Kaspersky Research Sandbox

Kaspersky Threat Attribution Engine

Kaspersky Similarity

Kaspersky Threat Analysis

kaspersky bring on the future

Kaspersky Threat Analysis

Kaspersky Threat Analysis

Al enfrentarse a una ciberamenaza potencial, las decisiones que toma y su eficiencia resultan aspectos críticos. En la actualidad, es imposible evitar los ataques selectivos solo con herramientas antivirus tradicionales. Los motores antivirus son capaces de detener solo amenazas conocidas y sus variaciones, mientras que los sofisticados atacantes usan todos los medios a su disposición para evadir la detección automática. La cantidad de alertas de seguridad que procesan los centros de operaciones de seguridad (SOC) crece exponencialmente día a día. Con la cantidad de muestras de malware generadas cada día, se vuelve casi inviable priorizar, evaluar y validar con eficiencia las alertas.

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

Además de contar con herramientas de análisis de amenazas tradicionales como los sandbox, Kaspersky Threat Analysis ofrece tecnologías de atribución de última generación y otras soluciones de similitud: un enfoque híbrido que brinda un análisis de amenazas eficiente para poder tomar decisiones informadas y mantener las infraestructuras protegidas.

Kaspersky Threat Analysis se proporciona a través de la unión de interfaces web y RESTful, y les permite a los usuarios configurar parámetros específicos para analizar los objetos sospechosos con un alto grado de eficiencia. Varias herramientas de análisis de amenazas se combinan para permitirles a usted y a su equipo 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 herramientas avanzadas 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.

Hay versiones disponibles en la nube y en las instalaciones.

Sandbox

Kaspersky Research Sandbox se desarrolló 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 adquirimos durante nuestra investigación ininterrumpida de amenazas, lo que nos permite detectar más de 420 000 objetos maliciosos nuevos cada día. Ofrece un método 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, evita la divulgación de datos fuera de la organización. Kaspersky Research Sandbox en las instalaciones también permite crear entornos de ejecución personalizados para el análisis y adaptarlos a entornos reales. De este modo, 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 los rasgos maliciosos solo durante su comportamiento. Kaspersky Research Sandbox permite emular el comportamiento y resaltar las 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 en función de métricas y datos obtenidos durante la ejecución del archivo que muestra el nivel de riesgo del objeto analizado

Técnicas antievasión y tecnologías de simulación humana avanzadas

Carga manual de muestras y una API REST mejorada para su integración en flujos de trabajo automatizados.

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

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

Más de 1000 búsquedas únicas para la extracción de tácticas, técnicas y procedimientos (TTP) mediante MITRE ATT&CK

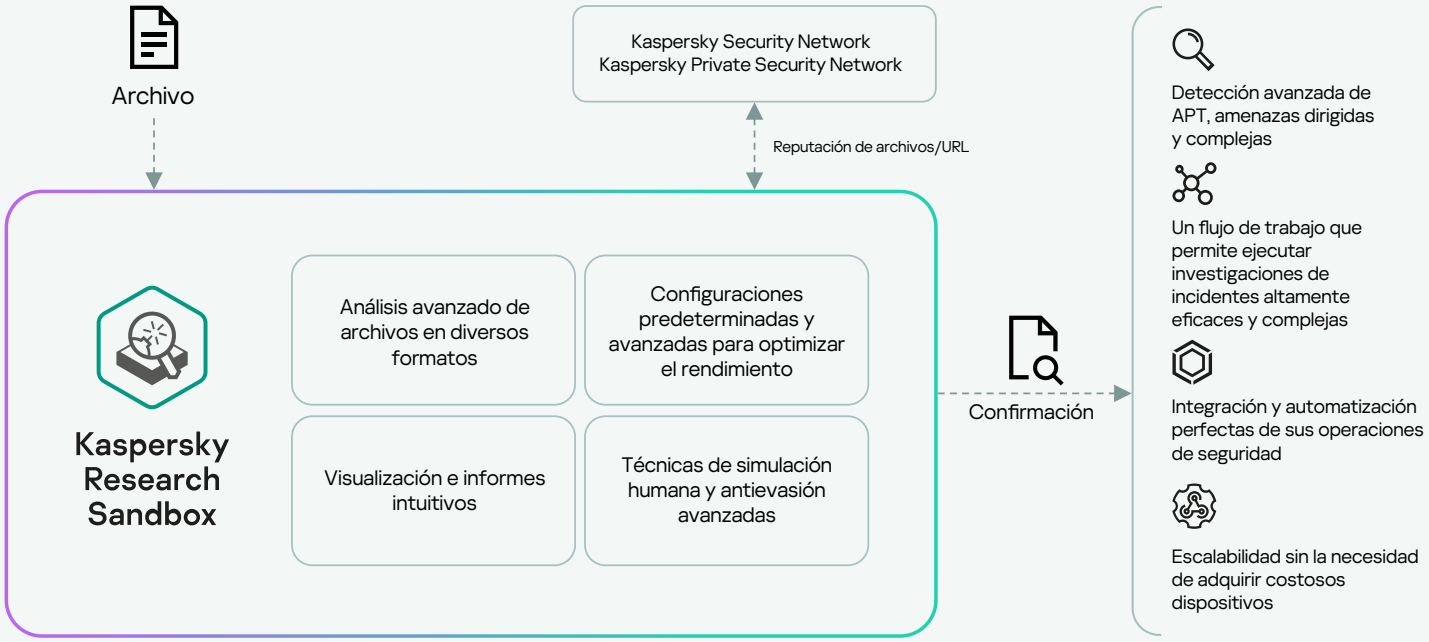
Compatibilidad con el modo interactivo (previsto para el primer trimestre de 2024)

