KASPERSKY ENDPOINT SECURITY FOR BUSINESS: TECNOLOGÍA EN ACCIÓN

Para las amenazas visibles e invisibles

KASPERSKY lab

THE POWER OF PROTECTION

Kaspersky.com/business
#Securebiz

CONTENIDO

El 94 % de las empresas han experimentado algún tipo de amenaza de seguridad externa

Fuente: Informe de riesgos de Kaspersky Lab Global IT del año 2014

PROTEJA SU EMPRESA DE LAS AMENAZAS VISIBLES... E INVISIBLES

Nunca antes ha sido tan importante contar con la seguridad de TI correcta.

LO QUE NO CONOCE *PUEDE* HACERLE DAÑO

Más del 30 % de las brechas de seguridad ocurren en empresas de 100 o menos empleados.[1] Un 44 % de las pequeñas y medianas empresas (pymes) padecen los ataques de los cibercriminales.[2]

Sin embargo, muchos no son conscientes de las amenazas reales que los delitos cibernéticos y malware avanzado representan para sus empresas. Mientras que casi una quinta parte de las pequeñas y medianas empresas reconocen que no han tomado medidas para protegerse contra los delitos informáticos, solo el 60 % mantiene activamente su software antimalware actualizado.[3]

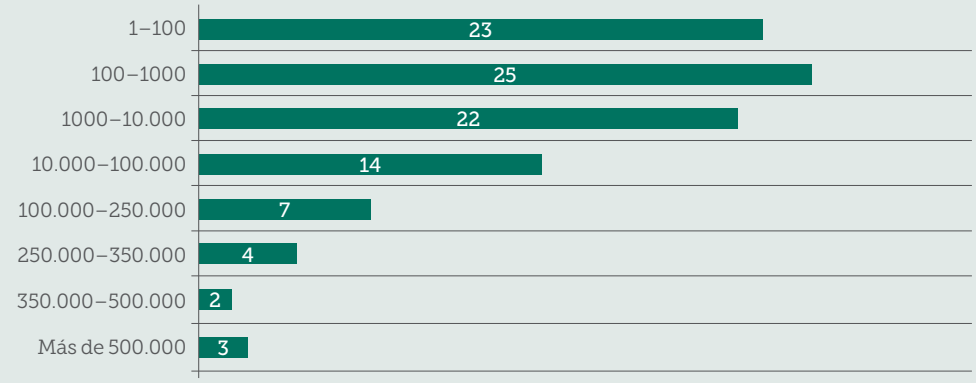
Pensar que su empresa es demasiado pequeña para ser de interés es exactamente la mentalidad que los cibercriminales aprovechan para ejecutar malware cada vez más sofisticado contra su empresa. Ellos saben que muchas pymes no lo hacen: usted es un objetivo.

[1] Informe de investigaciones sobre brechas de seguridad de Verizon correspondientes al año 2013
[2] Encuesta del año 2013 realizada por la National Small Business Association (Asociación nacional de pequeñas empresas)
[3] Kaspersky Lab, Threatpost, 24 de mayo de 2013

AMENAZAS INVISIBLES

Supongamos que usted es parte del 80 % de las pymes con algún tipo de solución de seguridad de TI en funcionamiento. No se conforme tan pronto: la mayoría de los usuarios de las empresas subestiman los volúmenes de amenaza.[4] Solo el cuatro por ciento de los encuestados pudo siquiera acercarse a la cantidad de amenazas que se detectan a diario.[4]

NÚMERO OBSERVADO DE NUEVAS MUESTRAS DE MALWARE DETECTADAS DIARIAMENTE (%)



Fuente: Informe de riesgos de Kaspersky Lab Global IT del año 2014

En este contexto, no es de extrañar que algunos usuarios consideren la seguridad de TI como un "commodity o básico", es decir, un producto en el cual no ven mucha diferencia entre las diferentes opciones disponibles. Este es un mito peligroso; incluso una diferencia del uno por ciento en las tasas de detección puede resultar en cientos de miles de elementos de malware introducidos ilegalmente a través de las redes en el transcurso de un año. ¿Cómo sabemos eso?

- Kaspersky Lab detecta 325.000 nuevos elementos de malware cada día.
- En el segundo trimestre de 2014, nuestra solución antimalware detectó 528.799.591 ataques de virus en sistemas de usuario final e identificó un total de 114.984.065 de objetos maliciosos únicos en el proceso.[5]

Las amenazas más peligrosas son las que desconocemos, esas son las amenazas que los expertos de Kaspersky Lab controlan, analizan y mitigan cada día. Buscamos problemas. Y cuando los encontramos, utilizamos más de una década de valiosa experiencia e inteligencia sobre amenazas para proporcionar la protección adicional contra las amenazas que más necesita evadir su organización, en especial cuando se trata de malware avanzado y amenazas persistentes avanzadas (APT).

