



Descubra cómo protegerse de sus adversarios: obtenga una visión completa del panorama de amenazas de su organización

Panorama de amenazas en el Portal de Kaspersky Threat Intelligence

kaspersky preparados para el futuro



Kaspersky Threat Intelligence Portal

Panorama de amenazas de su organización en el Portal de Kaspersky Threat Intelligence

El panorama mundial de las amenazas evoluciona constantemente: cada día surgen nuevos métodos de ataque, y los ya conocidos se vuelven más sofisticados. En la actualidad, es cada vez más importante que los equipos de seguridad de la información sean capaces de priorizar con eficacia las amenazas a las que hay que responder con rapidez. Sin embargo, ¿cómo puede centrarse en las vulnerabilidades más importantes para su empresa, industria y región?



Portal de Kaspersky Threat Intelligence

Los usuarios tienen una oportunidad única de evaluar su panorama de amenazas en la sección **Panorama de Amenazas**, diseñada específicamente para proporcionar información sobre los atacantes dirigidos a una industria y región específicas, combinando tecnologías de detección con inteligencia global sobre amenazas. Esta sección proporciona un contexto completo y actualizado sobre las amenazas asociadas a sus posibles adversarios, así como sobre sus tácticas, técnicas y procedimientos (TTP).

Además, proporciona la siguiente **información detallada sobre las amenazas** :



Ubicación geográfica



Industria



Tipos de amenazas



Ciberdelincuentes



Técnicas, tácticas y procedimientos (TTP)



Software malicioso que usan



Indicadores de compromiso (IoC) pertinentes

Los datos de inteligencia de amenazas se recopilan **en tiempo real mediante una serie de sistemas expertos** que Kaspersky ha utilizado durante más de 25 años para combatir la ciberdelincuencia. Entre estos se incluyen Kaspersky Security Network, que recibe datos anónimos de millones de usuarios en todo el mundo, el procesamiento automático de millones de archivos al día, rastreadores web, granjas de bots, trampas de spam, honeypots, sensores, DNS pasivos, fuentes de la red abierta y oscura, y socios. Durante el último cuarto de siglo, usamos estos datos para lograr los puntajes más altos en pruebas independientes y revisiones externas. Los datos obtenidos son analizados minuciosamente por los equipos de investigación de amenazas de Kaspersky y procesados por modernos sistemas automatizados, como entornos de prueba, motores heurísticos y herramientas de similitud, lo que los transforma en información confiable, verificada y actualizada.

Más información

¿Cómo funciona?

Fuentes de Kaspersky Threat Intelli-

Telemetría
KSN

Sensores

Rastreadores web

Granjas de bots

Trampas de
spam/IoT

DNS pasivo

Socios
y OSINT



Analizar

Más de
400 000

Muestras de archivos
maliciosos a diario



Kaspersky
Threat Intelligence
Portal



Perfiles de
ciberdelincuentes

- Nombres/Alias
- Descripciones
- Países/Industrias
- TTP
- Software/Informes



Perfiles de
software

- Nombres/Alias
- Descripciones
- Ciberdelincuentes
- TTP
- Reglas SIGMA



Informes de Kaspersky Threat
Intelligence (APT, crimeware, ICS)

- Reglas YARA, SIGMA, de Suricata
- TTP
- IOC



TTP de MITRE ATT&CK

Threat Landscape



Filtros

Industrias

Países

Ciberdelin-
cuentes

Plataformas

Mapa de calor de
MITRE ATT&CK

Descripciones detalladas de las TTP
basadas en el flujo de datos diarios
de muestras maliciosas

