kaspersky preparados para el futu

Kaspersky
Threat Intelligence

Kaspersky Threat Data Feeds

Descripción general

¿Qué incluyen las fuentes de datos?

Las entradas de las fuentes proporcionadas por Kaspersky contienen datos contextuales que permiten confirmar y priorizar con rapidez las amenazas:

- Nombres de amenazas
- Direcciones IP y nombres de dominio identificados de recursos web maliciosos
- Hashes de archivos maliciosos
- Identificadores de objetos vulnerables y en riesgo
- Tácticas, técnicas y procedimientos de ataques según la clasificación de MITRE ATT&CK
- Marcas de fecha y hora
- Posición geográfica
- Popularidad, y más

El servicio Kaspersky Threat Data Feed ofrece inteligencia de amenazas en tiempo real, permitiendo a las organizaciones proteger sus redes y sistemas contra ciberamenazas. Estas fuentes de datos incluyen información sobre malware conocido, sitios web de phishing, exploits y vulnerabilidades recientes, entre otros tipos de ciberamenazas. Las organizaciones pueden usar esta información para bloquear el tráfico malicioso, actualizar su software de seguridad y tomar otras medidas para protegerse de los ciberataques.

Los datos se recopilan a partir de una amplia variedad de fuentes confiables, como Kaspersky Security Network, nuestros propios rastreadores web, el servicio de monitoreo de botnets (supervisión 24/7 de las botnets, sus objetivos y actividades), trampas de spam y datos de grupos de investigación y socios.

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.

Las fuentes de datos ayudan a recopilar información general sobre un evento y a profundizar en los detalles. También ayudan a responder a las preguntas "¿Quién? ¿Qué? ¿Dónde? ¿Por qué?" e identificar el origen de un ataque, lo que permite tomar decisiones rápidas y proteger a la empresa de amenazas de cualquier complejidad.

Intelligence Collection

- Telemetría KSN
- Sensores
- Rastreadores web
- DNS pasivo
- Granjas de bots
- Partners
- Trampas de spam/IoT
- OSINT

Intelligence Analysis

- Uso de sandbox
- Investigación humana
- Análisis de reputación
- ML / IA

Intelligence Production

Kaspersky Threat Intelligence → **Kaspersky Threat Data Feeds**

Intelligence Dissemination

Controles de seguridad reforzados de TI

- SIEM
- SOAR
- IRP
- TIP
- EDR
- XDR
- NGFW
- IDS
- IPS
- Proxy
- y otros

¿Cómo usar las fuentes de datos?

Nombre de la fuente	Prevención	Detección	Investigación
Fuente de datos de direcciones URL maliciosas	•	•	•
Fuente de datos de direcciones URL de ransomware	•	•	•
Fuente de datos de dirrecciones URI de phishing	•	•	•
Fuente de datos de direcciones URL de C&C de botnets	•	•	•
Fuente de datos de direcciones URL de C&C de botnets móviles	•	•	•
Fuente de datos de hashes maliciosos	•	•	•
Fuente de datos de hashes maliciosos móviles	•	•	•
Fuente de datos de reputación de direcciones IP	•	•	•
Fuente de datos de direcciones URL de IoT	•	•	•
Fuente de datos de vulnerabilidades	•	•	•
Fuente de datos de vulnerabilidades de ICS	•	•	•
Fuente de datos sobre vulnerabilidades industriales de ICS en formato OVAL		•	
Fuente de datos de hashes de ICS	•	•	•
Fuente de datos de pDNS			•

Nombre de la fuente	Prevención	Detección	Investigación
Fuente de datos de reglas de Suricata		•	
Fuente de datos del agente de seguridad para la nube (CASB)		•	
Fuente de datos de hashes de APT		•	•
Fuente de datos de direcciones IP de APT		•	•
Fuente de datos de direcciones URL de APT		•	•
Fuente de datos de reglas Yara para APT		•	•
Fuente de datos de amenazas a software de código abierto	•	•	•
Fuente de datos de hashes de crimeware		•	•
Fuente de datos de direcciones URL de crimeware			•
Fuente de datos de reglas Yara para crimeware			•
Fuente de datos de reglas Sigma	•		
Fuente de datos de direcciones IP de seguridad de redes	•	•	
Fuente de datos de direcciones URL de seguridad de redes	•	•	
Fuente de datos de filtrado web de seguridad de redes	•	•	

La lista de fuentes de datos de amenazas de Kaspersky se amplía constantemente.

