KASPERSKY lab

KASPERSKY SECURITY INTELLIGENCE SERVICES

2015

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 datos importantes, 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 inteligencia 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 empresa no utiliza productos de Kaspersky Lab, puede beneficiarse de los servicios de inteligencia de seguridad de Kaspersky Lab.

LA SEGURIDAD QUE DESTACA

La inteligencia de seguridad líder en el mundo está incorporada en nuestro ADN: nos ayuda a ofrecer las tecnologías antimalware más potentes del mercado e influye en todo lo que hacemos.

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 expertos 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 empresas de seguridad y fuerzas del orden más respetadas del mundo, incluidos la Interpol, Europol, CERT, City of London Police, etc., han buscado activamente nuestra asistencia.

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 Meraki, Blue Coat, Juniper Networks, Alcatel Lucent y muchos otros, utilizan nuestras tecnologías en sus propios productos y servicios.

FORMACIÓN SOBRE CIBERSEGURIDAD

Estos innovadores programas de formación le permiten aprovechar los conocimientos, la experiencia y la inteligencia en ciberseguridad de Kaspersky Lab.

La formación y la concienciación sobre la ciberseguridad son ahora aspectos fundamentales para las empresas, que deben enfrentarse a un número cada vez mayor de amenazas que no dejan de evolucionar. El personal de seguridad debe conocer las técnicas avanzadas de seguridad que constituyen un componente fundamental de las estrategias de mitigación y gestión eficaces de amenazas empresariales. Al mismo tiempo, todos los empleados deben tener conocimientos básicos acerca de los peligros existentes y sobre los métodos de trabajo seguro.

Los cursos de formación sobre ciberseguridad de Kaspersky Lab han sido desarrollados específicamente para las empresas que quieran mejorar la protección de las infraestructuras y la propiedad intelectual. Todos los cursos se ofrecen en inglés.

CURSOS

SENSIBILIZACIÓN NO IT	FORMACIÓN SOBRE SEGURIDAD DE IT	
Empleados	Nivel 1 - Principiante	
PLATAFORMA DE FORMACIÓN ONLINE	FUNDAMENTOS BÁSICOS DE SEGURIDAD Conocimientos básicos sobre IT	FUNDAMENTOS PRÁCTICOS DE LA SEGURIDAD CON LABORATORIOS Conocimientos básicos sobre IT
Superiores inmediatos	Nivel 2 - Intermedio	
CYBERSAFETY GAMES	CIENCIA FORENSE DIGITAL Se requieren conocimientos de administrador del sistema	ANÁLISIS DE MALWARE E INGENIERÍA INVERSA Se requieren conocimientos de programación
Directores de la empresa	Nivel 3 - Avanzado	
EVALUACIÓN DE LA CULTURA DE LA CIBERSEGURIDAD	CIENCIA FORENSE DIGITAL AVANZADA Se requieren conocimientos avanzados de administrador del sistema	ANÁLISIS AVANZADO DE MALWARE E INGENIERÍA INVERSA Se requieren conocimientos de ensamblador

CONCIENCIACIÓN SOBRE LA CIBERSEGURIDAD

Módulos de formación interactiva online y programa de formación CyberSafety Games in situ para todos los empleados que utilizan ordenadores o dispositivos móviles en el trabajo y para los que se encargan de su gestión.

Aproximadamente el 80 % de los ciberincidentes se deben a errores humanos. Las empresas gastan millones en programas de concienciación sobre la ciberseguridad, pero muy pocos CISO están realmente satisfechos con los resultados. ¿Cuál es el problema?

La mayoría de cursos de concienciación sobre la ciberseguridad son demasiado largos, técnicos y, en esencia, negativos. Este enfoque no apuesta por los principales puntos fuertes del ser humano, es decir, sus principios para tomar decisiones y sus capacidades de aprendizaje, y como resultado puede hacer que la formación resulte ineficaz.

Por lo tanto, las empresas buscan enfoques más complejos que tengan en cuenta el comportamiento (como el desarrollo de una cultura corporativa) y que ofrezcan un retorno de la inversión realizada en la concienciación sobre la seguridad que resulte cuantificable y que merezca la pena.