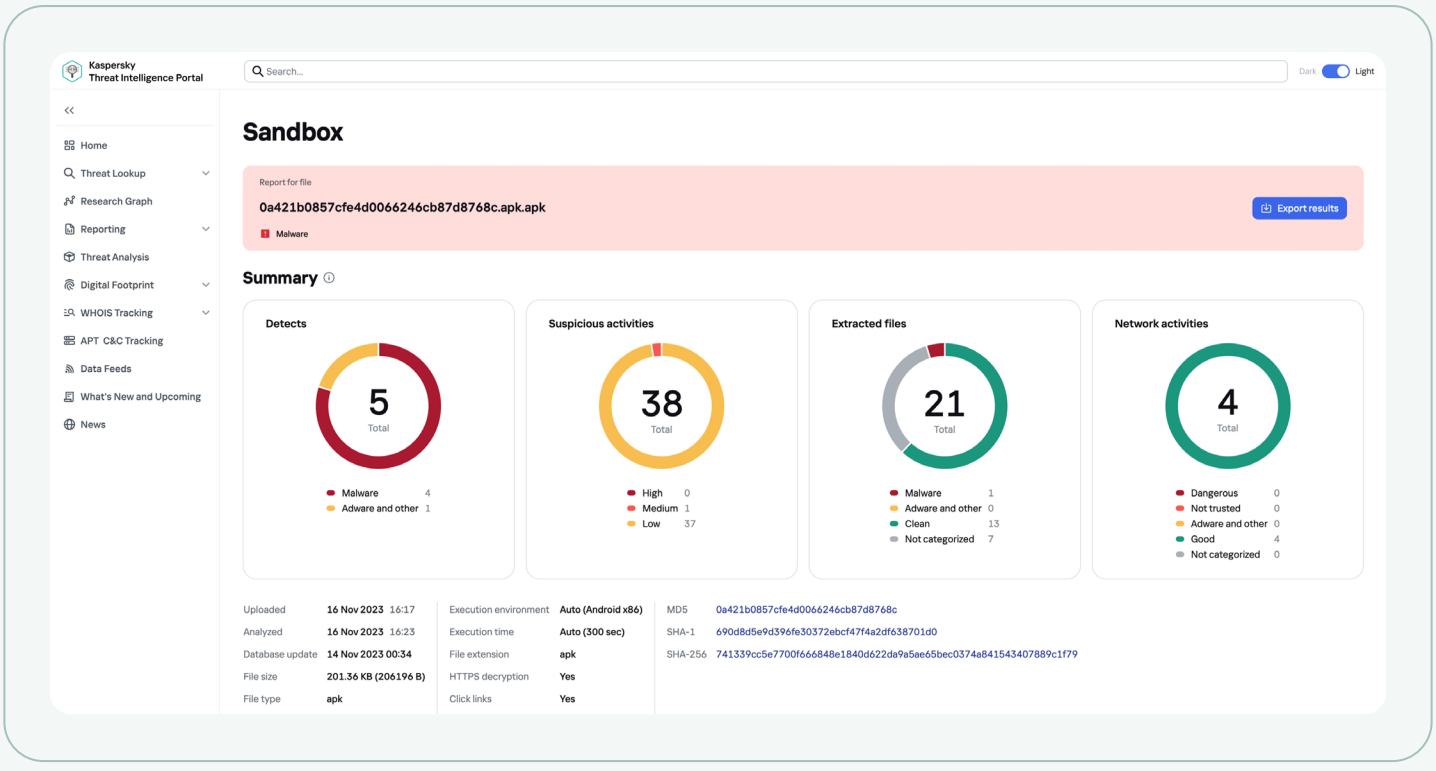
El producto es compatible con implementaciones en sistemas físicos. La configuración del hardware depende del rendimiento necesario y se puede escalar. Requiere al menos una conexión ISP independiente (se recomiendan dos o más para la tolerancia a errores), 100 Mbps para cada canal.

