kaspersky PREPARADOS PARA EL FUTURO

Kaspersky Threat Attribution Engine

El seguimiento, el análisis, la interpretación y la mitigación de las amenazas para la seguridad de IT es una tarea colosal, puesto que no dejan de evolucionar. La inteligencia ante amenazas tiene un valor real más allá de lo que se espera de un foco emergente en el sector de la seguridad de la información, y la atribución de amenazas es probablemente el punto de interés y la contención más importantes en lo que respecta a la inteligencia ante amenazas.

Aspectos destacados del producto:

- Proporciona acceso instantáneo a un repositorio de datos seleccionados sobre cientos de actores y muestras de APT.
- 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 abierta para su integración en flujos de trabajo automatizados.
- Se puede implementar en entornos seguros y aislados para proteger sus sistemas y datos y, al mismo tiempo, cumplir los requisitos normativos pertinentes.
- Mantiene una privacidad y confidencialidad absolutas en todos los envíos para evitar la exposición de información confidencial.

Y existe una razón clara para ello. El tiempo medio entre la detección y la respuesta suele ser demasiado largo en casos de amenazas muy sofisticadas debido al empleo de complejos procesos de investigación e ingeniería inversa. En muchos casos, es suficiente para que los atacantes logren sus objetivos. La atribución correcta y oportuna no solo ayuda a reducir los tiempos de respuesta a incidentes de horas a minutos, sino que también reduce la cantidad de falsos positivos.

Identificar un ataque dirigido, evaluar el perfil de los atacantes y crear factores de atribución para los diferentes actores de amenazas es un trabajo extenso y exhaustivo que puede tardar años. La creación de atribuciones operativas también requiere una gran cantidad de datos acumulados en el transcurso de los años, así como un equipo de investigadores altamente capacitado y con experiencia en dicho tipo de investigación. En conjunto, los investigadores realizan un seguimiento de la actividad de diferentes grupos y completan la base de datos con los fragmentos de información. De este modo, la base de datos se convierte en un recurso valioso que se puede compartir como una herramienta.

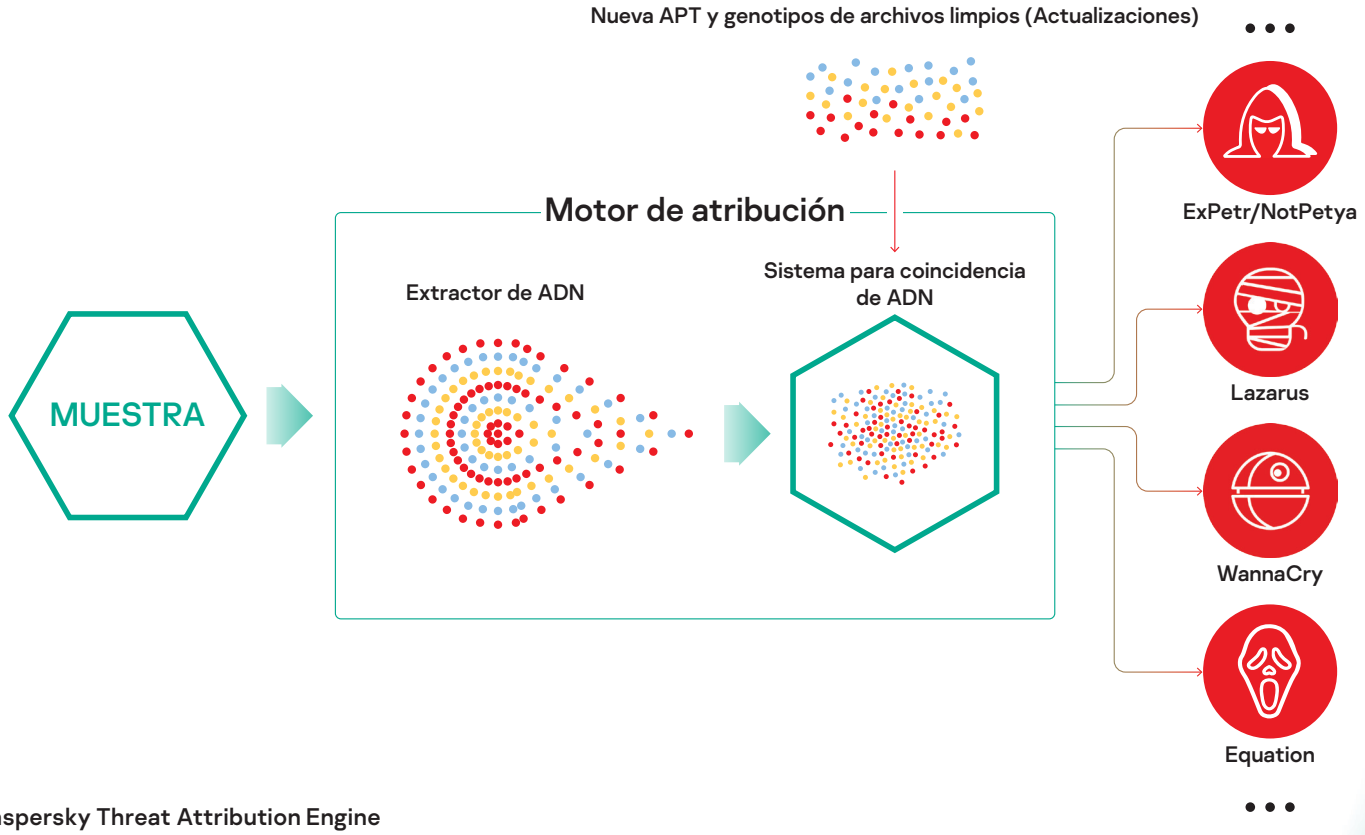
Kaspersky Threat Attribution Engine incorpora la base de datos de muestras de malware APT y permite limpiar los archivos recopilados por los expertos de Kaspersky durante los últimos 22 años. Realizamos el seguimiento de más de 600 actores y campañas de amenazas y, cada año, publicamos más de 120 informes sobre inteligencia de APT. Nuestra investigación constante respalda la realidad de la exhaustiva recopilación de APT que contiene más de 60 000 archivos. Mejora la detección de indicadores falsos y hace que la atribución sea lo más precisa posible con las herramientas automatizadas.