Los cursos de concienciación sobre la ciberseguridad de Kaspersky Lab funcionan de la siguiente manera:

- Cambian el comportamiento al estimular el compromiso de la persona con el trabajo seguro, creando así un entorno corporativo en el que "como a todo el mundo le importa la ciberseguridad, a mí también".
- Combinan un enfoque basado en la motivación, técnicas de aprendizaje mediante ludificación, ataques simulados y formación en habilidades de ciberseguridad interactivas exhaustivas.

FUNCIONAMIENTO

Exhaustiva, pero sencilla	La formación abarca una amplia gama de problemas de seguridad, desde cómo se producen las fugas de datos hasta los ataques de malware en Internet y el uso seguro de las redes sociales, mediante una serie de ejercicios sencillos. Utilizamos técnicas de aprendizaje, como dinámicas de grupo, módulos interactivos, dibujos animados y ludificación, para que el proceso de aprendizaje sea atractivo.
Motivación permanente	Creamos momentos de formación mediante la ludificación y la competitividad, y luego reforzamos esos momentos a lo largo del año a través de ejercicios de ataques simulados, evaluaciones y campañas de formación.
Modificación de las creencias	Enseñamos a las personas que son los seres humanos, y no las máquinas, los principales objetivos de los cibercriminales. Mostramos cómo, si se trabaja teniendo en cuenta la seguridad, las personas pueden evitar ser víctimas y arriesgarse y exponer a su lugar de trabajo a los ataques.
Diseño de una cultura de ciberseguridad corporativa	Formamos a los directivos para que sean defensores de la seguridad; una cultura donde la ciberseguridad es algo instintivo que se logra con el compromiso y el ejemplo de los directivos, y no puede simplemente ser impuesta por el departamento de IT.
Enfoque positivo y de colaboración	Demostramos cómo las prácticas de seguridad realizan una aportación positiva a la eficiencia de la empresa y promovemos una colaboración más eficaz con otros departamentos internos, incluido el equipo de seguridad de IT.
Evaluable	Proporcionamos herramientas para evaluar los conocimientos de los empleados, junto con evaluaciones a nivel corporativo para analizar las actitudes del personal de seguridad respecto a la ciberseguridad en su trabajo diario.

FORMACIÓN SOBRE SEGURIDAD PARA EL PERSONAL DE IT

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, en su caso.

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.

¿PRINCIPIANTE, INTERMEDIO O EXPERTO?

El programa lo cubre todo, desde los principios básicos de la seguridad a la ciencia forense digital avanzada y el análisis de malware, lo que permite a las empresas mejorar sus conocimientos sobre ciberseguridad en tres dominios principales:

- Conocimientos básicos sobre el tema
- Ciencia forense digital y respuesta a incidentes
- Análisis de malware e ingeniería inversa

VENTAJAS DE LOS SERVICIOS

NIVEL 1 – Fundamentos básicos de seguridad
Dotar a los administradores de IT y seguridad de conocimientos básicos sobre los últimos avances en medidas de seguridad de IT prácticas de un líder del sector.

NIVEL 1 – Fundamentos prácticos de seguridad
Conocimientos en profundidad sobre la seguridad a través de ejercicios prácticos con herramientas modernas relacionadas con la seguridad.

NIVELES 2-3 – Ciencia forense digital
Mejorar la experiencia del equipo interno de ciencia forense digital y de respuesta a incidentes.

NIVELES 2-3 – Análisis de malware e ingeniería inversa
Mejorar la experiencia del equipo interno de análisis de malware e ingeniería inversa.

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
NIVEL 1 – FUNDAMENTOS BÁSICOS DE SEGURIDAD		
• Descripción general del mercado de las ciberamenazas y la comunidad criminal • Spam y phishing, seguridad para el correo electrónico • Tecnologías de protección contra el fraude • Exploits, amenazas persistentes avanzadas y móviles • Conceptos básicos de investigación mediante el uso de herramientas web públicas • Protección del lugar de trabajo	2 días	• Identificar los incidentes de seguridad y tomar decisiones para resolverlos • Reducir la carga de los departamentos de seguridad de la información • Aumentar el nivel de seguridad de cada lugar de trabajo con herramientas adicionales • Realizar investigaciones sencillas • Analizar correos electrónicos phishing • Reconocer los sitios web falsos o infectados

