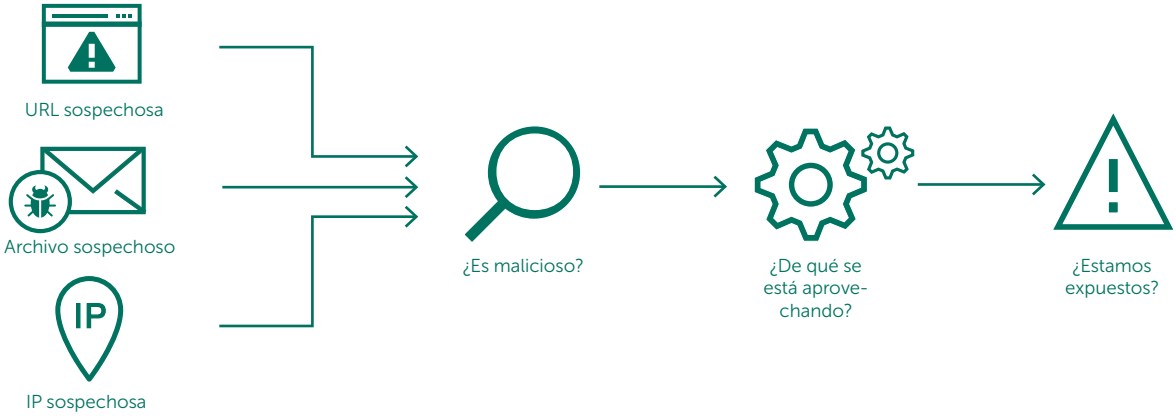
CERRANDO EL CÍRCULO DE LA DEFENSA DE LA RED

KASPERSKY lab

Hoy en día, la ciberdelincuencia no conoce fronteras y sus capacidades técnicas mejoran rápidamente. Los ciberdelincuentes utilizan recursos de la red oscura para amenazar a sus objetivos, con lo que los ataques son cada vez más sofisticados. La frecuencia, la complejidad y la confusión en torno a las ciberamenazas crecen de forma sostenida a medida que se producen nuevos intentos de poner en peligro sus defensas. Los atacantes utilizan complicadas cadenas, así como tácticas, técnicas y procedimientos (TTP) personalizados en sus campañas para interrumpir las actividades de su negocio, robar sus activos y dañar a sus clientes.

El acceso a Kaspersky Threat Lookup ofrece inteligencia fiable e inmediata sobre ciberamenazas, objetos legítimos, sus interconexiones e indicadores; todo ello mejorado con contexto útil para informar a su empresa o sus clientes sobre las implicaciones y los riesgos asociados. Ahora puede mitigar y responder a las amenazas de forma más eficiente, defendiéndose frente a los ataques antes incluso de que tengan lugar.
Kaspersky Threat Lookup ofrece todos los conocimientos adquiridos por Kaspersky Lab sobre ciberamenazas y sus relaciones, reunidos en un único y potente servicio web. El objetivo es proporcionar a los equipos de seguridad el mayor número de datos posible, evitando los 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, hash de archivos, nombres de amenazas, datos estadísticos y de comportamiento, datos de WHOIS y DNS, etc. El resultado es una visibilidad global de las amenazas nuevas y emergentes, que le ayuda a proteger su organización y mejorar la respuesta ante incidentes.



Funciones:

- **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. Los productos de Kaspersky Lab lideran el campo de las pruebas antimalware[1], lo que demuestra la calidad inigualable de nuestra inteligencia de seguridad al proporcionar los más altos índices de detección, sin apenas falsos positivos.
- **Cobertura alta y en tiempo real:** la inteligencia frente a amenazas se genera automáticamente en tiempo real, en función de las conclusiones recopiladas a nivel mundial (gracias a que Kaspersky Security Network ofrece visibilidad de un importante porcentaje de todo el tráfico de Internet y todos los tipos de datos, con decenas de millones de usuarios finales en más de 213 países), lo que ofrece una alta cobertura y precisión.
- **Búsqueda de amenazas:** hay que ser proactivo en la prevención, detección y respuesta a los ataques, para minimizar su impacto y frecuencia. Se debe realizar un seguimiento y eliminar drásticamente a los atacantes 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.
- **Datos enriquecidos:** la inteligencia frente a amenazas de Kaspersky Threat Lookup abarca una amplia variedad de tipos de datos diferentes, que incluyen hash, URL, IP, WHOIS, pDNS, GeoIP, atributos de archivos, datos estadísticos y de comportamiento, cadenas de descargas, marcas de tiempo y mucho más. Con la ayuda de estos datos, puede sondear el panorama diverso de amenazas de seguridad a las que se enfrenta.
- **Disponibilidad continua:** la inteligencia frente a amenazas se genera y supervisa mediante una infraestructura muy tolerante a fallos, lo que garantiza una disponibilidad continua y un rendimiento constante.
- **Revisión continua por parte de expertos en seguridad:** cientos de expertos, incluidos analistas de seguridad de todo el mundo, y expertos en seguridad de fama mundial del equipo GReAT y de equipos de I+D de vanguardia, contribuyen de forma conjunta a generar valiosa inteligencia frente amenazas del mundo real.

