Anticípese a sus adversarios

Kaspersky Threat Intelligence

kaspersky BRING ON THE FUTURE

Kaspersky Threat Intelligence

Kaspersky Threat Intelligence le da acceso a la inteligencia que necesita para mitigar las ciberamenazas, proporcionada por nuestro equipo líder mundial de investigadores y analistas.

Los conocimientos, la experiencia y la profunda inteligencia de Kaspersky en todos los aspectos de la ciberseguridad nos convierten en el partner de confianza de los organismos de seguridad y gobierno más importantes del mundo, entre las que se incluyen la Interpol e importantes equipos CERT. Kaspersky Threat Intelligence le ofrece acceso inmediato a inteligencia frente a amenazas tácticas, operativas y estratégicas.

Además, Kaspersky Threat Intelligence ofrece una visión integral del panorama mundial de las amenazas, ya que combina fuentes de inteligencia, fuentes de datos de amenazas e investigación interna, todo ello analizado por nuestro equipo de especialistas para ofrecer información práctica que permita a las organizaciones protegerse contra las ciberamenazas.

Kaspersky Threat Intelligence le da poder

Identifique y prevenga amenazas de forma proactiva

Kaspersky Threat Intelligence le informa sobre las últimas amenazas y vulnerabilidades, para que así pueda tomar medidas proactivas a fin de proteger sus sistemas antes de que se produzca un ataque.

Obtenga visibilidad de su huella digital

Kaspersky Threat Intelligence le proporciona una visión integral de su huella digital, e incluye cualquier activo que pueda ser vulnerable a un ataque o riesgo.

Mejore su capacidad de detección de amenazas

Kaspersky Threat Intelligence le permite aumentar sus soluciones de seguridad existentes con la inteligencia frente a amenazas más reciente, lo que mejora su capacidad de detección y bloqueo de amenazas avanzadas.

Mejore su respuesta ante incidentes

Kaspersky Threat Intelligence ofrece información en tiempo real sobre amenazas emergentes e indicadores de peligro, para que pueda responder con rapidez y eficacia a los incidentes.

Cumpla con normativas y estándares

Todas las empresas están sujetas a diversos estándares y normativas dentro de su sector. Kaspersky Threat Intelligence respalda el cumplimiento de normativas, ya que le brinda ayuda para cumplir con estos requisitos.

Enriquezca sus habilidades internas

El equipo de especialistas de Kaspersky se encuentra entre los investigadores con mayor experiencia y aprecio del sector, y brinda una gran cantidad de conocimientos y experiencia a sus equipos de seguridad de la información.

Kaspersky Threat Data Feeds

Los ciberataques se producen todos los días. Las ciberamenazas crecen constantemente en frecuencia, complejidad y ofuscación, a medida que intentan comprometer sus defensas. Sus adversarios usan complicadas cadenas de ataque de intrusiones, campañas y tácticas, y técnicas y procedimientos (TTP) personalizados para interrumpir sus actividades comerciales o hacerles daño a sus clientes. Una protección eficaz requiere nuevos métodos, basados en la inteligencia frente a amenazas.

Al integrar las fuentes de inteligencia frente a amenazas más actualizadas con información sobre IP, URL y hashes de archivos sospechosos y peligrosos a sistemas de seguridad existentes (como SIEM, SOAR y plataformas de inteligencia sobre amenazas), los equipos de seguridad pueden automatizar el proceso inicial de evaluación de alertas a la vez que proporcionan a sus especialistas en evaluación el contexto suficiente para identificar de inmediato las alertas que deben investigarse o derivarse a equipos de respuesta ante incidentes para una mayor investigación y respuesta.

Las fuentes de datos de amenazas de Kaspersky ofrecen información de inteligencia frente a amenazas en tiempo real para que pueda proteger sus redes y sistemas de las ciberamenazas. Las fuentes de datos incluyen información sobre malware, sitios web de phishing y las últimas vulnerabilidades y exploits conocidos, y otros tipos de ciberamenazas, e información que le permitirá bloquear el tráfico malicioso, actualizar su software de seguridad y tomar otras medidas de protección contra los ciberataques.

Datos contextuales

Todos los registros de cada fuente de datos se mejoran con contexto útil (nombres de amenazas, marcas de tiempo, geolocalización, direcciones IP resueltas de recursos web infectados, hashes, popularidad, entre otros). Los datos contextuales permiten tener un panorama general lo que valida y respalda el amplio uso de los datos. En contexto, los datos pueden usarse para responder con mayor facilidad a las preguntas "quién, qué, dónde y cuándo" a fin de identificar a sus adversarios, permitirle tomar decisiones rápidas y actuar.

Cómo funciona

1

Los datos se recopilan a partir de una amplia variedad de fuentes de confianza, como Kaspersky Security Network y nuestras propias arañas web, el servicio de supervisión de amenazas de redes de bots (rastrea redes de bots y sus objetivos las 24 horas del día, los 7 días de la semana), trampas de spam, datos de grupos de investigación, partners, y mucho más.

2

Toda la información recopilada se verifica y depura con atención y en tiempo real mediante diversos métodos de preprocesamiento: entornos de prueba, análisis estadístico y heurístico, herramientas de similitud, elaboración de perfiles de comportamiento y análisis de especialistas.

3

Las fuentes de datos permiten recopilar información sobre amenazas acerca de una alerta o incidente, y profundizar en los detalles. También ayudan a responder las preguntas "¿quién?, ¿qué?, ¿dónde? y ¿por qué?", y a identificar el origen de un ataque, lo que permite tomar decisiones rápidas para proteger su empresa de amenazas de cualquier complejidad.

Las entradas de las fuentes que brinda Kaspersky incluyen datos contextuales que le permiten confirmar y priorizar las amenazas con rapidez:

- Nombres de las amenazas
- Direcciones IP y nombres de dominio de recursos web maliciosos
- Hashes de archivos maliciosos
- Objetos vulnerables y en riesgo
- Tácticas, técnicas y procedimientos de ataque según la clasificación de MITRE ATT&CK
- Marcas de tiempo
- Geolocalización
- Popularidad, y más

Beneficios de Kaspersky Threat Data Feeds

Mejore y acelere la respuesta ante incidentes y las capacidades de análisis forense

automatizando el proceso de evaluación inicial y proporcionando a sus analistas de seguridad el contexto suficiente para identificar de inmediato las alertas que se deben investigar o escalar a los equipos de respuesta ante incidentes para una mayor investigación y respuesta.

Refuerce sus soluciones de seguridad

incluidos SIEM, firewalls, sistemas IPS/IDS, proxies de seguridad, soluciones DNS, soluciones contra APT, con contexto procesable e indicadores de compromiso (IoC) continuamente actualizados para obtener información sobre los ciberataques y una mayor comprensión de la intención, las capacidades y los objetivos de sus adversarios. Los principales SIEM (como HP ArcSight, IBM QRadar, MS Sentinel, Splunk, etc.) y las plataformas de IT son totalmente compatibles.

Evite la filtración de activos confidenciales y propiedad intelectual

de los equipos infectados fuera de su organización. Detecte con rapidez los activos infectados para proteger la reputación de su marca, mantener su ventaja competitiva y asegurar oportunidades comerciales.

Haga crecer su empresa de MSSP

proporcionando inteligencia frente a amenazas líder del sector como servicio premium a sus clientes. Como CERT, mejore y amplíe sus capacidades de identificación y detección de ciberamenazas.

Kaspersky CyberTrace

El continuo crecimiento de la cantidad de fuentes de datos de amenazas y de fuentes de inteligencia frente a amenazas disponibles dificulta a las empresas la tarea de determinar qué información es relevante para ellas. Al mismo tiempo, la inteligencia frente a amenazas se presenta en muchos formatos diferentes e incluye un gran número de indicadores de compromiso (IoC), lo que dificulta su procesamiento por parte de los SIEM y otros controles de seguridad de la red.

Mediante la integración de la inteligencia frente a amenazas más actualizada y legible por máquina a los controles de seguridad existentes (como los sistemas SIEM), los centros de operaciones de seguridad pueden automatizar el proceso de evaluación inicial y, al mismo tiempo, ofrecer a sus analistas de seguridad suficiente contexto para identificar de inmediato las alertas que se deben investigar o derivar a los equipos de respuesta ante incidentes para una mayor investigación y respuesta.

