Kaspersky Research Sandbox

Kaspersky Threat Attribution Engine

Kaspersky Similarity

Kaspersky Threat Analysis

kaspersky preparados para el futuro

Kaspersky Threat Analysis

Kaspersky Threat Analysis

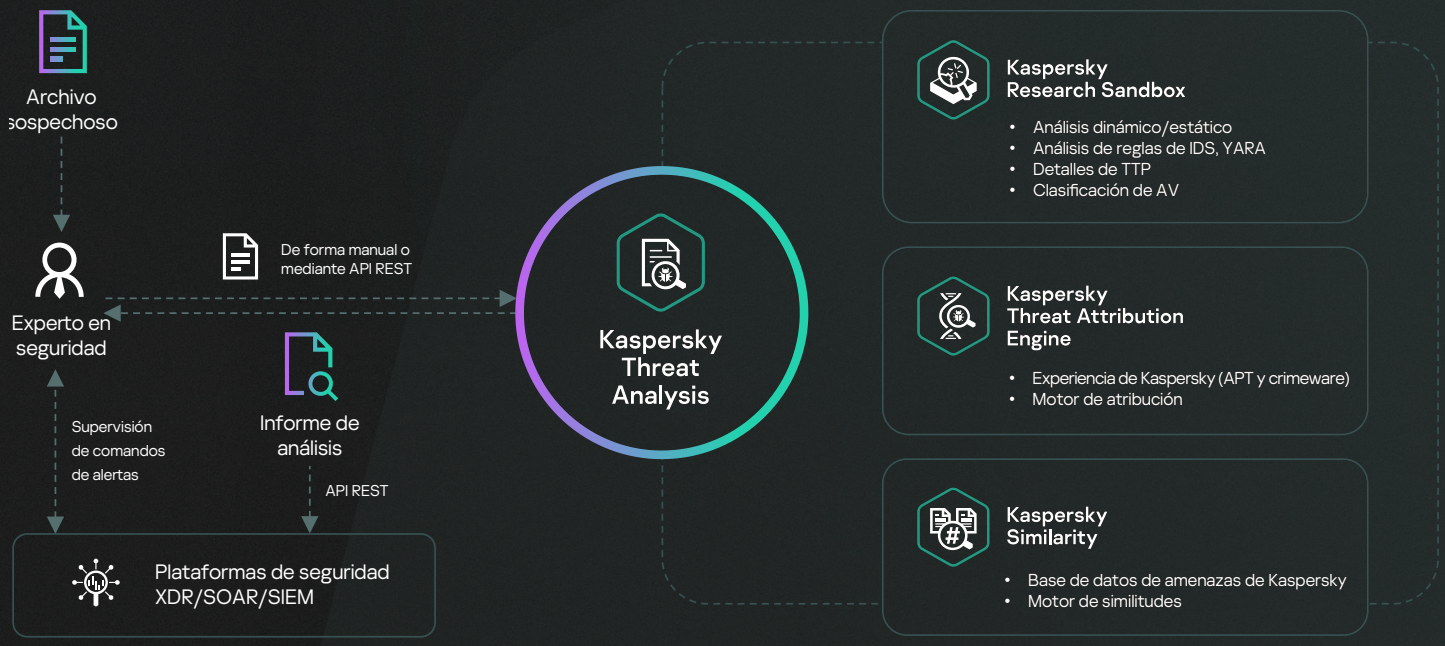
Ante una potencial ciberamenaza, las decisiones que tomes y tu habilidad para tomarlas pueden resultar aspectos críticos. En la actualidad, es imposible evitar los ataques dirigidos con herramientas antivirus tradicionales. Los motores antivirus son capaces de detener solo amenazas conocidas y sus variaciones, mientras que los sofisticados actores de las amenazas usan todos los medios a su disposición para evadir la detección automática. La cantidad de alertas de seguridad procesadas por los centros de operaciones de seguridad (SOC) crece exponencialmente día tras día. Con la cantidad de muestras de malware que se generan cada día, resulta casi imposible priorizar, evaluar y validar con eficacia las alertas.

La combinación de inteligencia de amenazas, análisis dinámico, atribución de amenazas y tecnologías de similitud ofrece una herramienta poderosa para la detección de objetos maliciosos emergentes. Para ayudar a los investigadores de seguridad a mantenerse informados acerca de las amenazas emergentes y existentes, Kaspersky proporciona un único marco resistente para automatizar los análisis de rutina de archivos sospechosos.