TEMAS	Duración	Habilidades adquiridas
NIVEL 1 – FUNDAMENTOS PRÁCTICOS DE SEGURIDAD		
• Fundamentos de seguridad • Inteligencia de fuente abierta • Seguridad para redes de empresa • Seguridad de las aplicaciones y prevención de exploits • Ataques DDoS y amenazas bancarias • Seguridad para la LAN inalámbrica y la red móvil global • Amenazas bancarias y móviles • Respuesta a incidentes de seguridad en entornos virtuales y en la nube	5 días	• Proporcionar investigaciones básicas, mediante recursos públicos, motores de búsqueda especializados y redes sociales • Crear un perímetro de red seguro • Conocimientos básicos sobre las pruebas de penetración • Inspeccionar el tráfico para detectar distintos tipos de ataques • Garantizar un desarrollo de software seguro • Identificar la inserción de código malicioso • Realizar análisis de malware básicos y análisis forenses digitales
NIVEL 2 – CIENCIA FORENSE DIGITAL GENERAL		
• 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
NIVEL 2 – ANÁLISIS GENERAL 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
NIVEL 3 – 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
NIVEL 3 – ANÁLISIS AVANZADO DE MALWARE E INGENIERÍA INVERSA		
• Objetivos y técnicas del análisis de malware e ingeniería inversa • Técnicas avanzadas de análisis estáticos y dinámicos • (descompresión manual) • Técnicas de desofuscación • Análisis de rootkit y bootkit • Análisis de exploits (.pdf, .doc, .swf, etc.) • Análisis de malware de sistemas que no sean Windows (Android, Linux, Mac OS)	5 días	• Utilizar las prácticas recomendadas globales en ingeniería inversa • Reconocer las técnicas contrarias a la ingeniería inversa (ofuscación, antidepuración) • Aplicar análisis de malware avanzado para rootkits/ bootkits • Analizar el shellcode del exploit, incrustado en diferentes tipos de archivo • Analizar malware de sistemas que no sean Windows

THREAT INTELLIGENCE SERVICES

El seguimiento, el análisis, la interpretación y la mitigación de las amenazas para la seguridad de la IT es una tarea colosal, puesto que no dejan de evolucionar. Empresas de todos los sectores 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.

Security 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
- Seguimiento de botnets
- Informes de inteligencia de APT

FUENTES DE DATOS DE AMENAZAS

Refuerce sus soluciones de defensa de la red, incluidos SIEM, firewalls, IPS/IDS, protección contra APT y tecnologías de simulación y sandbox, con datos completos que se actualizan continuamente y ofrecen información sobre las ciberamenazas y los ataques dirigidos.

Las familias y variantes de malware han crecido de manera exponencial en los últimos años; Kaspersky Lab detecta actualmente alrededor de 325 000 muestras de malware nuevas cada día. Para defender sus endpoints contra estas amenazas, la mayoría de las empresas implementan medidas de protección clásicas, como soluciones antimalware, prevención de intrusiones o sistemas de detección de amenazas. En un entorno tan cambiante donde la ciberseguridad siempre trata de mantenerse un paso por delante del cibercrimen, estas soluciones clásicas deben reforzarse mediante el acceso a la inteligencia más reciente contra amenazas.

Las fuentes de datos de amenazas de Kaspersky Lab están diseñadas para integrarse en los sistemas de información relacionada con la seguridad y gestión de eventos (SIEM) existentes, ofreciendo así un nivel adicional de protección. Por ejemplo, la integración de las fuentes de datos de amenazas permite correlacionar los registros que recibe el SIEM de diferentes dispositivos de red con las fuentes de datos de URL que proceden de Kaspersky Lab. Se incluye una conexión con HP ArcSight SIEM. También hay conectores para Splunk y QRadar disponibles.

CASOS DE USO/VENTAJAS DEL SERVICIO

Las fuentes de datos de amenazas de Kaspersky Lab:

- Potencian su solución SIEM con el aprovechamiento de datos sobre URL dañinas. El sistema SIEM recibe una notificación sobre las URL de malware, de phishing y de mando y control (C&C) de botnet a partir de los registros que recibe el SIEM de diferentes dispositivos de red (PC de los usuarios, proxies de red, firewalls, otros servidores).
- Potencian sus soluciones principales de defensa de la red, como firewalls, IPS/IDS, soluciones SIEM, protección contra APT, tecnologías de simulación y sandbox, dispositivos UTM, etc. con inteligencia de amenazas continuamente actualizada.
- Mejoran su capacidad para realizar análisis forenses proporcionando a los equipos de seguridad información significativa acerca de las amenazas y sobre los planteamientos tras los ataques dirigidos.
- Apoyan sus investigaciones. La información acerca de URL dañinas y hashes MD5 de archivos maliciosos realiza una valiosa aportación a los proyectos de investigación sobre amenazas.