Kaspersky CyberTrace es una plataforma de inteligencia frente a amenazas que permite una integración perfecta de las fuentes de datos de amenazas con las soluciones SIEM para ayudar a los analistas a aprovechar con mayor eficacia la inteligencia sobre amenazas en su actual flujo de trabajo de operaciones de seguridad. Se integra con cualquier fuente de inteligencia frente a amenazas (de Kaspersky, otros proveedores, OSINT o las fuentes de sus clientes) en formatos JSON, STIX, XML y CSV, y admite la integración inmediata con numerosas soluciones de SIEM y fuentes de registros.

Instrumentos

Kaspersky CyberTrace ofrece un conjunto de instrumentos para operar la inteligencia frente a amenazas con eficacia:

Una base de datos de indicadores con búsqueda de texto completo y la capacidad de realizar búsquedas mediante consultas avanzadas permite realizar búsquedas complejas en todos los campos de indicadores, incluidos los de contexto.

Las estadísticas del uso de fuentes para medir la eficacia de las fuentes integradas y la matriz de intersección de fuentes permiten seleccionar los proveedores de inteligencia frente a amenazas más importantes.

El etiquetado de IoC simplifica su administración. Puede crear cualquier etiqueta y especificar su peso (importancia) y usarla para etiquetar IoC de forma manual. También puede ordenar y filtrar IoC de acuerdo con estas etiquetas y sus pesos.

Un gráfico de investigación permite explorar de forma visual datos y detecciones almacenados en CyberTrace y descubrir características de las amenazas.

La función de exportación de indicadores permite exportar conjuntos de indicadores a controles de seguridad como listas de políticas (listas de bloqueo) y compartir datos sobre amenazas entre instancias de Kaspersky CyberTrace o con otras plataformas informáticas.

La función de correlación histórica (RetroScan) le permite analizar los elementos observables de eventos previamente comprobados usando las fuentes más recientes para encontrar amenazas que no se habían detectado.

La multitenencia es compatible con los MSSP y los casos de uso de grandes empresas.

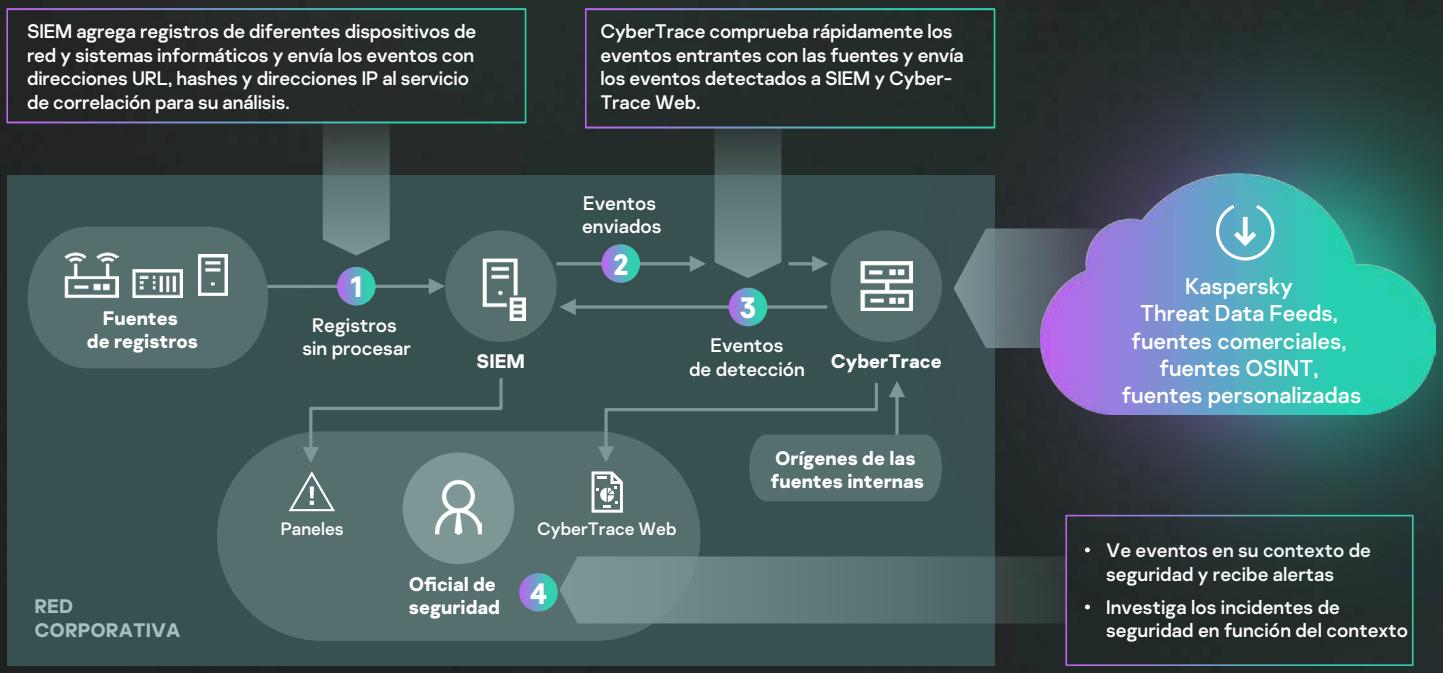
Un filtro envía eventos de detección a las soluciones de SIEM, lo que reduce la carga de los SIEM y de los analistas.

HTTP RestAPI le permite buscar y gestionar la inteligencia frente a amenazas.

Las páginas con información detallada sobre cada indicador brindan un análisis aún más profundo. En cada página, encontrará la información completa sobre un indicador de todos los proveedores de inteligencia frente a amenazas (desduplicación) para que los analistas puedan evaluar las amenazas en los comentarios y agregar inteligencia interna sobre el indicador.

La herramienta usa un proceso interno de análisis y correlación de datos entrantes, lo que reduce en gran medida la carga de trabajo de SIEM. Kaspersky CyberTrace analiza los registros y eventos entrantes, concilia rápidamente los datos resultantes con las fuentes y genera sus propias alertas de detección de amenazas.

Arquitectura



Kaspersky CyberTrace y lKaspersky Threat Data Feeds permiten que sus analistas de seguridad realicen las siguientes acciones:

Sintetizar y priorizar grandes cantidades de alertas de seguridad con eficacia

Mejorar y acelerar los procesos de evaluación y respuesta inicial

Formar una defensa proactiva e inteligente

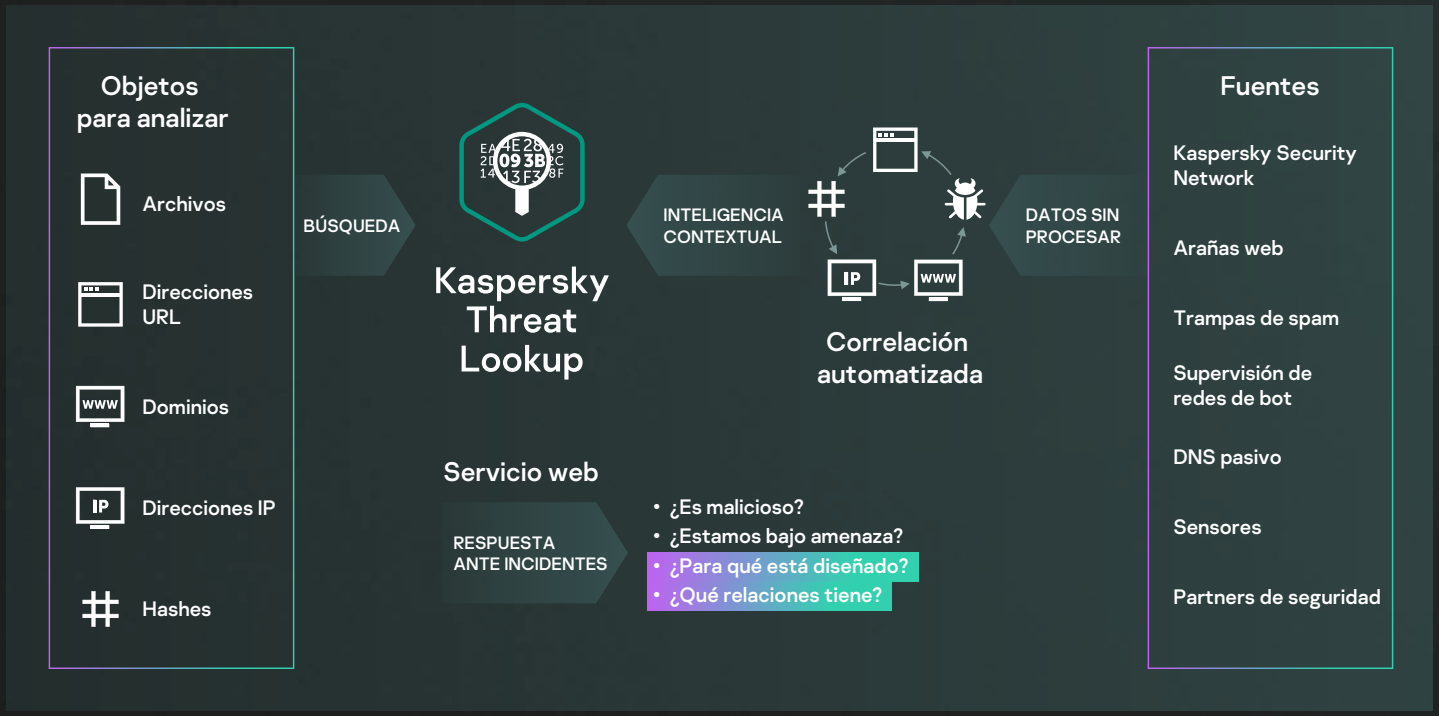
Identificar de inmediato las alertas críticas para la empresa y tomar decisiones más informadas sobre cuáles se deben escalar a los equipos de respuesta ante incidentes

