CERRAMOS EL CÍRCULO DE DEFENSA DE LA RED

KASPERSKY lab

El cibercrimen actual desconoce límites y las capacidades técnicas están mejorando con rapidez: los cibercriminales se han volcado a la Web oculta para obtener recursos con los que amenazar a sus objetivos y lanzar ataques más y más sofisticados. Las ciberamenazas son cada vez más frecuentes, complejas y confusas, a medida que se realizan nuevos intentos para vulnerar sus defensas. Los atacantes están usando cadenas de ataque complicadas, así como tácticas, técnicas y procedimientos (TTP) personalizados, para inhabilitar las operaciones de las empresas, robar sus recursos y perjudicar a sus clientes.

Kaspersky Threat Lookup le dará acceso a inteligencia confiable e inmediata sobre ciberamenazas, objetos lícitos, interconexiones e indicadores, con un marco de información contextual práctica que permitirá a su empresa y a sus clientes conocer los riesgos e implicaciones de cada caso. Ahora podrá responder a las amenazas y mitigarlas de manera más eficiente, y defenderse de ataques incluso antes de que tengan lugar.
Kaspersky Threat Lookup le ofrece todos los conocimientos que hemos adquirido sobre las ciberamenazas y sus relaciones a través de un único y poderoso servicio web. El objetivo es facilitar la mayor cantidad posible de datos a sus equipos de seguridad, de manera que puedan prevenir ciberataques antes de que afecten a la organización. La plataforma recupera la última inteligencia disponible sobre direcciones URL, dominios, direcciones IP, hashes de archivo, nombres de amenazas, datos estadísticos y de comportamiento, datos de WHOIS/DNS, etc. Con ello se obtiene una visión global y completa de las amenazas nuevas y emergentes, que lo ayudará a proteger su organización y a optimizar la respuesta ante un incidente.

Características:

- **Inteligencia de confianza:** un atributo clave de Kaspersky Threat Lookup es la confiabilidad de sus datos de inteligencia, enriquecidos con información contextual práctica. Los productos de Kaspersky Lab son líderes en las pruebas antimalware[1], lo que demuestra la calidad sin igual de nuestra inteligencia de seguridad, ya que ofrecemos las más altas tasas de detección, con casi cero falsos positivos.
- **Cobertura alta y en tiempo real:** la inteligencia de amenazas se genera automáticamente y en tiempo real, a partir de descubrimientos registrados en todo el mundo (gracias a Kaspersky Security Network, que nos ofrece una visión de un porcentaje significativo de todo el tráfico de Internet y de toda clase de datos, ya que conecta a decenas de millones de usuarios finales en más de 213 países). Combinados, estos factores se traducen en un alto nivel de cobertura y precisión.
- **Búsqueda de amenazas:** sea proactivo en la prevención, la detección y la respuesta a ataques a fin de minimizar su impacto y frecuencia. Rastree y elimine a los atacantes en forma agresiva y con la mayor antelación posible. Mientras más pronto descubra una amenaza, menor será el daño resultante, más rápido se efectuarán las reparaciones y más pronto volverán a la normalidad las operaciones de la red.
- **Datos enriquecidos:** la inteligencia de amenazas que ofrece Kaspersky Threat Lookup consta de toda clase de datos: hashes, URL, IP, whois, pDNS, GeoIP, atributos de archivos, datos estadísticos y de comportamiento, cadenas de descarga, marcas de fecha y hora, y mucho más. Con la ayuda de estos datos, podrá sondear el diverso panorama de amenazas que atentan contra su seguridad.
- **Disponibilidad continua:** la inteligencia de amenazas se genera y controla a través de una infraestructura altamente tolerante a fallas, que garantiza una disponibilidad continua y un rendimiento uniforme.
- **Revisión continua por parte de expertos en seguridad:** nuestra inteligencia cuenta con el aval y aporte de cientos de expertos, como los afamados investigadores de nuestro equipo de seguridad GReAT, equipos de I+D de vanguardia y analistas de seguridad de todo el mundo.