Principales 10 estadísticas

- TTP
- Vulnerabilidades
- Ciberdelincuentes
- Software
- Industrias

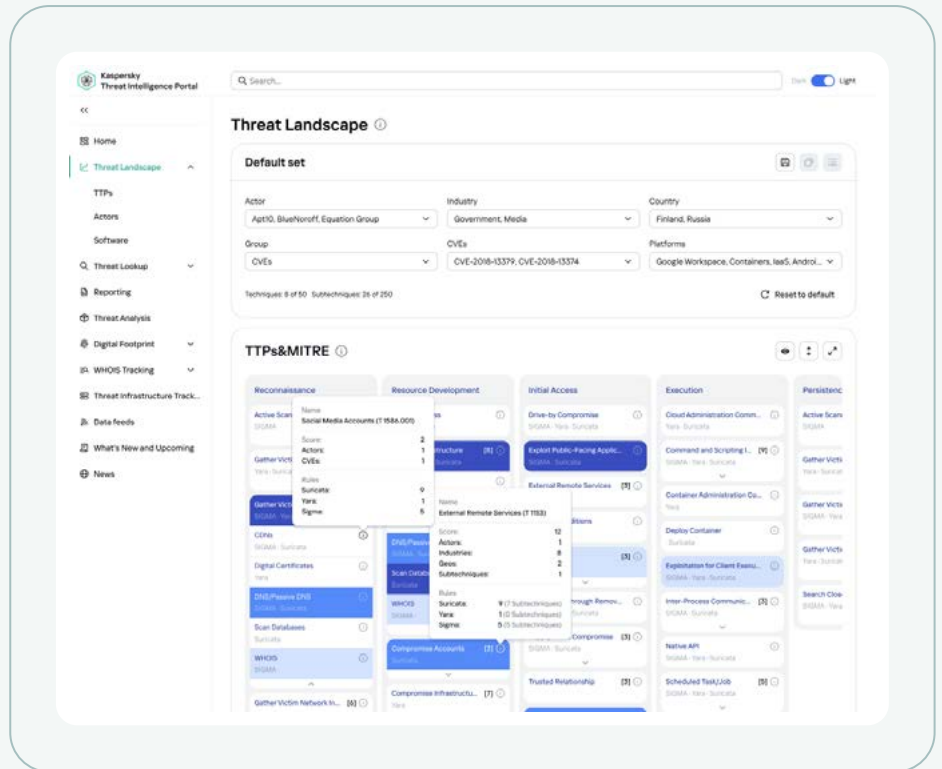
Mitigaciones

Procesamos **cientos de miles de muestras de archivos maliciosos a diario**, extrayendo su geolocalización y datos de la industria. Luego, los sistemas internos de Kaspersky identifican las TTP asociadas y atribuyen los archivos a malware y grupos de ciberdelincuentes conocidos. La sección Panorama de Amenazas también se basa en un flujo continuo de datos de incidentes reales de todo el mundo, proporcionados por nuestros equipos de expertos en investigación.

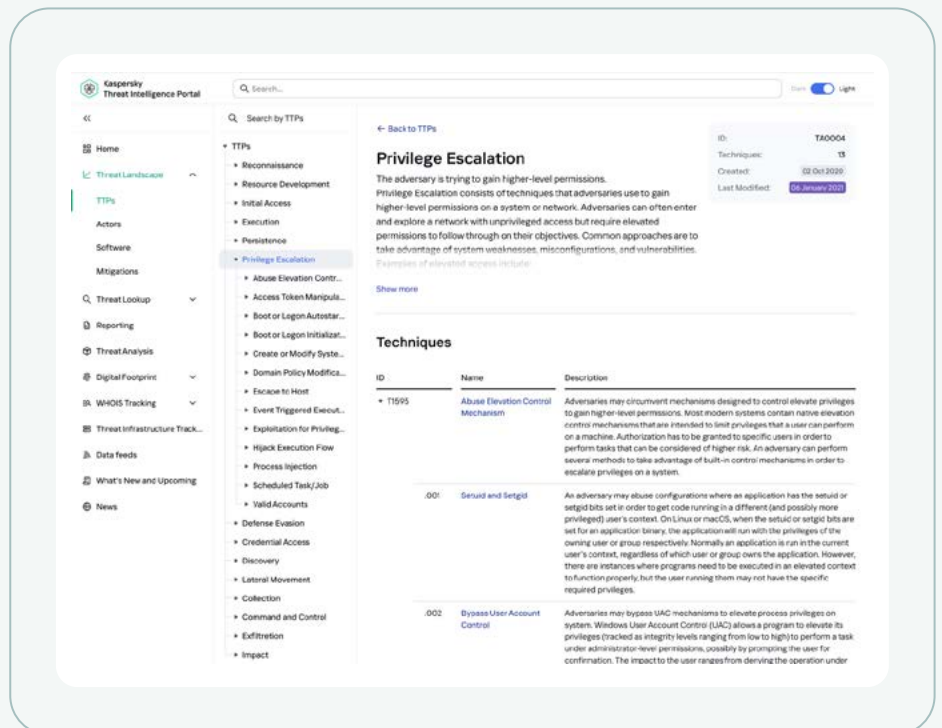
Una vez aplicados los filtros, los usuarios del Portal de Kaspersky Threat Intelligence pueden crear su propio panorama de amenazas, **de acuerdo con el marco MITRE ATT&CK**, y obtener la información más actualizada sobre sus adversarios potenciales. Esta información incluye técnicas, tácticas y procedimientos (TTP) que es más probable que se utilicen para llevar a cabo un ataque, descripciones detalladas de los ciberdelincuentes, el malware que emplean, y las TTP asociadas. También se incluyen informes con descripciones detalladas de los ataques, así como mitigaciones, es decir, recomendaciones específicas para evitar que una técnica se ejecute con éxito.

