KASPERSKY lab

Kaspersky Cybersecurity Services

www.kaspersky.es
#truecybersecurity

Hoy en día, el cibercrimen no conoce fronteras y sus capacidades técnicas están mejorando rápidamente: estamos viendo cómo los ataques son cada vez más sofisticados. Nuestra misión es salvar al mundo de todos los tipos de ciberamenazas. Para lograrlo, y para hacer que el uso de Internet sea seguro, compartir la inteligencia de amenazas en tiempo real es de vital importancia. El acceso oportuno a la información es fundamental para mantener una protección eficaz de los datos y las redes.

Eugene Kaspersky
Director ejecutivo y presidente de Kaspersky Lab

Introducción

Cada día aparecen más ciberamenazas, en todas sus diferentes apariencias y a través de una gran variedad de vectores de ataque.

No hay una solución única que ofrezca una protección completa. No obstante, incluso en nuestro entorno de Big Data, saber dónde buscar el peligro ya es un gran avance a la hora de luchar contra las amenazas más recientes.

Como directivo, es su responsabilidad proteger a su empresa de las amenazas de hoy en día y prever los peligros que nos esperan en los próximos años. Se necesita algo más que protección operacional inteligente contra las amenazas conocidas: es necesario un nivel de inteligencia de seguridad estratégica que muy pocas empresas pueden desarrollar de forma interna, ya que carecen de los recursos necesarios.

En Kaspersky Lab, entendemos que se necesitan relaciones duraderas para garantizar la prosperidad a largo plazo de una empresa.

Kaspersky Lab es un valioso partner empresarial que siempre está disponible para compartir la información más reciente con su equipo a través de diferentes canales. Nuestra amplia gama de métodos de distribución ayudan a su centro de operaciones de seguridad (SOC)/equipo de seguridad de IT a que permanezca totalmente equipado para proteger a la empresa de cualquier amenaza online.

Incluso si su organización no utiliza productos de Kaspersky Lab, puede beneficiarse de Kaspersky Lab Cybersecurity Services.

Kaspersky Cybersecurity Services

- **Kaspersky Threat Intelligence Services**
- **Kaspersky Threat Hunting Services**
- **Kaspersky Security Training**
- **Kaspersky Incident Response Services**
- **Kaspersky Security Assessment Services**

La seguridad que destaca

La **inteligencia de seguridad líder en el mundo está incorporada en nuestro ADN**: nos ayuda a ofrecer la protección antimalware más potente del mercado e.

Somos una empresa impulsada por la tecnología, desde los cargos superiores hasta los inferiores, empezando por nuestro director ejecutivo, Eugene Kaspersky.

Nuestro equipo de análisis e investigación global (GReAT), un grupo de élite de investigación y análisis en seguridad de IT, ha sido pionero en el descubrimiento de muchas de las amenazas de malware y ataques dirigidos más peligrosos del mundo.

Muchas de las organizaciones de seguridad y fuerzas del orden más respetadas del mundo, incluidos la Interpol, Europol, CERT, City of London Police, etc., han buscado activamente nuestra colaboración.

Kaspersky Lab desarrolla y perfecciona de forma interna todas sus propias tecnologías básicas, por lo que nuestros productos e inteligencia son, por naturaleza, más fiables y eficaces.

Los analistas del sector más respetados, incluidos Gartner, Forrester Research e International Data Corporation (IDC), nos clasifican como un líder en muchas de las principales categorías de seguridad de IT.

Más de 130 OEM, incluidos Microsoft, Cisco, Blue Coat, Juniper Networks, Alcatel Lucent y muchos otros, utilizan nuestras tecnologías en sus propios productos y servicios.

Kaspersky Threat Intelligence Services

El seguimiento, el análisis, la interpretación y la mitigación de las amenazas para la seguridad de la IT es una tarea inmensa, puesto que no dejan de evolucionar. Empresas de todos los segmentos se enfrentan a la falta de información relevante y actualizada que necesitan para poder gestionar los riesgos derivados de las amenazas a la seguridad de IT.

Kaspersky Cybersecurity Services

- **Kaspersky Threat Intelligence Services**
  - Fuentes de datos de amenazas
  - Informes de inteligencia APT
  - Informes sobre amenazas personalizados
  - Kaspersky Threat Lookup
  - Kaspersky Phishing Tracking
  - Kaspersky Botnet Tracking
- **Kaspersky Threat Hunting Services**
- **Kaspersky Security Training**
- **Kaspersky Incident Response Services**
- **Kaspersky Security Assessment Services**

Threat Intelligence Services de Kaspersky Lab le proporciona acceso a la inteligencia que necesita para mitigar estas amenazas, proporcionada por nuestro equipo líder de investigadores y analistas.

Gracias a sus conocimientos, experiencia e inteligencia avanzada sobre todos los aspectos de la ciberseguridad, Kaspersky Lab se ha convertido en el partner de confianza de las fuerzas del orden y las agencias gubernamentales más importantes del mundo, entre las que se incluyen la Interpol e importantes equipos CERT. Y hoy, usted ya puede utilizar esta misma inteligencia para su organización.

Kaspersky Lab Threat Intelligence Services incluye:

- Fuentes de datos de amenazas
- Informes de inteligencia APT
- Informes sobre amenazas personalizados
- Kaspersky Threat Lookup
- Kaspersky Phishing Tracking
- Kaspersky Botnet Tracking

Fuentes de datos de amenazas

Proveedores y empresas de seguridad de primer nivel utilizan las fuentes de datos de amenazas de gran tradición y reconocimiento, de Kaspersky para **producir soluciones de seguridad superiores o para proteger su negocio**.

Los ciberataques se producen a diario. La frecuencia, la complejidad y la dedicación en torno a las ciberamenazas crecen de forma sostenida a medida que intentan **poner en peligro sus defensas**. Actualmente, los adversarios utilizan complicadas **cadenas de ataque** de intrusión, campañas, así como **tácticas, técnicas y procedimientos (TTP) personalizados para interrumpir las actividades de su negocio o dañar a sus clientes**.

Kaspersky Lab ofrece fuentes de datos de amenazas **que se actualizan de forma constante** con el fin de **informar a su empresa o sus clientes sobre los riesgos** y las implicaciones que se asocian a las ciberamenazas, lo que le ayuda a **mitigar las amenazas de forma más eficiente** y a **defenderse de los ataques** incluso antes de que se inicien.

Ciclo de inteligencia

Fuentes de datos

Las fuentes incluyen conjuntos de:

- Fuentes de reputación de IP: conjunto de direcciones IP con contexto que cubre los hosts sospechosos y maliciosos.
- Fuentes de URL maliciosas y de phishing: cubren los enlaces y sitios web maliciosos y de phishing.
- Fuentes de URL de mando y control de botnets: cubren servidores de mando y control de botnets de escritorio y objetos maliciosos relacionados.
- Fuentes de URL de mando y control de botnets móviles: cubren los servidores de mando y control de botnets móviles. Identifican máquinas infectadas que se comunican con mandos y controles.
- Fuentes de hash maliciosas: cubren el malware más peligroso, frecuente y emergente.
- Fuentes de hash maliciosas móviles: respaldan la detección de objetos maliciosos que infectan plataformas móviles iPhone y Android.
- Fuentes de datos de troyanos P-SMS: respaldan la detección de troyanos de SMS que permiten a los atacantes robar, eliminar y responder a mensajes SMS, así como realizar llamadas con cargos premium para los usuarios de móviles.
- Fuentes de datos de listas blancas: ofrecen a las soluciones y los servicios de terceros un conocimiento sistemático del software legítimo.
- **¡NUEVO! Transformaciones de Maltego de Kaspersky**: proporcionan a los usuarios de Maltego un conjunto de transformaciones que ofrecen acceso a las fuentes de datos de amenazas de Kaspersky Lab. Las transformaciones de Kaspersky para Maltego permite comprobar URL, hash y direcciones IP con respecto a las fuentes de Kaspersky Lab. Las transformaciones pueden determinar la categoría de un objeto, así como proporcionar contexto útil sobre él.

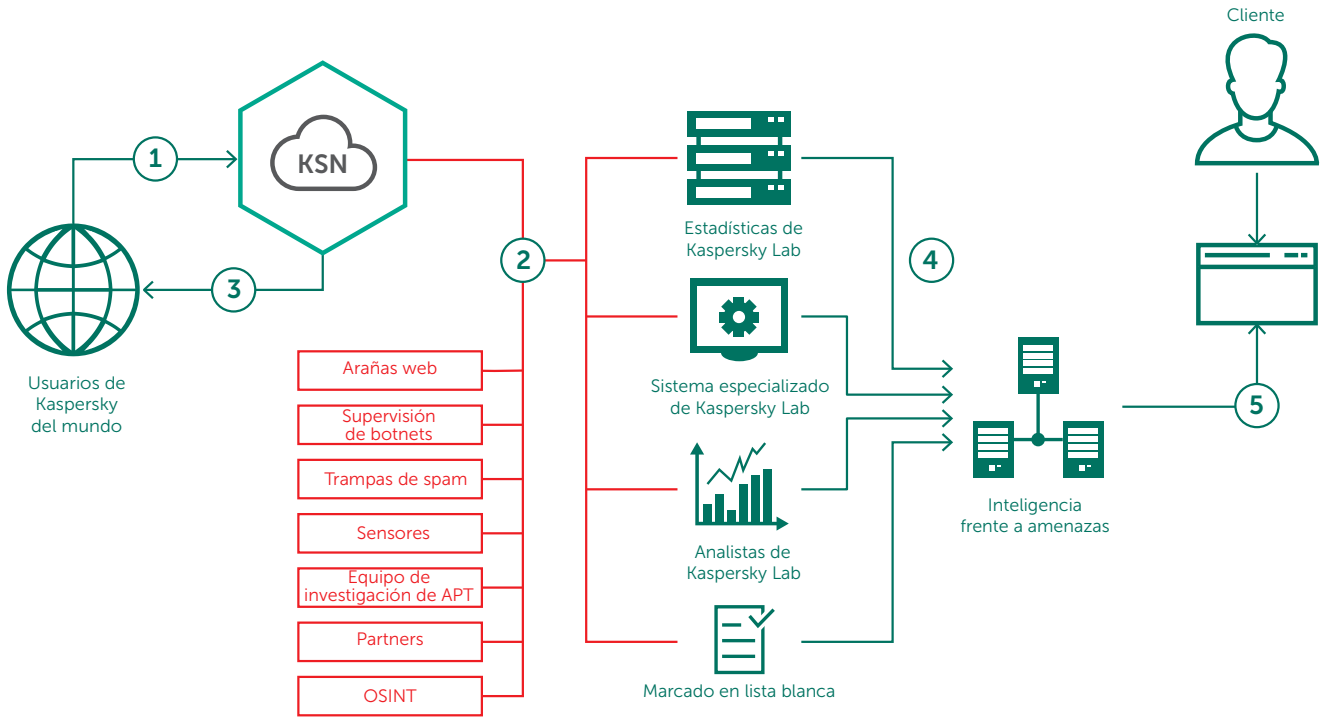
Datos contextuales

Todos los registros de cada fuente de datos se mejoran con **contexto útil** (nombres de amenazas, marcas de tiempo, geolocalización, direcciones IP resueltas de recursos web infectados, hash, popularidad, etc.). Los datos contextuales ayudan a revelar una "visión de conjunto", lo que mejora la validación y complementación de un uso variado de los datos. Cuando están en contexto, los datos se pueden utilizar de forma más inmediata para responder a **quién, qué, dónde y cuándo**, lo que permite identificar a los adversarios y ayuda a tomar decisiones y acciones puntuales **específicas para su organización.**

Recopilación y procesamiento

Las fuentes de datos proceden de una fusión de fuentes heterogéneas de gran fiabilidad como, por ejemplo, Kaspersky Security Network y nuestras propias arañas web, nuestro servicio de supervisión de botnets (supervisión ininterrumpida de botnets y de sus objetivos y actividades), trampas de spam, equipos de investigación y partners.