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 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.

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 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
Threat Analysis

Kaspersky
Threat Attribution
Engine

Atribución de amenazas

Se requiere un esfuerzo de gran envergadura para llevar a cabo el rastreo, el análisis, la interpretación y la mitigación de las amenazas de seguridad de TI, que están en constante evolución. Dejando de lado el revuelo, la inteligencia de amenazas es realmente valiosa y la atribución de amenazas es un elemento clave aquí.

Hay versiones disponibles en la nube y en las instalaciones.

Atributos

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

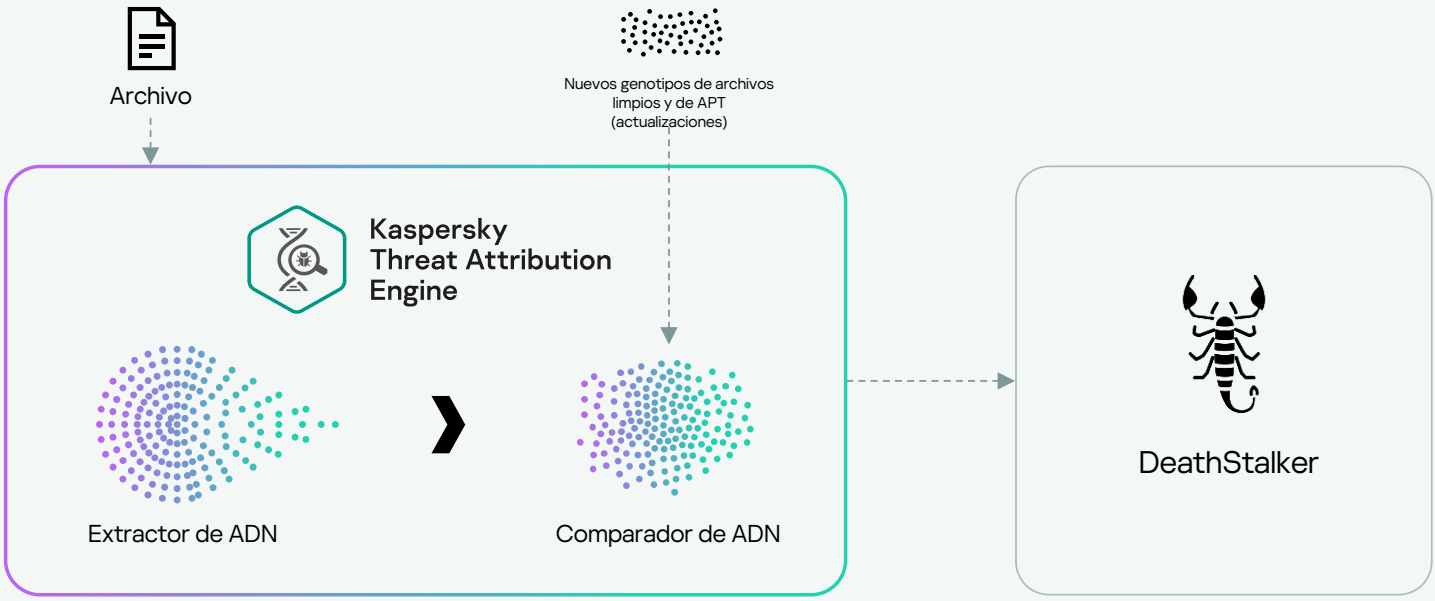
Hacemos seguimiento a más de 1100 atacantes y campañas, y publicamos más de 200 informes sobre inteligencia de amenazas al año. Nuestra investigación continua respalda una recopilación de APT que contiene más de 80 000 archivos que, junto con el uso de herramientas automatizadas, ofrecen niveles de atribución de una precisión 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 de APT conocido, grupos de hackers y ataques selectivos anteriores, lo cual ayuda a distinguir entre las amenazas de alto riesgo y los incidentes menos serios, con el fin de que pueda tomar medidas proactivas a tiempo y así evitar que un atacante logre infiltrarse en su sistema. Kaspersky Threat Attribution Engine se puede implementar en entornos seguros y herméticos, lo que restringe el acceso de cualquier agente externo a la información procesada y los objetos enviados.