Kaspersky Threat Lookup

La ciberdelincuencia no conoce fronteras y sus capacidades técnicas mejoran con rapidez. Los ciberdelincuentes usan recursos de la red oscura para amenazar a sus objetivos, por lo que los ataques son cada vez más sofisticados. Las ciberamenazas crecen constantemente en frecuencia, complejidad y ofuscación, a medida que se realizan nuevos intentos de comprometer sus defensas. Los atacantes usan complicadas cadenas, así como tácticas, técnicas y procedimientos (TTP) personalizados en sus campañas para interrumpir las actividades empresariales, robar sus activos y hacerles daño a sus clientes.

Kaspersky Threat Lookup ofrece todos los conocimientos adquiridos por Kaspersky Lab sobre ciberamenazas y sus relaciones, y los reúne en un único y potente servicio web. El objetivo es proporcionar a los equipos de seguridad la mayor cantidad de datos posible, para evitar ciberataques antes de que afecten a su organización. La plataforma recupera la inteligencia frente a amenazas más reciente y detallada sobre URL, dominios, direcciones IP, hashes de archivos, nombres de amenazas, datos estadísticos y de comportamiento, datos de WHOIS y DNS, atributos de archivos, datos de geolocalización, cadenas de descarga, marcas de tiempo, entre muchos otros. El resultado es una visibilidad global de las amenazas nuevas y emergentes, que le permite proteger su organización y mejorar sus índices de respuesta ante incidentes.

Cómo funciona



Aspectos destacados

Inteligencia de confianza

Un atributo clave de Kaspersky Threat Lookup es la fiabilidad de nuestros datos de inteligencia frente a amenazas, que se mejoran con contexto útil. Kaspersky lidera el campo de las pruebas antimalware, lo que demuestra la calidad inigualable de nuestra inteligencia de seguridad al proporcionar los más altos índices de detección, sin apenas falsos positivos.

Caza de amenazas

Debe actuar de forma proactiva en la prevención y detección de ataques, y también en la respuesta a ellos, para minimizar su impacto y frecuencia. Se debe realizar un seguimiento de los ataques y eliminarlos de forma drástica lo antes posible. Cuanto antes se detecte una amenaza, menos daños provocará, antes será posible llevar a cabo las reparaciones necesarias y con mayor prontitud podrán volver a la normalidad las operaciones de red.

Fácil de usar

Interfaz web o RESTful API. Use el servicio en modo manual mediante una interfaz web (a través de un navegador web) o acceda a través de una simple RESTful API, según sus preferencias.

Amplia gama de formatos de exportación

Exporte indicadores de compromiso (IoC) o contexto útil sobre los formatos de uso compartido legibles por máquina más ampliamente usados y organizados (como STIX, OpenIOC, JSON, Yara, Snort o incluso CSV) para sacar el máximo beneficio de la inteligencia frente a amenazas, automatizar el flujo de trabajo de operaciones o integrarlos en los controles de seguridad como SIEM.

Beneficios de Kaspersky Threat Lookup

Realice búsquedas exhaustivas sobre indicadores de amenaza con un contexto de amenazas altamente validado que le permite priorizar los ataques y enfocarse en mitigar las amenazas que impliquen el mayor riesgo para su empresa.

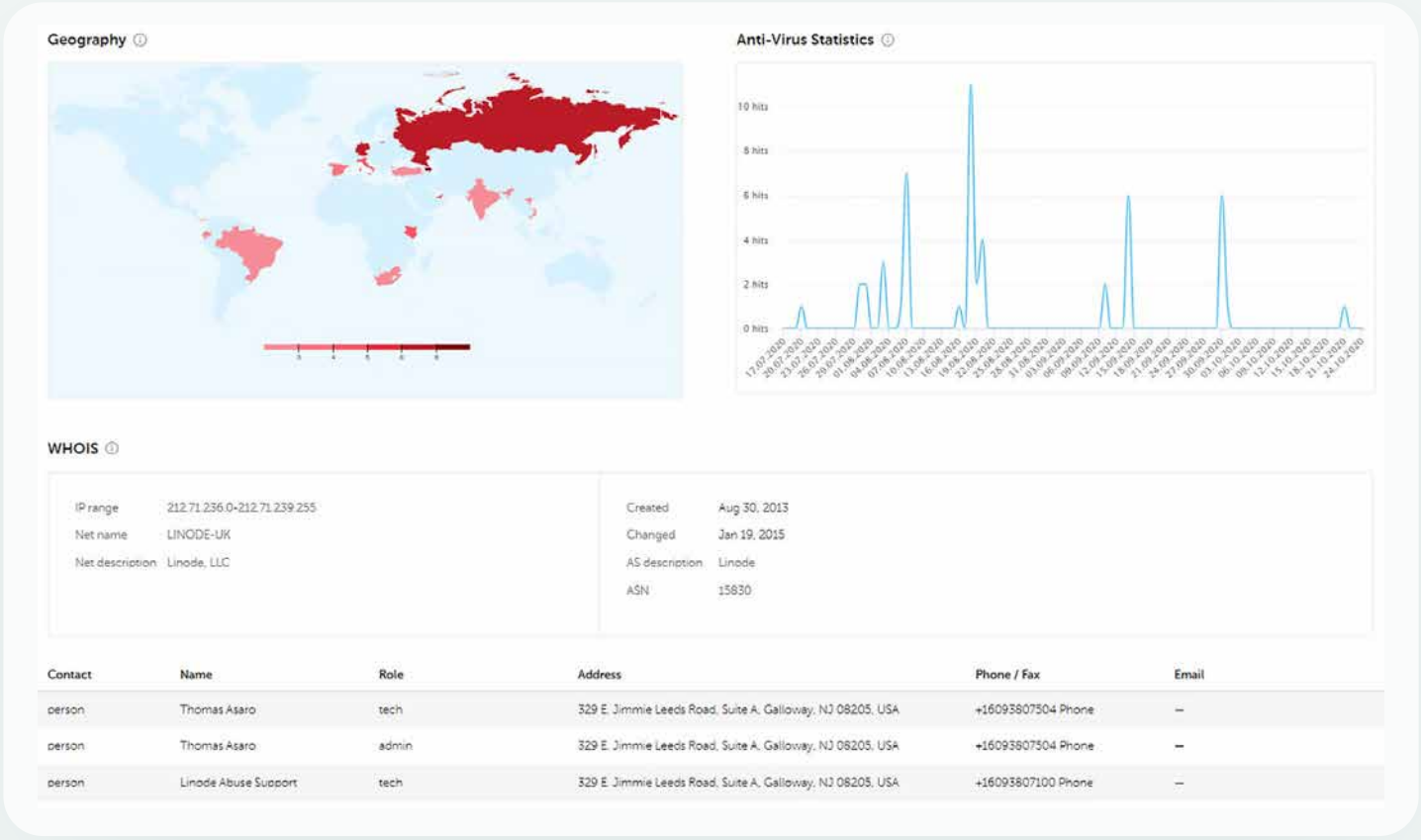
Diagnostique y analice incidentes de seguridad en hosts y en la red de forma más eficiente y eficaz, y priorice las señales de sistemas internos frente a amenazas desconocidas.