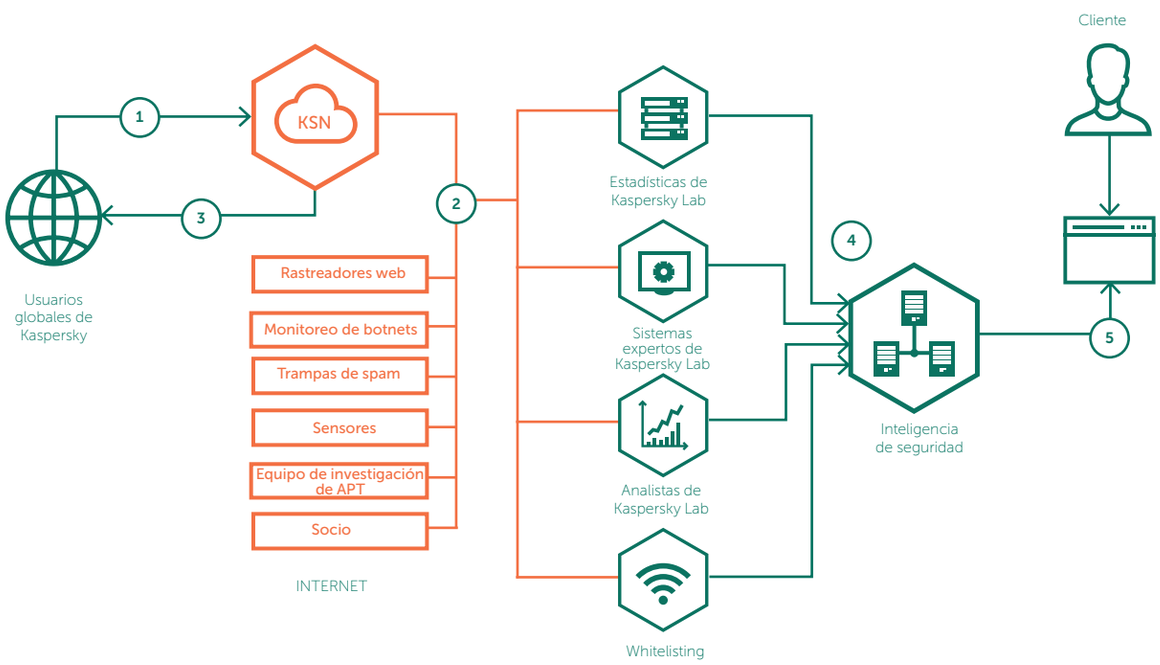
- **Análisis en "sandbox":**[2] detecte amenazas desconocidas ejecutando objetos sospechosos en un entorno seguro y revise el alcance completo del comportamiento y los artefactos de las amenazas a través de informes de fácil lectura.
- **Amplia gama de formatos de exportación:** los IOC (indicadores de compromiso) y la información contextual pueden exportarse en formatos muy utilizados, como STIX, OpenIOC, JSON, YARA, Snort o incluso CSV. Con ello, podrá disfrutar de todos los beneficios de la inteligencia de amenazas en formatos organizados y procesables, que le permitirán automatizar el flujo de trabajo de operaciones o integrar la información en un sistema SIEM u otros controles de seguridad.
- **Interfaz web o API RESTful fáciles de usar:** use el servicio en modo manual con una interfaz web (a través de un navegador) o acceda a él mediante una sencilla API RESTful, según lo prefiera.

Ventajas clave:

- **Optimice y agilice su capacidad de respuesta ante un incidente, además de sus habilidades forenses,** proporcionando a los equipos de seguridad o del SOC información relevante sobre las amenazas y una perspectiva global de lo que subyace a los ataques dirigidos. Diagnostique y analice incidentes de seguridad en hosts y en la red con mayor eficiencia, y priorice las señales de sus sistemas internos frente a amenazas desconocidas para minimizar el tiempo de respuesta a incidentes e interrumpir la cadena de ataque antes de que se pongan en riesgo los sistemas y datos críticos.
- **Realice búsquedas detalladas de indicadores de amenaza,** como direcciones IP o URL, dominios y hashes de archivo. Los datos contextuales altamente validados sobre cada amenaza le permitirán priorizar ataques, tomar mejores decisiones a la hora de asignar personal y recursos, y concentrarse en mitigar las amenazas que representen el riesgo más alto para su empresa.
- **Mitigue los ataques dirigidos.** Optimice su infraestructura de seguridad con inteligencia de amenazas táctica y estratégica, que lo ayudará a definir medidas de defensa adaptadas a los riesgos específicos que enfrente su organización.