Descripción de las fuentes de datos de amenazas de Kaspersky

Fuentes comerciales

Las fuentes comerciales proporcionan acceso a la colección más integral de información disponible a través de una suscripción. La información se actualiza de forma regular. Según el tipo de fuente, la regularidad de las actualizaciones puede variar de varios minutos a varias horas. Además de las fuentes de datos enumeradas, puede solicitar la creación de una fuente personalizada adaptada a sus necesidades.

Nombre de la fuente	Descripción de la fuente	Tipo de indicador	Casos de uso
Fuente de datos de direcciones URL maliciosas	Recursos web desde los que se distribuye el malware	Máscara	• Los sistemas de administración de seguridad de la información están abiertos al enriquecimiento con fuentes externas de información. La conexión de estos flujos a SIEM / SOAR / IRP permite a los usuarios responder a las amenazas actuales de manera oportuna y crear un contexto adicional cuando se investiga un incidente. • La integración con los sistemas de seguridad de redes y correo electrónico (por ejemplo, NGFW / IDS / IPS / Correo / Seguridad web) ayuda a prevenir incidentes cibernéticos mediante el enriquecimiento de las capacidades nativas de control de seguridad con los indicadores de compromiso (IOC) procedentes de la fuente de datos.
Fuente de datos de direcciones URL de ransomware	Recursos web desde los que se distribuye el ransomware		
Fuente de datos de dirrecciones URl de phishing	Recursos web de phishing		
Fuente de datos de direcciones URL de C&C de botnets	Servidores de comando y control (C&C) de botnets y objetos maliciosos relacionados (bots)		
Fuente de datos de direcciones URL de C&C de botnets móviles	Servidores de C&C de botnets móviles con objetos maliciosos asociados (bots)		

#Prevención

#Detección

#Investigación

Nombre de la fuente	Descripción de la fuente	Tipo de indicador	Casos de uso	
Fuente de datos de hashes maliciosos	Hashes de archivos maliciosos comunes	Hash	• Integración con los sistemas de seguridad de la infraestructura (Endpoint Security, Server Security, Mail / Web Security) para evitar que el malware se descargue y ejecute, así como para detectar el malware ya en ejecución. • La integración con los sistemas SIEM / SOAR / IRP permite a los usuarios responder con rapidez a las amenazas actuales y crear un contexto adicional cuando se investiga un incidente.	#Prevención #Detección #Investigación
Fuente de datos de hashes maliciosos móviles	Hashes de archivos maliciosos comunes para sistemas operativos móviles (Android e iOS)			
Fuente de datos de reputación de direcciones IP	Varias categorías de direcciones IP sospechosas y maliciosas	IP	• La integración con los sistemas de seguridad de redes y correo electrónico (NGFW / Mail Security) ayuda a prevenir incidentes cibernéticos al complementar la base de datos nativa de indicadores de compromiso con datos sobre las amenazas actuales. • La integración con los sistemas de clases SIEM / SOAR / IRP permite a los usuarios responder con rapidez a las amenazas actuales y crear un contexto adicional cuando se investiga un incidente.	#Prevención #Detección #Investigación
Fuente de datos de direcciones URL de IoT	Recursos web que distribuyen software malicioso para dispositivos de IoT (cámaras IP, aspiradoras inteligentes, teteras, cafeteras, etc.)	Máscara		
Fuente de datos de vulnerabilidades	Vulnerabilidades de software empresarial	CVE	• Identificación de elementos vulnerables de la infraestructura mediante la integración con analizadores de vulnerabilidades y sistemas de administración de activos. • Integración con sistemas de protección de endpoints para impedir la ejecución de software que contenga vulnerabilidades críticas. • Detección de la ejecución de software vulnerable. • Asistencia en las investigaciones. • Recomendaciones para mitigar las vulnerabilidades.	#Prevención #Detección #Investigación
Fuente de datos de vulnerabilidades de ICS	Vulnerabilidades en el software y hardware de ICS, así como en el software corporativo usado en la infraestructura de control de procesos.			