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, varios analizadores, herramientas de similitud, creación de perfiles de análisis, etc.), validación de analistas y verificación de listas blancas:



Las fuentes de datos de amenazas de Kaspersky se componen de datos de indicadores de amenaza concienzudamente revisados, obtenidos del mundo real en tiempo real.

Características destacadas del servicio

- Las fuentes de datos repletas de **falsos positivos** carecen de valor, por lo que se realizan pruebas y se le aplican filtros muy exhaustivos antes de publicarlas para garantizar la entrega de datos 100 % revisados.
- Las fuentes de datos se generan automáticamente en tiempo real, en función de las conclusiones recopiladas a nivel mundial (Kaspersky Security Network ofrece visibilidad de un importante porcentaje de todo el tráfico de Internet, con decenas de millones de usuarios finales en más de 213 países), lo que ofrece unos altos **índices de detección** y precisión.
- Todas las fuentes se generan y se controlan mediante una infraestructura muy tolerante a fallos, lo que garantiza una **disponibilidad continua**.
- Las fuentes de datos permiten la **detección inmediata de URL** utilizadas para alojar phishing, malware, exploits, URL de mando y control de botnets y otro contenido malicioso.
- El **malware** en todos los tipos de tráfico (web, correo electrónico, P2P, IM,...) y dirigidos a plataformas móviles también se puede **detectar e identificar de forma inmediata**.
- Los formatos de **divulgación** ligeros sencillos (**JSON, CSV, OpenIoC, STIX**) a través de **HTTPS** o mecanismos de entrega específicos permiten una integración fácil de las fuentes en las soluciones de 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 estas fuentes. Los responsables de la seguridad reciben información crucial y alertas generadas a partir de los datos de la más alta calidad, sin riesgo de que se vean desbordados por indicadores y advertencias innecesarios.
- **Facilidad de implementación**. Se combina toda la documentación complementaria, muestras, un responsable técnico de cuenta específico y soporte técnico de Kaspersky Lab para permitir la integración sencilla.

Ventajas

- **Refuerce sus soluciones de defensa de la red**, incluidos SIEM, firewalls, IPS/IDS, proxy de seguridad, soluciones DNS, protección contra APT con indicadores de compromiso (IOC) continuamente actualizados y contexto útil, que proporcionan información sobre ciberataques y una mayor comprensión de la intención, las capacidades y los objetivos de sus adversarios. Los principales SIEM (incluidos HP ArcSight, IBM QRadar, Splunk, etc.) son totalmente compatibles.
- Desarrolle o mejore la **protección antimalware para dispositivos de red de perímetro** (como routers, pasarelas, dispositivos UTM).
- **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 cruciales y los datos se vean comprometidos.
- **Proporcione inteligencia frente a amenazas a suscriptores empresariales**. Aproveche la información de primera mano sobre malware emergente y otras amenazas maliciosas para **fortalecer de forma preventiva su posición de defensa y evitar riesgos**.
- **Ayude a mitigar los ataques dirigidos**. Mejore su posición 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.
- Utilice la inteligencia frente a amenazas para **detectar contenido malicioso alojado en sus redes y centros de datos**.
- **Evite la sustracción de activos confidenciales y de propiedad intelectual** de las máquinas infectadas fuera de la organización, detectando rápidamente activos infectados, evitando la ventaja competitiva y la pérdida de oportunidades de negocio, y protegiendo la reputación de su marca.
- Lleve a cabo búsquedas en profundidad de los indicadores de amenazas como protocolos de mando y control, direcciones IP, URL maliciosas o hash de archivos, con contexto de las amenazas validado que le permite la priorización de los ataques, mejora las decisiones de gasto en IT y de asignación de recursos, y **le ayuda a centrarse en la mitigación de esas amenazas que suponen el mayor riesgo para su negocio**.
- Utilice nuestra experiencia e inteligencia contextual útil para **mejorar la protección ofrecida por sus productos y servicios**, como el filtrado de contenido web, el bloqueo de spam o phishing, etc.
- **Como MSSP**, haga crecer su empresa proporcionando inteligencia frente a amenazas líder del sector como servicio premium a sus clientes. **Como CERT**, mejore y amplíe sus capacidades de identificación y detección de ciberamenazas.

Los informes de inteligencia de APT de Kaspersky proporcionan:

- **Acceso exclusivo** a descripciones técnicas de amenazas de vanguardia durante la investigación en curso, antes de hacerse públicas.
- **Información sobre APT no públicas**. No todas las amenazas de alto perfil están sujetas a notificación pública. Algunas, debido a las víctimas afectadas, la confidencialidad de los datos, la naturaleza del proceso de reparación de vulnerabilidades o las actividades de orden público asociadas, nunca se hacen públicas. Sin embargo, todas se comunican a nuestros clientes.
- Datos técnicos **complementarios detallados**, incluida una lista ampliada de indicadores de compromiso (IOC), disponible en formatos estándar, como OpenIOC o STIX, y acceso a nuestras reglas YARA.
- **Supervisión continua de campañas de APT.** Acceso a inteligencia procesable durante la investigación (información sobre la distribución de APT, IOC e infraestructura C&C).
- **Contenido para diferentes públicos.** Cada uno de los informes contiene un resumen ejecutivo que ofrece información de nivel C orientada y fácil de comprender que describe la APT relacionada. El resumen ejecutivo va seguido de una descripción técnica detallada de la APT con los IOC y reglas YARA relacionados que proporciona a los investigadores de seguridad, analistas de malware, ingenieros de seguridad, analistas de seguridad de red e investigadores de APT un consejo viable para una protección excelente contra la amenaza relacionada.
- **Análisis retrospectivo.** Se ofrece acceso a todos los informes privados publicados con anterioridad durante todo el periodo de su suscripción.
- **Portal de inteligencia de APT.** Todos los informes, incluidos los más recientes de IOC, están disponibles a través de nuestro portal de inteligencia de APT que crea una experiencia de usuario perfecta para nuestros clientes. También hay disponible una API.

Nota: Limitación de suscriptores

Debido a la confidencialidad y especificidad de algunos de los datos contenidos en los informes proporcionados por este servicio, estamos obligados a limitar las suscripciones exclusivamente a organismos gubernamentales y empresas públicas y privadas de confianza.

Informes de inteligencia APT

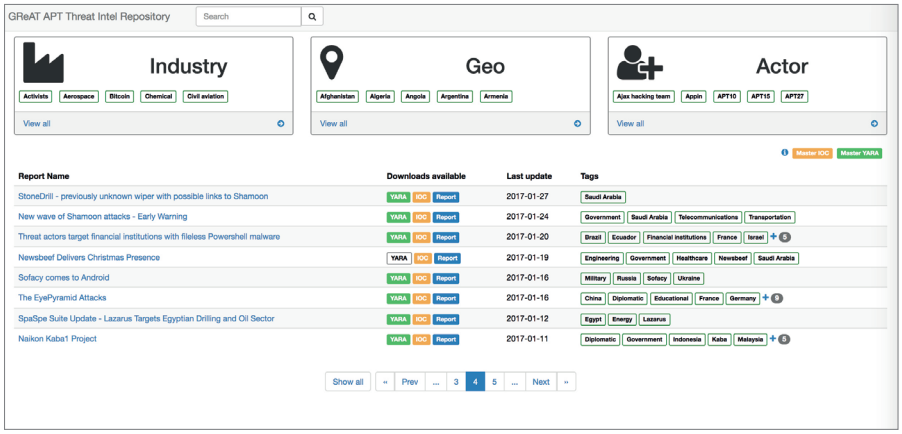
Mejore su concienciación y conocimientos acerca de las campañas de ciberespionaje de alto perfil con los completos y prácticos informes de Kaspersky Lab.

Si aprovecha la información proporcionada en estos informes, puede responder rápidamente a las nuevas amenazas y vulnerabilidades y, con ello, bloquear los ataques a través de vectores conocidos, reducir los daños causados por ataques avanzados y mejorar su estrategia de seguridad o la de sus clientes.

Kaspersky Lab ha descubierto algunos de los ataques de APT más importantes. Sin embargo, no todas las amenazas persistentes avanzadas (APT) se notifican de inmediato y muchas ni siquiera se anuncian públicamente.

Como suscriptor de los informes de inteligencia de APT de Kaspersky, le proporcionamos acceso permanente y en exclusiva a nuestras investigaciones y descubrimientos sobre las APT detectadas al instante, así como a todos los datos técnicos relevantes en una amplia variedad de formatos. Entre dicha información también se incluirán las amenazas que nunca se harán públicas. Durante 2016 hemos creado más de 100 informes.

Nuestros expertos, los cazadores de APT más cualificados y competentes del sector, también le alertarán de inmediato de los cambios que detecten en las tácticas de los grupos cibercriminales. Además, contará con acceso a toda la base de datos de informes de APT de Kaspersky Lab, otro eficaz componente de investigación y análisis de su defensa de seguridad corporativa.



Informes sobre amenazas personalizados

Informes sobre amenazas específicos del cliente

¿Cuál es la mejor manera de organizar un ataque contra su empresa? ¿Qué rutas y qué información están disponibles para un atacante que se dirija específicamente a usted? ¿Ya se ha organizado un ataque o está a punto de enfrentarse a una amenaza?

Los informes sobre amenazas específicos del cliente de Kaspersky responden a estas y otras preguntas, ya que nuestros expertos componen una imagen exhaustiva de su actual estado de ataque e identifican puntos débiles a punto para exploits y revelan pruebas de ataques pasados, presentes y previstos.

Con ayuda de toda esta información, podrá centrar su estrategia de defensa en las áreas identificadas como los principales objetivos de los cibercriminales, y actuar rápidamente y con precisión para repeler a los intrusos y minimizar el riesgo de éxito de un ataque.

Desarrollados con inteligencia de fuente abierta (OSINT), el análisis en profundidad de los sistemas y bases de datos especializados de Kaspersky Lab y nuestros conocimientos sobre las redes clandestinas de cibercriminales, estos informes abarcan áreas como:

- **Identificación de vectores de amenazas**: identificación y análisis de estado de los componentes críticos de la red disponibles externamente, incluidos cajeros

automáticos, sistemas de videovigilancia y otros sistemas que utilizan tecnologías móviles, perfiles de sus empleados en las redes sociales y cuentas de correo electrónico personales, que son posibles blancos de ataque.