Aspectos destacados

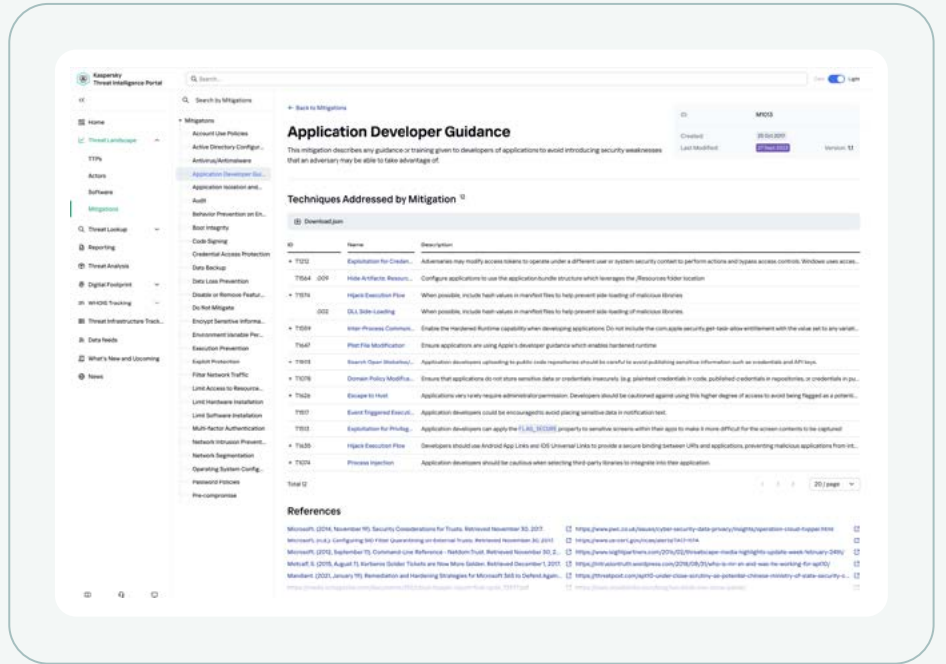
Mapa de calor de MITRE ATT&CK que permite a su organización crear un panorama único de amenazas en tiempo real. Mediante la aplicación de filtros, el usuario accede a los datos más recientes, incluidas actualizaciones de las últimas 24 horas, recopiladas por nuestros sistemas y expertos a través de investigaciones continuas. Además, ofrece la capacidad de guardar capas para organizaciones internacionales.



