KASPERSKY ENDPOINT SECURITY FOR BUSINESS: TECNOLOGÍA EN ACCIÓN

Para las amenazas que ve
y las que no ve

KASPERSKY lab

THE POWER
OF PROTECTION

kaspersky.com/business
#Securebiz

ÍNDICE

El 94 % de las empresas ha experimentado alguna forma de amenaza a la seguridad externa

Fuente: Informe de riesgos de IT globales de Kaspersky Lab de 2014

PROTEJA SU EMPRESA DE LAS AMENAZAS QUE VE Y LAS QUE NO VE

Contar con la seguridad de IT correcta nunca había sido tan importante.

LO QUE NO CONOCE *PUEDE* HACERLE DAÑO

Más del 30 % de las brechas en la seguridad se producen en las empresas con 100 empleados o menos.[1] El 44 % de las pequeñas y medianas empresas (pymes) han sido atacadas por cibercriminales.[2]

No obstante, muchas de ellas no son conscientes de las amenazas extremadamente reales que el cibercrimen y el malware sofisticado suponen para sus negocios. Mientras que casi una quinta parte de las empresas más pequeñas reconoce que no han tomado medidas para protegerse contra el cibercrimen, tan solo el 60 % mantiene activamente su software antimalware actualizado.[3]

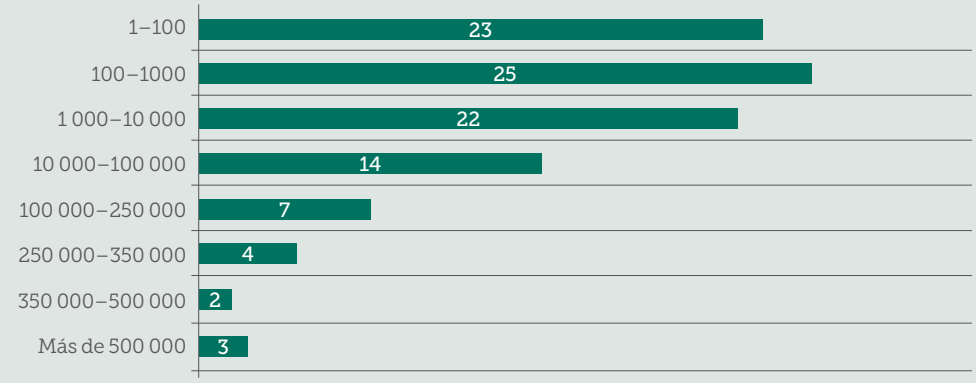
Pensar que su empresa es demasiado pequeña para resultar interesante para los cibercriminales es exactamente la mentalidad que ellos están explotando para atacar su empresa con malware cada vez más sofisticado. Saben que muchas pymes no lo son: usted es uno de sus objetivos.

[1] Data Breach Investigations Report (Informe de investigación de filtraciones de datos) de Verizon, 2013
[2] Encuesta de 2013 de National Small Business Association (Asociación nacional de la pequeña empresa)
[3] Kaspersky Lab, Threatpost, 24 de mayo de 2013

LO QUE NO VE

Supongamos que usted forma parte del 80 % de las pymes que cuentan con algún tipo de solución de seguridad de IT. No se dé por satisfecho: la mayoría de los usuarios empresariales subestiman en gran medida los volúmenes de amenazas.[4] Solo el 4 % de los encuestados apenas se acercaron a la cifra correcta al adivinar cuántas amenazas se detectan cada día.[4]

NÚMERO PERCIBIDO DE MUESTRAS DE MALWARE NUEVO DETECTADAS DIARIAMENTE (%)



Fuente: Informe de riesgos de IT globales de Kaspersky Lab de 2014

En este contexto, no es de extrañar que algunos usuarios consideren la seguridad de IT como un "commodity" y vean pocas diferencias entre las distintas opciones disponibles para ellos. Se trata de un mito peligroso: incluso un 1 % de diferencia en los índices de detección puede traducirse en cientos de miles de elementos de malware que se introducen a través de las redes en el transcurso de un año. ¿Cómo lo sabemos?

