**NO DEJE QUE LE EXTORSIONEN.
COMIENCE A PROTEGER SU EMPRESA HOY MISMO.**

¿POR QUÉ PROTEGERSE CONTRA EL RANSOMWARE CON KASPERSKY LAB?

EL PROBLEMA

El 2016 fue el año de la revolución del ransomware a la vista de los problemas que causó en todo el mundo, y de la cantidad de datos, los dispositivos, las empresas y usuarios individuales a los que afectó. En 2016 el criptomalware también extendió sus tentáculos sobre las empresas y se convirtió en uno de los tres problemas de seguridad de IT más preocupantes para las pymes.

2016 EN CIFRAS

El 20 % DE LAS EMPRESAS DE TODO EL MUNDO sufrieron un incidente de seguridad de IT como resultado de un ataque de ransomware.*

El 42 % DE PEQUEÑAS Y MEDIANAS EMPRESAS han sido atacadas por ransomware en los últimos 12 meses.

UNA EMPRESA FUE ATACADA por ransomware cada **40 segundos**

EL COSTE MEDIO DE los daños causados por un ataque de criptomalware en una pyme asciende a **99 000 USD**

El 67 % APROXIMADO DE REPRESENTANTES DE PYMES admiten haber sufrido una pérdida total o parcial de datos empresariales debido a criptomalware.

1 de cada 5 PYMES QUE PAGARON EL RESCATE nunca recuperaron sus datos.

1.445.434 USUARIOS INDIVIDUALES DE PC fueron objeto de ataques de cryptors.

62 NUEVAS FAMILIAS DE RANSOMWARE hicieron aparición.

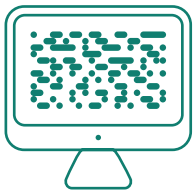
**Encuesta de riesgos de seguridad de IT empresarial de 2016*

LA SOLUCIÓN

En 2014, no mucho después de que los ataques de ransomware se convirtieran en una epidemia, los productos de Kaspersky Lab fueron mejorados con funcionalidad anticriptomalware. Desde entonces, nuestra gama de tecnologías antiransomware se ha expandido significativamente para responder a esta amenaza en constante evolución.

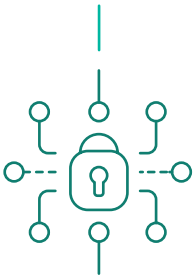
PROTECCIÓN A VARIOS NIVELES DE KASPERSKY LAB

Las soluciones de seguridad de Kaspersky Lab proporcionan protección a varios niveles contra criptomalware, tanto en términos de elementos de infraestructura como de tecnologías utilizadas para bloquear el ransomware.



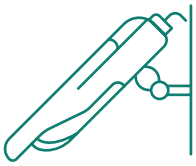
La identificación fiable de software malicioso y la protección contra amenazas conocidas, desconocidas y sofisticadas se ofrece a través de una combinación de tecnologías de detección precisas basadas en listas negras y aprendizaje mecánico proactivo, todo ello aprovechando las capacidades de procesamiento de grandes volúmenes de datos globales de Kaspersky Security Network (KSN).

Los controles de seguridad, incluida la supervisión de dispositivos, web e inicio de las aplicaciones, permiten a los usuarios restringir el uso de dispositivos no solicitados, sitios web o el lanzamiento de aplicaciones no autorizadas o en las que no se confía, lo que limita la posibilidad de ataque del software malicioso, incluidos los cryptors.



Puede configurarse la función de control de privilegios en las aplicaciones para limitar los derechos de acceso a determinados recursos de aplicaciones, incluidos los archivos de sistema y de usuario, e impedir que el ransomware pueda cifrarlos al no contar con derechos de "escritura".

La función de protección automática frente a vulnerabilidades vela constantemente para evitar que el software malicioso pueda aprovechar las vulnerabilidades del sistema operativo o de las aplicaciones que son objeto de ataque con mayor frecuencia.



System Watcher supervisa los procesos de las aplicaciones y compara su comportamiento con patrones de actividad peligrosos, lo que permite detectar y bloquear las acciones de las aplicaciones maliciosas. Cuando se detecta un intento de cifrado, System Watcher crea una copia temporal de los archivos a los que ha accedido, para permitir la reversión de las acciones maliciosas y la recuperación de la información.

La tecnología anticryptor para servidores de Kaspersky Lab entra en acción cuando se detecta un intento de cifrado procedente de una estación de trabajo infectada a través de una red local: cuando un cryptor intenta cifrar los archivos situados en recursos compartidos, como los servidores de la empresa, el componente anticryptor bloquea el acceso desde la estación de trabajo afectada hasta el recurso compartido, y detiene el proceso de cifrado.

Las funciones de evaluación de vulnerabilidades y gestión de parches incluidas en Kaspersky Endpoint Security for Business indicen en mejorar más si cabe la seguridad mediante la automatización del proceso de mitigación de vulnerabilidades de software, lo que minimiza la probabilidad de éxito de un ataque de cualquier tipo de software malicioso dirigido a penetrar la red de IT.

PROTECCIÓN DE EFICACIA DEMOSTRADA FRENTE AL RANSOMWARE

VALIDADA POR LAS IMPLEMENTACIONES DE LOS CLIENTES

COLLEZIONE, una de las principales marcas de moda de Turquía, utiliza Kaspersky Endpoint Security for Business Advanced.

"...Nos impresionó especialmente el hecho de que la protección contra el ransomware resultara satisfactoria en todas nuestras pruebas", recuerda el Gökhan Zengin, director de informático de Collezione.

JJW HOTELES, una premiada empresa hostelera y del sector del entretenimiento utiliza Kaspersky Endpoint Security for Business Select.

"Desde que instalamos Kaspersky Lab no hemos tenido problemas de ransomware ni otros ataques", señala Tiago Reis, director de infraestructura de IT del grupo de Internacional MBI.

Herramienta antiransomware de Kaspersky

Sitio web global de Kaspersky Lab

Blog B2B de Kaspersky Lab