Además de contar con herramientas de análisis de amenazas tradicionales como el sandbox, Kaspersky Threat Analysis ofrece tecnologías de atribución de última generación y otras soluciones relacionadas, un enfoque híbrido que brinda un análisis de amenazas eficiente, para poder tomar decisiones informadas y mantener la infraestructura protegida.

Kaspersky Threat Analysis se proporciona a través de la unión de interfaces web y RESTful, y permite a los usuarios configurar parámetros específicos para analizar los objetos sospechosos con un alto grado de eficacia. Se combinan varias herramientas de análisis de amenazas para que tú y tu equipo puedan analizar la situación desde todos los ángulos, con informes completos y detallados para responder de manera rápida y efectiva.

Funcionamiento



Kaspersky
Threat Analysis

Kaspersky
Research
Sandbox

Tecnologías sandbox

son potentes herramientas de análisis dinámico que permiten investigar los orígenes de las muestras de archivos para recopilar indicadores de compromiso (IoC) basados en análisis de comportamiento e identificar objetos maliciosos que las herramientas antivirus tradicionales no detectan.

Se ofrecen versiones en la nube y en las instalaciones.

Sandbox

Kaspersky Research Sandbox se ha desarrollado directamente a partir del entorno de sandbox de nuestro laboratorio, una tecnología con más de dos décadas de evolución. Incorpora todo el conocimiento sobre los comportamientos de malware que hemos adquirido durante nuestra investigación continua de amenazas, lo que nos permite detectar más de 420 000 objetos maliciosos nuevos cada día. Ofrece un enfoque híbrido que combina el análisis de comportamiento y sólidas técnicas antievasión con tecnologías de simulación del comportamiento humano.

Esta tecnología, que se implementa en las instalaciones, impide la exposición de datos fuera de la organización. Kaspersky Research Sandbox en las instalaciones también permite crear entornos de ejecución personalizados para análisis al adaptarlos a entornos reales, lo que aumenta la precisión de la detección de amenazas y la velocidad de la investigación.

¿Por qué usarlo?

Los archivos sospechosos, no detectados por herramientas antivirus, revelan sus rasgos maliciosos recién durante el comportamiento. Kaspersky Research Sandbox permite emular el comportamiento y resaltar acciones peligrosas.

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 sobre la base de métricas y datos obtenidos durante la ejecución del archivo que muestran el nivel de riesgo del objeto analizado

Técnicas antievasión y tecnologías de simulación humana avanzadas

Incluye la carga de muestras manual y API REST mejorada para su integración con flujos de trabajo automatizados

Posibilidad de analizar más de 200 tipos de archivos con informes de análisis detallados

Posibilidad de añadir reglas Suricata personalizadas para analizar el tráfico de red y usarlas junto con las reglas Suricata

SOC de Kaspersky utiliza más de 700 indicadores de ataque propios que cubren el 100 % de todas las tácticas, técnicas y procedimientos (TTP) conocidos de los adversarios. Más de 1000 búsquedas únicas para la extracción de TTP mediante MITRE ATT&CK

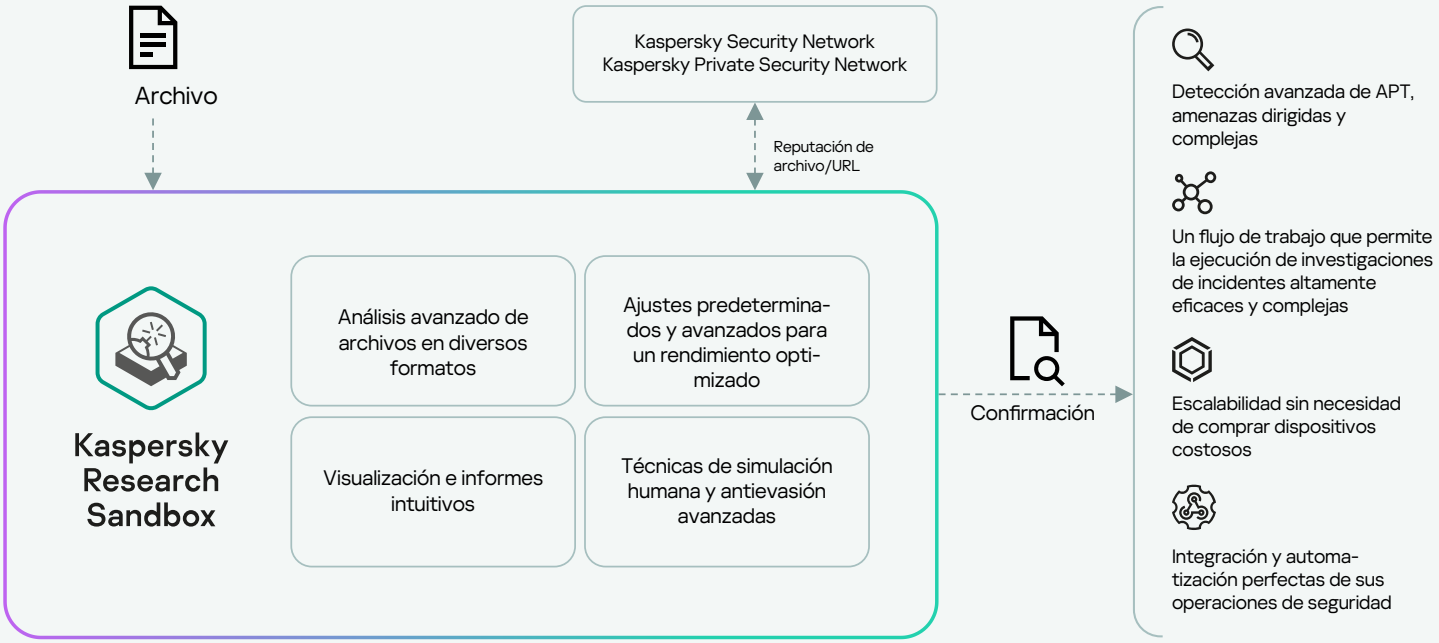
Compatibilidad con el modo interactivo (esperado para el primer trimestre de 2024)