- Kaspersky Lab detecta 325 000 nuevos elementos de malware cada día.
- En el segundo trimestre de 2014, nuestras soluciones antimalware detectaron 528 799 591 ataques de virus en sistemas de usuarios finales e identificaron un total de 114 984 065 objetos maliciosos únicos durante el proceso.[5]

Las amenazas más peligrosas son las que no conocemos: las amenazas que los expertos de Kaspersky Lab supervisan, analizan y mitigan todos los días. Buscamos cuáles son los problemas. Y cuando los encontramos, utilizamos más de una década de inteligencia sobre amenazas y experiencia para proporcionar la protección adicional contra las amenazas que su empresa necesita evitar urgentemente, sobre todo cuando se trata de malware sofisticado y amenazas persistentes avanzadas (APT, del inglés "Advanced Persistent Threats").

Existe una creciente brecha entre lo que las empresas creen que es el panorama actual de amenazas y lo que en realidad es. Es lo que llamamos las "carencias de percepción". Demuestra que las empresas, independientemente de su tamaño, infravaloran tremendamente tanto la cantidad como la gravedad de las amenazas a las que enfrentan.

Costin Raiu, equipo de análisis e investigación global, Kaspersky Lab

[4] Informe de riesgos de IT globales de Kaspersky Lab de 2014
[5] Informe de Kaspersky Lab sobre la evolución de las amenazas del 2º trimestre de 2014

TECNOLOGÍA PROACTIVA, REACTIVA E INTELIGENTE

Kaspersky Lab tiene una larga trayectoria en la realización de algunos descubrimientos de las amenazas más destacadas, incluidas Carbanak (el ciberrobo de banca electrónica más grande del mundo), Dark Hotel, The Mask, Icefog y Octubre Rojo. Más de un tercio de nuestros empleados trabajan en investigación y desarrollo. Se centran exclusivamente en el desarrollo de tecnologías con el fin de combatir y anticiparse a las amenazas en constante evolución que nuestros equipos especializados de investigadores de inteligencia y análisis investigan cada día.

La comprensión de Kaspersky Lab sobre el funcionamiento interno de algunas de las amenazas más sofisticadas del mundo nos ha permitido desarrollar una plataforma en varios niveles de tecnologías de seguridad para luchar contra las amenazas conocidas, desconocidas y sofisticadas. Nuestras tecnologías detectan y mitigan las amenazas que ve y las que no ve.

¿Cómo lo hacemos? A continuación vamos a describir la forma en que las diversas tecnologías antimalware y de detección de amenazas de Kaspersky Lab funcionan simultáneamente desde el momento en que se carga un archivo. Se trata de una combinación única de tecnologías de inteligencia que ofrecen detección y prevención de amenazas completas en varios niveles en los endpoints y otros elementos de la infraestructura de IT.

DETECCIÓN DE AMENAZAS CONOCIDAS

Desde el momento en el que un archivo está a punto de descargarse, una página web está a punto de abrirse o una aplicación está a punto de iniciarse, los motores avanzados de Kaspersky Lab comprueban, detectan y protegen simultáneamente contra virus, troyanos, rootkits, gusanos, spyware, scripts, adware y otros objetos y amenazas maliciosas conocidas, desconocidas y sofisticadas en la web y el correo electrónico. En el caso de las amenazas conocidas, estos motores constan en su núcleo de las siguientes tecnologías:

NETWORK ATTACK BLOCKER

Analiza todo el tráfico de la red mediante el uso de firmas conocidas para detectar y bloquear ataques basados en la red, incluido el análisis de puertos, ataques de denegación de servicio (DoS, del inglés "denial-of-service"), saturaciones del búfer y otras actividades maliciosas remotas.

MARCADO EN LISTA NEGRA

Equipos especializados de analistas de malware mantienen las bases de datos de Kaspersky Lab actualizadas con las firmas y los datos de malware más recientes. Estas se utilizan para bloquear de forma automática todo el malware conocido.

FILTRADO DE URL

Analiza y controla el tráfico entrante/saliente de las URL y lo compara con la base de datos de sitios maliciosos y de phishing conocidos de Kaspersky Lab, y bloquea los ataques basados en la web, el malware polimórfico de servidores y los servidores de "mando y control" (C&C).