- **Análisis de seguimiento de malware y ciberataques**: identificación, supervisión y análisis de muestras de malware activas o inactivas dirigidas a su empresa, actividad pasada o actual de botnets y actividades sospechosas basadas en la red.
- **Ataques de terceros**: pruebas de amenazas y actividad de botnets específicamente dirigidas a sus clientes, partners y suscriptores, cuyos sistemas infectados podrían utilizarse para atacarle.
- **Filtración de información**: por medio de la vigilancia discreta de foros y comunidades online clandestinos, descubrimos si los hackers están hablando de planes de ataque dirigidos a usted o, por ejemplo, si un empleado sin escrúpulos comercia con información.
- **Estado actual de los ataques**: los ataques de APT pueden continuar de manera inadvertida durante muchos años. Si detectamos un ataque actual que afecta a su infraestructura, le asesoramos sobre su corrección eficaz.

Inicio rápido – Fácil de utilizar – Sin necesidad de recursos

Una vez que se establecen los parámetros y los formatos de datos preferidos, no se necesita ninguna infraestructura adicional para empezar a usar este servicio de Kaspersky Lab.

Los informes sobre amenazas personalizados de Kaspersky no afectan a la integridad ni a la disponibilidad de los recursos, incluidos los recursos de red.

El servicio se puede prestar como proyecto puntual o de forma periódica mediante suscripción (por ejemplo, trimestralmente).

Informes sobre amenazas específicos del país

La ciberseguridad de un país comprende la protección de todas sus principales instituciones y organizaciones. Las amenazas persistentes avanzadas (APT) contra autoridades gubernamentales pueden afectar a la seguridad nacional. Los posibles ciberataques contra los sectores de la fabricación, el transporte, las telecomunicaciones, la banca y otros sectores fundamentales pueden conllevar importantes daños en el nivel estatal, como pérdidas financieras, accidentes de producción, bloqueo de las comunicaciones en red y descontento popular.

Disponer de una visión general de la superficie de ataque actual y las tendencias actuales de malware y ataques de hackers dirigidos contra su país le permitirá centrar su estrategia de defensa en las áreas identificadas como los principales objetivos de los ciberdelincuentes, y actuar rápidamente y con precisión para repeler a los intrusos y minimizar el riesgo de éxito de un ataque.

Creados mediante enfoques que van de la inteligencia de fuente abierta (OSINT) al análisis en profundidad de los sistemas y bases de datos especializados de Kaspersky Lab y nuestros conocimientos sobre las redes clandestinas de cibercriminales, estos informes sobre amenazas específicos del país abarcan áreas como:

- **Identificación de vectores de amenazas**: identificación y análisis de estado de los recursos de IT cruciales del país disponibles de forma externa, lo que incluye aplicaciones gubernamentales vulnerables, equipos de telecomunicaciones, componentes de sistemas de control industrial (como SCADA, PLC, etc.), cajeros automáticos, etc.
- **Análisis de seguimiento de malware y ciberataques**: identificación y análisis de campañas de APT, muestras de malware activas o inactivas, actividad de botnets pasados o presentes, y otras amenazas destacadas dirigidas contra su país, en función de los datos disponibles en nuestros exclusivos recursos de supervisión internos.
- **Filtraciones de información**: por medio de la supervisión discreta de foros y comunidades online clandestinos, detectamos si los hackers están hablando de planes de ataque dirigidos contra determinadas organizaciones. También revelamos importantes cuentas comprometidas, que pueden suponer riesgos para las organizaciones e instituciones afectadas (por ejemplo, cuentas que pertenecen a empleados de organismos gubernamentales disponibles en el robo de Ashley Madison, que se pueden emplear para operaciones de chantaje).

Los informes de inteligencia frente a amenazas de Kaspersky no afectan a la integridad y la disponibilidad de los recursos de red inspeccionados. El servicio se basa en métodos de reconocimiento de red no intrusivos y en el análisis de la información disponible en fuentes abiertas y recursos de acceso limitado.

Como conclusión del servicio se le proporcionará un informe que incluirá la descripción de las amenazas destacadas para diferentes sectores e instituciones estatales, además de información adicional sobre los resultados del análisis técnico detallado. Los informes se entregan mediante mensajes cifrados por correo electrónico.

Búsqueda de amenazas

Características destacadas del servicio

- **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], demostrando la calidad inigualable de nuestra inteligencia de seguridad al proporcionar los más altos índices de detección, sin apenas falsos positivos.
- **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 los ataques 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.
- **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.

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 de ataques, 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.

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, atributos de archivos, datos de geolocalización, cadenas de descargas, marcas de tiempo, 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.

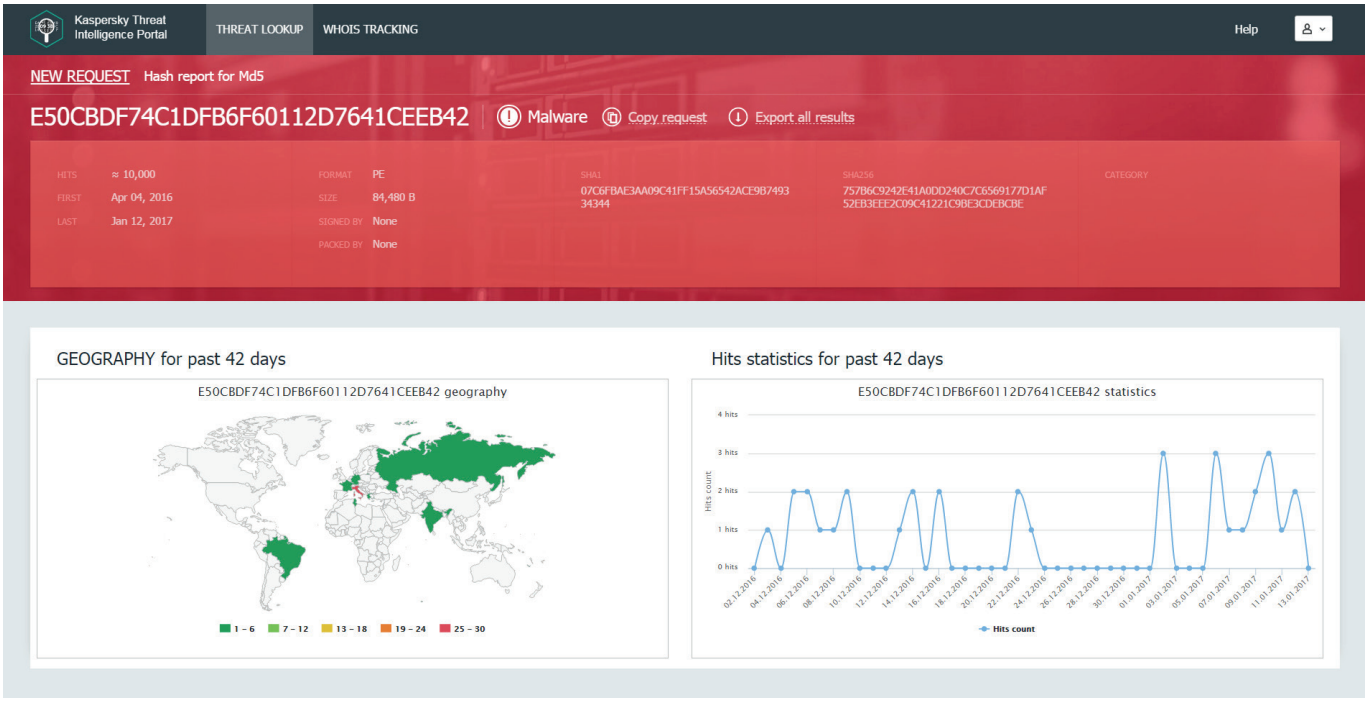
la inteligencia frente a amenazas ofrecida por Kaspersky Threat Lookup se genera y supervisa en tiempo real mediante una infraestructura muy tolerante a fallos, lo que garantiza una disponibilidad continua y un rendimiento constante. Cientos de expertos, incluidos analistas de seguridad de todo el mundo, y expertos en seguridad de fama mundial de nuestro equipo GReAT y de equipos de I+D de vanguardia, contribuyen de forma conjunta a generar valiosa inteligencia frente a amenazas del mundo real.

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 suponen el 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.

1 http://www.kaspersky.com/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.

Cada notificación de Kaspersky Phishing Tracking se entrega a través de HTTPS e incluye:

- Captura de pantalla de la URL de phishing.
- Código HTML de la URL de phishing.
- Archivo JSON que incluye los siguientes campos:
  - URL de phishing;
  - Nombre de marca a la que va dirigida la URL de phishing;
  - Marca de tiempo de la primera vez que se vio;
  - Marca de tiempo de la última vez que se vio;
  - Popularidad de la URL de phishing;
  - Geolocalización de los usuarios afectados por la URL de phishing;
  - Tipo de datos robados (información de tarjetas de crédito, credenciales para banco, correo electrónico o redes sociales, información personal, etc.);
  - Tipo de ataque (amenaza para bloquear una cuenta, oferta para descargar un archivo, solicitud para actualizar información personal, etc.);
  - Direcciones IP resueltas de esta URL de phishing;
  - Datos de WHOIS;
  - Y mucho más.

Seguimiento de phishing

El phishing, y especialmente el spear-phishing dirigido, es uno de los métodos de fraude online más peligrosos y eficaces de la actualidad. Los sitios web falsos capturan inicios de sesión y contraseñas con objeto de secuestrar las identidades online de los usuarios y, a continuación, robar dinero o distribuir spam y malware a través de cuentas de correo electrónico o plataformas de redes sociales que se hayan visto comprometidas. Es un arma poderosa en la defensa contra el cibercrimen y la frecuencia y diversidad de los ataques sigue acelerándose.

Y no solo se ven afectadas las instituciones financieras. Todos, desde los minoristas online a los ISP e instituciones gubernamentales, corren el riesgo ahora de sufrir un ataque activo de spear-phishing. Las copias perfectas de su sitio web completo con la marca corporativa o mensajes que parecen proceder directamente de sus propios ejecutivos, pueden persuadir fácilmente a los usuarios para entregar datos confidenciales, dañándose ellos mismos y causando enormes daños potenciales a la empresa.

Un único ataque de phishing con éxito puede tener un gran impacto en la víctima corporativa. Además de las pérdidas directas, están todos los costes indirectos, como la limpieza de los sitios web y las cuentas que han sido vulnerados. Y, por supuesto, existe el daño en la reputación, que puede suponer lo peor de todo: el debilitamiento de la confianza del usuario en los servicios online que pueden representar pérdidas de clientes y afrontar desafíos de credibilidad en los siguientes años. Hoy en día, el cibercrimen 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 de ataques, 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.

Nuestra solución: Kaspersky Phishing Tracking Service

Este servicio realiza un seguimiento activo y avisa en tiempo real de la aparición de sitios de phishing dirigidos contra su marca, y le ofrece informes continuos relevantes, precisos y detallados sobre phishing o actividad fraudulenta directamente relevante para su negocio, incluidas URL de malware y de phishing introducidas que intentan robar credenciales, información confidencial, información financiera y datos personales de sus usuarios. El servicio también supervisa dominios de nivel superior (TLD) específicos o incluso regiones completas para detectar la aparición de los sitios de phishing.