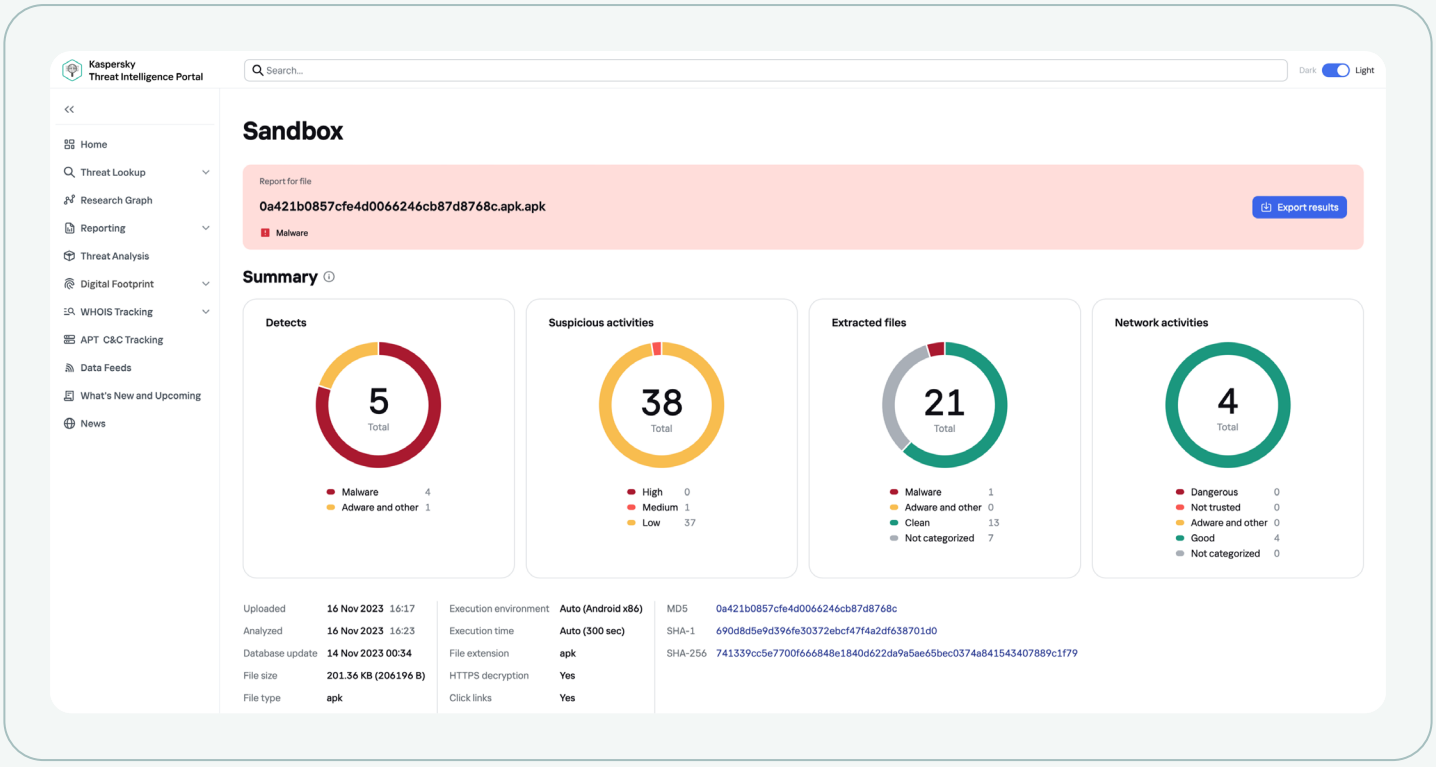
El producto es compatible con la implementación en hardware. La configuración del hardware depende del rendimiento requerido y se puede escalar. Requiere al menos una conexión ISP independiente (se recomiendan dos o más para la tolerancia a errores), 100 Mbps para cada canal.