FIREWALL

Analiza todos los paquetes que entran y salen de la red, y les bloquea o permite su acceso en función de los riesgos de seguridad. Las conexiones no autorizadas se bloquean, por lo que se reduce la superficie de ataque y la posibilidad de infección. A los equipos infectados o vulnerados de cualquier otra forma se les limita su actividad en la red, reduciendo así su capacidad para propagar malware y limitando los daños causados por las infracciones de las políticas de seguridad.

Las tecnologías basadas en firmas de Kaspersky Lab se han creado a partir de años de experiencia y conocimientos acumulados. Todas las tecnologías anteriores destacan en el bloqueo de malware conocido (y gracias a Kaspersky Security Network, tal como se describe más adelante, muchas de las amenazas desconocidas permanecen siéndolo durante un corto periodo de tiempo). Pero, ¿qué hay de las esquivas amenazas desconocidas o sofisticadas que hemos mencionado anteriormente? También tenemos la solución para esto...

[6] La tecnología antispam de Kaspersky Lab consiguió el primer puesto en la prueba de spam de VB en noviembre de 2014, con una tasa de detección del 99,75 % y cero falsos positivos.

DETECCIÓN DE AMENAZAS DESCONOCIDAS

Una vez que todos los archivos se han sometido a las comprobaciones basadas en firmas para la posible detección de las amenazas conocidas, es hora de echar un vistazo a lo que sucede en el momento del inicio. Las tecnologías proactivas en varios niveles de Kaspersky Lab analizan y controlan los archivos cuando se ejecutan para buscar actividad sospechosa o maliciosa que sugiera la actividad de una amenaza desconocida.

ANÁLISIS EXHAUSTIVOS

Los análisis exhaustivos ofrecen protección proactiva contra las amenazas que no pueden detectarse con las bases de datos antivirus convencionales. Los análisis exhaustivos de Kaspersky Lab permiten la detección de nuevo malware o modificaciones desconocidas de malware conocido. El análisis estático analiza el código para detectar señales de comandos sospechosos asociados con malware, mientras que el análisis dinámico examina el código de equipo que el archivo podría tratar de ejecutar, respondiendo a las "llamadas" emuladas con "respuestas" posibles para determinar si el código es seguro o no.

ANTIPHISHING EXHAUSTIVO

En ataques de phishing extremadamente nuevos donde solo un pequeño número de usuarios se han visto afectados, la tecnología de Kaspersky Lab puede buscar pruebas adicionales de actividad sospechosa, como vocabulario, formularios de entrada o secuencias de símbolos ilegibles. Esto se suma al enfoque más tradicional de base de datos descrito anteriormente.

Las amenazas de phishing han sido el punto de partida para muchas de las amenazas recientes muy peligrosas y sofisticadas.

SISTEMA DE PREVENCIÓN DE INTRUSIONES BASADO EN HOST (HIPS, DEL INGLÉS "HOST INTRUSION PREVENTION SYSTEM")

HIPS de Kaspersky Lab añade un nivel adicional de protección, ya que detecta y gestiona la actividad y las aplicaciones sospechosas para prevenir la ejecución de las amenazas. HIPS ayuda a controlar la forma en que las aplicaciones se comportan mediante el establecimiento de niveles de confianza tras el análisis inicial. Estos niveles definen cuáles son los recursos que pueden usar, a qué tipo de datos pueden acceder o qué tipo de datos pueden modificar, etc. Restringe la ejecución de programas potencialmente peligrosos sin que el rendimiento de las aplicaciones autorizadas y seguras se vea afectado. Una aplicación que no es fiable no tendrá autorización para hacer nada, ni siquiera iniciarse.

CONTROL DE APLICACIONES Y MARCADO EN LISTA BLANCA

El control de aplicaciones bloquea o autoriza el uso de las aplicaciones especificadas por el administrador. El enfoque de Kaspersky Lab se basa en el marcado dinámico en lista blanca, es decir, listas continuamente actualizadas de las aplicaciones y categorías de software fiables que solo se pueden ejecutar en función de determinadas reglas y políticas especificadas. Kaspersky Lab cuenta con una base de datos y un laboratorio de marcado en lista blanca especializados de más de mil millones de archivos, que aumenta a un ritmo de un millón por día.