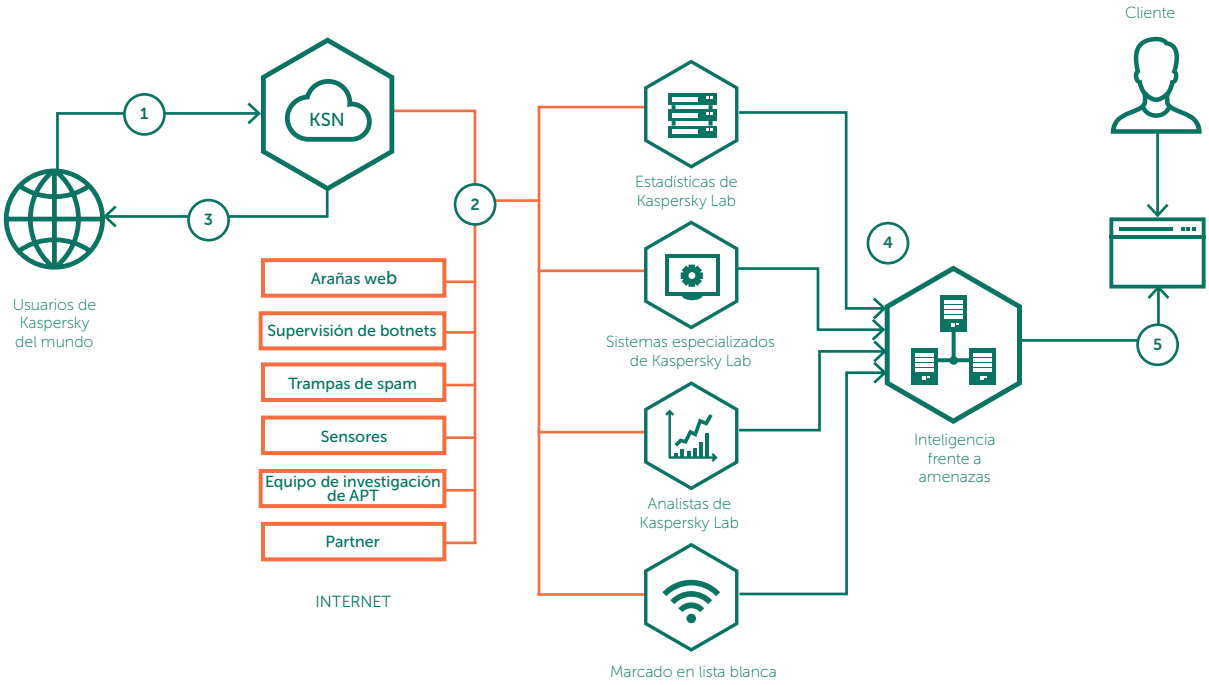
- **Análisis sandbox:**[2] detección de amenazas desconocidas mediante la ejecución de los objetos sospechosos en un entorno seguro y revisión del alcance completo del comportamiento de la amenaza y los artefactos mediante informes de fácil lectura.
- **Amplia gama de formatos de exportación:** indicadores de compromiso (IOC) o contexto útil sobre los formatos de uso compartido legibles por máquina más ampliamente utilizados y más organizados, como STIX, OpenIOC, JSON, Yara, Snort o incluso CSV, para disfrutar de todas las ventajas de la inteligencia frente a amenazas, automatizar el flujo de trabajo de operaciones o integrarlos en los controles de seguridad como SIEM.
- **Interfaz web o API RESTful fáciles de usar:** uso del servicio en modo manual mediante una interfaz web (a través de un navegador web) o acceso a través de una sencilla API RESTful, según las preferencias.