¿Por qué usarlo?

La atribución de un archivo a un atacante determinado, junto con el conocimiento de este atacante, permite conocer el lugar de esta muestra en la cadena de eliminación cibernética (cyber kill chain) específica a este adversario. A su vez, ofrece información acerca de dónde buscar otros IoC e indicadores de ataque (IoA) y cómo 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 atacantes 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 eficiencia en la evaluación de alertas y la priorización de amenazas automatizadas o manuales

Cuenta con una funcionalidad que permite agregar atacantes y muestras privados, además de entrenar al producto para que detecte muestras similares a los archivos de la recopilación privada.

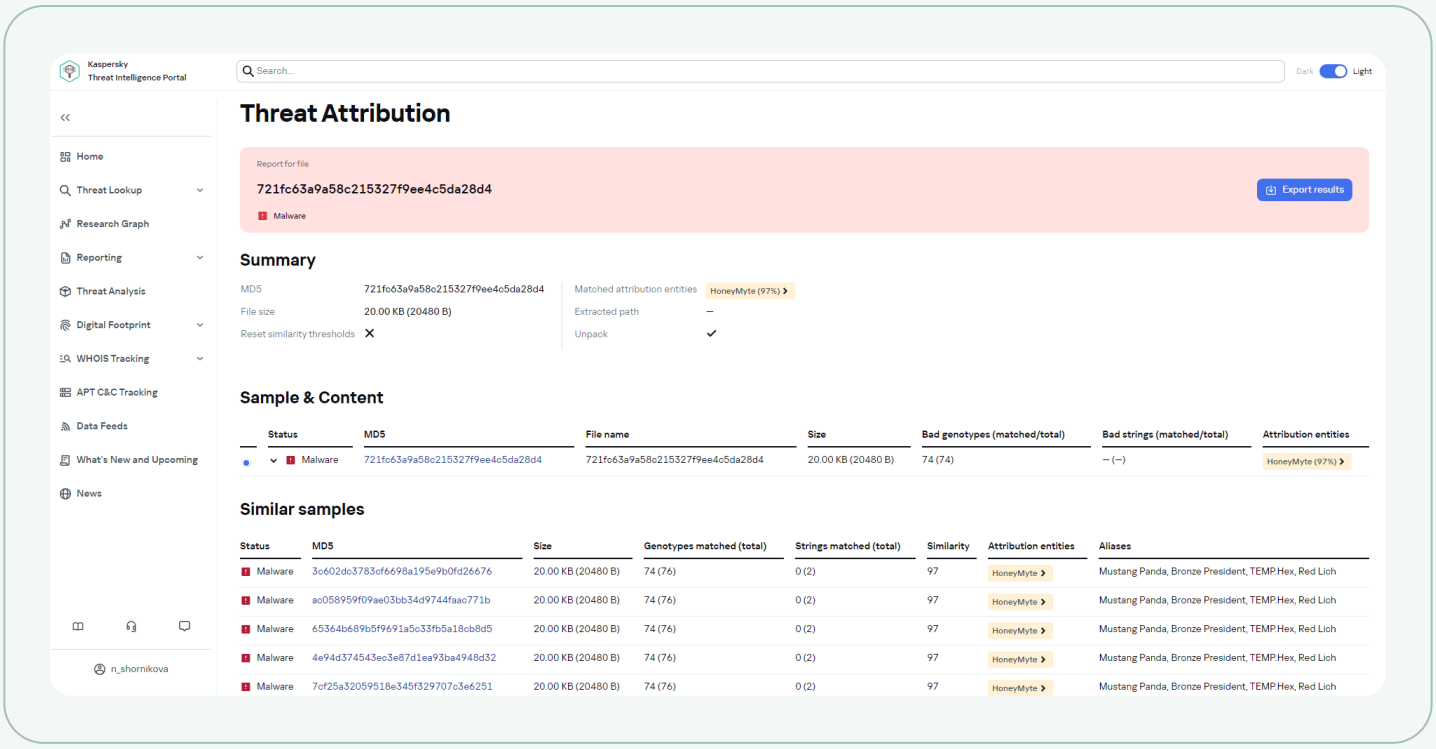
Carga manual de muestras y una API REST mejorada para su integración en flujos de trabajo automatizados.

