



# Kaspersky Research Sandbox

## 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

Tomar una decisión inteligente basada en el comportamiento de un archivo o URL, a la vez que se analiza la memoria del proceso, la actividad de la red, etc., es la estrategia óptima para entender las sofisticadas amenazas dirigidas y personalizadas de hoy.

En la actualidad, el malware utiliza una amplia variedad de métodos para evitar la ejecución de su código si esto pudiera llevar a la exposición de su actividad maliciosa. Si el sistema no cumple con los parámetros requeridos, lo más probable es que el programa malicioso se autodestruya sin dejar rastro. 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 ha sido desarrollado directamente a partir del entorno de sandbox de nuestro laboratorio, una tecnología con más de una década de evolución. Incorpora todo el conocimiento sobre los comportamientos de malware adquirido durante nuestra investigación continua 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 impide la exposición de datos fuera de la organización.

Ofrece un enfoque híbrido que combina el análisis de comportamiento y sólidas técnicas antievasión con tecnologías de simulación del comportamiento humano. Kaspersky Research Sandbox también permite personalizar las imágenes del sistema para análisis y adaptarlas a entornos reales, lo que aumenta la exactitud 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 haya datos expuestos 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 añadir reglas Suricata personalizadas para analizar el tráfico de red (se pueden usar junto con las reglas Suricata predefinidas)



Compatibilidad con implementaciones de hardware y escalabilidad simple según el rendimiento requerido

## Arquitectura de alto nivel de Kaspersky Research Sandbox



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

**Kaspersky Research Sandbox se basa en una tecnología patentada propia (patente núm. US10339301). Al crear 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 puede 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, por lo que el código malicioso se ve obligado a ejecutarse antes.**

**Puede que el malware no muestre su comportamiento malicioso si se dirige a una aplicación específica que falta en el sandbox. Para resolver este desafío, los investigadores deben revisar los registros, averiguar lo que falta, añadirlo 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; 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 le permite definir los procedimientos de respuesta adecuados:

## Resumen

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

## Mapa de ejecución

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

## Imágenes PE cargadas

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

## Operaciones de procesos

Una lista de las interacciones que ha tenido el archivo con varios procesos y que se han registrado durante la ejecución del archivo.

## Archivos instalados

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

## Matriz MITRE ATT&CK

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

## Nombres de detecciones

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

## Actividades sospechosas

Una lista de las actividades sospechosas registradas.

## Operaciones de los archivos

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

## Operaciones de sincronización

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

## HTTPS/HTTP/DNS/IP/TCP/UDP y más

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

## Reglas de red activadas

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

## Capturas de pantalla

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

## Operaciones del registro

Una lista de las operaciones que se han llevado a cabo en el registro del sistema operativo y que se han detectado 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.

## Volcado de tráfico de red (PCAP)

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

**Kaspersky Research Sandbox es el instrumento de elección para detectar amenazas desconocidas. Es un instrumento más maduro y más centrado en las amenazas avanzadas que cualquier otra solución.**



# Kaspersky Research Sandbox

[Más información](#)

[www.kaspersky.es](http://www.kaspersky.es)

© 2022 AO Kaspersky Lab  
Las marcas comerciales y de servicios registradas  
pertenece a sus respectivos propietarios.