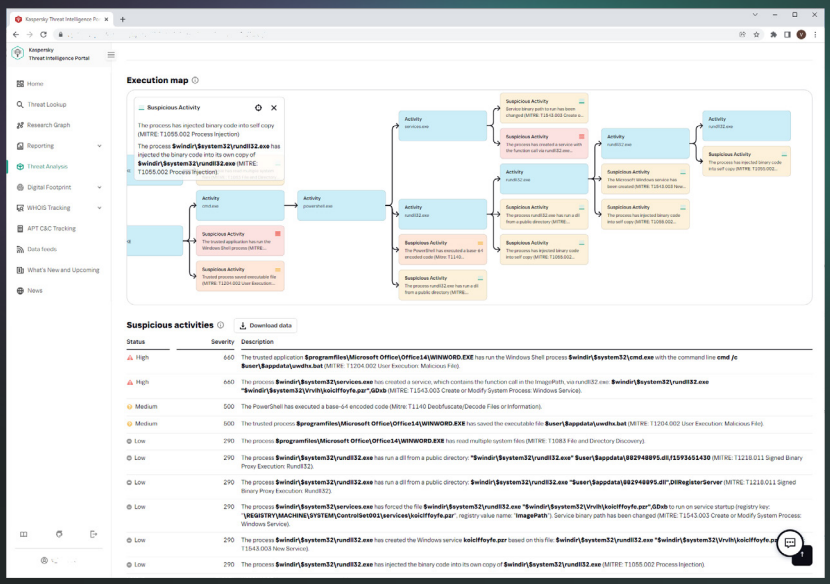
Rilevamento e mitigazione delle minacce proattivi

Il malware si avvale di tutta una serie di metodi per agire senza essere rilevato. 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 essere in grado di imitare accuratamente il normale comportamento dell'utente finale.

Kaspersky Cloud Sandbox fornisce in tal senso un approccio ibrido, volto a combinare le informazioni di Threat Intelligence ricavate dall'analisi di petabyte di dati statistici (grazie al Kaspersky Security Network e altri sistemi proprietari), l'analisi comportamentale e sofisticate tecniche antievasione con tecnologie in grado di simulare l'attività umana, come il click automatico, lo scorrimento dei documenti e processi fittizi.

Questo prodotto è stato sviluppato nel nostro laboratorio di sandboxing interno, evolvendosi per oltre un decennio. La tecnologia unisce tutte le conoscenze relative al comportamento del malware acquisite in oltre 20 anni di ricerca continua sulle minacce. Questo ci consente di rilevare oltre 360.000 nuovi oggetti pericolosi al giorno per fornire ai nostri clienti soluzioni di sicurezza leader di settore.

Nell'ambito del nostro Threat Intelligence Portal, Cloud Sandbox rappresenta il componente principale nel flusso di lavoro in termini di Threat Intelligence. Mentre Threat Lookup recupera le più recenti e dettagliate informazioni di Threat Intelligence riguardo a URL, domini, indirizzi IP, hash di file, denominazioni delle minacce, dati statistici/comportamentali, dati WHOIS/DNS e via dicendo, Cloud Sandbox collega tali conoscenze agli IoC generati attraverso l'analisi dei campioni di malware.



Ora è possibile condurre con elevata efficacia complesse indagini sugli incidenti, per un'immediata comprensione della natura delle minacce: vengono in tal modo acquisite informazioni particolarmente dettagliate, in grado di rivelare le correlazioni esistenti tra i vari indicatori delle minacce.

In genere, quando si deve far fronte ad attacchi multilivello, il processo di ispezione può richiedere un uso estensivo di risorse. Kaspersky Cloud Research Sandbox ottimizza le attività di analisi forense e incident response, garantendo la scalabilità necessaria per l'elaborazione automatica dei file senza la necessità di acquistare costose apparecchiature o preoccuparsi delle risorse di sistema.

www.kaspersky.it