Kaspersky Research Sandbox

kaspersky BRING ON THE FUTURE

Tecnologías sandbox

Las tecnologías sandbox son herramientas potentes que permiten investigar los orígenes de muestras de archivos, recopilar indicadores de compromiso (IOC) según los análisis de comportamiento y detectar objetos maliciosos previamente no detectados.

Kaspersky Research Sandbox

La estrategia óptima para comprender las sofisticadas amenazas selectivas y personalizadas de hoy es tomar una decisión inteligente basada en el comportamiento de los archivos y URL mientras se analiza la memoria del proceso, la actividad de la red, etc.

En la actualidad, el malware utiliza una amplia variedad de métodos para evitar la ejecución de su código si esto pudiera poner en evidencia su actividad maliciosa. Si el sistema no cumple con los parámetros requeridos, el programa malicioso se autodestruirá con toda seguridad, sin dejar rastros. Para que se ejecute el código malicioso, el entorno de sandbox debe ser capaz de imitar con precisión el comportamiento normal del usuario final.

Kaspersky Research Sandbox se desarrolló directamente a partir del entorno de sandbox de nuestro laboratorio, una tecnología con más de una década de evolución. Incorpora todos los conocimientos sobre comportamientos de malware que adquirimos durante nuestra investigación ininterrumpida de amenazas, lo que nos permite detectar más de 380 000 objetos maliciosos nuevos cada día. Esta potente tecnología, que se implementa en las instalaciones, también evita la divulgación de datos fuera de la organización.

Ofrece un método híbrido que combina el análisis de comportamiento y sólidas técnicas antievasión con tecnologías de simulación del comportamiento humano. Kaspersky Research Sandbox también permite personalizar imágenes del sistema para análisis y adaptarlas a entornos reales. De este modo, aumenta la precisión de la detección de amenazas y la velocidad de la investigación.

Aspectos destacados del producto:

- Análisis automatizado de objetos en entornos Windows, Linux y Android
- Imágenes personalizadas que permiten el análisis de amenazas en aplicaciones y sistemas operativos Windows (solo en entornos reales)
- Puntuación de amenazas en función de métricas y datos obtenidos durante la ejecución del archivo que muestra el nivel de riesgo del objeto analizado
- Implementación en las instalaciones para garantizar que no se divulguen datos fuera de la organización
- Técnicas antievasión y tecnologías de simulación humana avanzadas
- Envío manual de archivo/URL y API RESTful
- Posibilidad de analizar más de 100 tipos de archivos con informes de análisis detallados
- Posibilidad de agregar reglas Suricata personalizadas para analizar el tráfico de red (se pueden usar junto con las reglas Suricata predefinidas)
- Compatibilidad con implementaciones de sistemas físicos y escalabilidad simple según el rendimiento necesario

Arquitectura de alto nivel de Kaspersky Research Sandbox

El producto es compatible con implementaciones en sistemas físicos. La configuración del hardware depende del rendimiento necesario y se puede escalar. Requiere una conexión de red de 100 Mbps para cada canal y al menos una conexión de un proveedor de servicios de Internet (ISP) independiente (se recomiendan dos o más para tolerancia a fallas). El ISP debe estar atento y listo para detectar tráfico malicioso.

Kaspersky Research Sandbox se basa en una tecnología patentada propia (patente núm. US10339301). Si crean las condiciones exactas que activan la ejecución de malware, los investigadores pueden analizar un archivo o una URL sospechosos en un solo intento.

Para evitar que lo detecten, el archivo malicioso podría investigar primero si se encuentra en una máquina virtual o permanecer inactivo hasta que el sandbox ya no esté en funcionamiento. En estos casos, la tecnología patentada acelera el flujo de tiempo dentro de la máquina virtual para que el código malicioso se vea obligado a ejecutarse antes.

Es posible que el malware no muestre su comportamiento malicioso si su objetivo es una aplicación específica que falta en el sandbox. Para abordar esta dificultad, los investigadores deben revisar los registros, averiguar lo que falta, agregarlo a una máquina virtual y volver a ejecutar el proceso. Cuando el malware intenta acceder a una aplicación, el sistema patentado lo intercepta. No espera hasta que el archivo termine de ejecutarse, sino que detiene el proceso para crear la aplicación requerida, así como el contenido.

Informes de análisis detallados

Una vez finalizado el análisis, Research Sandbox proporciona un informe detallado sobre el comportamiento y la funcionalidad de la muestra analizada, lo que permite definir los procedimientos de respuesta adecuados:

Resumen

Información general sobre los resultados tras la ejecución del archivo o la navegación de la URL.

Nombres de detecciones

Una lista de las detecciones (tanto de antivirus como de comportamiento) que se registraron durante la ejecución del archivo.

Reglas de red activadas

Una lista de las reglas Suricata de red que se activaron durante el análisis del tráfico del objeto ejecutado.

Mapa de ejecución

Secuencia representada con gráficos sobre las actividades de un objeto y sus relaciones.

Actividades sospechosas

Una lista de las actividades sospechosas registradas.