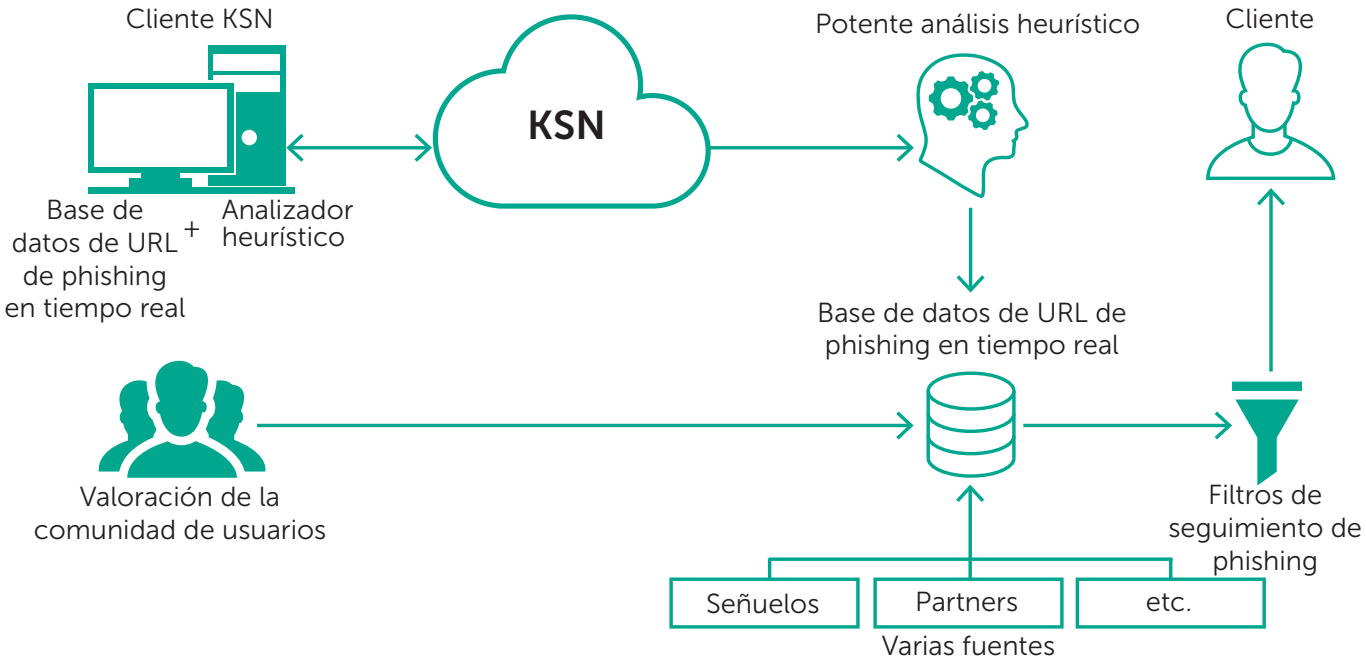
Las amenazas de phishing confirmadas por notificaciones de correo electrónico contra sus marcas, nombre de empresa o marcas comerciales son continuas. Cada notificación proporciona cobertura profunda, alta precisión e información fiable sobre los ataques de phishing cada vez más sofisticados, lo que le permite reaccionar rápidamente a dominios y URL de phishing generados dinámicamente, así como a brotes de phishing. Junto con una lista de sitios de phishing, recibirá información adicional para que pueda tomar inmediatamente medidas específicas contra cualquier ataque de phishing.

Gracias a esta inteligencia oportuna y validada profesionalmente, puede actuar rápidamente y con precisión para mitigar el impacto de la actividad de phishing en su organización y sus usuarios, adoptando una postura proactiva contra el fraude.

Fuentes de inteligencia

Kaspersky Phishing Tracking sintetiza datos de fuentes de inteligencia heterogéneas y muy fiables, incluidos Kaspersky Security Network (KSN), potentes motores heurísticos, señuelos de correo electrónico, arañas web, trampas de spam, equipos de investigación, partners y datos históricos sobre objetos maliciosos que hemos estado recopilando durante casi dos décadas. A continuación, se inspeccionan completamente los datos agregados en tiempo real y se optimizan utilizando varias técnicas de procesamiento previo que incluyen criterios estadísticos, sistemas especializados de Kaspersky Lab (sandboxes, motores heurísticos, herramientas de similitud, creación de perfiles de análisis, etc.), validación de analistas de contenido y herramientas de verificación de listas blancas.

La cobertura mundial de Kaspersky Security Network, en combinación con las tecnologías de detección de Kaspersky Lab y un aluvión de pruebas y filtros garantizan la detección máxima de cualquier tipo de ataque y amenazas de phishing y sin falsos positivos, ya que está continuamente confirmado por pruebas independientes*.



Alerta anticipada de ataques de phishing

La suscripción a Kaspersky Phishing Tracking Service ofrece una ventaja esencial contra sus atacantes. Armado con una alerta anticipada de ataques de phishing, en curso o aún en planificación, dirigidos a sus marcas, servicios online y clientes, le permite proteger los recursos y reducir los riesgos de forma más pragmática, más precisa y más rentable.

Un paso por delante

Se proporciona información crucial en tiempo real, así como a través de informes periódicos sobre actividades maliciosas que indican que se están planificando ataques avanzados, así como los que están en curso. Ahora es usted, no a los cibercriminales que le tienen en su punto de mira, quién está un paso por delante.

Mejora de la experiencia de sus usuarios

Una vez que conoce y entiende a sus adversarios de spear-phishing, puede planificar la protección apropiada, desde la prohibición de software obsoleto hasta la introducción de autorización basada en SMS, todo lo cual ayuda a sus clientes online a sentirse mejor protegidos y tranquilos.

Minimización del impacto

Conocer las URL de sitios web de phishing significa que se puede notificar a los ISP que alojan los sitios, evitando la fuga de datos personales adquiridos por el sitio y deteniendo el ataque antes de que se desarrolle.

Estar mejor informado

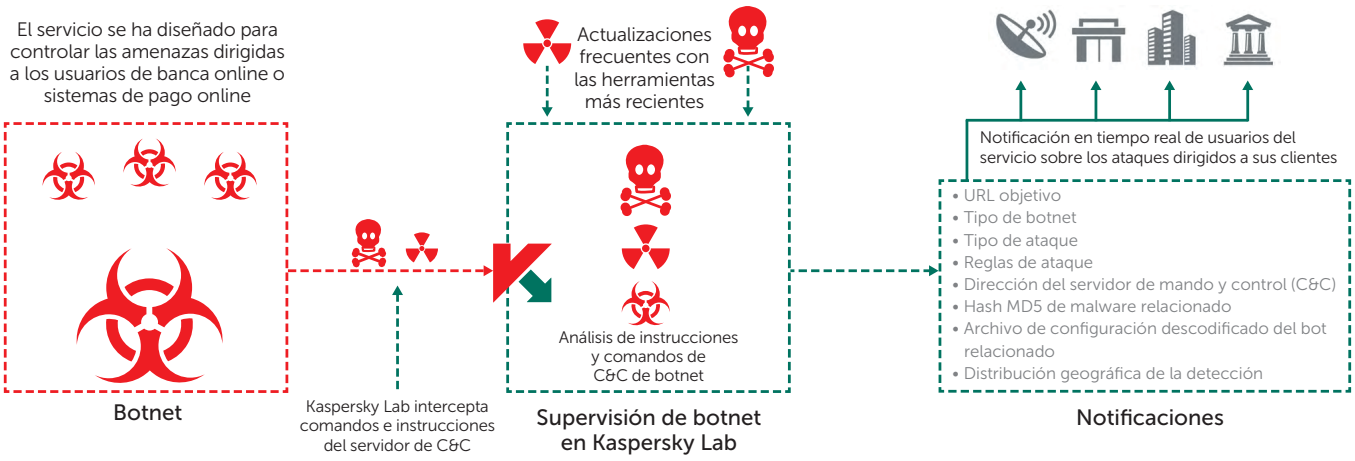
Este flujo de información relevante, precisa y detallada, sin "falsos positivos" ni pérdida de tiempo, proporciona nueva información para ayudar a informar y mejorar su estrategia de seguridad actual y futura. Ahora, usted y su empresa pueden adoptar una posición proactiva e informada contra el fraude online.

AV comparatives Approved 2016 Anti-Phishing

* Existen informes de pruebas de AV-Comparatives disponibles a petición.

Seguimiento de botnets

Servicios expertos de supervisión y notificación para identificar los botnets que son una amenaza para su reputación y para sus clientes.



Casos de uso y ventajas del servicio

- Las alertas proactivas acerca de las amenazas procedentes de botnets destinados a sus usuarios online le permiten mantenerse siempre un paso por delante del ataque
- La identificación de una lista de URL de servidores de mando y control (C&C) destinadas a sus usuarios online permite bloquearlas mediante el envío de solicitudes a los CERT o cuerpos de seguridad
- Mejora de sus operaciones bancarias online/cajones de pago gracias a la comprensión de la naturaleza del ataque
- Formación de los usuarios online para reconocer y evitar que les engañen con la ingeniería social utilizada en los ataques

Actúe en tiempo real:

El servicio incluye una suscripción de notificaciones personalizadas que contienen información de inteligencia sobre las marcas afectadas obtenida mediante el seguimiento de las palabras clave de los botnets que vigila Kaspersky Lab. Las notificaciones se pueden enviar por correo electrónico o RSS en formato HTML o JSON. Las notificaciones incluyen lo siguiente:

- **URL objetivo**: el malware de bots está diseñado para esperar hasta que el usuario acceda a las URL de la organización objetivo y, en ese momento, ejecuta el ataque.
- **Tipo de botnet**: comprenda exactamente la amenaza de malware que el cibercriminal utiliza para poner en peligro las transacciones de sus clientes. Algunos ejemplos son Zeus, SpyEye, Citadel, etc.
- **Tipo de ataque**: identifique con qué finalidad se utiliza el malware. Por ejemplo, para insertar datos web, borrar el contenido de la pantalla, hacer capturas de vídeo o reenviar al usuario a URL de phishing.
- **Reglas de ataque**: conozca las reglas de inserción de códigos web que se utilizan, como por ejemplo solicitudes HTML (OBTENCIÓN/PUBLICACIÓN) o los datos de la página web antes y después de la inserción.
- **Dirección del servidor de mando y control (C&C)**: permite notificar el proveedor de servicios de Internet del servidor atacante para agilizar el desbaratamiento de la amenaza.
- **Hash MD5 de malware relacionado**: Kaspersky proporciona la suma de verificación, que se utiliza para comprobar el malware.
- **Archivo de configuración descodificado del bot relacionado**: para identificar todas las URL objetivo.
- **Distribución geográfica de la detección (10 países principales)**: con datos estadísticos de las muestras de malware relacionadas de todo el mundo.

Kaspersky Threat Hunting Services

Los equipos de seguridad de todos los sectores están trabajando duro para crear sistemas que proporcionen una protección completa contra las ciberamenazas de rápida evolución. Pero la mayoría de estos adoptan un enfoque basado en "alerta" de incidentes de ciberseguridad, reaccionando solo después de que se haya producido un incidente. Según un estudio reciente, una gran proporción de los incidentes de seguridad sigue pasando inadvertida. Estas amenazas se mueven bajo el radar, ofreciendo a las empresas, básicamente, una falsa sensación de seguridad. Como resultado, las organizaciones reconocen cada vez más la necesidad de perseguir de forma proactiva las amenazas que no son detectadas pero están activas dentro de sus infraestructuras. Kaspersky Threat Hunting Services ayudan a descubrir amenazas avanzadas ocultas dentro de la organización, utilizando técnicas de búsqueda de amenazas proactivas llevadas a cabo por profesionales de seguridad altamente cualificados y experimentados.