Potencie sus capacidades de respuesta ante incidentes y de búsqueda de amenazas para interrumpir la cadena de ataques antes de que los sistemas críticos y los datos estén en riesgo.

Busque indicadores de amenaza desde una interfaz web o RESTful API.

Examine datos avanzados, que incluyen certificados, nombres usados con frecuencia, rutas de archivos o URL relacionadas con el fin de detectar nuevos objetos sospechosos.

Compruebe si el objeto detectado es común o único y comprenda por qué un objeto se debe tratar como malicioso.



Kaspersky Research Sandbox

Es imposible evitar los ataques dirigidos solo con herramientas antivirus tradicionales. Los motores antivirus solo pueden detener las amenazas conocidas y sus variantes, mientras que los actores de amenazas sofisticados usan una enorme gama de técnicas para eludir la detección automática. Las pérdidas derivadas de incidentes de seguridad de la información siguen creciendo, lo que evidencia la importancia de la detección inmediata de amenazas para garantizar una respuesta rápida y contrarrestarlas antes de que se produzca un daño significativo.

Tomar una decisión inteligente basada en el comportamiento de un archivo, a la vez que se analiza la memoria de procesamiento, la actividad de la red, entre otras cuestiones, es la mejor estrategia para entender las sofisticadas amenazas dirigidas y personalizadas más recientes. Aunque los datos estadísticos pueden carecer de información sobre malware modificado hace poco tiempo, las tecnologías con entornos de prueba son herramientas poderosas que permiten la investigación de los orígenes de las muestras de archivos, la recopilación de IoC basados en el análisis de comportamiento y la detección de objetos maliciosos no identificados con anterioridad.

Kaspersky Research Sandbox le permite investigar los orígenes de las muestras de archivos, recopilar IoC basados en análisis de comportamiento y detectar objetos maliciosos antes no vistos. Ofrece un enfoque híbrido que combina la inteligencia frente a amenazas proveniente de petabytes de datos estadísticos (gracias a Kaspersky Security Network y otros sistemas patentados), el análisis de comportamiento y una sólida antievasión con tecnologías de simulación del comportamiento humano, tales como auto clickers, desplazamientos de documentos y procesos ficticios.

Detección y mitigación de amenazas proactivas

El malware usa una variedad de métodos para ocultar su ejecución y pasar desapercibido. 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 pruebas debe ser capaz de imitar con precisión el comportamiento normal del usuario final.

Kaspersky Research Sandbox ofrece un enfoque híbrido que combina la inteligencia frente a amenazas proveniente de petabytes de datos estadísticos (gracias a Kaspersky Security Network y otros sistemas patentados), el análisis de comportamiento y una sólida antievasión con tecnologías de simulación del comportamiento humano, tales como auto clickers, desplazamientos de documentos y procesos ficticios.

Este servicio se desarrolló en nuestro laboratorio interno de entornos de prueba y evoluciona desde hace más de una década. La tecnología posee todo el conocimiento sobre el comportamiento de malware de más de 25 años de investigación de amenazas continua. Nos permite detectar más de 400000 objetos maliciosos nuevos cada día y proporcionar a nuestros clientes soluciones de seguridad líderes en el sector.

Kaspersky Research Sandbox se puede administrar tanto desde una plataforma de gestión centralizada basada en la nube, como desde una consola sin conexión en entornos aislados, para aprovechar la inteligencia frente a amenazas e incorporar reglas de detección personalizables.

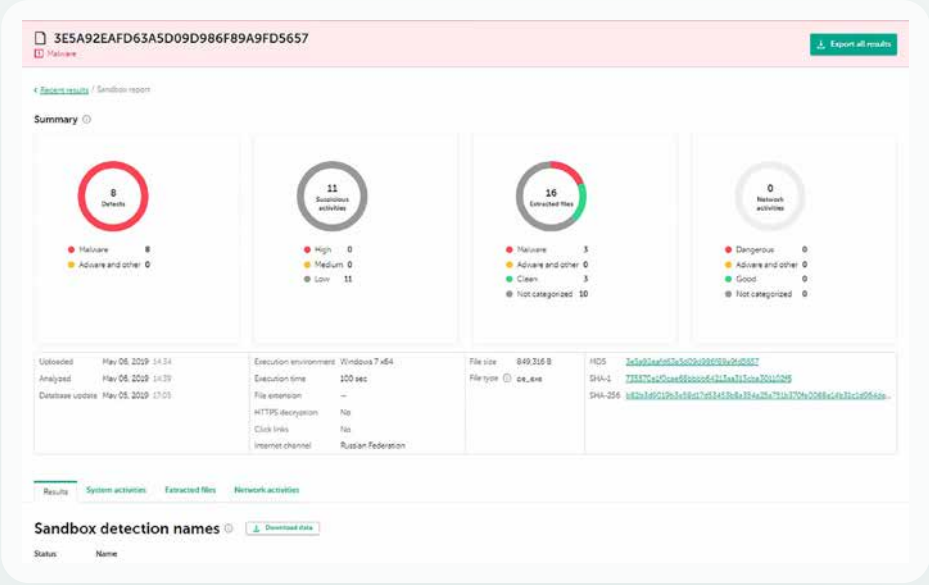
Como parte del portal de inteligencia frente a amenazas, Cloud Research Sandbox es el componente final en su flujo de trabajo de inteligencia sobre amenazas. Mientras Threat Lookup recupera la inteligencia detallada frente a amenazas más reciente relacionada con direcciones URL, dominios, direcciones IP, hashes de archivos, nombres de amenazas, datos estadísticos y de comportamiento, datos de WHOIS/DNS, entre otros, Research Sandbox permite vincular ese conocimiento con los IoC que genera la muestra analizada.

Informes integrales

- Puntuación unificada de amenazas
- Actividades del sistema sospechosas con descripciones detalladas
- DLL cargados y ejecutados
- Archivos creados, modificados y eliminados
- Volcados de memoria de procesos y volcados de tráfico de red (PCAP)
- Extensiones mutuas creadas (mutexes)
- Claves de registro creadas y modificadas
- Procesos creados por el archivo ejecutado
- Actividades de red (SMB, SMTP, IP, TCP, UDP, DNS, SSL, FTP, IRC, POP3, sesiones SOCKS, HTTP(s), solicitudes y respuestas)
- Inteligencia detallada frente a amenazas con contexto práctico para cada indicador de compromiso (IoC) descubierto
- Mapa detallado de ejecuciones con las técnicas MITRE ATT&CK resaltadas
- Detección y activación de reglas IDS por parte de YARA (incluidas las personalizadas)
- Descarga y análisis de un archivo alojado en una determinada URL
- Clics en vínculos de documentos de Microsoft Office (Word, Excel, PowerPoint, Publisher, Outlook) y Adobe Reader
- Posibilidad de exportar los detalles del análisis en formatos STIX, JSON, CSV
- Variedad de entornos, incluido el sistema operativo móvil (Android), y capacidades de personalización del entorno
- Parámetros personalizados de ejecución de archivos
- Diferentes canales de Internet, posibilidad de dirigir el tráfico a través de un canal de VPN personalizado
- RESTful API
- Capturas de pantalla y mucho más

Con Kaspersky Research Sandbox puede llevar a cabo complejas y eficaces investigaciones de incidentes, con las que obtendrá una comprensión inmediata de la naturaleza de la amenaza, para luego hacer deducciones lógicas mientras realiza un análisis detallado con el fin de revelar los indicadores de amenazas interrelacionados.

La inspección puede consumir muchos recursos, en especial cuando se trata de ataques de múltiples etapas. Kaspersky Research Sandbox potencia sus actividades forenses y de respuesta ante incidentes, lo que permite escalar respecto del procesamiento de archivos automático sin tener que adquirir dispositivos costosos ni preocuparse por los recursos del sistema.