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.

Esquema operativo de alto nivel de Kaspersky Research Sandbox





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.
Nombres de detecciones	Una lista de las detecciones (tanto de antivirus como de comportamiento) que se han registrado durante la ejecución del archivo.
Reglas de red activadas	Una lista de las reglas Suricata de red que se han activado 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 han detectado durante la ejecución del archivo o la navegación de la URL.
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 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.
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.
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.
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 el archivo ejecutado ha guardado.
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.
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 han registrado durante la emulación se presentan como una matriz MITRE ATT&CK.

Kaspersky
Threat Analysis

Kaspersky Threat Attribution Engine

Atribución de amenazas

El seguimiento, el análisis, la interpretación y la mitigación de las amenazas para la seguridad de la TI es una tarea colosal, puesto que no dejan de evolucionar. Dejando de lado el revuelo, la inteligencia de amenazas es realmente valiosa, y la atribución de amenazas es un elemento clave aquí.

Se ofrecen versiones en la nube y en las instalaciones.

Atribución

Kaspersky Threat Attribution Engine es una herramienta de análisis exclusiva que proporciona información acerca del origen de malware de alto perfil y sus posibles autores. Vincula rápidamente un archivo sospechoso con amenazas persistentes avanzadas (APT), actores y campañas conocidos mediante un algoritmo único y una base de datos especial que contiene muestras de malware APT y el mayor conjunto de archivos limpios de la industria, recopilados por expertos de Kaspersky durante los últimos 25 años, y más.

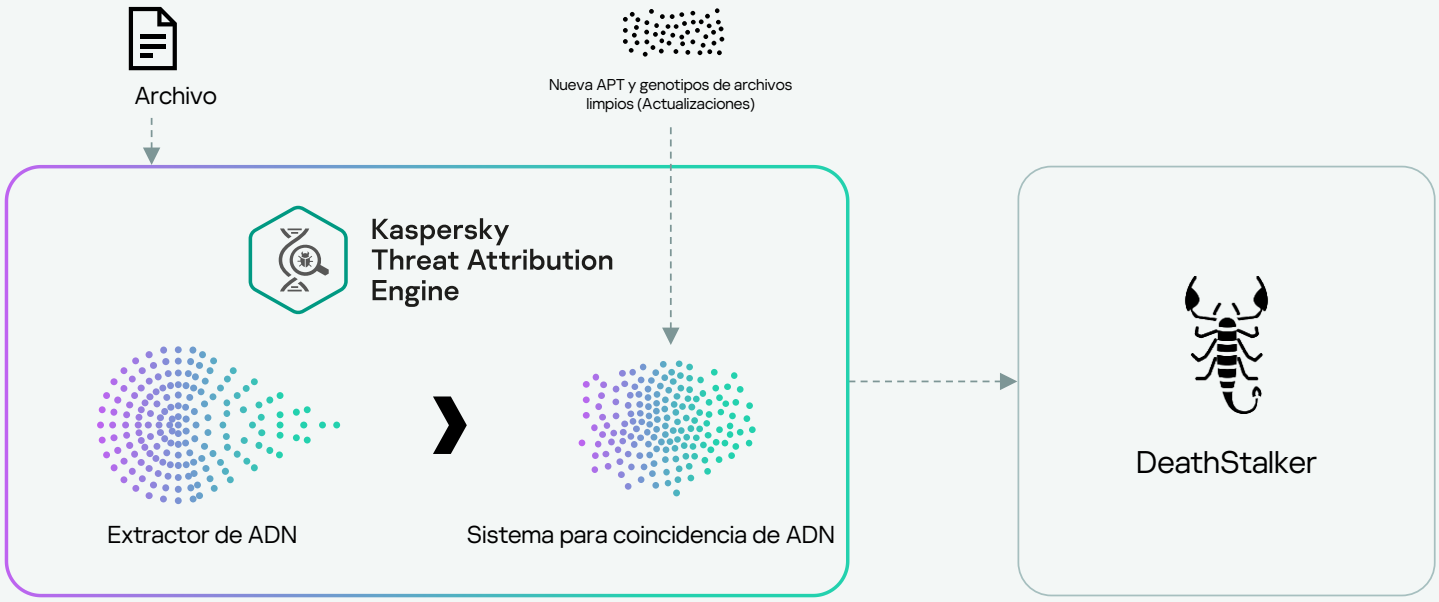
Hacemos seguimiento a más de 1100 atacantes y campañas, y publicamos más de 200 informes sobre inteligencia de amenazas al año. Nuestra investigación continua respalda una recopilación de APT que contiene más de 80 000 archivos que, en combinación con el uso de herramientas automatizadas, ofrecen niveles de atribución de una exactitud sobresaliente.