Nombre de la fuente	Descripción de la fuente	Tipo de indicador	Casos de uso	
Fuente de datos sobre vulnerabilidades industriales de ICS en formato OVAL	Reglas para las búsquedas automatizadas de vulnerabilidades del software de ICS	Verificación OVAL	• Enriquecimiento de los analizadores de vulnerabilidades de software más conocidos para detectar software de ICS vulnerable.	#Detección
Fuente de datos de hashes de ICS	Archivos maliciosos comunes que representan una amenaza para ICS	Hash	• En el perímetro de las redes OT, de manera similar a los casos de uso de fuentes de datos de hashes maliciosos. • Dentro de las redes OT para detectar archivos potencialmente peligrosos.	#Prevención #Detección #Investigación
Fuente de datos de pDNS	Registros de búsquedas de servidores de nombres de dominio (DNS) para dominios en las direcciones IP correspondientes durante un período de tiempo	IP, FQDN	• Proporcionar contexto en la investigación de incidentes cibernéticos	#Investigación
Fuente de datos de reglas de Suricata	Reglas para detectar varias categorías de amenazas en el tráfico de red, como amenazas avanzadas persistentes (APT), C&C de botnets, ransomware, etc.	Reglas de Suricata	• Integración con sistemas NGFW / IDS / IPS / NTA / NDR para enriquecer las reglas de detección de actividades maliciosas.	#Detección
Fuente de datos del agente de seguridad para la nube (CASB)	Dominios y hosts relacionados con servicios en la nube populares	Máscara	• Creación de una solución de CASB, en particular, para establecer políticas de acceso a los servicios en la nube.	#Detección

Nombre de la fuente	Descripción de la fuente	Tipo de indicador	Casos de uso	
Fuente de datos de hashes de APT	Hashes de archivos usados por grupos de APT para realizar ataques selectivos	Hash	• Integración con los sistemas de seguridad de la infraestructura (Endpoint and Server Security) para evitar que el malware se descargue y ejecute, así como para detectar el malware ya en ejecución. • La integración con los sistemas de seguridad de redes y correo electrónico (por ejemplo, NGFW / IDS / IPS / Correo / Seguridad web) ayuda a prevenir incidentes cibernéticos mediante el enriquecimiento de las capacidades nativas de control de seguridad con los indicadores de compromiso (IOC) procedentes de la fuente de datos. • La integración con sistemas de clase SIEM / SOAR / IRP permite a los usuarios crear un contexto adicional cuando se investiga un incidente, así como responder a tiempo a las amenazas actuales relacionadas con los ataques selectivos o relacionadas con los miembros de grupos de APT.	#Detección #Investigación
Fuente de datos de direcciones IP de APT	Información sobre los elementos de infraestructura necesarios para llevar a cabo ataques selectivos	IP		
Fuente de datos de direcciones URL de APT		Máscara		
Fuente de datos de reglas Yara para APT	Reglas YARA para identificar archivos usados en ataques selectivos	Regla YARA	• Búsqueda proactiva de señales de ataques selectivos en la infraestructura de una organización. • Útil para investigar incidentes cibernéticos.	#Detección #Investigación
Fuente de datos de amenazas a software de código abierto	Paquetes de software de código abierto que contengan vulnerabilidades, funcionalidades maliciosas o que pongan en riesgo funcionalidades por motivaciones políticas (bloqueo en determinadas regiones, eslóganes políticos, etc.)	Nombre y versión del paquete	• Diseñado para el análisis de componentes de software desarrollado como parte del proceso de desarrollo seguro (DevSecOps) con el fin de proteger el software de los ataques a la cadena de suministro, la detección temprana y la eliminación de vulnerabilidades, así como para evitar el uso de paquetes que contengan funciones no declaradas de orientación política (NDV).	#Prevención #Detección #Investigación