Kaspersky Threat Attribution Engine

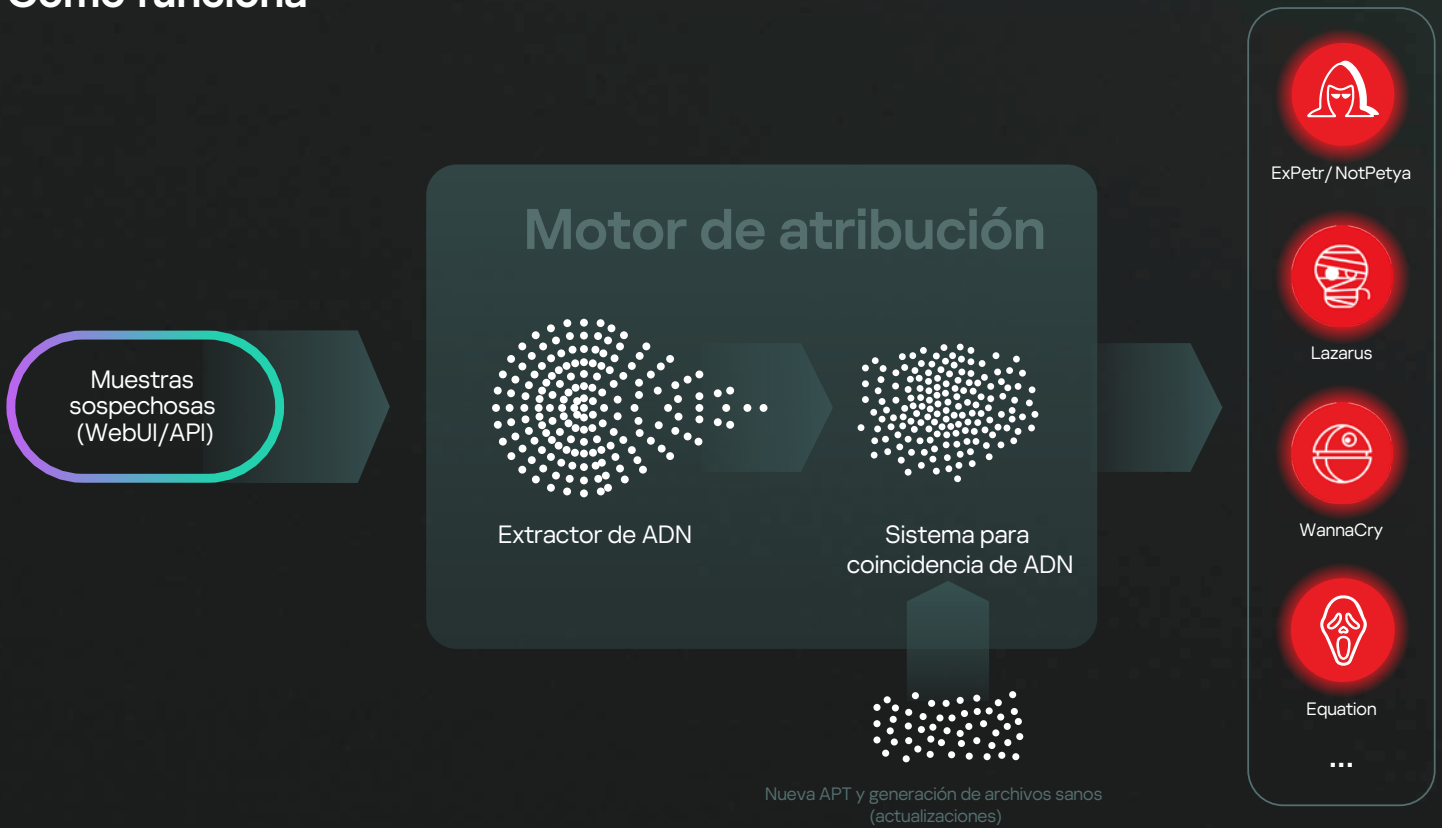
Hay una buena razón por la cual la atribución de amenazas tiene un papel tan importante en la ciberseguridad. El retraso promedio entre la detección de amenazas muy sofisticadas y la respuesta ante ellas puede ser extremadamente prolongado debido a los complejos procesos de investigación e ingeniería inversa que implican. En muchos casos, este retraso puede darles a los atacantes el tiempo suficiente para lograr sus objetivos. La atribución correcta y oportuna no solo permite reducir los tiempos de respuesta ante incidentes de horas a minutos, sino que también minimiza 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 complejo que puede tardar años. Además, la creación de una atribución útil requiere una gran cantidad de datos acumulados a lo largo del tiempo y un equipo muy habilidoso de investigadores con la experiencia pertinente en investigación. Estos investigadores, por lo general, seguirán la actividad de diferentes grupos y completarán la base de datos con toda la información recopilada. Entonces, esta base de datos se convierte en un valioso recurso que se puede compartir para usarlo como herramienta.

Kaspersky Threat Attribution Engine incorpora la base de datos de muestras de malware APT y archivos sanos que recopilan especialistas de Kaspersky desde hace más de 25 años. Hacemos seguimiento a más de 1100 atacantes y campañas, y publicamos más de 120 informes sobre inteligencia frente a amenazas al año. Nuestra continua investigación respalda la recopilación de APT, que contiene alrededor de 83 000 archivos. Esto mejora la detección de indicadores falsos y, junto con el uso de herramientas automatizadas, da como resultado niveles de atribución altamente precisos.

El producto ofrece un enfoque único para comparar muestras similares mientras garantiza índices casi nulos de falsos positivos. Todos los nuevos ataques se pueden vincular rápidamente con un malware APT conocido, grupos de hackers y ataques dirigidos anteriores, lo cual permite distinguir las amenazas de alto riesgo de los incidentes menos serios, con el fin de que pueda tomar medidas proactivas a tiempo y así evitar que un atacante logre un punto de apoyo en su sistema.

Cómo funciona



Para vincular el malware con las entidades de atribución, Kaspersky Threat Attribution Engine usa un método patentado único de búsqueda de similitudes entre archivos. Este método abarca lo siguiente:

1

Análisis de la genética de una muestra mediante la extracción de los siguientes elementos de su código:

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

2

Búsqueda automática en los archivos analizados de genotipos y cadenas que se parezcan a los genotipos y las cadenas de muestras de APT que se habían analizado anteriormente o que ya estaban vinculados con entidades de atribución.

3

Generación de un informe sobre el origen de la muestra analizada, entidades de atribución relacionadas y toda similitud entre esta muestra y muestras conocidas de APT, en función de genotipos y cadenas similares que se hayan encontrado en las muestras de APT.

El producto se puede implementar en un entorno seguro y aislado, lo que restringe el acceso de cualquier tercero a la información procesada y a los objetos enviados. Una API conecta Engine a otros marcos y herramientas con el fin de implementar la atribución en la infraestructura existente y los procesos automatizados.

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).
- Permite una priorización de las amenazas y una evaluación de las alertas automáticas o manuales eficaces.
- Admite la incorporación de actores y objetos privados al entrenar al producto para que detecte muestras similares a los archivos almacenados en sus ubicaciones privadas.
- Permite la carga manual de muestras y ofrece una funcionalidad de RESTful API mejorada para integrarlas con flujos de trabajo automatizados.
- Admite la implementación en Amazon Web Services (AWS), lo que permite una configuración rápida del producto y un ahorro de costos, dado que no se necesita invertir en hardware de antemano.
- Exporta con facilidad a reglas YARA para realizar más búsquedas o análisis automatizados de archivos similares o integraciones con soluciones de terceros.
- Exporta con facilidad a formato STIX 2.1 (los formatos TXT y JSON también son compatibles) para realizar un análisis más automatizado de registros de seguridad o integración con controles de seguridad o soluciones de terceros.
- Permite descomprimir archivos protegidos con contraseñas mediante contraseñas personalizadas.
- Proporciona acceso fácil a documentación y al Contrato de licencia de usuario final (EULA) en la interfaz web.
- Envía atributos en archivos paralelos para su análisis en una única solicitud.