El producto ofrece un enfoque único hacia la comparación de muestras similares al tiempo que garantiza índices de falsos positivos casi nulos. Todos los ataques nuevos se pueden vincular rápidamente con un malware APT conocido, grupos de piratas informáticos y ataques dirigidos anteriores, lo cual ayuda a distinguir las amenazas de alto riesgo de los incidentes menos serios, con el fin de que puedas tomar medidas proactivas a tiempo y así evitar que un atacante logre un punto de apoyo en tu sistema. Kaspersky Threat Attribution Engine se puede implementar en entornos seguros y herméticos, lo que restringe el acceso de cualquier tercero a la información procesada y a los objetos enviados.

¿Por qué usarlo?

La atribución de un archivo a un actor determinado, junto con el conocimiento de este actor de amenazas, permite conocer el lugar de esta muestra en la cadena de ataques en general, específica para este adversario. A su vez, ofrece información acerca de dónde buscar otros IoC e indicadores de ataques (IoA), y para no pasar por alto el ataque en su totalidad, al bloquear solo un archivo en particular.

Esquema operativo de alto nivel de Kaspersky Threat Attribution Engine



Aspectos destacados del producto

Proporciona acceso instantáneo a un repositorio de datos seleccionados sobre miles de agentes y muestras de APT, y amenazas más generales (a través del motor antivirus).

Información única acerca de campañas de alto perfil (más de 400) investigadas por expertos de Kaspersky.

Ofrece una priorización de las amenazas y un análisis de las alertas automáticas o manuales eficaces.

Cuenta con una funcionalidad que permite añadir actores y muestras privados, además de entrenar al producto para detectar las muestras similares a los archivos de su recopilación privada.

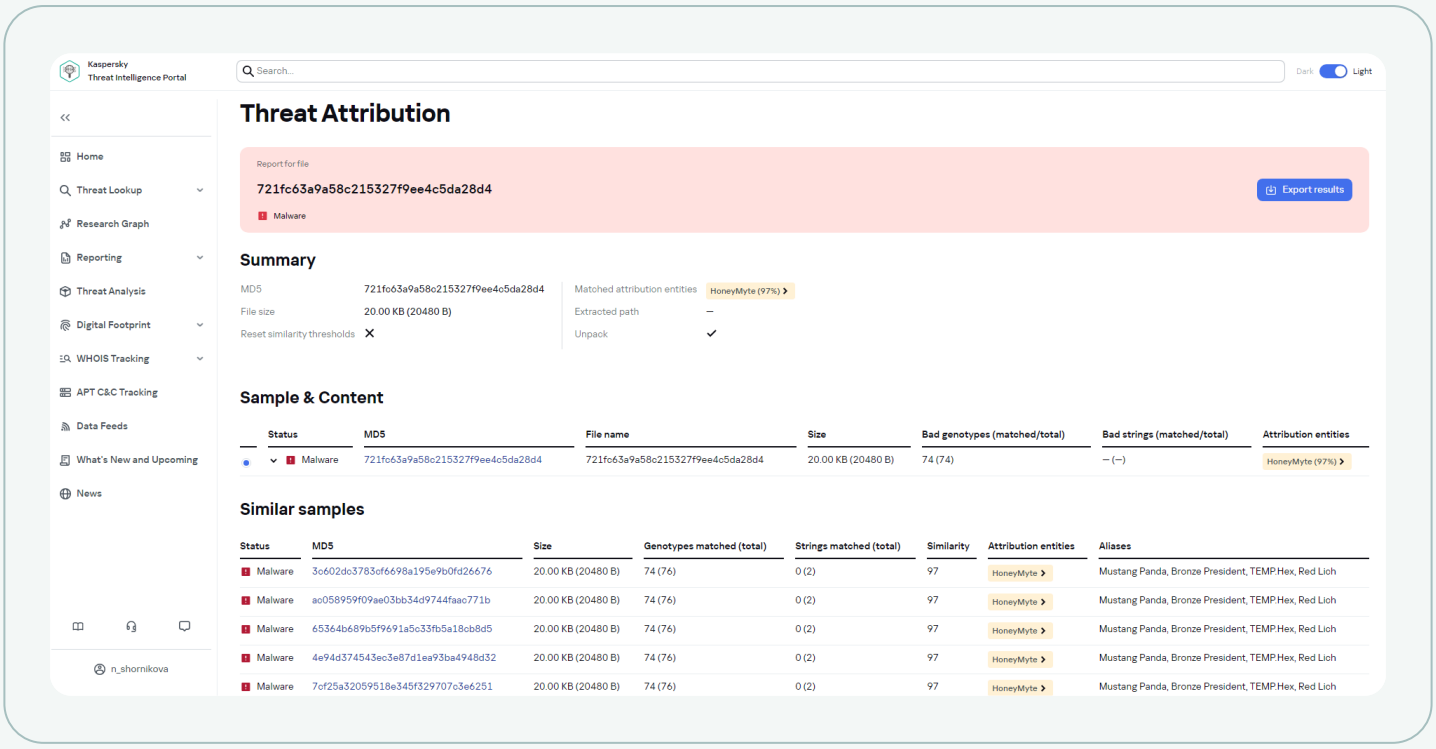
Incluye la carga de muestras manual y API REST mejorada para su integración con flujos de trabajo automatizados