Ventajas clave:

- **Mejore y acelere la respuesta ante incidentes y las capacidades de análisis de ciencia forense** al facilitar a los equipos de seguridad y SOC la información relevante sobre amenazas, y datos globales de lo que hay detrás de los ataques dirigidos. 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, para minimizar el tiempo de respuesta e interrumpir la cadena de ataque antes de que los sistemas críticos y los datos se vean comprometidos.
- **Lleve a cabo búsquedas en profundidad de los indicadores de amenaza**, como direcciones IP, dominios o hash de archivos, con contexto de las amenazas altamente validado que le permite priorizar los ataques, mejorar las decisiones de asignación de personal y recursos, y centrarse en la mitigación de las amenazas que presentan un mayor riesgo para su negocio.
- **Mitigue los ataques dirigidos.** Mejore su infraestructura de seguridad con inteligencia táctica y estratégica frente a amenazas, gracias a la adaptación de las estrategias defensivas para contrarrestar las amenazas específicas a las que se enfrenta su organización.

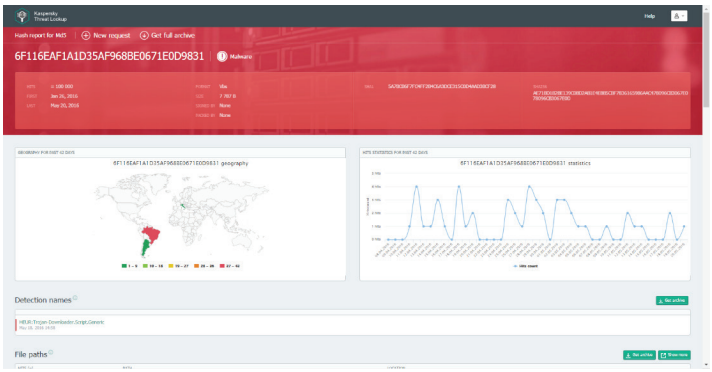
Fuentes de inteligencia frente a amenazas:

La inteligencia frente a amenazas se incorpora a partir de una fusión de fuentes heterogéneas de alta fiabilidad, que incluyen Kaspersky Security Network (KSN) y nuestras propias arañas web, nuestro servicio de supervisión de botnets (supervisión ininterrumpida de botnets y sus objetivos y actividades), trampas de spam, equipos de investigación, partners y otros datos históricos sobre objetos maliciosos recopilados por Kaspersky Lab a lo largo de más de dos décadas. A continuación, todos los datos agregados se inspeccionan cuidadosamente en tiempo real mediante varias técnicas de procesamiento previo; por ejemplo, criterios estadísticos, sistemas especializados de Kaspersky Lab (sandboxes, motores heurísticos, herramientas de similitud, creación de perfiles de análisis), validación de análisis y verificación de listas blancas.



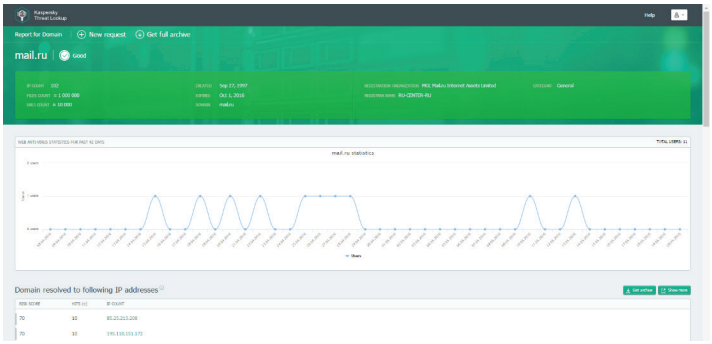
La inteligencia frente amenazas de Kaspersky se compone de datos de indicadores de amenaza concienzudamente revisados, obtenidos del mundo real en tiempo real.

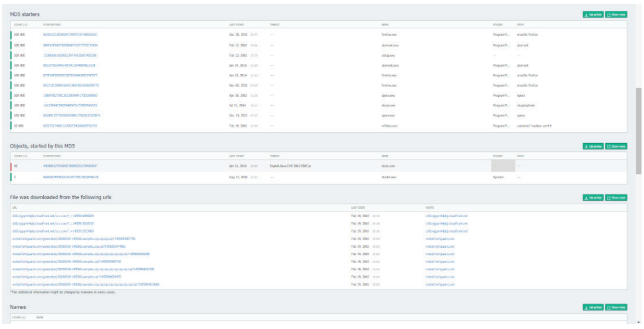
[1] http://www.kaspersky.es/top3
[2] El lanzamiento de esta función está planificado para el primer semestre de 2017.