Kaspersky Cybersecurity Services

- **Kaspersky Threat Intelligence Services**
- **Kaspersky Threat Hunting Services**
  Protección gestionada de Kaspersky
  Targeted Attack Discovery
- **Kaspersky Security Training**
- **Kaspersky Incident Response Services**
- **Kaspersky Security Assessment Services**

Ventajas de los servicios

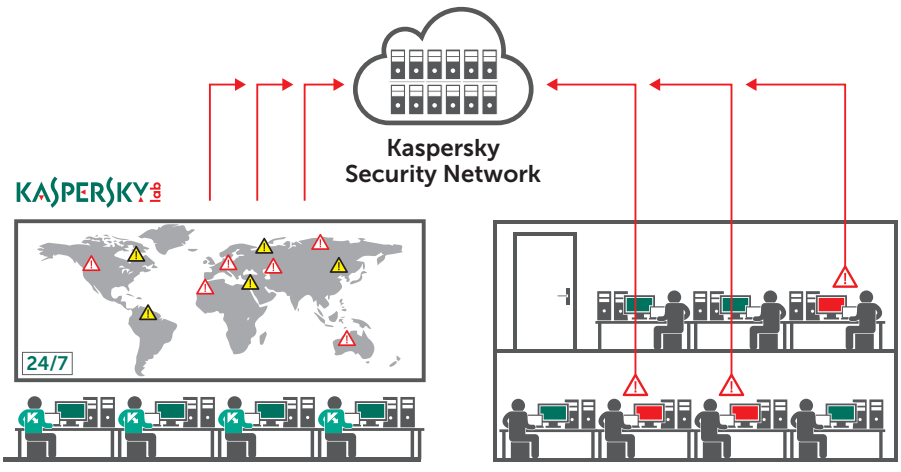
- Detección rápida y eficiente, que permite una mitigación y acción correctiva más rápidas y efectivas.
- Sin falsos positivos que hagan perder el tiempo, gracias a la clara identificación inmediata y la clasificación de cualquier actividad sospechosa.
- Reducción general de los costes de seguridad. Sin necesidad de utilizar y formar a una amplia gama de especialistas internos que puede necesitar.
- La garantía de saber que está continuamente protegido contra las amenazas más complejas e innovadoras que no son de malware.
- Información sobre los atacantes, su motivación, sus métodos y herramientas, así como los posibles daños que pueden infligir, lo que respalda el desarrollo de una estrategia de protección totalmente fundamentada y eficiente.

Protección gestionada de Kaspersky

El servicio de protección gestionada de Kaspersky ofrece a los usuarios de Kaspersky Endpoint Security y Kaspersky Anti Targeted Attack Platform un servicio totalmente gestionado, desplegando una gama única de medidas técnicas avanzadas para detectar y evitar ataques dirigidos en su organización El servicio incluye supervisión continua por parte de los expertos de Kaspersky Lab y análisis constante de datos de ciberamenazas, lo que garantiza la detección en tiempo real de campañas de ciberespionaje y cibercrimen nuevas y conocidas dirigidas contra sistemas de información cruciales.

Características destacadas del servicio

- Un alto nivel de protección contra ataques dirigidos y malware con supervisión permanente y asistencia de su propio "equipo estrella" de expertos de Kaspersky Lab, que utilizan un amplio conjunto de habilidades especializadas e inteligencia continua frente a amenazas.
- Detección de ataques que no son de malware, ataques que incluyen herramientas conocidas anteriormente y ataques que explotan las vulnerabilidades de día cero.
- Protección inmediata contra cualquier amenaza detectada a través de actualizaciones automáticas de la base de datos de virus.
- Análisis retrospectivo de incidentes y búsqueda de amenazas, incluidos los métodos y tecnologías utilizados por los actores de amenazas contra su organización.
- Enfoque integrado: la cartera de Kaspersky Lab incluye todas las tecnologías y servicios que necesita para implementar un ciclo completo de protección frente a ataques dirigidos: Preparación – Detección – Investigación – Análisis de datos – Protección automatizada.



Targeted Attack Discovery

Los expertos de Kaspersky Lab ofrecen un servicio específico de detección de ataques dirigidos proactivo para garantizar la verdadera seguridad de los activos de su empresa.

Los resultados de Targeted Attack Discovery le permitirán identificar la actividad de cibercrimen y ciberespionaje actual en su red, comprender los motivos subyacentes y las posibles fuentes de estos incidentes, así como planificar eficazmente actividades de mitigación que le ayudarán a evitar ataques similares en el futuro. Si está preocupado por los ataques dirigidos a su sector, si ha anotado posibles comportamientos sospechosos en sus propios sistemas o si su organización simplemente reconoce las ventajas de las inspecciones preventivas, los servicios de Kaspersky Targeted Attack Discovery se han diseñado para indicarle:

- Si está siendo atacado actualmente, cómo y por quién
- Cómo está afectando este ataque a sus sistemas y qué puede hacer al respecto
- La mejor forma de evitar más ataques

Cómo funciona el servicio

Nuestros expertos independientes reconocidos a nivel mundial revelarán, identificarán y analizarán los incidentes en curso, las amenazas avanzadas persistentes (APT), así como las actividades de cibercrimen y ciberespionaje en su red. Le ayudarán a descubrir actividades maliciosas, comprender las posibles fuentes de incidentes y planificar las acciones correctivas más eficaces.

Para ello, utilizamos:

- El análisis de fuentes de inteligencia frente a amenazas para comprender el panorama de amenazas específicas de su organización
- La realización de exploraciones en profundidad de la infraestructura y datos de IT (como archivos de registro) para descubrir posibles signos de riesgo
- El análisis de sus conexiones de red salientes para identificar cualquier actividad sospechosa
- Detección de las probables fuentes del ataque y otros sistemas potencialmente comprometidos

Resultados

Nuestras conclusiones se entregan en un informe detallado que abarca:

Nuestros descubrimientos generales: confirmación de la presencia o ausencia de signos de riesgo en su red.

Análisis en profundidad: de datos de inteligencia frente a amenazas recopilados y de los indicadores de compromiso (IOC) revelados.

Descripciones detalladas: de vulnerabilidades explotadas, posibles fuentes de ataque y componentes de la red afectados.

Recomendaciones de acciones correctivas: pasos sugeridos para mitigar las consecuencias del incidente revelado y para proteger sus recursos de ataques similares en el futuro.

Servicios adicionales

También puede pedir a nuestros expertos que analicen los síntomas de un incidente, que realicen un análisis digital profundo de ciertos sistemas, que identifiquen un binario del malware (si lo hay) y que realicen el análisis de malware. Estos servicios opcionales se ofrecen por separado, con más recomendaciones de acciones correctivas.

También podemos, a petición, implementar la plataforma **Kaspersky Anti Targeted Attack (KATA)** en su red, de forma permanente o como un ejercicio de "prueba de concepto". Esta plataforma combina las últimas tecnologías y análisis globales para detectar y responder rápidamente a los ataques dirigidos, así como contrarrestar el ataque en todas las fases de su ciclo de vida en su sistema.

El servicio de forma más detallada

Kaspersky Targeted Attack Discovery incluye las siguientes actividades:

Recopilación y análisis de inteligencia frente a amenazas. El objetivo es obtener una instantánea en el momento de su superficie de ataque: amenazas y ataques de cibercrimen y ciberespionaje dirigidas potencialmente o de forma activa a sus activos. Aprovecharemos las fuentes de inteligencia internas y externas, incluidas las comunidades de estafadores clandestinas, así como los sistemas de supervisión internos de Kaspersky Lab. El análisis de esta inteligencia nos permite identificar, por ejemplo, puntos débiles de su infraestructura de interés actual para los cibercriminales o cuentas comprometidas.

Recopilación de datos en tiempor real y respuesta temprana ante incidentes. Junto con la actividad de inteligencia frente a amenazas realizada en nuestros propios laboratorios, los expertos de Kaspersky Lab estarán in situ recopilando artefactos de la red y del sistema, junto con cualquier información de SIEM disponible. También podemos realizar un breve análisis de vulnerabilidades para revelar la mayoría de errores críticos de seguridad para una acción inmediata. Si un incidente ya ha tenido lugar, recopilaremos pruebas para su investigación. En esta fase, le proporcionaremos nuestras recomendaciones provisionales para acciones correctivas a corto plazo.

Análisis de datos. La red y los artefactos del sistema recopilados se analizan en el laboratorio, utilizando la base de conocimientos de Kaspersky Lab de IOC, listas negras de mando y control, tecnología sandbox, etc. para entender exactamente lo que está sucediendo en su sistema. Si, por ejemplo, se identifica un nuevo malware en esta fase, le ofreceremos consejo y las herramientas (es decir, reglas YARA) para detectarlo de inmediato. Nos mantendremos en estrecho contacto con usted, trabajando de forma remota con sus sistemas si es necesario.

Preparación del informe. Por último, prepararemos nuestro informe formal con resultados de detección de ataques dirigidos y nuestras recomendaciones para aplicar actividades correctivas adicionales.

Kaspersky Security Training

La formación sobre la ciberseguridad es ahora la herramienta fundamental para las empresas, que deben enfrentarse a un número cada vez mayor de amenazas que no dejan de evolucionar. El personal de seguridad de IT debe formarse en el uso de técnicas avanzadas porque es un factor imprescindible de las estrategias de gestión y mitigación eficaces de las amenazas a la empresa.

Kaspersky Cybersecurity Services

- **Kaspersky Threat Intelligence Services**
- **Kaspersky Threat Hunting Services**
- **Kaspersky Security Training**
  - Ciencia forense digital
  - Análisis de malware e ingeniería inversa
  - Ciencia forense digital avanzada
  - Análisis avanzado de malware e ingeniería inversa
  - Respuesta ante incidentes
  - Yara
  - Administración de KATA
  - Analista de seguridad de KATA
- **Kaspersky Incident Response Services**
- **Kaspersky Security Assessment Services**

Estos cursos tienen contenidos muy amplios, que cubren desde las técnicas, las evaluaciones y los aspectos de ciberseguridad más básicos hasta los más avanzados. Todos los cursos están disponibles a través de clases en las instalaciones del cliente o en una oficina de Kaspersky Lab local o regional, según corresponda.

La estructura de los cursos combina teórica y práctica. Al término de cada curso, se invita a los asistentes a completar una evaluación para validar sus conocimientos.

Ventajas de los servicios

Ciencia forense digital y ciencia forense digital avanzada

Mejore la experiencia del equipo interno de ciencia forense digital y de respuesta ante incidentes. Los cursos se han diseñado para cubrir brechas de experiencia: desarrollo y mejora de habilidades prácticas en la búsqueda de pistas de cibercrimen y en el análisis de diferentes tipos de datos para restaurar los plazos y fuentes de ataque. Tras finalizar el curso, los estudiantes serán capaces de investigar los incidentes informáticos correctamente y mejorar el nivel de seguridad de la empresa.