Admite la implementación en infraestructuras en la nube como Amazon Web Services (AWS), lo cual permite una configuración rápida del producto y un ahorro de costes, dado que no se necesita invertir en hardware de antemano.

Exportación a reglas YARA para más análisis/búsqueda automatizados de archivos similares o integración con soluciones de terceros.

Exportación a formato STIX 2.1 (los formatos TXT y JSON también son compatibles) para un análisis más automatizado de registros de seguridad o integración con controles de seguridad/soluciones de terceros

Operatividad para descomprimir archivos protegidos con contraseña con contraseñas personalizadas.



Método de búsqueda patentado

Para vincular el malware con las entidades de atribución, Kaspersky Threat Attribution Engine utiliza un método patentado único de búsqueda de genotipos y cadenas similares entre archivos. Este método abarca lo siguiente:

Análisis de la genética de una muestra

mediante la extracción de los siguientes elementos del código:

- Genotipos: piezas distintivas de código binario.
- Cadenas: cadenas distintivas de caracteres.

Análisis automático de archivos analizados

en busca de genotipos y cadenas que se parezcan a los genotipos y las cadenas de muestras de APT que se hayan analizado anteriormente o que ya estén vinculados con entidades de atribución.

Sobre la base de genotipos y cadenas similares

que se hayan encontrado en las muestras de APT, generación de un informe sobre el origen de la muestra analizada, entidades de atribución relacionadas y cualquier similitud entre esta muestra y muestras conocidas de APT.

Kaspersky Threat Analysis

Kaspersky Similarity

Similitud de archivos

Para construir una línea de defensa efectiva, no siempre es necesario conocer al enemigo en persona. Kaspersky Similarity permite la identificación de muestras de archivos con funciones similares para conseguir protección frente a amenazas desconocidas y evasivas.

Hay una versión en la nube disponible a través de Kaspersky Threat Intelligence Portal.