Kaspersky Lab ofrece tres tipos de fuentes de datos de amenazas:

1. URL y máscaras maliciosas
2. Hash MD5 de base de datos de objetos maliciosos
3. Fuentes de datos de amenazas móviles

DESCRIPCIÓN DE LAS FUENTES DE DATOS

URL maliciosas: conjunto de URL que abarcan enlaces y sitios web maliciosos. Hay registros enmascarados y no enmascarados disponibles.

URL de phishing: conjunto de URL identificadas por Kaspersky Lab como sitios de phishing. Hay registros enmascarados y no enmascarados disponibles.

URL de mando y control de la botnet: conjunto de URL de servidores de mando y control (C&C) de botnet y objetos maliciosos relacionados.

Hash de malware (ITW): conjunto de hash de archivos y sus correspondientes veredictos, que abarcan la mayoría de malware peligroso y prevalente, distribuidos a través de la inteligencia de KSN.

Hash de malware (UDS): conjunto de hash de archivos detectados por las tecnologías con asistencia en la nube de Kaspersky (UDS, sistema de detección urgente, del inglés "Urgent Detection System") basado en los metadatos y las estadísticas de un archivo (sin tener el objeto en sí). Permite la identificación de objetos maliciosos nuevos y emergentes (de día cero) que no se detectan mediante otros métodos.

Hash de malware móvil: conjunto de hash de archivos para detectar objetos maliciosos que infectan plataformas móviles.

Fuente de datos de troyanos P-SMS: conjunto de hash de troyanos con el contexto correspondiente para detectar troyanos de SMS que conllevan llamadas con cargos premium para los usuarios de móviles y que permiten a un atacante robar, eliminar y responder a mensajes de SMS.

URL de mando y control de botnet móviles: conjunto de URL con contexto que abarca los servidores de mando y control de botnet móviles.

SEGUIMIENTO DE BOTNETS

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

Muchos ciberataques se realizan con botnets. Aunque este tipo de ataques pueden ir dirigidos a los usuarios normales de Internet, suelen estar destinados a los clientes de empresas específicas y sus clientes online.

La solución experta de Kaspersky Lab controla la actividad de los botnets y proporciona notificaciones rápidas (en el plazo de 20 minutos) sobre las amenazas relacionadas con los usuarios de sistemas bancarios y de pago online individuales. Esta información puede utilizarse para advertir e informar a los clientes, los proveedores de servicios de seguridad y las fuerzas del orden locales sobre las amenazas actuales. Ya puede proteger la reputación de su organización y de sus clientes con el servicio de seguimiento de botnets Botnet Tracking Service de Kaspersky Lab.