Beneficios de Kaspersky Threat Attribution Engine

Kaspersky Threat Attribution Engine calcula la puntuación de reputación

de la muestra y revela su genética y atribución de código. Esto ofrece datos acerca del origen de la muestra y puede permitir su atribución a posibles autores.

Su equipo de seguridad puede agregar sus propias entidades privadas de atribución

y muestras relacionadas a la base de datos de Kaspersky Threat Attribution Engine. El equipo puede entrenar la aplicación para que atribuya las muestras enviadas a estas muestras y entidades de atribución privadas.

El proceso de atribución solo lleva segundos

en comparación con los meses y años que se requerían antes.

Kaspersky Threat Attribution Engine amplía y fortalece

la cartera de Kaspersky para agencias de ciberseguridad nacional y centros de operaciones de seguridad (SOC) comerciales brindándoles apoyo en el establecimiento de un proceso de administración de incidentes eficaz.

Kaspersky APT Intelligence Reporting

Los clientes de Kaspersky APT Intelligence Reporting reciben un acceso único y continuo a nuestras investigaciones y descubrimientos, incluidos datos técnicos completos (en una variedad de formatos) sobre cada APT a medida que se descubren, así como sobre las amenazas que nunca se harán públicas. Los informes contienen un resumen ejecutivo que ofrece a los directivos información orientada y fácil de entender, y que describe la APT relacionada, junto con una descripción técnica detallada de la APT con los IoC y las reglas YARA relacionadas para brindar a los investigadores de seguridad, analistas de malware, ingenieros de seguridad, analistas de seguridad de redes e investigadores de APT datos procesables que permitan emitir una respuesta rápida y precisa ante la amenaza.

Nuestros especialistas también le enviarán notificaciones de inmediato sobre cualquier cambio que detecten en las tácticas de los grupos ciberdelincuentes. Además, tendrá acceso a la base de datos completa de informes de ATP, otro componente de investigación y análisis importante en sus defensas de seguridad.

Más de 300
actores de amenaza

Más de 160
informes privados al año

Más de 12 000
indicadores de compromiso

Más de 400
campañas

Más de 700
reglas Yara

Oferta de Kaspersky APT Intelligence Reporting

Perfiles de actores de amenazas

Asignación a MITRE ATT&CK

Resumen ejecutivo

Información orientada a directivos

Análisis técnico detallado
- Métodos de ataque
- Exploits usados
- Descripción del malware
- Descripciones de protocolos e infraestructura de C&C
- Análisis de víctimas
- Análisis de filtración de datos
- Atribuciones

Conclusiones y recomendaciones

Indicadores de compromiso (IoC) y reglas YARA

Beneficios de Kaspersky APT Intelligence Reporting

Información acerca de APT no públicas

Por diversas razones, no todas las amenazas de alto perfil se hacen públicas, pero las compartiremos con usted.

Acceso privilegiado

Recibirá descripciones técnicas sobre las amenazas más recientes durante investigaciones en curso antes de que se hagan públicas.

Análisis retrospectivo

Acceso a todos los informes privados publicados con anterioridad durante todo el período de suscripción.

Acceso a datos técnicos

Incluye una lista ampliada de IoC, disponible en formatos estándar, como openIOC o STIX y acceso a nuestras reglas YARA.

Información sobre los perfiles de los actores de amenazas

Incluidos el posible país de origen y la actividad principal, las familias de malware usadas, los sectores y las zonas geográficas de destino, y las descripciones de todos los TTP usados, con asignación a MITRE ATT&CK.

Integración y automatización perfectas

RESTful API para una integración y automatización perfectas de sus flujos de trabajo de seguridad.

Supervisión continua de campañas de APT

Acceso a inteligencia procesable durante la investigación con información sobre la distribución de APT, IoC, infraestructura de mando y control, etc.

MITRE ATT&CK

Todos los TPP descritos en los informes se asignan a MITRE ATT&CK, lo que facilita una mejor detección y respuesta mediante el desarrollo y priorización de los casos de uso de supervisión de seguridad correspondientes, la realización de análisis de brechas y la prueba de las defensas actuales contra los TPP relevantes.

Kaspersky Crimeware Intelligence Reporting

El ciberdelito impulsado por motivos económicos no se limita a sectores específicos. Y mientras los ataques contra dispositivos de infraestructuras financieras, como cajeros automáticos y puntos de venta (PoS), continúen, todas las empresas de todos los sectores están expuestas al ransomware. En estos últimos dos años, se observó que los límites entre los distintos tipos de actores y amenazas se volvieron más difusos. Esto incluye la aparición de campañas de amenazas persistentes avanzadas (APT) centradas no solo en el ciberespionaje, sino también en el robo de dinero para financiar otras actividades en las que participa el grupo de APT. No debemos subestimar la creciente sofisticación de las amenazas por crimeware.

Kaspersky Crimeware Intelligence Reporting mejora las estrategias defensivas con información oportuna sobre campañas de malware, ataques dirigidos contra instituciones financieras e información sobre herramientas de crimeware usadas para atacar bancos, empresas de procesamiento de pagos y sus infraestructuras específicas.

Oferta de Kaspersky Crimeware Intelligence Reporting

- Descripciones detalladas de malware popular, extendido y ampliamente usado
- Notas de investigación y advertencias tempranas, que incluyen información sobre amenazas de malware nuevas y actualizadas
- Información sobre campañas de malware peligrosas y extendidas
- Descripciones detalladas de amenazas dirigidas contra infraestructuras financieras y sus herramientas de ataque correspondientes que los ciberdelincuentes desarrollan o venden en la red oscura en varias zonas geográficas

Beneficios de Kaspersky Crimeware Intelligence Reporting

Acceso privilegiado

Recibirá descripciones técnicas sobre las amenazas más recientes durante investigaciones en curso antes de que se hagan públicas.

Análisis retrospectivo

Acceso a todos los informes privados publicados con anterioridad durante todo el período de suscripción.

Integración y automatización perfectas

RESTful API para una integración y automatización perfectas de sus flujos de trabajo de seguridad.

Acceso a datos técnicos

Incluye una lista ampliada de IoC, disponible en formatos estándar, como openIOC o STIX y acceso a nuestras reglas YARA.

Información sobre los perfiles de los actores de crimeware

Incluidos el posible país de origen y la actividad principal, las familias de malware usadas, los sectores y las zonas geográficas de destino, y las descripciones de todos los TTP usados, con asignación a MITRE ATT&CK.

Kaspersky ICS Threat Intelligence Reporting

Kaspersky ICS Threat Intelligence Reporting ofrece inteligencia detallada y un mayor conocimiento de las campañas maliciosas que apuntan a las organizaciones industriales, así como información sobre las vulnerabilidades que se encuentran en los sistemas de control industrial (ICS) más populares y las tecnologías subyacentes. Los informes se entregan a través de Kaspersky Threat Intelligence Portal, lo que significa que puede comenzar a usar el servicio de inmediato.

Todas las investigaciones de inteligencia frente a amenazas relacionadas con ICS las realiza un equipo específico, Kaspersky ICS CERT:

- Fundado en 2016
- Primer equipo CERT creado por una organización comercial
- Alrededor de 20 especialistas muy calificados en investigación de amenazas y vulnerabilidades de ICS, respuesta ante incidentes y análisis de seguridad

Informes que se incluyen en su suscripción

Informes de APT

Informes sobre nuevas APT y campañas de ataque de gran volumen dirigidas a organizaciones industriales, así como actualizaciones de amenazas activas.

Vulnerabilidades encontradas

Informes sobre vulnerabilidades identificadas por Kaspersky en los productos más populares usados en sistemas de control industrial, Internet industrial de las cosas e infraestructuras en diversos sectores

Análisis y mitigación de vulnerabilidades

En nuestras asesorías, recibirá recomendaciones prácticas de los especialistas de Kaspersky para poder identificar y mitigar las vulnerabilidades en su infraestructura.