Similitud

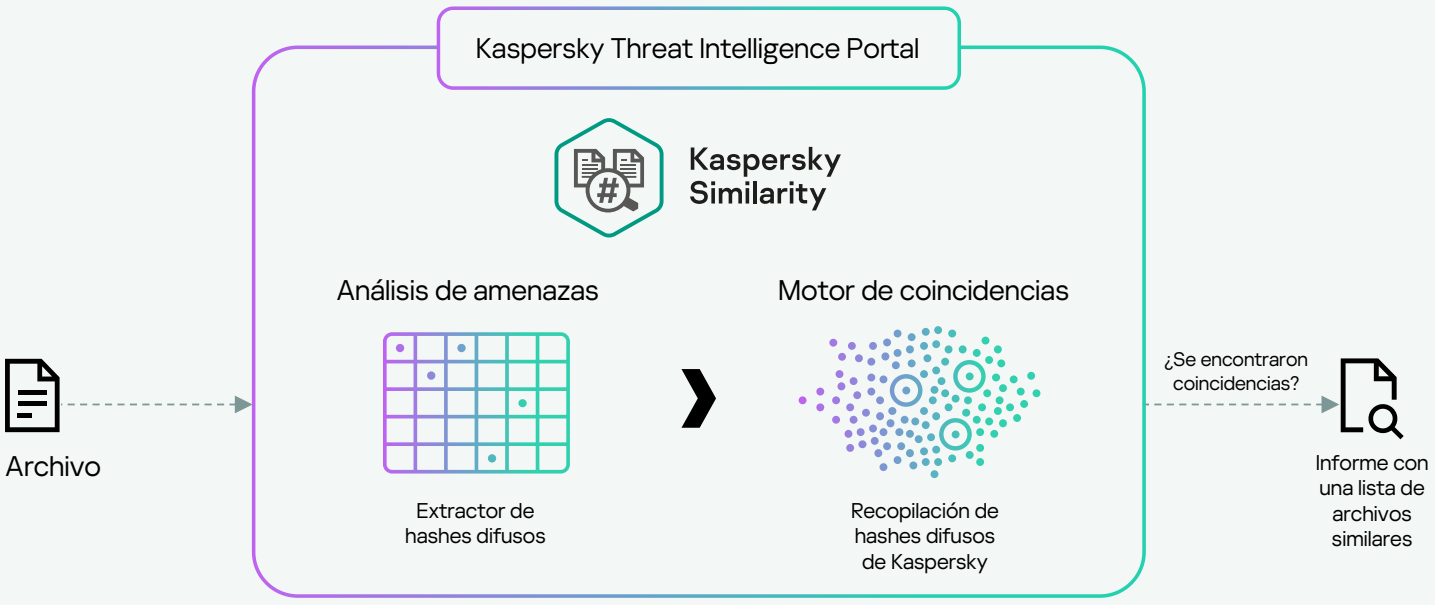
Kaspersky Similarity es una función adicional disponible a través de Threat Intelligence Portal para usuarios de Kaspersky Research Sandbox y Kaspersky Threat Attribution Engine que ayuda a identificar archivos parecidos que se comportan de forma similar.

Los archivos similares se buscan y se calculan para el archivo original mediante tecnología de última generación inventada por expertos de Kaspersky, utilizando más de 50 tipos de hash de similitud únicos. Esto permite garantizar resultados de similitud precisos y de un alto nivel de confianza.

¿Por qué usarlo?

Para encontrar malware similar (p. ej., evasivo) y buscarlo en la infraestructura, de manera de tener la certeza de que un pequeño cambio en la muestra, realizado por un adversario, permanezca en el radar de seguridad. La tecnología se distingue de la atribución: se detectan incluso archivos de malware similares no atribuidos.

Esquema de trabajo de alto nivel de Kaspersky Similarity



Informes de similitud

Cada archivo tiene un formato, compresores usados, secciones, cadenas, tablas de importación, etc. que son específicos. Los expertos de Kaspersky han creado un conjunto de hashes para determinar la similitud entre diferentes archivos sobre la base de estos atributos. Kaspersky Similarity permite a los usuarios enviar un archivo sospechoso, extraer sus hashes difusos y compararlos con hashes difusos de archivos anteriores en la base de datos de amenazas de Kaspersky. Si se encuentran coincidencias, genera una lista de hashes para los principales archivos maliciosos similares, conocidos por Kaspersky y clasificados sobre la base de la puntuación de similitud. El informe incluye el contexto adicional, con metadatos para cada archivo similar:

- Confianza de similitud
- Estado del archivo (malware, adware u otros)
- Nombre de la amenaza
- Marcas horarias de la primera y última detección
- Cantidad de coincidencias (detecciones)
- Hash de archivo
- Tipo de archivo
- Tamaño del archivo