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 costos, dado que no se necesita invertir en hardware de antemano.

Exportación a reglas YARA para más análisis o 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 exclusivo 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

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.

Operación basada en genotipos y cadenas similares

que se hayan encontrado en las muestras de APT, que genera un informe sobre el origen de la muestra analizada, las entidades de atribución relacionadas y cualquier semejanza 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 de vista. Kaspersky Similarity permite la identificación de muestras de archivos con funciones similares, para brindar protección frente a amenazas desconocidas y evasivas.

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

Similitud

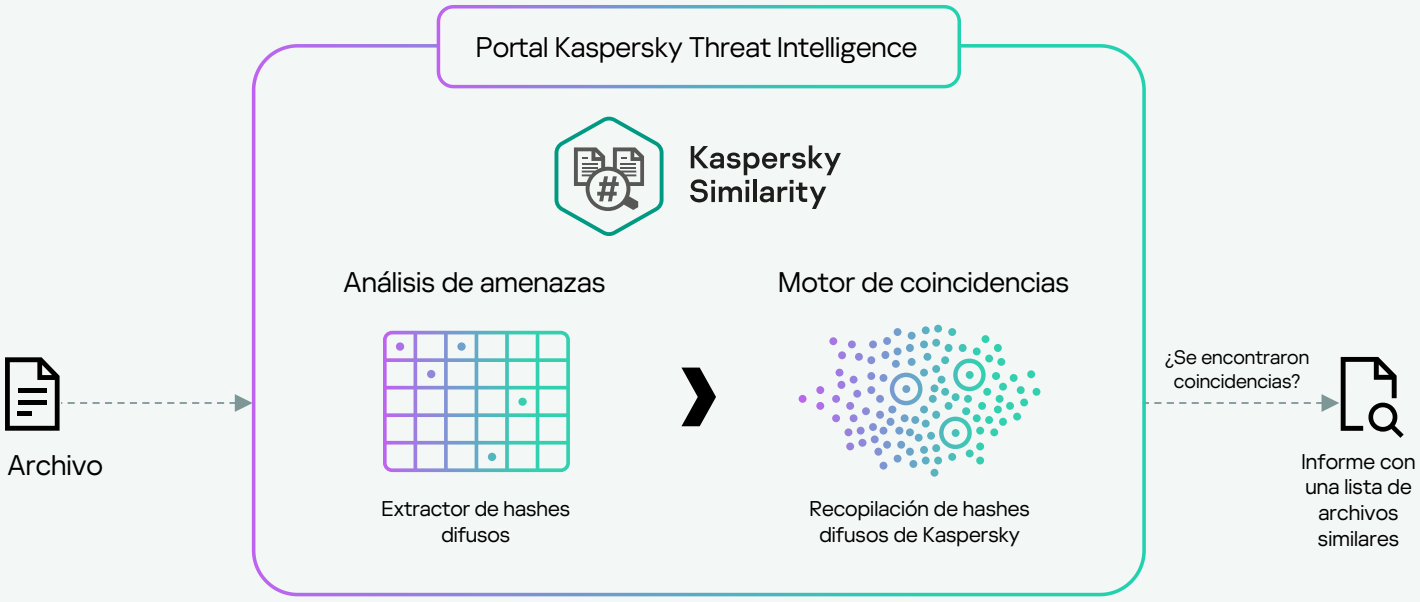
Kaspersky Similarity es una función adicional disponible a través de Threat Intelligence Portal para usuarios de Kaspersky Research Sandbox y Kaspersky Threat Attribution Engine, que ayuda a identificar archivos parecidos que se comportan de manera similar.

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 confiabilidad.

¿Por qué usarlo?

Puede identificar malware similar (por ej., evasivo) y buscarlo en la infraestructura, de manera de tener la confianza de que un pequeño cambio en la muestra, realizado por el adversario, no escapa del radar de seguridad. Esta tecnología se distingue de la atribución: incluso se pueden detectar archivos de malware similares no atribuidos.