Nombre de la fuente	Descripción de la fuente	Tipo de indicador	Casos de uso	
Fuente de datos de hashes de crimeware	Hashes de archivos usados en campañas fraudulentas descritas en los informes de crimeware de Kaspersky	Hash	• Detección de actividad maliciosa asociada a las acciones fraudulentas de los intrusos. • Ayuda en la resolución de incidentes proporcionando información adicional que contienen las fuentes de datos de amenazas.	#Detección #Investigación
Fuente de datos de direcciones URL de crimeware	Información sobre los elementos de infraestructura relacionados con las campañas fraudulentas descritas en los informes de crimeware de Kaspersky	Máscara		
Fuente de datos de reglas Yara para crimeware	Reglas Yara para identificar archivos usados en campañas fraudulentas descritas en los informes de crimeware de Kaspersky	Regla YARA	• Búsqueda proactiva de señales de campañas fraudulentas en la infraestructura de una organización. • Útil para investigar incidentes cibernéticos.	#Investigación
Fuente de datos de reglas Sigma	Reglas en formato YAML para detectar actividades maliciosas	Reglas SIGMA	• Integración con SIEM / EDR para detectar actividades maliciosas	#Detección
Fuente de datos de direcciones IP de seguridad de redes	Lista de direcciones IP para las listas de alertas y rechazados de NGFW	IP	• Integración con los controles de seguridad de red (NGFW) para aumentar su nivel de protección	#Detección #Prevención

Nombre de la fuente	Descripción de la fuente	Tipo de indicador	Casos de uso	
Fuente de datos de direcciones URL de seguridad de redes	Lista de direcciones URL para las listas de alertas y rechazados de NGFW	URL	• Integración con los controles de seguridad de red (NGFW) para aumentar su nivel de protección	#Detección #Prevención
Fuente de datos de filtrado web de seguridad de redes	Lista de dominios categorizados para las listas de alertas y rechazados de NGFW	URL	• Integración con los controles de seguridad de red (NGFW) para aumentar su nivel de protección	#Detección #Prevención

Fuentes de demostración

Las fuentes de demostración son solo para fines de evaluación. Los datos contienen muestras limitadas con información reducida de forma considerable y actualizaciones menos frecuentes.
La estructura de las fuentes es similar al formato de las fuentes comerciales, pero puede variar en algunos casos.

- Fuente de datos de reputación de direcciones IP de demostración
- Fuente de datos de direcciones URL de C&C de botnets de demostración
- Fuente de datos de hashes maliciosos de demostración
- Fuente de datos de direcciones IP de APT de demostración
- Fuente de datos de direcciones URL de APT de demostración
- Fuente de datos de reglas Sigma de demostración
- Fuente de datos de hashes de APT de demostración
- Fuente de datos de reglas de Suricata de demostración
- Fuente de datos de reglas de Suricata de demostración
- Fuente de datos de vulnerabilidades de ICS de demostración
- Fuente de datos de vulnerabilidades de ICS en formato OVAL de demostración
- Fuente de datos de hashes de crimeware de demostración
- Fuente de datos de direcciones URL de crimeware de demostración

Solicite una demo

Kaspersky Threat Intelligence

Su contexto de respaldo valioso

Threat Data Feeds de Kaspersky mejora las capacidades de detección de sus controles de seguridad existentes, incluyendo los sistemas SIEM, los sistemas de detección de intrusos, los proxis de seguridad, etc.

Conozca más

https://latam.kaspersky.com