Evolución del panorama de amenazas

Informes sobre cambios significativos en el panorama de amenazas para los sistemas de control industrial, factores críticos recién detectados que afecten los niveles de seguridad de ICS y exposición de ICS a amenazas, con información regional, nacional y sectorial

Qué podrá hacer con los datos de inteligencia frente a amenazas

Detención y prevención

Informes de amenazas para proteger los activos importantes, como los componentes de software y hardware, y garantizar la seguridad y la continuidad del proceso tecnológico

Evaluación de vulnerabilidades

Evaluación de la vulnerabilidad de sus activos y entornos industriales basada en análisis precisos del alcance y la gravedad de la vulnerabilidad para tomar decisiones fundamentadas sobre la administración de parches o la implementación de otras medidas preventivas recomendadas por Kaspersky

Correlación

Atribución de cualquier actividad sospechosa y maliciosa que detecte en entornos industriales con los resultados de la investigación de Kaspersky a la campaña maliciosa en cuestión, identificación de amenazas y respuesta rápida ante incidentes

Aprovechamiento de la información

Información sobre tecnologías, tácticas y procedimientos de ataques, vulnerabilidades recientemente descubiertas y otros cambios importantes en el panorama de amenazas para realizar lo siguiente:

- Identificar y evaluar los riesgos planteados por las amenazas notificadas y otras amenazas similares.
- Planificar y diseñar cambios en la infraestructura industrial para garantizar la seguridad de la producción y la continuidad de los procesos tecnológicos.
- Realizar actividades de concientización sobre seguridad basadas en el análisis de casos reales para crear situaciones de capacitación de personal y planificar ejercicios de "equipo rojo contra equipo azul".
- Tomar decisiones estratégicas fundamentadas para invertir en ciberseguridad y garantizar la resiliencia de sus operaciones.

Kaspersky Digital Footprint Intelligence

A medida que su empresa crece, la complejidad y la distribución de sus entornos informáticos también lo hacen, lo que plantea un reto: proteger su presencia digital de amplia distribución sin control directo ni propiedad. Los entornos dinámicos e interconectados permiten a las empresas obtener importantes beneficios. Sin embargo, la interconectividad, cada vez más expandida, también está ampliando la superficie de ataque. A medida que los atacantes se vuelven más hábiles, es vital no solo tener una imagen precisa de la presencia en línea de su organización, sino también ser capaz de rastrear sus cambios y reaccionar ante las amenazas externas dirigidas a los activos digitales expuestos.

Las organizaciones usan una amplia gama de herramientas de seguridad en sus operaciones de protección, pero sigue habiendo amenazas digitales al acecho que requieren capacidades muy específicas: detectar y mitigar filtraciones de datos, supervisar planes y esquemas de ataque de los ciberdelincuentes ubicados en foros de la red oscura, etc. Para ayudar a sus analistas de seguridad a explorar la visión de los adversarios sobre los recursos de su empresa, descubrir los posibles vectores de ataque de los que dispone con rapidez y ajustar sus defensas en consecuencia, Kaspersky creó Kaspersky Digital Footprint Intelligence.

Oferta de Kaspersky Digital Footprint Intelligence

Reconocimiento de la red

Identificación de los recursos de red del cliente y de los servicios expuestos que son un posible punto de entrada para desplegar un ataque. Análisis personalizado de las vulnerabilidades existentes, con puntuación adicional y evaluación integral de los riesgos en función de la puntuación base CVSS, la disponibilidad de exploits públicos, la experiencia en pruebas de penetración y la ubicación de los recursos de red (hospedaje e infraestructura).

Protección de marca

Supervisión y bloqueo del uso no autorizado de la marca de una empresa en línea. Identificación de cuentas y aplicaciones falsas en redes sociales, sitios web de phishing y otras actividades fraudulentas que pueden dañar la reputación de una empresa o engañar a los clientes. Eliminación de cuentas falsas de redes sociales y aplicaciones falsas en mercados móviles.

Vigilancia de la red oscura

Supervisión continua de recursos de la red oscura (foros, blogs de ransomware, servicios de mensajería instantánea, sitios tor, etc.), detectando cualquier referencia y amenaza relacionada con su empresa, clientes y partners. Análisis de ataques dirigidos activos o en fase de planificación, campañas de APT dirigidas a su empresa, industria y regiones de operación.

Descubrimiento de filtraciones de datos

Detección de credenciales en riesgo de empleados, partners y clientes, tarjetas bancarias, números de teléfono y otra información confidencial que pueda usarse para desplegar un ataque o pueda suponer riesgos para la reputación de su empresa.

Fuentes de inteligencia

Es esencial que usted tenga una comprensión integral de la postura de seguridad externa de la empresa. Para brindar esta información, los analistas de seguridad de Kaspersky recopilan y agregan información de las siguientes fuentes de inteligencia:

Sus datos no estructurados

- Direcciones IP
- Dominios de la empresa
- Marcas
- Palabras clave

Inventario del perímetro de la red

Red oscura, profunda y superficial

Base de conocimientos de Kaspersky

Informes analíticos

Alertas de amenazas

Diez solicitudes de eliminación al año

Búsqueda en tiempo real en las fuentes de Kaspersky, OSINT, la red superficial y la red oscura

Cómo funciona

Configuración	Recopilación	Filtrado	Reacción
Descubrimiento de información sobre los activos digitales de la empresa	Recopilación automatizada de datos de las redes superficiales, profundas y oscuras, y de la base de datos de inteligencia frente a amenazas de Kaspersky	Detección de amenazas, análisis y priorización gestionados por analistas	Envío de inteligencia completa

Valores empresariales

Kaspersky Digital Footprint Intelligence ofrece potentes beneficios y un valor significativo a su organización:

Proteja su marca

Detecte amenazas potenciales en tiempo real para proteger la reputación de su marca, preservar la confianza de sus clientes y reducir el riesgo de pérdidas financieras y daños en las operaciones empresariales.

Reduzca los riesgos cibernéticos

Brinde a las partes interesadas (director de experiencia de cliente y junta directiva) información sobre dónde ubicar el gasto en ciberseguridad lo que revelará las brechas de la configuración actual y los riesgos que acarrean.

Reaccione más rápido

El contexto adicional de las alertas de seguridad mejora la respuesta ante incidentes y reduce su tiempo medio de respuesta (MTTR).

Reduzca la superficie de ataque

Gestione la presencia digital de su empresa y controle los recursos de red externos para minimizar los vectores de ataque y las vulnerabilidades que pueden usarse en un ataque.

Comprenda a sus adversarios

Más vale prevenir que curar: sepa lo que los ciberdelincuentes planean y mencionan sobre su empresa en la red oscura para que la empresa esté preparada.

Conozca lo desconocido

Mejore su capacidad de resistencia ante ciberataques e identifique las amenazas externas a la jurisdicción de sus equipos de seguridad internos.

Kaspersky Takedown Service

Los ciberdelincuentes crean dominios maliciosos y de phishing que se usan para atacar a su empresa y sus marcas. La incapacidad para mitigar estas amenazas con rapidez, una vez identificadas, puede provocar una pérdida de ingresos, daños a la marca, pérdida de confianza de los clientes, filtraciones de datos, y mucho más. De todos modos, gestionar la eliminación de estos dominios es un proceso complejo que requiere experiencia y tiempo.

Kaspersky Takedown Service mitiga rápidamente las amenazas planteadas por los dominios maliciosos y de phishing antes de que causen algún daño a su marca y empresa. La gestión integral del proceso completo les ahorra a los clientes tiempo y recursos valiosos. El servicio se ofrece en todo el mundo.

Kaspersky bloquea más de 15 000 direcciones URL de phishing o estafas, y evita más de un millón de intentos de hacer clic en este tipo de URL cada día. Nuestra gran experiencia en el análisis de dominios maliciosos y de phishing significa que sabemos cómo recopilar toda la evidencia necesaria para comprobar que sean maliciosos. Nos ocuparemos de gestionar su eliminación y permitiremos acciones rápidas para minimizar los riesgos digitales, a fin de que su equipo pueda concentrarse en otras tareas prioritarias.

Kaspersky protege de manera eficaz los servicios en línea y la reputación de sus clientes mediante el trabajo colaborativo con organizaciones internacionales, agencias de seguridad nacionales y regionales (como la Interpol, Europol, la Unidad de delitos digitales de Microsoft, la Unidad nacional de delitos de alta tecnología [NHTCU] de la Policía Nacional de los Países Bajos y la Policía de la ciudad de Londres), así como con los equipos de respuesta ante emergencias informáticas (CERT) de todo el mundo.