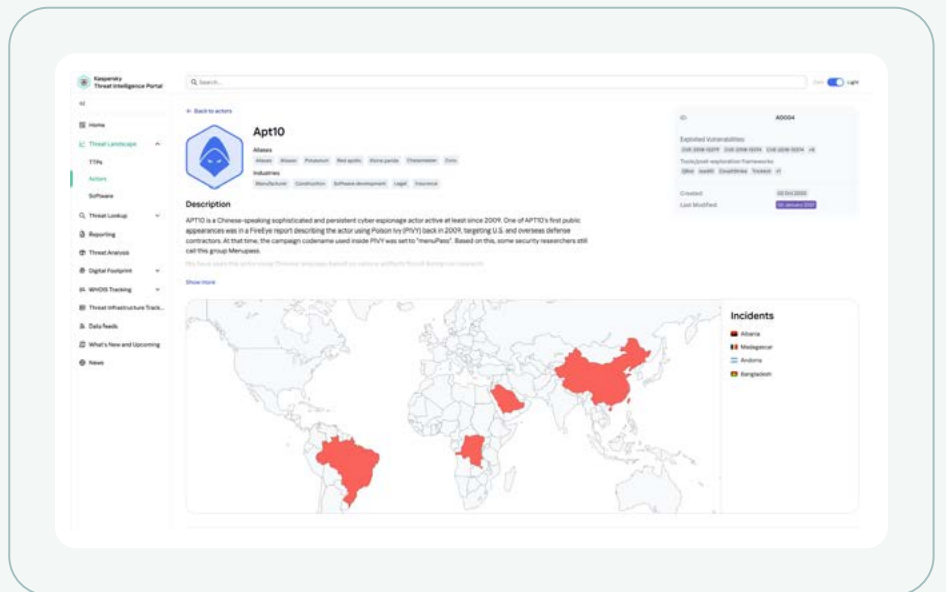
Información en tiempo real sobre las técnicas, las tácticas y los procedimientos de los atacantes según los sistemas expertos de Kaspersky.



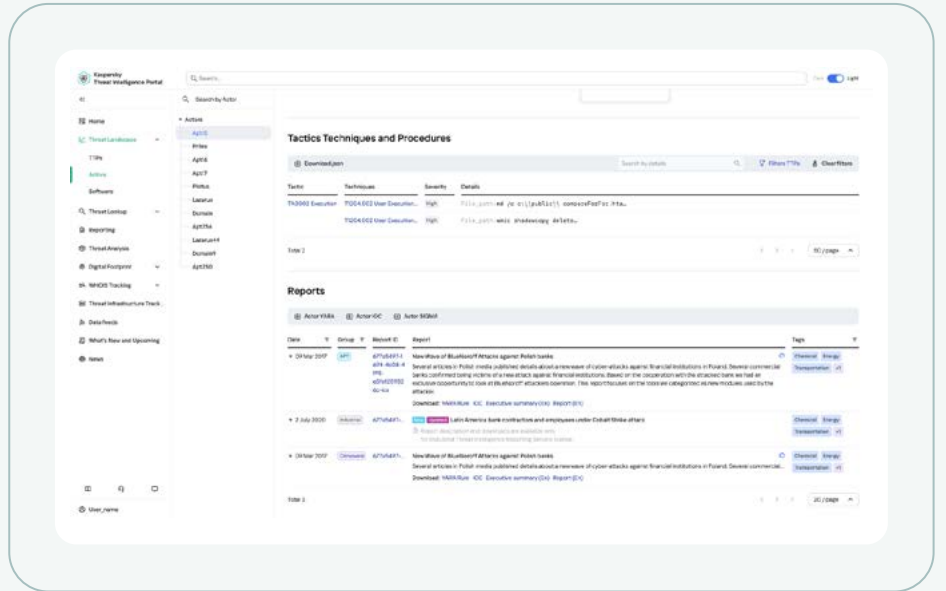
La sección Mitigaciones proporciona descripciones detalladas de las medidas preventivas y de protección para ayudar a las organizaciones a evitar brechas de seguridad.