Los controles de aplicaciones y el marcado en lista blanca reducen los riesgos planteados por las amenazas que aún no conocemos; la mayor parte del malware se propaga como un archivo ejecutable que no se encontrará en ninguna lista blanca. Las empresas que adoptan este enfoque (y las tecnologías compatibles) pueden evitar así la ejecución de cualquier archivo malicioso sin necesidad de identificar o saber lo que esos archivos son en realidad.

KASPERSKY SECURITY NETWORK

Kaspersky Security Network es un eficaz laboratorio global de amenazas en la nube que detecta, analiza y gestiona las amenazas y las fuentes de ataques online conocidas, desconocidas y nuevas en cuestión de segundos, y distribuye dicha inteligencia directamente a los sistemas del cliente.

Mediante el uso en tiempo real de datos anónimos procedentes de 60 millones de sensores de endpoints a nivel mundial, cada archivo que pasa por los sistemas protegidos de Kaspersky Lab se somete a los análisis basados en la inteligencia sobre amenazas pertinentes. Estos mismos datos garantizan que se llevan a cabo las acciones más apropiadas. Al funcionar de forma conjunta con todos los demás componentes del motor de Kaspersky Lab, Kaspersky Security Network habilita la protección contra las amenazas desconocidas antes de que estén disponibles las firmas, porque las respuestas basadas en firmas tradicionales pueden tardar varias horas en producirse, en tanto que las respuestas de Kaspersky Security Network tardan unos 40 segundos.

DETECCIÓN DE AMENAZAS SOFISTICADAS

El archivo se ha descargado e iniciado; las tecnologías de Kaspersky Lab lo han analizado, han aplicado la inteligencia y lo han bloqueado o permitido en función de la información que disponen sobre las amenazas conocidas y desconocidas.

Pero, ¿qué sucede con las amenazas sofisticadas?

Las tecnologías de detección de amenazas sofisticadas de Kaspersky Lab están diseñadas para detectar y bloquear las amenazas sofisticadas mediante el uso de una serie de mecanismos de comportamiento sofisticados y proactivos que permiten supervisar los comportamientos del proceso, detectar patrones sospechosos, bloquear actividades maliciosas y revertir los cambios perjudiciales, incluidos los cryptors.

Vamos a echar un vistazo...

SUPERVISOR DEL SISTEMA

Supervisa y recopila datos de las aplicaciones y de otras actividades importantes del sistema mediante actividades de seguimiento y la detección de patrones de comportamiento. Esta información se proporciona a los demás componentes de protección de Kaspersky Lab que hemos descrito. Cualquier actividad que coincida con los patrones de amenazas se aborda de acuerdo con las políticas establecidas por el administrador, o bien se utiliza el valor predeterminado, que consiste en finalizar el proceso malicioso y ponerlo en cuarentena para su posterior análisis.

El controlador que intercepta operaciones de archivos para el componente antimalware de Kaspersky también recopila información sobre los cambios realizados en el registro, mientras que el firewall recopila información sobre la actividad de las aplicaciones. Toda esta información se introduce en Supervisor del sistema que, a su vez, dispone de su propio módulo que puede reaccionar ante los eventos complejos del sistema, como la instalación de controladores.

Las acciones maliciosas y los patrones de comportamiento destructivos que sugieren la presencia de malware se bloquean.

PREVENCIÓN AUTOMÁTICA CONTRA EXPLOITS (AEP, DEL INGLÉS AUTOMATIC EXPLOIT PREVENTION)

Esta tecnología está dirigida específicamente contra el malware que explota las vulnerabilidades en el software. Desarrollado a partir del análisis profundo de las funciones y los comportamientos de los exploits más comunes, la tecnología resultante es capaz de identificar patrones de comportamiento característicos de los exploits y bloquearlos para que no se completen.

AEP actúa como una red de seguridad, un nivel adicional de seguridad que complementa las demás tecnologías de Kaspersky Lab. Funciona de forma conjunta con Supervisor del sistema de Kaspersky Lab.