Análisis de malware e ingeniería inversa y análisis avanzado de malware e ingeniería inversa

La formación sobre ingeniería inversa se ha diseñado para ayudar a los grupos que responden a incidentes en la investigación de ataques maliciosos. Este curso está dirigido a los empleados del departamento de IT y a administradores de sistemas. Los estudiantes aprenderán a analizar software malicioso, recopilar IOC (indicadores de compromiso), escribir firmas para la detección de malware en los equipos infectados y restaurar archivos y documentos infectados o cifrados.

Respuesta ante incidentes

Este curso guiará a su equipo interno a través de todas las fases del proceso de respuesta ante incidentes y les proporcionará los amplios conocimientos necesarios para llevar a cabo acciones correctivas adecuadas para incidentes.

Yara

Le ayudará a aprender a escribir las reglas Yara más eficaces, cómo probarlas y mejorarlas hasta el punto de que encuentren amenazas que nada más puede detectar.

Administración de KATA

La formación de administración de KATA proporciona todos los conocimientos necesarios para planificar, instalar y configurar la solución con el fin de optimizar su eficiencia de detección de amenazas.

Analista de seguridad de KATA

El curso de formación incluye una serie de ejercicios prácticos basados en escenarios reales de detección de amenazas que proporcionan los conocimientos necesarios para supervisar, interpretar y responder de forma fiable a alertas de KATA.

Experiencia práctica

Con ayuda de un proveedor de seguridad líder, podrá trabajar y aprender codo con codo con nuestros expertos mundiales; toda una inspiración para los participantes, gracias a su propia experiencia en la vanguardia de la detección y prevención del cibercrimen.

Descripción del programa

Temas	Duración	Habilidades adquiridas
Ciencia forense digital		
• Introducción a la ciencia forense digital • Respuesta activa y obtención de pruebas • Datos internos del registro de Windows • Análisis de artefactos de Windows • Ciencia forense de navegadores • Análisis de correo electrónico	5 días	• Desarrollar un laboratorio de ciencia forense digital • Recopilar pruebas digitales y gestionarlas correctamente • Reconstruir un incidente y utilizar marcas de tiempo • Encontrar rastros de intrusión basados en artefactos de sistemas operativos Windows • Encontrar y analizar el historial del navegador y el correo electrónico • Poder aplicar las herramientas y los instrumentos de la ciencia forense digital
Análisis de malware e ingeniería inversa		
• Objetivos y técnicas del análisis de malware e ingeniería inversa • Datos internos, archivos ejecutables, ensamblador x86 de Windows • Técnicas de análisis estáticos básicas (extracción de cadenas, análisis de importación, • puntos de entrada PE de un vistazo, descompresión automática, etc.) • Técnicas de análisis dinámicos básicas (depuración, herramientas de supervisión, interceptación de tráfico, etc.) • Análisis de archivos .NET, Visual Basic, Win64 • Técnicas de análisis de scripts y no PE (archivos por lotes; Autoit; Python; Jscript; JavaScript; VBS)	5 días	• Crear un entorno seguro para el análisis de malware: implementar sandbox y todas las herramientas necesarias • Comprender los principios de la ejecución del programa de Windows • Descomprimir, depurar y analizar objetos maliciosos, identificar sus funciones • Detectar sitios maliciosos a través del análisis de malware de scripts • Realizar análisis de malware urgentes
Ciencia forense digital avanzada		
• Ciencia forense detallada de Windows • Recuperación de datos • Ciencia forense de red y nube • Ciencia forense de memoria • Análisis de la escala de tiempo • Práctica de ciencia forense de ataque con un objetivo en el mundo real	5 días	• Poder realizar análisis detallados del sistema de archivos • Poder recuperar archivos eliminados • Poder analizar el tráfico de red • Detectar actividades maliciosas de volcados • Reconstruir la escala de tiempo del incidente
Análisis avanzado de malware e ingeniería inversa		
• Objetivos y técnicas del análisis de malware e ingeniería inversa • Técnicas de análisis estático avanzado (análisis estadístico del shellcode, análisis del encabezado PE, TEB, PEB, funciones de carga mediante diferentes algoritmos de hash) • Técnicas de análisis dinámico avanzado (estructura de PE, descompresión manual y avanzada, descompresión de empaquetadores maliciosos que almacenan todo el archivo ejecutable en formato cifrado) • Ingeniería inversa de APT (cubre un escenario de ataque de APT, desde el correo electrónico de phishing hasta profundizar al máximo posible) • Análisis de protocolos (análisis del protocolo de comunicación C2 cifrado y cómo descifrar el tráfico) • Análisis de rootkits y bootkits (depuración del sector de inicio mediante Ida y VMWare, depuración de kernel mediante dos máquinas virtuales y análisis de muestras de rootkit)	5 días	• Capacidad para seguir las prácticas recomendadas de ingeniería inversa mientras se reconocen las técnicas contrarias a la ingeniería inversa (ofuscación, antidepuración) • Capacidad para aplicar análisis de malware avanzado para la disección de rootkits y bootkits • Capacidad para analizar shellcode de exploits incrustado en diferentes tipos de archivos y malware no Windows

Descripción del programa

Temas	Duración	Habilidades adquiridas
Respuesta ante incidentes		
• Introducción a la respuesta ante incidentes • Detección y análisis primario • Análisis digital • Creación de reglas de detección (YARA, Snort, Bro)	5 días	• Diferenciación de las APT del resto de amenazas • Comprensión de las distintas técnicas y la anatomía de ataque dirigido de los atacantes • Aplicación de métodos específicos de supervisión y detección • Seguimiento del flujo de trabajo de la respuesta ante incidentes • Reconstrucción de la cronología y lógica del incidente • Creación de reglas e informes de detección
Yara		
• Breve introducción de la sintaxis de YARA • Sugerencias y trucos para crear reglas rápidas y eficaces • Generadores de YARA • Comprobación de reglas YARA para falsos positivos • Búsqueda de nuevas muestras no detectadas en VT • Uso de módulos externos de YARA para búsqueda efectiva • Búsqueda de anomalías • Muchos ejemplos de la vida real • Conjunto de ejercicios para mejorar sus habilidades de YARA	2 días	• Creación de reglas YARA eficaces • Comprobación de reglas YARA • Mejorarlas hasta el punto de que encuentren amenazas que nadie más detecte
Administración de KATA		
• Escenarios de implementación de soluciones habituales y ubicaciones de servidores • Consideraciones de tamaño • Modelo de licencias • Servidor sandbox • Nodo central • Sensor • Integración con la infraestructura • Instalación del sensor de endpoint • Adición de una licencia y actualización de las bases de datos • Algoritmo de funcionamiento de soluciones	1 día	• Diseño del plan de implementación ajustado al entorno de un cliente • Instalación y configuración de todos los componentes de KATA • Mantenimiento y supervisión de la solución
Analista de seguridad de KATA		
• Interpretación de alertas de KATA • Explicación de tecnologías de detección y análisis • Explicación de motores de puntuación y riesgos	1 día	• Comprensión del funcionamiento de la puntuación y de cómo la emplean los motores de riesgos • Capacidad para supervisar, interpretar y responder de forma fiable a alertas de KATA

Kaspersky Incident Response Services

Mientras sus especialistas en seguridad y IT se esfuerzan por asegurarse de que cada componente de la red esté protegido contra intrusos y totalmente disponible para los usuarios legítimos, una sola vulnerabilidad puede ofrecer una puerta abierta a cualquier cibercriminal que tenga la intención de hacerse con el control de sus sistemas de información. Nadie es inmune: por muy eficaces que sean sus controles de seguridad, puede convertirse en una víctima.

Es cada vez más complicado evitar los incidentes de seguridad de la información. Sin embargo, aunque puede que no siempre sea posible detener los ataques antes de que penetren en su perímetro de seguridad, está absolutamente en nuestro poder limitar el daño y evitar la propagación del ataque.

El objetivo general de la respuesta ante incidentes es reducir el impacto de una brecha de seguridad o un ataque en su entorno de IT. El servicio abarca todo el ciclo de investigación del incidente, desde la adquisición de pruebas in situ hasta la identificación de indicadores adicionales de riesgo, con la preparación de un plan de corrección y la eliminación completa de la amenaza para su organización.

Para ello, utilizamos:

- Identificación de los recursos comprometidos.
- Aislamiento de la amenaza.
- Prevención de la propagación del ataque.
- Búsqueda y recopilación de pruebas.
- Análisis de las pruebas y reconstrucción de la cronología y la lógica del incidente.
- Análisis del malware utilizado en el ataque (si se detecta algún malware).
- Detección de las fuentes del ataque y otros sistemas potencialmente comprometidos (si es posible).
- Realización de análisis asistidos por herramientas de su infraestructura de IT para revelar posibles signos de riesgo.
- Análisis de las conexiones actuales entre su red y los recursos externos con el fin de detectar cualquier elemento sospechoso (como posibles servidores de mando y control).
- Eliminación de la amenaza.
- Recomendación de acciones de corrección adicionales que puede emprender.

En función de si cuenta o no con su propio equipo de respuesta ante incidentes, puede pedir a nuestros expertos que lleven a cabo el ciclo de investigación completo, para identificar y aislar de forma sencilla los equipos comprometidos y evitar la distribución de la amenaza, o para realizar un análisis de malware o ciencia forense digital.

Incident Response Services de Kaspersky Lab los llevan a cabo analistas e investigadores de detección de ciberintrusiones muy experimentados. Todo el peso de nuestra experiencia práctica mundial en ciencia forense digital y análisis de malware se aplica a la resolución del incidente de seguridad.

Análisis de malware

El análisis de malware ofrece una comprensión completa del comportamiento y los objetivos de los archivos de malware específicos dirigidos a su empresa. Los expertos de Kaspersky Lab llevan a cabo un análisis exhaustivo de la muestra de malware que proporciona, y crean un informe detallado que incluye:

- **Propiedades de la muestra:** una breve descripción de la muestra y una decisión sobre su clasificación como malware.

- **Descripción detallada del malware:** un análisis en profundidad de las funciones de la muestra de malware, el comportamiento y los objetivos de la amenaza (incluidos los indicadores de compromiso, IOC), para que disponga de la información necesaria para neutralizar sus actividades.

- **Acción correctiva:** en el informe se incluirán sugerencias para proteger totalmente a su empresa frente a este tipo de amenaza.

Ciencia forense digital

La ciencia forense digital puede incluir análisis de malware como se ha descrito anteriormente, si se ha detectado cualquier malware durante la investigación. Los expertos de Kaspersky Lab ensamblan las pruebas para entender exactamente lo que está sucediendo, incluidas las imágenes del disco duro, los volcados de memoria y los rastros de red. El resultado es una aclaración detallada del incidente. Como cliente, usted inicia el proceso con la recopilación de pruebas y una exposición del incidente. Los expertos de Kaspersky Lab analizan los síntomas del incidente, identifican el binario del malware (si lo hay) y realizan el análisis de malware con el fin de proporcionar un informe detallado con acciones correctivas.

Opciones de entrega

Los servicios de respuesta ante incidentes de Kaspersky Lab están disponibles de la siguiente forma:

- Mediante suscripción
- Como respuesta a un único incidente

Ambas opciones se basan en la cantidad de tiempo que nuestros expertos emplean resolviendo el incidente: se negocia con usted antes de firmar el contrato. Puede especificar el número de horas de trabajo que desea emplear o seguir las recomendaciones de nuestros expertos según el incidente concreto y sus requisitos individuales.