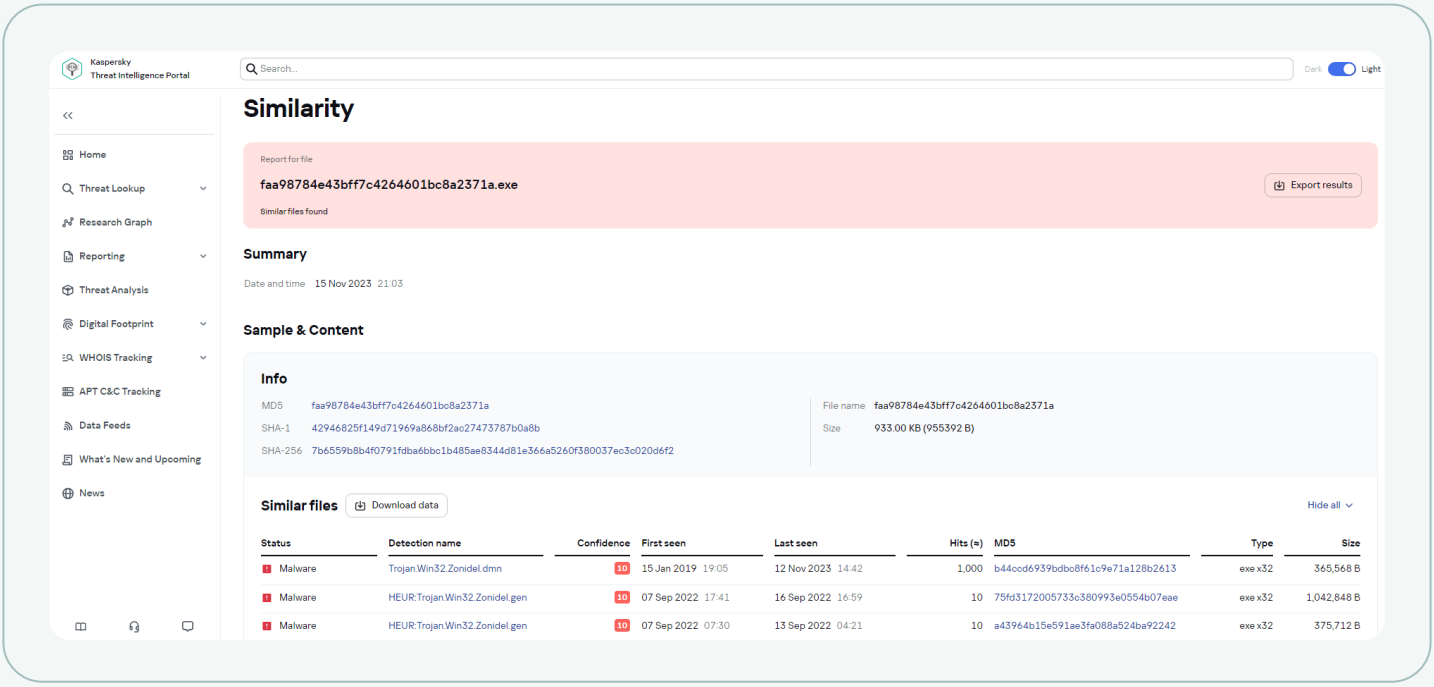
Puntos destacados de la funcionalidad

Utiliza una de las bases de datos de archivos maliciosos y limpios más amplias de la industria, recopilada durante los últimos 25 años, lo que permite una cobertura máxima para mayor exactitud en las comparaciones.

Incluye la carga de muestras manual y API REST mejorada para su integración en flujos de trabajo automatizados

Se proporciona a usuarios de Kaspersky Research Sandbox y Kaspersky Threat Attribution de manera gratuita, para mejorar la efectividad de ambas tecnologías y proporcionar información integral acerca del archivo analizado.

Los expertos de Kaspersky ya la utilizan ampliamente para explorar nuevas amenazas y ofrecer una protección incluso mayor en nuestros productos, lo que se demuestra de manera regular a través de las buenas calificaciones recibidas periódicamente en pruebas independientes:



Casos de uso de Kaspersky Threat Analysis

Kaspersky Threat Analysis proporciona instrumentos maduros para la detección de amenazas desconocidas, que pueden aplicarse de manera amplia en las siguientes situaciones:

Respuesta ante incidentes

Descubrimiento de amenazas evasivas

Análisis dinámico/estático de archivos sospechosos

Revelación de la relación entre un nuevo malware y determinado actor de amenazas, para conocer posibles movimientos adicionales del ataque

Búsqueda de amenazas

Análisis de infraestructura de los IoC recibidos a través del informe

Detección de modificaciones potencialmente maliciosas de archivos limpios populares

Identificación de IoC compartidos entre archivos maliciosos desconocidos y conocidos

Análisis de malware

Análisis de amenazas desconocidas

Detección de malware relacionado para ayudar en la ingeniería inversa de archivos ofuscados

Kaspersky Threat Analysis es una herramienta flexible de investigación con componentes interconectados que permite realizar una evaluación integral y multicapa de objetos sospechosos para la identificación y clasificación de ataques avanzados. Ayuda a equipos de SOC, investigadores de seguridad y analistas de malware a mantenerse informados acerca de amenazas relacionadas con malware existente y emergente, lo que les permite priorizar y responder a amenazas críticas de manera rápida y solucionarlas de forma más efectiva.

Kaspersky Threat Analysis

Más información

www.kaspersky.es

© 2023 AO Kaspersky Lab.
Las marcas comerciales y de servicios registradas pertenecen a sus respectivos propietarios.

#kaspersky
#bringonthefuture