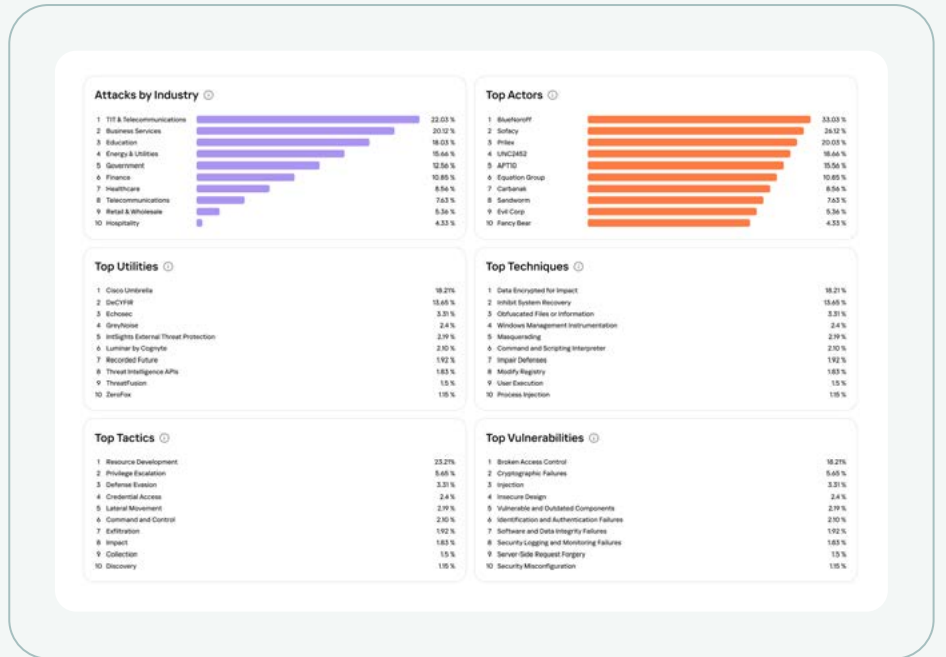
Acceso al repositorio más extenso de la industria, que incluye perfiles de ciberdelincuentes y malware con descripciones detalladas, recopiladas por los expertos de Kaspersky.



Disponibilidad de las reglas Sigma / Yara / de Suricata relacionadas con las técnicas, tácticas y procedimientos de MITRE ATT&CK para detectar amenazas relevantes para su organización.



Las 10 principales estadísticas sobre las industrias, los ciberdelincuentes, las TTP, las vulnerabilidades y el software.





El mundo actual de las ciberamenazas, en constante evolución, ofrece una gran cantidad de **datos de inteligencia de amenazas**, accesibles a través de una variedad de productos y servicios. Al comprender su propio panorama de amenazas, las organizaciones pueden tomar medidas estratégicas y razonables para defenderse de forma proactiva contra los ataques relevantes.

Beneficios de uso

Enfoque de defensa proactivo

Comprenda los vectores de ataque más probables de su organización para elaborar una estrategia de defensa eficaz.

Supervisión de la superficie de ataque

Identifique sus brechas de seguridad antes de que los atacantes las aprovechen.

Centrarse en las amenazas importantes

Capacidad para centrarse en las amenazas que tienen más probabilidades de afectar a su empresa, industria y región.

Planificación estratégica

Utilice la información del Panorama de Amenazas para planificar inversiones y desarrollar herramientas y métodos de protección.

Mejor eficacia de los departamentos de seguridad de la información

Aumente la eficacia del personal y reduzca sus costos mediante el acceso a la información sobre las amenazas pertinentes y las tendencias mundiales.

Conocimiento de las amenazas

Esté atento a las amenazas más recientes y sus tendencias globales para una defensa efectiva.



Si conoce al enemigo y se conoce a sí mismo, no debe temer el resultado de cien batallas. Si se conoce a sí mismo, pero no a su enemigo, por cada victoria que logre también sufrirá una derrota. Si no conoce ni al enemigo ni a sí mismo, fracasará en todas las batallas.

Sun Tzu

El arte de la guerra

Kaspersky Threat Intelligence

Kaspersky Threat Intelligence proporciona acceso a una variedad de información recopilada por nuestros analistas e investigadores de primer nivel. Estos datos ayudarán a cualquier organización **a contrarrestar con eficacia las ciberamenazas actuales.**

Nuestra empresa posee un profundo conocimiento, amplia experiencia en la investigación de ciberamenazas y una perspectiva única sobre todos los aspectos de la ciberseguridad. Esto ha convertido a Kaspersky en un socio de confianza para organizaciones gubernamentales y fuerzas de seguridad de todo el mundo, como Interpol y diversas unidades CERT. Kaspersky Threat Intelligence proporciona información actualizada de inteligencia sobre amenazas tácticas, operativas y estratégicas.



Kaspersky Threat Intelligence

Más
información

<https://latam.kaspersky.com>

© 2024 AO Kaspersky Lab.
Las marcas comerciales registradas y las marcas de
servicio pertenecen a sus respectivos propietarios.

#kaspersky
#bringonthefuture