Kaspersky Security Assessment Services

Security Assessment Services de Kaspersky Lab son los servicios ofrecidos por nuestros expertos internos, muchos de ellos autoridades mundiales por derecho propio, cuyos conocimientos y experiencia son fundamentales para nuestra reputación como líderes mundiales en inteligencia de seguridad.

Como no hay dos infraestructuras de IT que sean idénticas y como las ciberamenazas más peligrosas están hechas a medida para explotar las vulnerabilidades concretas de cada empresa, nuestros servicios expertos también están hechos a medida. Los servicios que se describen en las páginas siguientes forman parte de nuestro kit de herramientas profesionales: todos o algunos de estos servicios, en parte o en su totalidad, pueden aplicarse a medida que trabajemos con usted.

Nuestro objetivo es, sobre todo, trabajar de manera individualizada con usted, como sus asesores expertos, y ayudarle a evaluar sus riesgos, reforzar su seguridad y mitigar las amenazas futuras.

Security Assessment Services incluyen:

- Pen Testing
- Evaluación de seguridad de las aplicaciones
- Evaluación de seguridad de cajeros automáticos y puntos de venta
- Evaluación de seguridad de redes de telecomunicaciones

Kaspersky Cybersecurity Services

- **Kaspersky Threat Intelligence Services**
- **Kaspersky Threat Hunting Services**
- **Kaspersky Security Training**
- **Kaspersky Incident Response Services**
- **Kaspersky Security Assessment Services**
  - Pen Testing
  - Evaluación de seguridad de las aplicaciones
  - Evaluación de seguridad de cajeros automáticos y puntos de venta
  - Evaluación de seguridad de redes de telecomunicaciones

Pen Testing

Garantizar que su infraestructura de IT está totalmente protegida contra posibles ciberataques supone un reto continuo para cualquier organización, pero aún más para las grandes corporaciones con miles de empleados, cientos de sistemas de información y varias ubicaciones en todo el mundo.

Pen Testing son una demostración práctica de los posibles escenarios de ataque en los que un actor malicioso puede intentar eludir los controles de seguridad de su red corporativa para obtener privilegios elevados en sistemas importantes.

Los Pen Testing de Kaspersky Lab le permites conocer mejor las deficiencias de seguridad de su infraestructura, puesto que revela las vulnerabilidades, analiza las posibles consecuencias de las diferentes formas de ataque, evalúa la eficacia de sus medidas de seguridad actuales y propone acciones correctivas y mejoras.

Los Pen Testing de Kaspersky Lab le ayudan a usted y a su empresa a:

- **Identificar los puntos más débiles de la red,** para que pueda tomar decisiones bien fundamentadas acerca de dónde debe concentrar su atención y su presupuesto a fin de mitigar futuros riesgos.
- **Evitar las pérdidas económicas, operativas y de reputación causadas por los ciberataques** al impedir que se produzcan, por medio de la detección y solución proactivas de vulnerabilidades.
- **Cumplir las normas de organismos gubernamentales, del sector o internas de la empresa** que requieran esta forma de evaluación de la seguridad (por ejemplo, la norma relativa a la seguridad de los datos del sector de las tarjetas de pago, o PCI DSS).

Resultados de Pen Testing

El servicio está diseñado para revelar las deficiencias de seguridad que podrían explotarse para obtener acceso no autorizado a los componentes de red cruciales. Podrían ser, entre otras:

- Arquitectura de red vulnerable, insuficiente protección de la red
- Vulnerabilidades que conducen a la interceptación y la redirección del tráfico de red
- Autenticación y autorización insuficientes en diferentes servicios
- Credenciales de usuario poco seguras
- Errores de configuración, incluido un exceso de privilegios de usuario
- Vulnerabilidades provocadas por errores en el código de las aplicaciones (insertar código, atravesar rutas de acceso, vulnerabilidades de clientes, etc.)
- Vulnerabilidades provocadas por el uso de versiones anticuadas de hardware y software sin las actualizaciones de seguridad más recientes
- Revelación de información

Los resultados se distribuyen en un informe final que incluye información técnica detallada sobre el proceso de prueba, los resultados, las vulnerabilidades detectadas y recomendaciones para su corrección, así como un resumen esquemático de los resultados de la prueba en el que se ilustran los vectores de ataque. Si es necesario, también podemos proporcionar vídeos y presentaciones para su equipo técnico o directivo.

Ámbito y opciones del servicio

En función de sus necesidades y de su infraestructura de IT, puede decidir usar alguno de los siguientes servicios o todos ellos:

- **Pen Testing externa:** evaluación de seguridad realizada a través de Internet por un "atacante" sin conocimiento previo de su sistema.
- **Pen Testing interna:** escenarios basados en un atacante interno, como un visitante con únicamente acceso físico a sus oficinas o un contratista con acceso limitado a los sistemas.
- **Pruebas de ingeniería social:** evaluación de la concienciación sobre la seguridad entre su personal por medio de la emulación de ataques de ingeniería social, como phishing, enlaces pseudomaliciosos en correos electrónicos, archivos adjuntos sospechosos, etc.
- **Evaluación de seguridad de redes inalámbricas:** nuestros expertos visitarán su emplazamiento y analizarán los controles de seguridad Wi-Fi.

Puede incluir cualquier parte de su infraestructura de IT en el ámbito de las pruebas de penetración, pero le recomendamos que considere la totalidad de la red o sus sectores más grandes, ya que los resultados de las pruebas son siempre más valiosos cuando nuestros expertos trabajan bajo las mismas condiciones que un intruso potencial.

Acerca del enfoque de Kaspersky Lab ante Pen Testing

Aunque los Pen Testing emulan ataques reales de hackers, estas pruebas están muy controladas y las realizan expertos en seguridad de Kaspersky Lab con plena atención a la confidencialidad, integridad y disponibilidad de sus sistemas y con un respeto escrupuloso las normas y prácticas recomendadas internacionales, incluidas:

- Penetration Testing Execution Standard (PTES)
- NIST Special Publications 800-115 Technical Guide to Information Security Testing and Assessment
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assessment Framework (ISSAF)
- Clasificación de amenazas de Web Application Security Consortium (WASC)
- Guía de pruebas de Open Web Application Security Project (OWASP)
- Common Vulnerability Scoring System (CVSS)

Los miembros del equipo de proyecto son profesionales experimentados, con profundos conocimientos prácticos actuales sobre este tema, reconocidos como asesores de seguridad por líderes del sector como Oracle, Google, Apple, Microsoft, Facebook, PayPal, Siemens y SAP.

Opciones de entrega

Según el tipo de servicio de evaluación de seguridad, las características concretas de sus sistemas y sus prácticas de trabajo, los servicios de evaluación de seguridad pueden prestarse de manera remota o in situ. La mayoría de los servicios pueden prestarse de manera remota y las pruebas de penetración interna pueden realizarse incluso mediante un acceso VPN, mientras que algunos servicios (como la evaluación de seguridad de las redes inalámbricas) requieren una presencia in situ.

Evaluación de Seguridad de las aplicaciones

Tanto si desarrolla aplicaciones corporativas internamente como si las compra a terceros, sabrá que un solo error de código puede crear una vulnerabilidad que le expondrá a ataques que causan enormes pérdidas económicas o daños a su reputación. También pueden generarse nuevas vulnerabilidades durante el ciclo de vida de una aplicación, por medio de actualizaciones de software o configuración insegura de componentes, o a través de nuevos métodos de ataque.

La evaluación de seguridad de aplicaciones de Kaspersky Lab detecta vulnerabilidades en aplicaciones de cualquier tipo, desde soluciones basadas en la nube de gran envergadura, sistemas ERP, aplicaciones de banca online y otras

aplicaciones específicas de su empresa, hasta aplicaciones móviles e integradas para diferentes plataformas (iOS, Android, etc.).

Nuestros expertos, que combinan conocimientos prácticos y experiencia con prácticas recomendadas internacionales, detectan deficiencias de seguridad que podrían exponer a su empresa a amenazas como las siguientes:

- Filtración de datos confidenciales
- Infiltración y modificación de datos y sistemas
- Inicio de ataques de denegación del servicio
- Realización de actividades fraudulentas

Siguiendo nuestras recomendaciones, las vulnerabilidades detectadas en las aplicaciones pueden corregirse y así impedir esos ataques.

Ventajas de los servicios

Los servicios de evaluación de seguridad de aplicaciones de Kaspersky Lab ayudan a los propietarios y desarrolladores de aplicaciones a:

- **Evitar pérdidas económicas, operativas y de reputación**, al detectar y corregir de manera proactiva las vulnerabilidades utilizadas en los ataques contra aplicaciones
- **Ahorrar en gastos de corrección**, al rastrear las vulnerabilidades en aplicaciones aún en desarrollo y pruebas, antes de que lleguen al entorno de usuario, donde corregirlas puede implicar grandes trastornos y gastos
- **Disponer de un ciclo de vida de desarrollo de software seguro** (S-SDLC) comprometido con la creación y el mantenimiento de aplicaciones seguras
- **Cumplir las normas de organismos gubernamentales, del sector o internas de la empresa** relativas a la seguridad de las aplicaciones, como PCI DSS o HIPAA

Ámbito y opciones del servicio

Las aplicaciones evaluadas pueden incluir sitios web oficiales y aplicaciones empresariales estándar o basadas en la nube, incluidas aplicaciones incrustadas y móviles.

Los servicios se adaptan a sus necesidades y a las características de sus aplicaciones, y pueden incluir:

- **Pruebas de caja negra**: emulación de un atacante externo
- **Pruebas de caja gris**: emulación de usuarios legítimos con una amplia gama de perfiles
- **Pruebas de caja blanca**: análisis con acceso completo a la aplicación, incluido el código fuente; este método es el más eficaz en cuanto a número de vulnerabilidades detectadas
- **Evaluación de la eficacia de firewall de aplicaciones**: las aplicaciones prueban con y sin la protección de firewall activada, para detectar vulnerabilidades y comprobar si se bloquean los posibles exploits

Acerca del enfoque de Kaspersky Lab en cuanto a la evaluación de seguridad de aplicaciones

Las evaluaciones de seguridad de aplicaciones las realizan expertos en seguridad de Kaspersky Lab tanto manualmente como por medio de la aplicación de herramientas automáticas, con plena atención a la confidencialidad, integridad y disponibilidad de sus sistemas y con un respeto escrupuloso a las normas y prácticas recomendadas internacionales, como:

- Clasificación de amenazas de Web Application Security Consortium (WASC)
- Guía de pruebas de Open Web Application Security Project (OWASP)
- Guía de pruebas de seguridad móvil de OWASP
- Otras normas, según el negocio y la ubicación de su empresa

Resultados

Las vulnerabilidades que pueden identificarse mediante el servicio de evaluación de seguridad de aplicaciones de Kaspersky Lab incluyen:

- Deficiencias de autenticación y autorización, incluida la autenticación de varios factores
- Inserción de código (inserción de SQL, comandos del sistema operativo, etc.)
- Vulnerabilidades lógicas que conducen al fraude
- Vulnerabilidades del cliente (scripting entre sitios, falsificación de solicitudes entre sitios, etc.)
- Uso de criptografía poco segura
- Vulnerabilidades en las comunicaciones cliente-servidor
- Almacenamiento o transferencia de datos inseguros, por ejemplo, falta de enmascaramiento de PAN en sistemas de pago
- Errores de configuración, incluidos los que conducen a ataques de sesión
- Revelación de información confidencial
- Otras vulnerabilidades de aplicaciones web que conducen a las amenazas enumeradas en la clasificación de amenazas de WASC v2.0 y las diez amenazas principales (Top Ten) de OWASP.