Cómo funciona

Puede enviar sus solicitudes a través de Kaspersky CompanyAccount, nuestro portal corporativo de atención al cliente. Prepararemos toda la documentación necesaria y enviaremos la solicitud de eliminación a la autoridad local o regional pertinente (CERT, registro, etc.) que tenga los derechos legales necesarios para cerrar el dominio. Recibirá notificaciones en cada paso del proceso hasta que el recurso solicitado se elimine con éxito.

Protección sin esfuerzo

Kaspersky Takedown Service mitiga rápidamente las amenazas planteadas por los dominios maliciosos y de phishing antes de que causen algún daño a su marca y empresa. La gestión integral del proceso completo le ahorra tiempo y recursos valiosos.

Visibilidad completa

Se le informará en cada fase del proceso, desde el registro de su solicitud hasta la eliminación exitosa.

Administración integral

Gestionaremos todo el proceso de eliminación y minimizaremos su participación.

Cobertura mundial

No importa dónde esté registrado un dominio malicioso o de phishing, Kaspersky solicitará su eliminación a la organización regional con la autoridad legal pertinente.

Integración con Kaspersky Digital Footprint Intelligence

Kaspersky Takedown Service puede comprarse por separado, pero su integración con Kaspersky Digital Footprint Intelligence aprovecha al máximo la sinergia natural entre estos servicios. Kaspersky Digital Footprint Intelligence envía notificaciones en tiempo real sobre dominios de phishing y malware que pueden enviarse de inmediato a Kaspersky Takedown Service para su bloqueo.

Kaspersky Ask the Analyst

Los ciberdelincuentes desarrollan todo el tiempo formas sofisticadas de atacar a las empresas. Actualmente, la volátil situación de las amenazas está en rápido crecimiento y presenta técnicas de ciberdelincuencia cada vez más ágiles. Las organizaciones se enfrentan a incidentes complejos provocados por ataques no relacionados con el malware, ataques sin archivos, ataques "living-off-the-land" (que emplean herramientas de sistemas legítimos), vulnerabilidades de día cero y combinaciones de todos estos ataques integrados en amenazas complejas, similares a APT y ataques dirigidos.

En una época donde los ciberataques perjudican a las empresas, los profesionales de la ciberseguridad son más importantes que nunca. Sin embargo, encontrarlos y conservarlos no es una tarea fácil. Incluso si tiene un sólido equipo de ciberseguridad, no siempre puede esperar que sus especialistas combatan, sin otra ayuda, la guerra contra las amenazas sofisticadas: es importante que puedan obtener asistencia de expertos externos. La experiencia externa puede aclarar la posible trayectoria de los ataques complejos o APT, dar consejos útiles y soporte sobre la forma más decisiva de eliminarlos.

La investigación continua de amenazas permite a Kaspersky descubrir, supervisar e infiltrarse en comunidades y foros de la red oscura de todo el mundo, cuyo acceso está limitado a las personas seleccionadas. Nuestros analistas aprovechan este acceso para detectar e investigar de forma proactiva las amenazas más perjudiciales y notorias, así como las amenazas dirigidas a organizaciones específicas.

Kaspersky Ask the Analyst amplía nuestra cartera de inteligencia frente a amenazas, lo que le permite solicitar asesoramiento e información sobre amenazas específicas a las que se enfrenta o que le interesan. El servicio adapta las potentes capacidades de investigación e inteligencia frente a amenazas de Kaspersky a sus necesidades específicas, lo que le permite construir defensas resistentes contra las amenazas dirigidas a su organización.

Productos de Kaspersky Ask the Analyst (suscripción unificada basada en solicitudes)

APT y crimeware

Información adicional sobre informes publicados e investigaciones en curso (además del servicio APT o Crimeware Intelligence Reporting)

Descripciones de amenazas, vulnerabilidades e IoC relacionados

- Descripción general de una familia específica de malware
- Contexto adicional sobre las amenazas (hashes relacionados, direcciones URL, control numérico computarizado [CnC], etc.)
- Información sobre una vulnerabilidad específica (su nivel de estado crítico y los mecanismos de protección correspondientes en los productos de Kaspersky)

Solicitudes de ICS

- Información adicional sobre informes publicados
- Información de vulnerabilidades de ICS
- Estadísticas y tendencias de amenazas de ICS de una región o sector
- Información de análisis de malware de ICS sobre las normativas o estándares

Inteligencia de la red oscura

- Investigación de la red oscura en determinados artefactos, direcciones IP, nombres de dominio, nombres de archivos, correos electrónicos, vínculos o imágenes
- Análisis y búsqueda de información

Análisis de malware

- Análisis de muestras de malware
- Recomendaciones sobre otras medidas de corrección

Cómo funciona

Kaspersky Ask the Analyst puede comprarse por separado o como complemento de cualquiera de nuestros servicios de inteligencia frente a amenazas. Puede enviar sus solicitudes a través de Kaspersky CompanyAccount, nuestro portal corporativo de atención al cliente. Le responderemos por correo electrónico, pero, si lo desea, podemos organizar una videoconferencia o una sesión de pantalla compartida. Una vez aceptada su solicitud, se le informará del plazo estimado para procesarla.

Casos de uso

1. Aclarar cualquier detalle de los informes de inteligencia frente a amenazas publicados con anterioridad.
2. Obtener inteligencia adicional para los IoC ya proporcionados.
3. Obtener detalles sobre las vulnerabilidades y recomendaciones sobre cómo protegerse contra su abuso.
4. Recibir detalles adicionales sobre actividades específicas de la red oscura que sean de su interés.
5. Obtener un informe general de la familia de malware que incluya su comportamiento, su impacto potencial y detalles sobre cualquier actividad relacionada que Kaspersky haya observado.
6. Priorizar las alertas o incidentes de forma eficaz con información contextual detallada y la categorización de los IoC relacionados a través de breves informes.
7. Solicitar ayuda para identificar si la actividad inusual detectada está relacionada con una APT o un actor de crimeware.
8. Enviar archivos de malware para realizar un análisis integral que permita comprender el comportamiento y la funcionalidad de las muestras proporcionadas.

Beneficios de Kaspersky Ask the Analyst

Amplíe su experiencia

Obtenga acceso a pedido a los expertos del sector sin tener que buscar ni invertir en especialistas de tiempo completo que son difíciles de encontrar.

Acelere las investigaciones

Analice y priorice los incidentes con eficacia en función de información contextual personalizada y detallada.

Responda con rapidez

Responda rápidamente a las amenazas y vulnerabilidades gracias a nuestra asistencia para bloquear los ataques a través de vectores conocidos.

Amplíe sus conocimientos y recursos

Kaspersky Ask the Analyst le ofrece acceso a un grupo de investigadores de Kaspersky para cada caso en particular. El servicio facilita una comunicación integral entre expertos para aumentar sus capacidades actuales con nuestros conocimientos y recursos únicos.

Conclusión

Contrarrestar las ciberamenazas actuales requiere una visión global de las tácticas y herramientas que usan los actores de amenazas. La generación de esta inteligencia y la identificación de las contramedidas más eficaces requieren una dedicación constante y altos niveles de experiencia. Con los petabytes de datos de amenazas que se pueden extraer, las avanzadas tecnologías de aprendizaje automático y un conjunto exclusivo de expertos de todo el mundo, trabajamos para respaldar a nuestros clientes con la inteligencia frente a amenazas más actualizada de todo el mundo y permitirles conservar su inmunidad incluso ante ciberataques desconocidos.

Beneficios clave

Permite visualizar amenazas globales, detectar ciberamenazas a tiempo, priorizar alertas de seguridad y responder con eficacia ante incidentes de seguridad.

El conocimiento único de las tácticas, las técnicas y los procedimientos que usan los actores en diferentes sectores y regiones le permite protegerse, de forma proactiva, frente a amenazas específicas y complejas.

Una descripción general integral de su estado de seguridad con recomendaciones útiles sobre las estrategias de mitigación le permite enfocarse en su estrategia defensiva en las áreas identificadas como objetivos principales de ciberataque.

Previene el agotamiento de los analistas y ayuda a que su personal se concentre en las verdaderas amenazas.

La respuesta acelerada y mejorada ante incidentes y las capacidades de búsqueda permiten reducir el tiempo de espera contra ataques y minimizar en gran medida los posibles daños.

Kaspersky Threat Intelligence

Más información

latam.kaspersky.com

#kaspersky
#bringonthefuture