El producto ofrece un enfoque único para comparar las muestras por su similitud, a la vez que garantiza índices sin falsos positivos. Puede vincular rápidamente un nuevo ataque al malware APT conocido, a los ataques dirigidos anteriores y a grupos de hackers, lo que ayuda a diferenciar la amenaza de alto riesgo entre incidentes menos graves y a tomar medidas de protección oportunas para evitar que un atacante obtenga acceso al sistema.

Funcionamiento

Kaspersky Threat Attribution Engine analiza la "genética" del malware mediante la búsqueda de similitudes de código con muestras de APT investigadas y actores vinculados anteriormente de forma automatizada. Compara los "genotipos", como pequeños archivos binarios de los archivos descompuestos, con la base de datos de muestras de malware APT y proporciona un informe sobre el origen del malware, los agentes de amenazas y la similitud de los archivos con muestras de APT conocidas. Además, el producto permite que los equipos de seguridad añadan actores y objetos privados a su base de datos, y entrenen al producto para detectar muestras similares a los archivos de su recopilación privada. Con Threat Attribution Engine, el proceso de atribución solo tardará unos segundos en realizar la comparación con los años en los que se solicitó en el pasado.

El producto se puede implementar en un entorno seguro y hermético, lo que restringe el acceso de cualquier tercero a la información procesada y a los objetos enviados. Existe una interfaz API para conectar el motor a otros marcos y herramientas con el fin de implementar la atribución en la infraestructura existente y los procesos automatizados.



Kaspersky Threat Attribution Engine

Puede encontrar información detallada acerca del actor de APT relacionado en los informes de inteligencia de APT de Kaspersky[1]. Como suscriptor de Kaspersky APT Intelligence Reporting, le proporcionamos acceso permanente y en exclusiva a nuestras investigaciones y descubrimientos sobre las APT detectadas al instante, así como a todos los datos técnicos relevantes en una amplia variedad de formatos. A dicha información también se incorporan las amenazas que nunca se harán públicas.

Kaspersky Threat Attribution Engine amplía y fortalece aún más la cartera de Kaspersky para agencias de ciberseguridad nacional y centros de operaciones de seguridad (SOC) comerciales apoyándolos en el establecimiento de un proceso de administración de incidentes eficaz.

Kaspersky Attribution Engine mejora significativamente las operaciones de seguridad ayudando a realizar las siguientes actividades:

- Atribuir archivos rápidamente a los actores de APT conocidos para revelar las motivaciones, los métodos y las herramientas detrás de los incidentes cibernéticos.
- Evaluar con rapidez si usted es el objetivo del ataque o es una víctima secundaria para así establecer los procedimientos de contención y respuesta adecuados.
- Garantizar una mitigación de amenazas eficaz y oportuna de acuerdo con la inteligencia ante amenazas utilizable en la familia de APT de Kaspersky APT Intelligence Reporting.

1 Se debe adquirir una suscripción a Kaspersky APT Intelligence Reporting por separado

Noticias de ciberamenazas: www.securelist.lat
Noticias sobre seguridad de IT: business.kaspersky.com
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

Seguridad probada, independiente y transparente. Nos comprometemos a construir un mundo más seguro en el que la tecnología nos mejore la vida. Por eso la protegemos, para que todas las personas del mundo puedan beneficiarse de las oportunidades que brinda la tecnología. Proteja su futuro gracias a la ciberseguridad.

Más información en kaspersky.es/transparency

Proven. Transparent. Independent.