Esquema de trabajo de alto nivel de Kaspersky Similarity



Informes de similitud

Cada archivo tiene un formato específico, empaquetadores usados, secciones, cadenas, tablas de importación, etc. Los expertos de Kaspersky crearon un conjunto de hashes para determinar la similitud entre diferentes archivos, en función de estos atributos. Kaspersky Similarity les permite a los usuarios enviar un archivo sospechoso, extraer sus hashes difusos y compararlos con hashes difusos de archivos 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 según la puntuación de similitud. El informe contiene el contexto adicional, con metadatos para cada archivo similar:

- Confiabilidad 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 de archivo

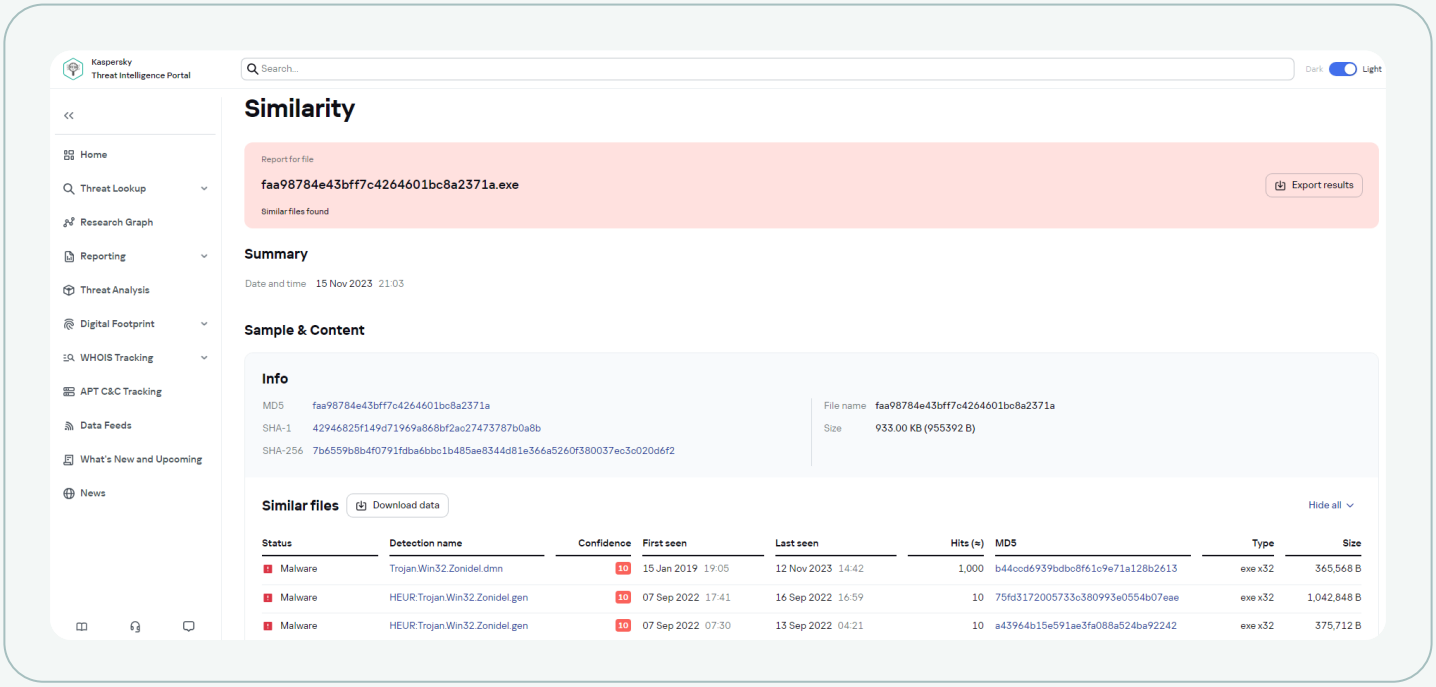
Puntos destacados de la funcionalidad

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

Carga manual de muestras y una API REST mejorada para su integración en flujos de trabajo automatizados.

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

Los expertos de Kaspersky ya la utilizan de manera extendida 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 a incidentes

Descubrimiento de amenazas evasivas

Análisis dinámico/estático de archivos sospechosos

Descubrimiento de la relación entre un nuevo malware y cierto atacante, para conocer posibles movimientos de ataque futuros

Búsqueda de amenazas

Análisis de infraestructura para los IoC recibidos a través del informe

Detección de posibles modificaciones maliciosas de archivos limpios populares

Identificación de los 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 identificar y clasificar ataques avanzados. Ayuda a los equipos de SOC, investigadores de seguridad y analistas de malware a mantenerse informados acerca de las amenazas relacionadas con malware existente y emergente, lo que les permite priorizar y abordar amenazas críticas de manera rápida y solucionarlas con mayor eficiencia.

Kaspersky Threat Analysis

Más información

https://latam.kaspersky.com

#kaspersky
#bringonthefuture