RESTAURACIÓN

Esta supervisión continua y detallada de los sistemas permite la ejecución de una funcionalidad de restauración del sistema excepcionalmente precisa, limitando el impacto de cualquier infección y devolviendo los sistemas a los parámetros seguros anteriores. Los mecanismos de restauración se pueden actualizar y funcionan con archivos ejecutables creados y modificados, modificaciones del MBR, y archivos y claves de registro importantes de Windows.

DENEGACIÓN PREDETERMINADA

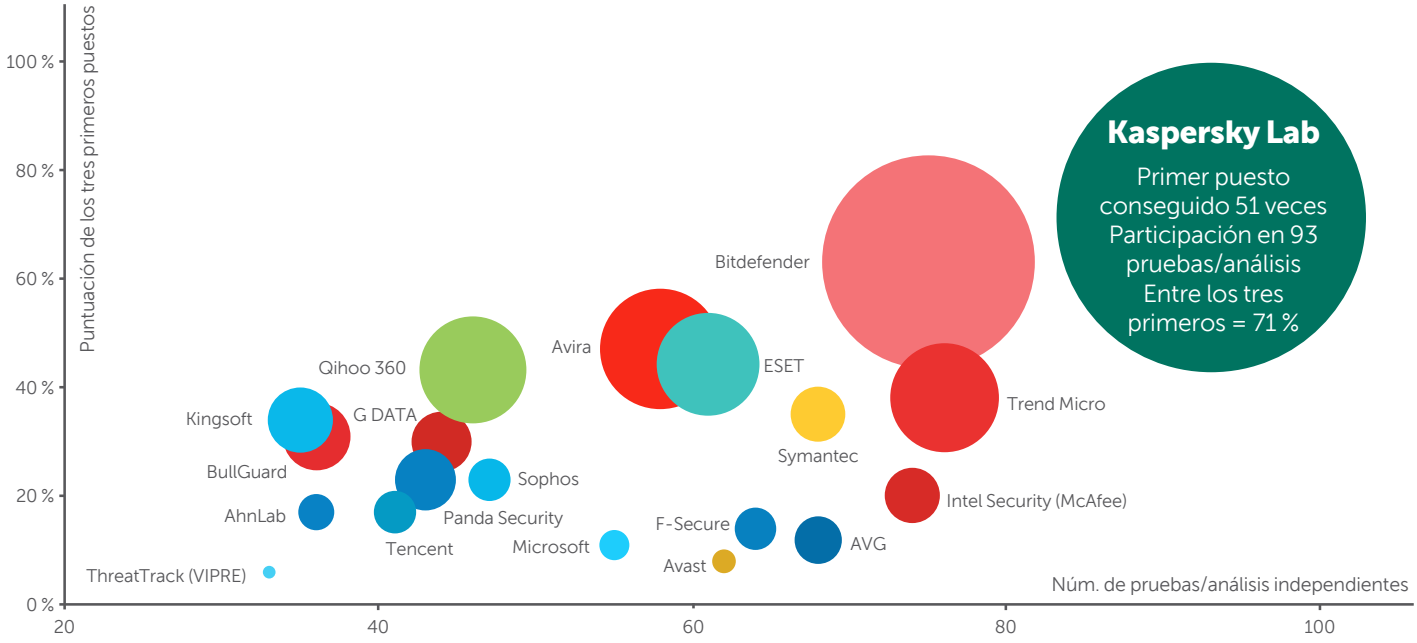
Se considera cada vez más como la medida de seguridad más eficaz que se puede adoptar contra las amenazas sofisticadas en constante evolución. Básicamente bloquea la ejecución de todas aplicaciones en cualquier estación de trabajo, a menos que su ejecución haya sido expresamente permitida por el administrador.

El modo de denegaciones predeterminadas implica que todas las nuevas variedades de malware basadas en archivos se bloquean automáticamente, incluso para los ataques dirigidos.

