# Kaspersky lanza Threat Hunting contra ataques dirigidos

Kaspersky Lab ha anunciado una mejora en la protección contra amenazas avanzadas con los nuevos servicios Kaspersky Threat Hunting, a los que define como **una nueva suite de servicios diseñados para mejorar la eficacia** de la protección contra ataques dirigidos. Según la firma de seguridad, si no se detecta un incidente de ciberseguridad dentro de la primera semana, las pérdidas financieras pueden duplicarse o más en una empresa, pasando de los 400.000 euros al 1.000.000 de euros.


De este modo, la suite incluye **Kaspersky Managed Protection y Targeted Attack Discovery,** servicios diseñados para dotar a los equipos de seguridad de experiencia de primer nivel que detecten y analicen amenazas avanzadas, en particular, las amenazas "fileless" (que no utilizan ningún archivo) y los ataques no maliciosos frecuentemente empleados por los ciberdelincuentes.

De acuerdo con la **Encuesta Global de Riesgos de Seguridad Informática de Kaspersky Lab 2017**, asegurar la detección rápida de una amenaza requiere recursos considerables y unas excelentes habilidades profesionales, algo que solo los equipos de los centros de operaciones de seguridad (SOC en sus siglas en inglés) poseen.

Dice el comunicado de prensa que "para ayudar a las empresas a detectar y analizar amenazas avanzadas que ya han penetrado en la infraestructura corporativa, Kaspersky Lab presenta Kaspersky Threat Hunting, la suite de servicios expertos que ofrece a las grandes empresas acceso 24/7 a la experiencia del equipo de cazadores de amenazas" de la marca. Hasta la fecha, los expertos de Kaspersky Lab han rastreado más de 100 APT (**amenazas persistentes avanzadas**) y operaciones. Solo en 2016, los especialistas de Kaspersky Lab redactaron más de 200 informes sobre amenazas complejas. Estos informes están disponibles para clientes corporativos a través de un modelo de suscripción.

Por su parte, **Targeted Attack Discovery es un servicio analítico puntual destinado a detectar rastros de ataques dirigidos en la infraestructura de un cliente en tiempo real** o después del ataque. Los expertos de Kaspersky Lab estudian la correlación entre los datos recopilados en la red corporativa y los datos sobre amenazas específicas en bases de datos abiertas y privadas. La recopilación y el análisis de la información obtenida permiten detectar actividades sospechosas, descubrir posibles fuentes de incidentes y dispositivos comprometidos.