Los resultados se distribuyen en un informe final que incluye información técnica detallada sobre los procesos de evaluación, los resultados, las vulnerabilidades detectadas y recomendaciones para su corrección, así como un resumen esquemático en el que se incluyen las consecuencias para el equipo directivo. Si es necesario, también podemos proporcionar vídeos y presentaciones para su equipo técnico o directivo.

Los miembros del equipo de proyecto son profesionales experimentados, con profundos conocimientos prácticos actuales sobre el tema, incluidas diferentes plataformas, lenguajes de programación, marcos, vulnerabilidades y métodos de ataque. Son ponentes en las principales conferencias internacionales y ofrecen asesoría sobre seguridad a los principales proveedores de aplicaciones y servicios en la nube, como Oracle, Google, Apple, Facebook y PayPal.

Opciones de entrega

Según el tipo de servicio de evaluación de seguridad, las características concretas de los sistemas incluidos y sus requisitos sobre condiciones de trabajo, los servicios de evaluación de seguridad pueden prestarse de manera remota o in situ. La mayoría de estos servicios se pueden realizar de manera remota.

Evaluación de seguridad de CAJEROS AUTOMÁTICOS Y PUNTOS DE VENTA

Los cajeros automáticos y dispositivos de puntos de venta ya no son vulnerables solo a ataques físicos como robos de cajeros o fraude de tarjeta. Conforme las medidas de protección aplicadas por los bancos y los proveedores de cajeros automáticos y puntos de venta evolucionan, también los ataques contra estos dispositivos cambian, siendo cada día más sofisticados. Los piratas informáticos explotan las vulnerabilidades de la infraestructura y aplicaciones de cajeros automáticos y puntos de venta, y están creando un malware específicamente adaptado a cajeros automáticos y puntos de venta. Los servicios de evaluación de seguridad de cajeros automáticos y puntos de venta de Kaspersky Lab ayudan a detectar las deficiencias de seguridad en sus cajeros automáticos y puntos de venta y a mitigar el riesgo de verse comprometidos.

La evaluación de seguridad de cajeros automáticos y puntos de venta es un análisis completo de su cajeros automáticos o dispositivos de punto de venta, diseñado para identificar vulnerabilidades que pueden ser utilizados por atacantes para actividades como la retirada de efectivo no autorizada, la realización de transacciones no autorizadas, la obtención de datos de tarjetas de pago de sus clientes o el inicio de la denegación de servicio. Este servicio descubre cualquier vulnerabilidad de su infraestructura de cajero automático y punto de venta que pueden aprovechar diferentes formas de ataque, resume las posibles consecuencias de la explotación, evalúa la eficacia de sus medidas de seguridad actuales y le ayuda a planificar otras acciones para solucionar las deficiencias detectadas y mejorar su seguridad.

Ventajas de los servicios

La evaluación de seguridad de cajeros automáticos y puntos de venta de Kaspersky Lab ayuda a los proveedores y las organizaciones financieras a:

- **Comprender las vulnerabilidades** de sus cajeros automáticos y dispositivos de punto de venta, y mejorar sus procesos de seguridad correspondientes
- **Evitar pérdidas financieras, operativas y de reputación** que se pueden producir por un ataque, mediante la detección y la solución proactivas de las vulnerabilidades que los atacantes pueden explotar.
- **Cumplir las normas de organismos gubernamentales, del sector o internas de la empresa**, que estipulan la realización de evaluaciones de seguridad, por ejemplo, PCI DSS (norma relativa a la seguridad de los datos del sector de las tarjetas de pago).

Ámbito del servicio

El servicio incluye un análisis completo de cajeros automáticos y puntos de venta, incluidas demostraciones de fuzzing y ataques en un entorno de prueba. Esto se puede proporcionar en un único cajero automático o dispositivo de punto de venta o en una red de dispositivos. Le recomendamos elegir para la evaluación el tipo de cajero automático o dispositivo de punto de venta de uso más común en su organización, o aquellos que sean más importantes (que, por ejemplo, ya hayan sufrido incidentes) en sus configuraciones típicas.

Resultados de la evaluación de seguridad de CAJEROS AUTOMÁTICOS Y PUNTOS DE VENTA

El servicio de evaluación de seguridad de cajeros automáticos y puntos de venta puede identificar una gama de vulnerabilidades, incluidas:

- Vulnerabilidades en la arquitectura de la red y la protección de red insuficiente.
- Vulnerabilidades que permiten a un atacante escapar del modo quiosco y obtener acceso no autorizado al sistema operativo.
- Vulnerabilidades en software de seguridad de terceros, lo que permite a los posibles atacantes superar los controles de seguridad.
- Protección insuficiente de dispositivos de entrada y de salida (lector de tarjetas, unidad dispensadora, etc.) incluidas las vulnerabilidades en comunicaciones del dispositivo, lo que puede permitir la interceptación y modificación de datos transferidos.
- Vulnerabilidades causadas por errores en el código de la aplicación o resultantes del uso de versiones de hardware y software obsoletas (desbordamientos de búfer, inyecciones de código, etc.).
- Revelación de información.

Una vez concluida la evaluación, recibirá un informe que contiene la información técnica detallada sobre el proceso de prueba, los resultados, las vulnerabilidades y las recomendaciones, así como un sencillo resumen ejecutivo que describe nuestras conclusiones según los resultados de la prueba y que ilustra los distintos vectores de ataque. Asimismo, también podemos proporcionar vídeos de demostraciones de ataques y presentaciones para su equipo técnico o directivo.

Enfoque de Kaspersky Lab en cuanto a la evaluación de seguridad de cajeros automáticos y puntos de venta

Durante el análisis, nuestros expertos no solo buscarán e identificarán deficiencias de configuración y vulnerabilidades en las versiones de software obsoletas, sino que analizarán profundamente la lógica detrás de los procesos realizados por los cajeros automáticos o dispositivos de punto de venta, llevando una investigación de seguridad destinada a identificar cualquier nueva vulnerabilidad (0 días) en nivel de componente. Si descubrimos vulnerabilidades que podría aprovechar un atacante (cuyo resultado sea, por ejemplo, la retirada de efectivo no autorizada), nuestros expertos le pueden ofrecer demostraciones de posibles escenarios de ataque utilizando herramientas o dispositivos de automatización especialmente diseñados.

Aunque una evaluación de seguridad de cajeros automáticos y puntos de venta implica emular el comportamiento del ataque de un hacker original para evaluar de forma práctica la eficacia de sus defensas, es totalmente segura y no invasiva. El servicio lo realizan expertos en seguridad de Kaspersky Lab experimentados que prestarán especial atención a la confidencialidad, integridad y disponibilidad de sus sistemas, en estricto cumplimiento de las normas y prácticas recomendadas internacionales. Si descubrimos una nueva vulnerabilidad en el cajero automático o punto de venta de un cliente, nos comprometemos a seguir una política de divulgación responsable, notificar al proveedor y proporcionar ayuda de asesoramiento para preparar una solución.

Kaspersky Lab ofrece evaluaciones de seguridad de cajeros automáticos y puntos de venta de acuerdo con las siguientes normas y prácticas recomendadas internacionales:

- Normas del sector de las tarjetas de pago
  - Norma de seguridad de datos
  - Norma de seguridad de datos de aplicaciones de pago
  - Seguridad de transacciones con PIN
- Open Source Security Testing Methodology Manual (OSSTMM)
- Information Systems Security Assessment Framework (ISSAF)
- Common Vulnerability Scoring System (CVSS)
- Las demás normas aplicables a modelos de negocio y ubicaciones geográficas concretos, según sea necesario.

Los miembros del equipo del proyecto son profesionales muy experimentados en seguridad práctica, que tienen un gran conocimiento sobre el terreno y mejoran constantemente sus habilidades; con regularidad ofrecen consultoría de seguridad a los proveedores de cajeros automáticos y puntos de venta y presentan los resultados de nuestras investigaciones de seguridad de cajeros automáticos y puntos de venta en importantes conferencias de seguridad de la información (como Black Hat).

Evaluación de seguridad de redes de telecomunicaciones

Descripción general de los servicios

La infraestructura de IT de una empresa de telecomunicaciones consta de una serie de redes interconectadas en función de varias funciones y tecnologías. Estas normalmente incluyen una red corporativa, que incluye los elementos de gestión, una red de radio principal (GSM/UMTS/LTE), que proporciona acceso a Internet de banda ancha a los suscriptores, canales de línea externa de alta velocidad específicos y servicios de alojamiento y en la nube. Cada pieza de esta infraestructura es esencial para la empresa y debe estar bien protegida contra ataques de hackers si se debe minimizar el riesgo financiero, operativo y de reputación. Los servicios de Kaspersky Lab para redes de telecomunicaciones le permiten reducir estos riesgos mediante el reconocimiento de las vulnerabilidades en sus sistemas y eliminándolos o solucionando sus efectos mediante la introducción de controles.

Kaspersky Lab ofrece los siguientes servicios de evaluación de seguridad para redes de telecomunicaciones:

- Pen Testing en la infraestructura de IT
- Evaluación de seguridad de la configuración de la infraestructura de IT
- Evaluación de seguridad de redes GSM/UMTS/LTE
- Evaluación de seguridad de aplicaciones (para aplicaciones que proporcionan varios servicios: IP-TV, portales de autoservicio de clientes, etc.)

- Evaluación de seguridad de VoIP
- Evaluación de seguridad de equipos de telecomunicaciones

Resultado de los servicios

Como resultado de cada valoración de seguridad, recibirá visibilidad técnica y de alto nivel de deficiencias de seguridad de sus redes de telecomunicaciones, así como conclusiones acerca de la eficacia de sus controles de seguridad. Estos resultados se pueden utilizar para mejorar la seguridad de la red y mitigar los riesgos financieros, operativos y de reputación asociados a las amenazas de seguridad de la información.

El informe contendrá la siguiente información:

- Conclusiones de alto nivel sobre los niveles de seguridad actuales de sus redes de telecomunicaciones
- Descripciones de la metodología y los procesos del servicio
- Descripciones detalladas de las vulnerabilidades detectadas, incluidos el nivel de gravedad, la complejidad de la explotación, el posible impacto en el sistema vulnerable e indicios de la existencia de la vulnerabilidad (si es posible)
- Recomendaciones sobre la eliminación de vulnerabilidades, incluidos los cambios en la configuración, actualizaciones, cambio de códigos fuente o implementación de controles compensatorios donde la eliminación de la vulnerabilidad es imposible

Kaspersky Lab
Enterprise Cybersecurity: **www.kaspersky.com/enterprise**
Noticias de ciberamenazas: **https://securelist.lat/**
Noticias de seguridad de IT: **business.kaspersky.com/**

#truecybersecurity
#HuMachine

www.kaspersky.es