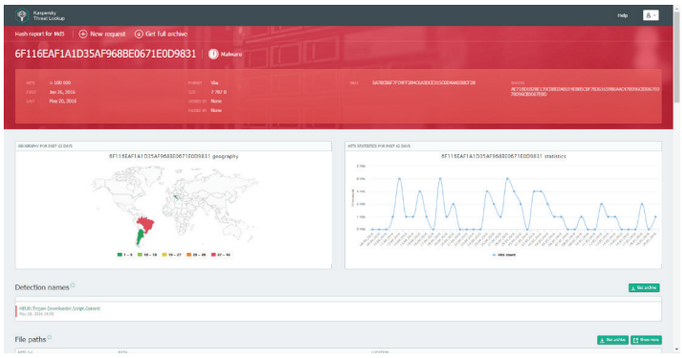
Fuentes de inteligencia de amenazas:

La inteligencia de amenazas se recopila a partir de una fusión de fuentes heterogéneas y altamente confiables, que incluyen Kaspersky Security Network (KSN), nuestros propios rastreadores web, nuestro servicio de supervisión de botnets (monitoreo constante de las botnets, sus objetivos y sus actividades), trampas de spam, equipos de investigación, socios y otros datos históricos sobre objetos maliciosos que Kaspersky Lab ha reunido durante casi dos décadas. Una vez recopilados, los datos se inspeccionan y refinan cuidadosamente en tiempo real, utilizando diversas técnicas de preprocesamiento: criterios estadísticos, sistemas expertos de Kaspersky Lab (sandboxes, motores heurísticos, herramientas de similitud, perfiles de comportamiento, etc.), validación de analistas, verificación con whitelisting y más.



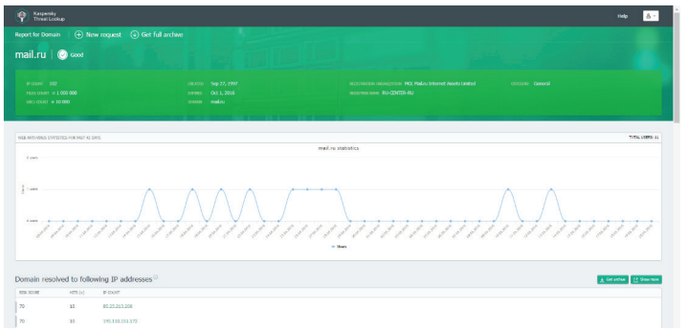
La inteligencia de amenazas de Kaspersky consta de indicadores de amenazas cuidadosamente validados, obtenidos del mundo real, en tiempo real.

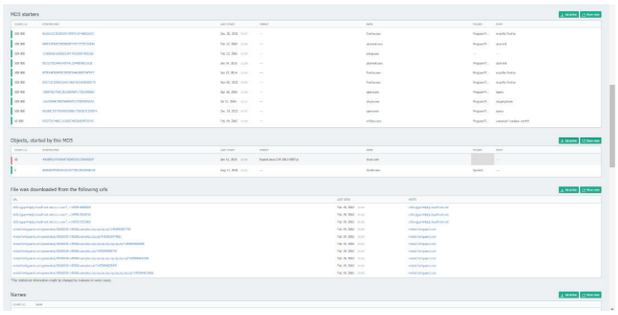
[1] https://latam.kaspersky.com/top3
[2] El lanzamiento de esta característica está previsto para la primera mitad de 2017.