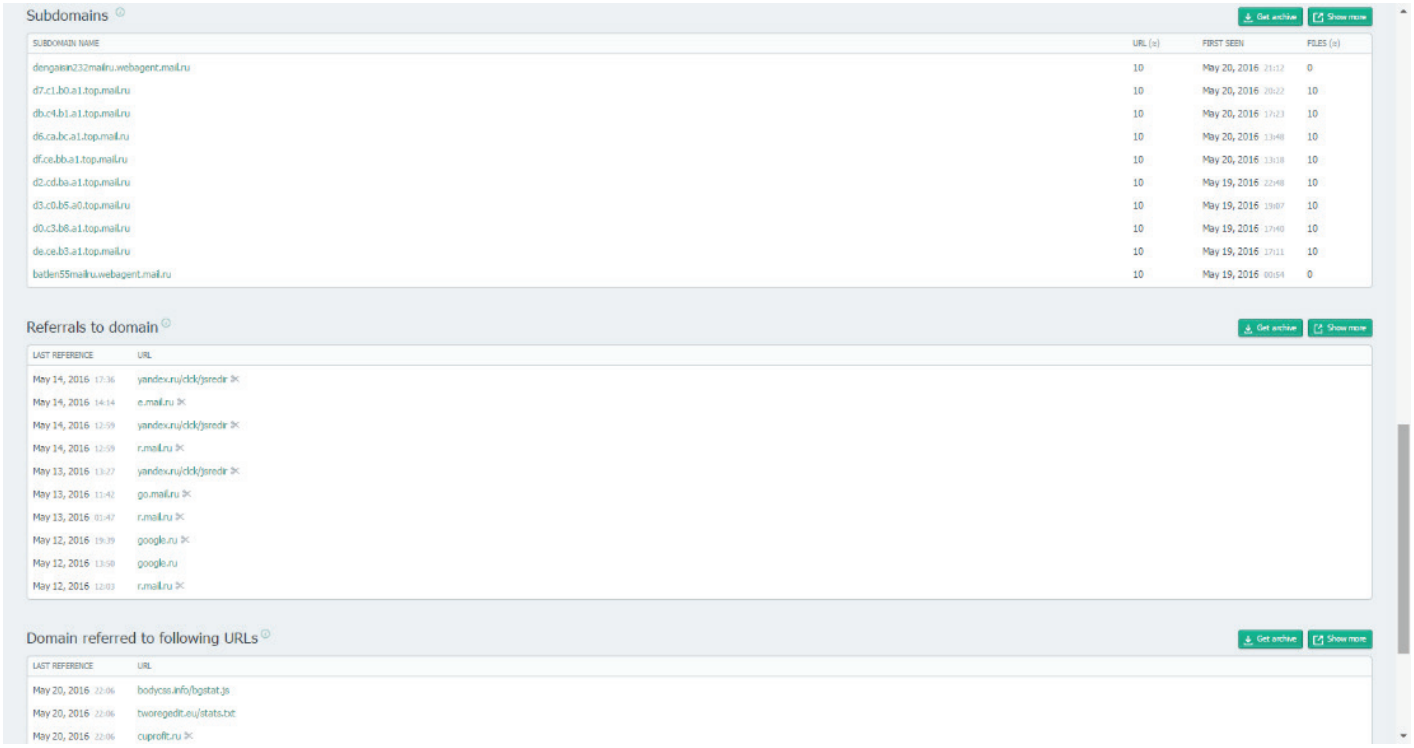
Ahora puede:

- Buscar indicadores de amenaza a través de una interfaz web o la API RESTful.
- Comprender por qué un objeto se debe tratar como malicioso.
- Comprobar si el objeto detectado es común o único.
- Examinar datos avanzados, que incluyen certificados, nombres usados habitualmente, rutas de archivos o URL relacionadas con el fin de detectar nuevos objetos sospechosos. Estos son solo algunos ejemplos. Hay muchísimas formas de aprovechar esta fuente completa y continua de datos sobre inteligencia relevantes y exhaustivos.





Conozca a sus amigos y también a sus enemigos. Identifique aquellos archivos, URL y direcciones IP que se haya demostrado que no son maliciosos, para aumentar la velocidad de la investigación. Cuando cada segundo cuenta, y mucho, no pierda su valioso tiempo en analizar los objetos de confianza.



Nuestra misión es salvar al mundo de todos los tipos de ciberamenazas. Para lograrlo, y para hacer que el uso de Internet sea seguro, es de vital importancia compartir y acceder a la inteligencia frente a amenazas en tiempo real. El acceso oportuno a la información es fundamental para mantener una protección eficaz de los datos y las redes. Ahora, Kaspersky Threat Lookup permite acceder a esta inteligencia de forma más eficiente y directa que antes.

KASPERSKY lab
THE POWER
OF PROTECTION