UN PEQUEÑO CAMBIO PUEDE MARCAR UNA GRAN DIFERENCIA

Como hemos visto, incluso un solo punto porcentual en los índices de detección puede traducirse en cientos de miles de elementos de malware que se introducen a través de las redes. También hemos visto cómo las "redes" adicionales de mitigación, detección y análisis de Kaspersky Lab pueden detectar amenazas desconocidas e incluso sofisticadas antes de que desplieguen sus actividades maliciosas.

KASPERSKY LAB: LA MEJOR PROTECCIÓN DEL SECTOR*



Los resultados de pruebas independientes demuestran consistentemente que Kaspersky Lab ofrece la mejor protección del sector. Tan solo en 2014, hemos participado en 93 pruebas y revisiones independientes, hemos conseguido el primer puesto 51 veces y hemos obtenido uno de los tres primeros puestos un 71 % de las veces. Esta es solo una de las razones por las que los OEM, incluidos Microsoft, Cisco Meraki, Juniper Networks y Alcatel Lucent, confían en Kaspersky Lab para proporcionar la seguridad que incluyen en sus propios productos.

Todas las tecnologías de seguridad de Kaspersky Lab se desarrollan y mantienen de forma interna, a partir de la misma base de código, lo que significa que todas ellas se integran perfectamente entre sí, permitiendo así la construcción de una plataforma en varios niveles que es más completa que la suma de sus partes. Este nivel de integración también se traduce en una mejora del rendimiento, actualizaciones más rápidas, y una apariencia y un comportamiento unificados en todas las soluciones, lo que le permite invertir su tiempo en centrarse en lo que mejor sabe hacer mientras que Kaspersky Lab se ocupa de la seguridad.

*Notas:
Según los resultados sintéticos de pruebas independientes realizadas en 2014 para productos dirigidos a empresas, consumidores y dispositivos móviles.

El resumen incluye pruebas realizadas por los siguientes laboratorios y revistas independientes:
AV-Comparatives, AV-Test, Dennis Technology Labs, MRG Effitas, NSS Labs, PC Security Labs, VirusBulletin.
El tamaño de la burbuja representa el número de primeros puestos obtenidos.

COMIENCE HOY MISMO: PRUEBA GRATUITA DE 30 DÍAS

Descubra cómo nuestra seguridad premium puede proteger su empresa contra el malware y el cibercrimen con una prueba sin compromiso.

Visite **kaspersky.com/trials** hoy mismo para descargar las versiones completas de los productos y evaluar la gran protección que ofrecen para su infraestructura de IT, endpoints y datos confidenciales de su empresa.

OBTENGA SU PRUEBA GRATUITA AHORA

ÚNASE A LA CONVERSACIÓN

#Securebiz

Véanos en YouTube

Síganos en Facebook

Síganos en Twitter

Únase a nosotros en LinkedIn

Véanos en Slideshare

Revise nuestro blog

Únase a nosotros en Threatpost

Véanos en Securelist

ACERCA DE KASPERSKY LAB

Kaspersky Lab es el mayor proveedor privado de soluciones de protección de endpoints del mundo. La empresa figura entre los cuatro proveedores principales de soluciones de seguridad para usuarios de endpoints.* A lo largo de sus más de 17 años de historia, Kaspersky Lab se ha mantenido como una empresa innovadora en seguridad de IT y suministra eficaces soluciones de seguridad digitales para grandes empresas, pymes y particulares. Kaspersky Lab, cuya sociedad de cartera está registrada en el Reino Unido, opera actualmente en casi 200 países y territorios de todo el mundo, y brinda protección a más de 400 millones de usuarios en todo el mundo. Más información en www.kaspersky.es.

* La empresa logró el cuarto puesto en el índice de IDC de ingresos de seguridad para endpoints en todo el mundo por proveedor de 2013. Este índice se publicó en el informe de IDC "Worldwide Endpoint Security 2014–2018 Forecast and 2013 Vendor Shares" (Previsión de seguridad mundial de endpoints 2014-2018 y acciones de los proveedores en 2013) (IDC núm. 250210, agosto de 2014). En el informe se clasifican los proveedores de software según los ingresos de ventas de soluciones de seguridad para endpoints en 2013.

kaspersky.com/business
#Securebiz