CASOS DE USO/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

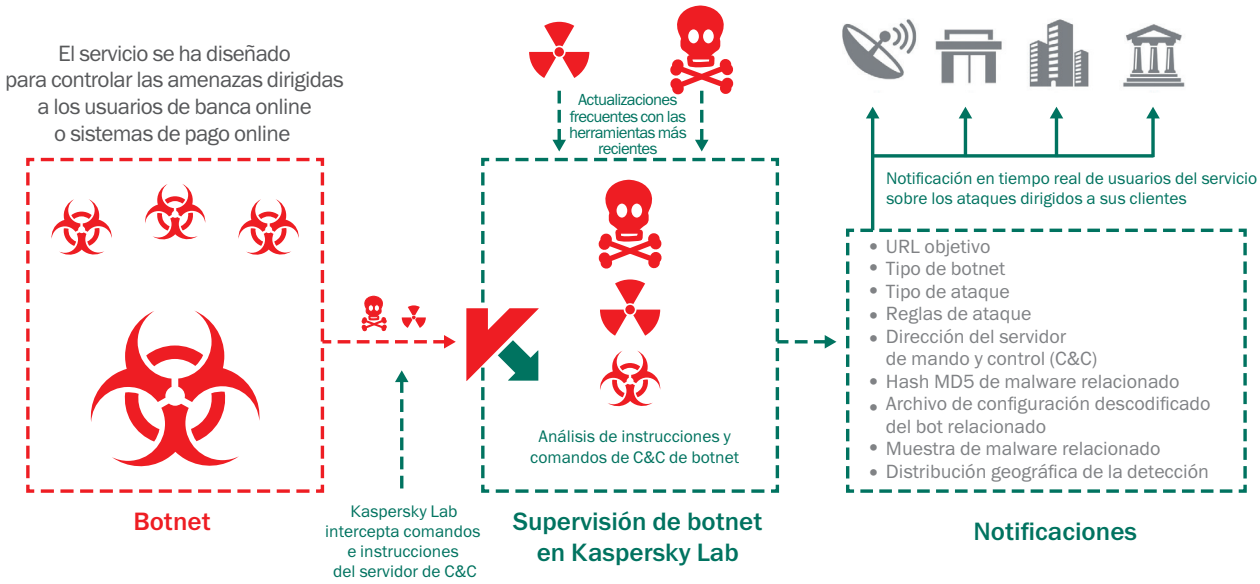
ACTÚE EN TIEMPO REAL:

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 y Citadel.
- **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.
- **Muestra de malware relacionada:** para el análisis inverso y de ciencia forense digital del ataque del botnet.
- **Distribución geográfica de la detección (10 países principales):** con datos estadísticos de las muestras de malware relacionadas de todo el mundo.

SEGUIMIENTO DE BOTNETS: ARQUITECTURA

DESDE EL SERVIDOR DE C&C



La solución de Kaspersky Lab está disponible en las versiones Standard o Premium, y ofrece una gran variedad de condiciones de servicio y URL supervisadas. Consulte a Kaspersky Lab o a su partner distribuidor para determinar qué paquete es el adecuado para su empresa.

NIVELES DE SUSCRIPCIÓN Y DISTRIBUCIÓN

Premium

Notificación por correo electrónico o formato JSON — **10 URL supervisadas**

- Archivo de configuración descodificado del bot relacionado
- Muestra de malware relacionada (a petición)
- Distribución geográfica de las detecciones de muestras de malware relacionadas

Notificación en formato de correo electrónico — **5 URL supervisadas**

- URL de destino (identificación de las URL desde las que los programas bot se destinan a los usuarios)
- Tipo de botnet (por ejemplo, Zeus, SpyEye, Citadel, Kins, etc.)
- Tipo de ataque
- Reglas de ataque, incluidas las siguientes: insertar datos web; captura de URL, pantalla, de vídeo, etc.
- Dirección de mando y control
- Hash MD5 de malware relacionado

Standard

INFORMES DE INTELIGENCIA

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 y las herramientas proporcionadas 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.

Informes de inteligencia de APT

No todas las amenazas persistentes avanzadas (APT) se notifican de inmediato y muchas ni siquiera se anuncian públicamente. Sea el primero en enterarse y conózcalas en exclusiva con nuestros informes de inteligencia procesables en profundidad sobre las APT.

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.

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 y ciberterroristas. 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.

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, muestras y herramientas 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.
- **Vigilancia continua de campañas de APT**. Acceso a inteligencia procesable durante la investigación (información sobre la distribución de APT, IOC e infraestructura C&C).
- **Análisis retrospectivo**. Se ofrece acceso a todos los informes privados publicados con anterioridad durante todo el periodo de su suscripción.

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

Informes de inteligencia de 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 de inteligencia de 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 (para informes específicos del cliente) y los formatos de datos preferidos, no se necesita ninguna infraestructura adicional para empezar a usar este servicio de Kaspersky Lab.

Los informes de inteligencia de amenazas de Kaspersky no afectan a la integridad y la disponibilidad de recursos, incluidos los recursos de red.

SERVICIOS EXPERTOS

Los servicios expertos de Kaspersky Lab son justo eso: 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.

Los servicios expertos incluyen:

- Investigación de incidentes
- Pruebas de penetración
- Evaluación de seguridad de las aplicaciones

INVESTIGACIÓN DE INCIDENTES

Ciencia forense digital | análisis de malware

La investigación de incidentes personalizada ayuda a su empresa a identificar y resolver incidentes de seguridad de IT.