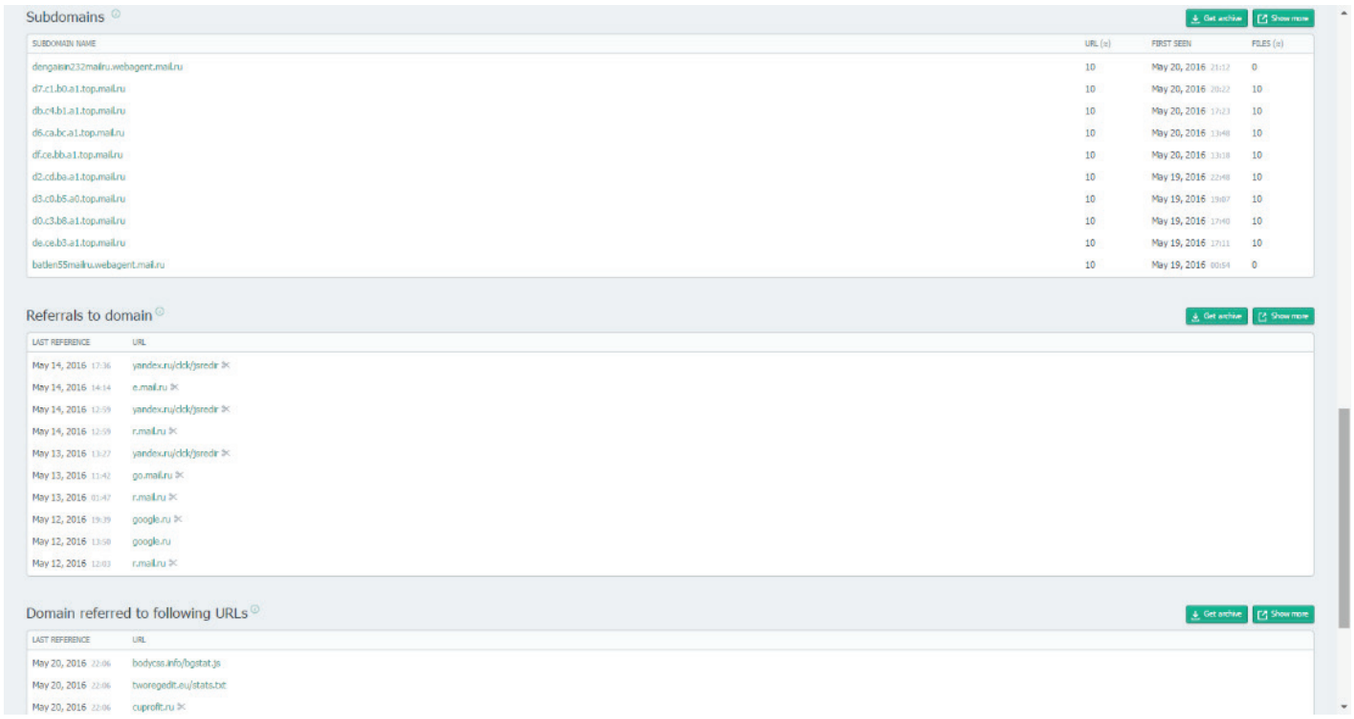
Ahora es posible:

- Buscar indicadores de amenazas mediante una interfaz web o una API RESTful.
- Comprender por qué es necesario tratar un objeto como malicioso.
- Verificar si el objeto descubierto es único en su clase o un problema generalizado.
- Analizar detalles avanzados, como certificados, nombres usuales, rutas de archivo o URL relacionadas, para descubrir nuevos objetos sospechosos. Estos son solo algunos ejemplos. Existen muchísimas maneras más de aprovechar esta fuente rica y continua de inteligencia detallada y relevante.





Sepa quién es su enemigo y quién, su amigo. Reconozca archivos, URL y direcciones IP que ya se sepa son inocuos para acelerar la investigación. Cuando cada segundo cuente, no desperdicie tiempo valioso analizando objetos confiables.



Nuestra misión es proteger 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 utilizar inteligencia de amenazas en tiempo real. El acceso oportuno a la información es fundamental para mantener una protección eficaz de sus datos y redes. Ahora, Kaspersky Threat Lookup permite que el acceso a esta inteligencia sea más eficaz y simple que nunca.

KASPERSKY lab

THE POWER
OF PROTECTION