Capturas de pantalla

Un conjunto de capturas de pantalla registradas durante la ejecución del archivo o la navegación de la URL.

Imágenes PE cargadas

Una lista de las imágenes PE cargadas que se detectaron durante la ejecución del archivo o la navegación de la URL.

Operaciones de archivos

Una lista de las operaciones de archivos que se registraron durante la ejecución del archivo o la navegación de la URL.

Operaciones del registro

Una lista de las operaciones que se llevaron a cabo en el registro del sistema operativo y que se detectaron durante la ejecución del archivo o la navegación de la URL.

Operaciones de procesos

Una lista de las interacciones que el archivo tuvo con varios procesos y que se registraron durante la ejecución del archivo.

Operaciones de sincronización

Una lista de las operaciones de los objetos de sincronización creados (exclusión mutua, evento, semáforo) que se registraron durante la ejecución del archivo o la navegación de la URL.

Archivos descargados

Una lista de los archivos extraídos del tráfico de red durante la ejecución del archivo o la navegación de la URL.

Archivos instalados

Una lista de los archivos (creados o modificados) que guardó el archivo ejecutado.

HTTPS/HTTP/DNS/IP/ TCP/UDP y más

Información sobre las sesiones o solicitudes de red que se registraron durante la ejecución del archivo o la navegación de la URL.

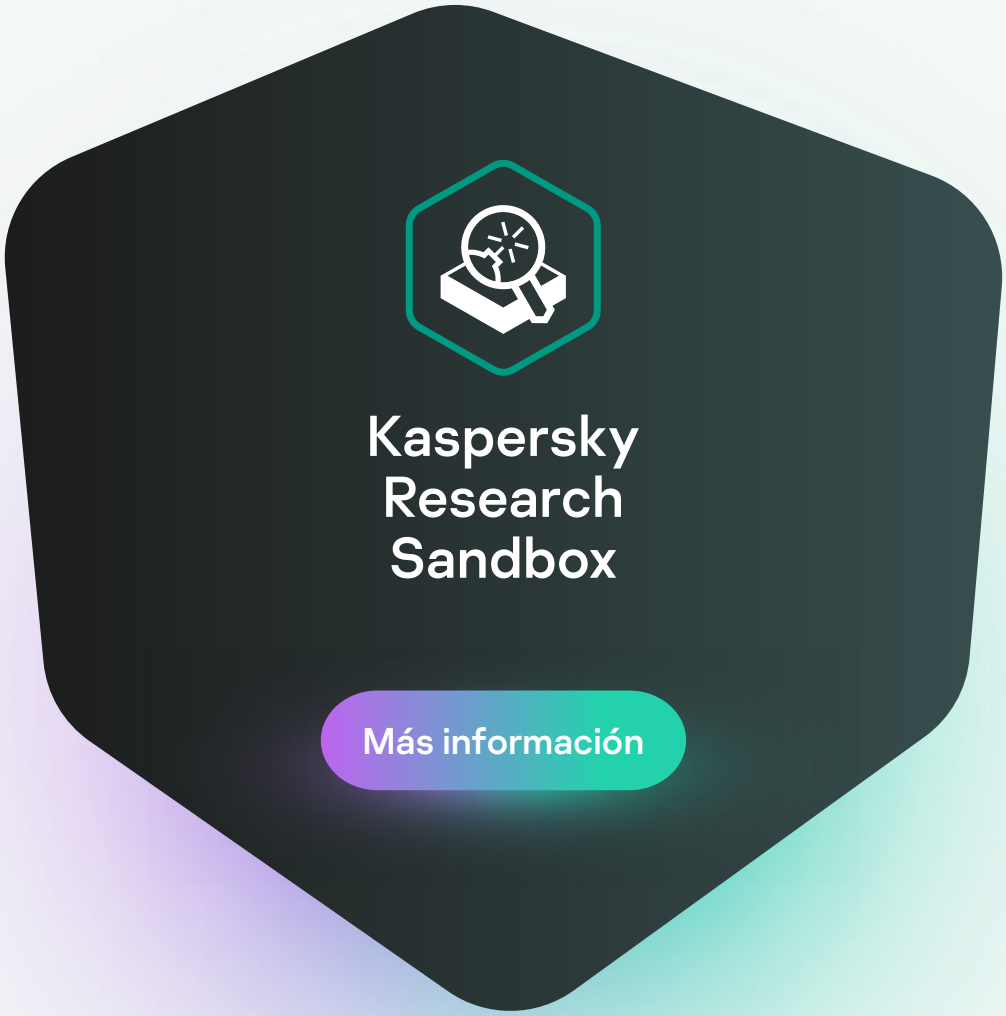
Volcado de tráfico de red (PCAP)

La actividad de la red se puede exportar en formato PCAP.

Matriz MITRE ATT&CK

Todas las actividades identificadas del proceso que se registraron durante la emulación se presentan como una matriz MITRE ATT&CK.

Kaspersky Research Sandbox es la mejor herramienta para detectar amenazas desconocidas. Es una herramienta más madura y más centrada en las amenazas avanzadas que cualquier otra solución.



www.kaspersky.es