Los ciberataques son un peligro cada vez mayor para las redes empresariales. Personalizados para explotar las vulnerabilidades exclusivas del objetivo seleccionado por los criminales, a menudo estos ataques están diseñados para robar o destruir información confidencial o de propiedad intelectual, socavar operaciones, dañar instalaciones industriales o robar dinero.

La protección de una empresa contra estos ataques sofisticados y bien planeados se ha vuelto cada vez más complicada. Incluso puede ser difícil establecer a ciencia cierta si su empresa está siendo atacada.

Los servicios de investigación de incidentes de Kaspersky Lab pueden ayudar a las empresas a formular sus estrategias de defensa mediante el análisis exhaustivo de las amenazas y el asesoramiento sobre las medidas apropiadas que se deben tomar para la resolución del incidente.

VENTAJAS DE LOS SERVICIOS

Los servicios de investigación de incidentes de Kaspersky Lab le ayudan a resolver problemas de seguridad reales y entender el comportamiento del malware y sus consecuencias, además de ofrecer orientación sobre las acciones correctivas. Este enfoque ayuda indirectamente a:

- Reducir los costes de la resolución de los problemas derivados de una ciberinfección
- Parar la filtración de información confidencial que potencialmente puede derivarse de los PC infectados
- Reducir el riesgo para la reputación causado por la infección que daña los procesos operativos
- Restaurar el funcionamiento normal de los PC dañados por la infección

Las investigaciones de Kaspersky Lab se llevan a cabo por analistas altamente experimentados con gran trayectoria práctica en ciencia forense digital y análisis de malware. Al término de la investigación, se le proporciona un informe detallado con los resultados completos de la ciberinvestigación y las propuestas de acciones correctivas.

CIENCIA FORENSE DIGITAL

La ciencia forense digital es un servicio de investigación destinado a producir una visión detallada de un incidente. La ciencia forense 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 explicación 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.

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 proporcionada por la empresa, 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.

OPCIONES DE DISTRIBUCIÓN

Los servicios de investigación de Kaspersky Lab están disponibles:

- mediante suscripción, en función de un número acordado de incidentes
- como respuesta a un único incidente

SERVICIOS DE PRUEBAS DE PENETRACIÓN

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

Mientras sus especialistas en seguridad e 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.

Las pruebas de penetración 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.

El servicio de pruebas de penetración de Kaspersky Lab le permite 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.

Las pruebas de penetración 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).

ÁMBITO Y OPCIONES DEL SERVICIO

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

- **Pruebas de penetración externa:** evaluación de seguridad realizada a través de Internet por un "atacante" sin conocimiento previo de su sistema.
- **Pruebas de penetración 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.

RESULTADOS DE LAS PRUEBAS DE PENETRACIÓN

El servicio de pruebas de penetración está diseñado para revelar las deficiencias de seguridad que podrían explotarse para obtener acceso no autorizado a los componentes de red críticos. 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.

ACERCA DEL ENFOQUE DE KASPERSKY LAB ANTE LAS PRUEBAS DE PENETRACIÓN

Aunque las pruebas de penetración 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 a 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 DISTRIBUCIÓN:

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.

SERVICIOS DE EVALUACIÓN DE SEGURIDAD DE 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.

Los servicios de evaluación de seguridad de aplicaciones de Kaspersky Lab detectan 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 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

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.

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 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

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 DISTRIBUCIÓN:

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.


Twitter.com/
kasperskyes


Facebook.com/
kasperskyes


Youtube.com/
Kasperskyespana

Kaspersky Lab España
www.kaspersky.es

Todo sobre la seguridad en Internet:
www.securelist.com

Encuentre un partner próximo:
http://www.kaspersky.es/partners/socios-kaspersky

Para obtener más información acerca de los productos y servicios descritos aquí, o para comunicarse con nosotros para saber si servicios pueden aplicarse a la seguridad de su empresa, póngase en contacto con nosotros a través de intelligence@kaspersky.com

Tenga en cuenta que los términos y condiciones aplicables pueden variar según la región, incluidos, entre otros: ámbito de trabajo, plazos, disponibilidad de servicios locales, idioma del servicio y costes.

Catálogo de servicios de inteligencia de seguridad, agosto de 2015, GL

KASPERSKY lab