SERVICIOS DE INTELIGENCIA: INVESTIGACIÓN DE INCIDENTES

ANÁLISIS DE MALWARE I CIENCIA FORENSE DIGITAL I RESPUESTA A INCIDENTES

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 determinar a ciencia cierta si su empresa está siendo atacada.

Los servicios de investigación 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 Kaspersky Lab ayudan a nuestros clientes 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 las empresas 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 los riesgos para la reputación** causada 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 a usted como cliente 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 utilizan diversas pruebas para entender exactamente lo que está sucediendo, incluidas las imágenes del disco duro, los volcados de memoria y los rastros de red. Todo esto ayuda a producir una explicación detallada del incidente.

El cliente lleva a cabo su propia evaluación del incidente y recopila pruebas, y presenta a Kaspersky Lab un esquema del incidente y las pruebas recopiladas de forma interna. A continuación, 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.

El cliente comienza la investigación por sí mismo: evalúa el incidente, recopila pruebas y realiza un análisis de ciencia forense digital. A continuación, proporciona a Kaspersky Lab el binario del malware. 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 organización frente a este tipo de amenaza.

RESPUESTA A INCIDENTES

La respuesta a incidentes es nuestro máximo nivel de servicio, que abarca todo el ciclo de investigación del incidente. Toda la experiencia en ciencia forense digital y análisis de malware se puede llevar a las instalaciones del cliente para ayudarle en la resolución de un incidente de seguridad.

Los expertos de Kaspersky Lab visitan el lugar de los hechos y llevan a cabo todos los aspectos de la investigación con el fin de proporcionar instrucciones específicas para la resolución del incidente, incluidas las acciones correctivas. El incidente se describe en un informe de investigación detallado.

OPCIONES DE ENTREGA

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

FLUJO DE INVESTIGACIÓN DE INCIDENTES

Kaspersky Lab ofrece tres niveles de investigación:

- Análisis de malware: le ayudará a comprender el comportamiento y los objetivos de los archivos de malware específicos que van dirigidos contra su empresa.
- Ciencia forense digital: proporciona una visión completa del incidente y el modo en que su empresa puede verse afectada.
- Respuesta a incidentes: una investigación del ciclo completo del incidente que incluye una visita in situ de los expertos de Kaspersky Lab.

No	Fases de investigación	Análisis de malware	Ciencia forense digital	Respuesta a incidentes
1	**Evaluación del incidente** • Respuesta rápida al incidente • Reducción al mínimo de las consecuencias • Análisis inicial del incidente, que se puede hacer in situ si es necesario, para establecer una comprensión plena del problema y determinar la manera de recopilar las pruebas necesarias			X
2	**Recopilación de pruebas** En función de la situación, recopilación de imágenes del disco duro, volcados de memoria y rastros de red, etc., relacionados con el incidente investigado			X
3	**Realización del análisis de ciencia forense** • Establecimiento de una imagen clara y detallada del incidente: – ¿Qué ha pasado? – ¿Quién era el objetivo? – ¿Cuándo ha sucedido? – ¿Dónde ha sucedido? – ¿Por qué ha sucedido? – ¿Cómo ha sucedido? • Análisis de las pruebas para encontrar el malware que provocó el incidente		X	X
4	**Realización del análisis de malware** Análisis del malware para entender cómo funciona, incluidos los siguientes factores: • Clasificación • Funciones • Vulnerabilidad y exploits relacionados • Medios de propagación • Actividad destructiva • Medios de instalación	X	X	X
5	**Creación de un plan de acciones correctivas** • Comprensión del objetivo del binario de malware • Desarrollo de métodos para detener su propagación • Desarrollo de planes de desinstalación	X	X	X
6	**Creación de un informe de la investigación** Al término de su análisis, los expertos de Kaspersky Lab proporcionan un informe detallado con los detalles de la investigación y las acciones correctivas	X	X	X

¿POR QUÉ KASPERSKY LAB?

- Fundada y dirigida por el experto en seguridad más prominente del mundo, Eugene Kaspersky
- Relaciones de colaboración con organismos encargados de hacer cumplir las leyes, como Interpol y CERTS
- Herramientas en la nube que supervisan millones de ciberamenazas en todo el mundo en tiempo real
- Equipos globales que analizan y comprenden todos los tipos de amenazas de Internet
- La mayor empresa de software de seguridad independiente del mundo centrada en la inteligencia sobre amenazas y el liderazgo en tecnología
- Líder indiscutible en más pruebas independientes de detección de malware que cualquier otro proveedor
- Identificado como líder por Gartner, Forrester e IDC

Para obtener más información sobre Kaspersky Intelligence Services, póngase en contacto con nosotros a través de intelligence@kaspersky.com.
PARA OBTENER MÁS INFORMACIÓN, VISITE www.kaspersky.es.

KASPERSKY lab