kaspersky PREPARADOS PARA EL FUTURO

Kaspersky Research Sandbox

Tomar una decisión inteligente basada en el comportamiento de un archivo, 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. Las tecnologías sandbox son herramientas poderosas que permiten la investigación de los orígenes de las muestras de archivos, los IOC de recopilación basados en análisis de comportamiento y la detección de objetos maliciosos no identificados con anterioridad.

Aspectos destacados del producto:

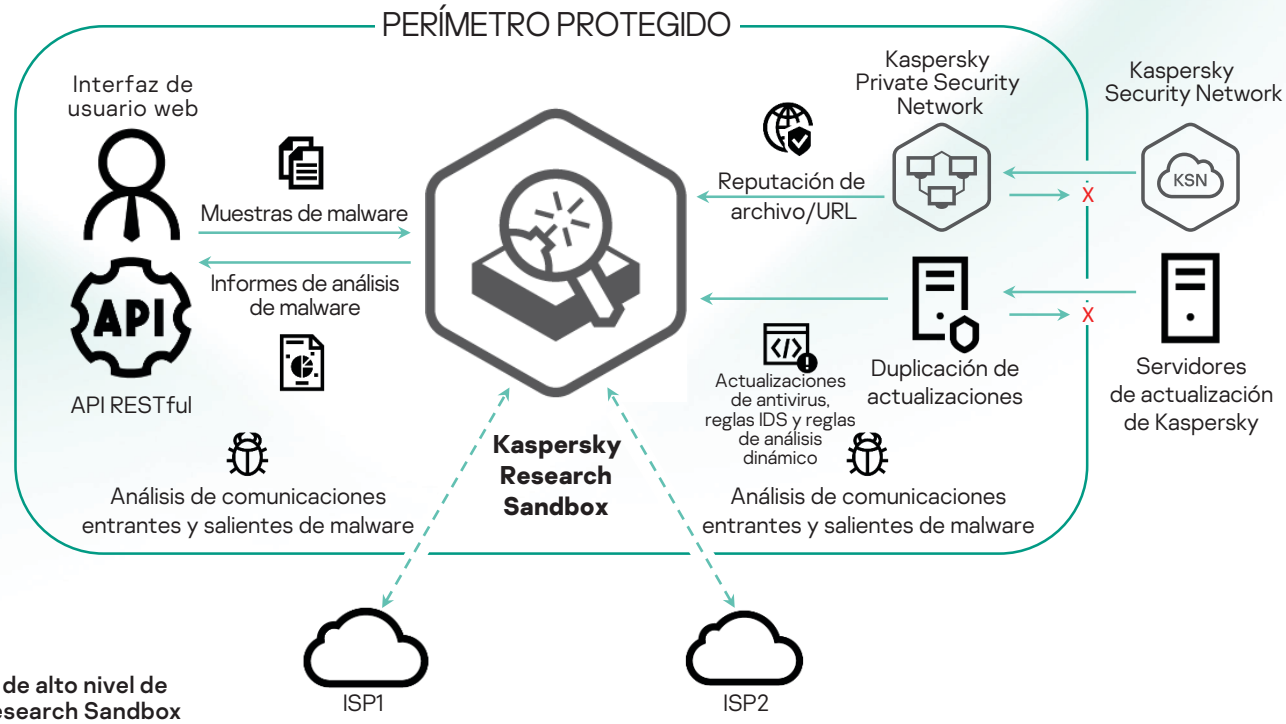
- La implementación en las instalaciones garantiza que no haya datos expuestos fuera de organización
- Compatibilidad con el análisis de más de cien tipos de archivos
- Técnicas antievasión avanzadas
- Emulación de la actividad del usuario
- Imágenes personalizadas que permiten analizar amenazas en una amplia gama de sistemas operativos y aplicaciones, y solo aquellos que se aplican a entornos reales
- Análisis independiente de cada proceso para detectar actividades sospechosas con conexiones de red asociadas
- Informes de análisis detallados, como todos los archivos extraídos, las actividades del sistema, las actividades de red (PCAP) y los gráficos visuales
- Compatibilidad con la integración con Kaspersky Private Security Network
- Envío manual de archivos y API RESTful para una integración y automatización perfectas de sus operaciones de seguridad

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, el programa malicioso casi con toda seguridad se autodestruirá, 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 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 por Kasperskya lo largo de nuestra investigación continua de amenazas, lo que nos permite detectar más de 350 000 objetos maliciososnuevos 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 una sólida antievasión con tecnologías de simulación del comportamiento humano. Kaspersky Research Sandbox también permite personalizar las imágenes de los sistemas para los análisis y adaptarlos a los entornos reales, lo que aumenta la precisión de la detección de amenazas y la velocidad de la investigación.

En el siguiente diagrama se describe la arquitectura de alto nivel de Kaspersky Research Sandbox.



Arquitectura de alto nivel de Kaspersky Research Sandbox

Para evitar la exposición, puede que un archivo malicioso investigue en primer lugar si se encuentra en una máquina virtual, o bien permanecer inactivo durante un periodo de tiempo 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, comprender lo que falta, agregarlo a una máquina virtual y volver a ejecutar este proceso. Al hacerlo, cuando el malware intenta acceder a una aplicación, el sistema patentado intercepta este intento. No espera hasta que finalice la ejecución del archivo, sino que detiene el proceso para crear la aplicación requerida, así como el contenido.

Las reglas de detección que describen cómo hay que reaccionar ante un evento específico no están preinstaladas ni implementadas en el interior del motor, pero pueden actualizarse y agregarse fácilmente.

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 sospechoso en un solo intento.

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 ISP independiente (se recomiendan dos o más para la tolerancia a errores). El ISP debe estar atento y listo para detectar tráfico malicioso.

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 de la ejecución de un archivo.
- **Nombres de detección de sandbox**: una lista de las detecciones (tanto de AV como de comportamiento) que se han registrado durante la ejecución del archivo.
- **Reglas de red activadas**: una lista de las reglas SNORT de red que se han activado durante el análisis del tráfico del objeto ejecutado.
- **Mapa de ejecución**: una secuencia representada gráficamente de las actividades del objeto (acciones que se han llevado a cabo en los archivos, los procesos y el registro, y la actividad de la red), así como la relación que existe entre ellas. El nodo raíz del árbol representa el objeto ejecutado.
- **Actividades sospechosas**: una lista de las actividades sospechosas registradas.
- **Capturas de pantalla**: un conjunto de capturas de pantalla registradas durante la ejecución del archivo.
- **Imágenes PE cargadas**: una lista de las imágenes PE cargadas que se han detectado durante la ejecución del archivo.
- **Operaciones de los archivos**: una lista de las operaciones de archivos que se han registrado durante la ejecución del archivo.
- **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.
- **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.
- **Sincronización de operaciones**: una lista de las operaciones de objetos de sincronización creados (mutex, evento, semáforo) y que se han registrado durante la ejecución del archivo.
- **Archivos descargados**: una lista de los archivos que se extrajeron del tráfico de red durante la ejecución del archivo.
- **Archivos instalados**: una lista de los archivos (creados o modificados) que el archivo ejecutado ha guardado.
- **Solicitudes HTTPS/HTTP/DNS**: listas de las solicitudes HTTPS/HTTP/DNS que se han registrado durante la ejecución del archivo.
- **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.

Noticias sobre ciberamenazas: www.securelist.es
Noticias sobre seguridad de TI: business.kaspersky.es
Seguridad de IT para pymes: https://www.kaspersky.es/small-to-medium-business-security
Seguridad de IT para grandes empresas: kaspersky.es/enterprise-security

www.kaspersky.es