Existe una creciente brecha entre la manera en que las empresas perciben el panorama de amenazas y la realidad en sí. Hemos llamado a esto la "brecha perceptiva". Esto demuestra que las organizaciones, independientemente de su tamaño, subestiman en un alto grado tanto la cantidad como la gravedad de las amenazas a las que se enfrentan.

Costin Raiu, Equipo de investigación y análisis mundial, Kaspersky Lab

[4] Informe de riesgos de Kaspersky Lab Global IT del año 2014
[5] Informe de evolución de amenazas de Kaspersky Lab Q2 del año 2014

PROACTIVAS, REACTIVAS, INTELIGENTES

Kaspersky Lab tiene una larga trayectoria en la realización de algunos de los descubrimientos de amenazas de más alto perfil y más relevantes, incluidos Carbanak (el ciberatraco bancario más grande del mundo), Dark Hotel, The Mask, Icefog y Red October. Más de un tercio de nuestros empleados trabajan en investigación y desarrollo. Ellos se centran exclusivamente en el desarrollo de tecnologías con el fin de contrarrestar y anticipar las amenazas en constante evolución que nuestros equipos de investigadores en 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 multicapas de tecnologías de seguridad para luchar contra amenazas conocidas, desconocidas y avanzadas. Nuestras tecnologías detectan y mitigan las amenazas visibles; así como las que no puede ver.

¿Cómo lo hacemos? Este es un recorrido a través de cómo las múltiples tecnologías de detección de amenazas y de antimalware de Kaspersky Lab trabajan simultáneamente, desde el momento en que se carga un archivo. Se trata de una combinación única de tecnologías de inteligencia dirigidas, que ofrecen detección integral multicapas en amenazas y prevención a través de endpoints y otros elementos de la infraestructura de TI.

DETECCIÓN DE AMENAZAS CONOCIDAS

Desde el momento en el que se inicia la descarga de un archivo, se abre una página web o se inicia una aplicación, los motores antimalware avanzados de Kaspersky Lab revisan, detectan y protegen simultáneamente contra virus, troyanos, rootkits, gusanos, spyware, scripts, publicidad, además de otros objetos y amenazas conocidas y desconocidas, incluyendo objetos y amenazas maliciosas basadas en la web y en correos electrónicos. Comencemos con las amenazas conocidas, en su núcleo, estos motores constan de:

BLOQUEADOR DE ATAQUES DE RED

Escanea todo el tráfico de la red, utilizando firmas conocidas para detectar y bloquear ataques basados en la red, incluidos escaneo de puertos, ataques por denegación de servicio (DoS), saturaciones del búfer y otras actividades maliciosas remotas.

LISTAS NEGRAS

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

FILTRACIÓN DE DIRECCIONES URL

Explora y comprueba las URL de tráfico entrante/saliente contra la base de datos de Kaspersky Lab en busca de sitios maliciosos conocidos y de phishing, y bloquea los ataques basados en la web, el malware polimórfico del lado del servidor y los servidores de "mando y control" (C&C).

FIREWALL

Analiza todos los paquetes que entran y salen de la red, los bloquea o los autoriza, 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. Las máquinas infectadas o comprometidas de alguna forma han limitado su actividad en la red, lo que ha disminuido su capacidad para propagar malware y se han limitado los daños causados por infracciones a la política de seguridad.

Las tecnologías basadas en firmas de Kaspersky Lab se crean con el respaldo de años de experiencia y conocimientos acumulados. Todas las excelentes tecnologías para bloquear malware conocidos (y gracias a Kaspersky Security Network, como se describe más adelante, muchas amenazas permanecen desconocidas solo durante un corto período). Pero, ¿qué sucede con las amenazas desconocidas o avanzadas que mencionamos anteriormente? También nos encargamos de eso...

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

DETECCIÓN DE AMENAZAS DESCONOCIDAS

Una vez que un archivo pasa por la detección basada en firmas para amenazas conocidas, es hora observar lo que sucede al momento de intentar la ejecución. Las tecnologías proactivas multicapas de Kaspersky Lab analizan y revisan archivos mientras los ejecutan, de esa forma buscan actividad sospechosa o maliciosa que sugiere que una amenaza desconocida está en acción.

LISTAS BLANCAS

El análisis de las listas blancas proporciona una protección proactiva contra amenazas no detectables mediante el uso de bases de datos de antivirus convencionales. La lista blanca de Kaspersky Lab activa la detección de nuevo malware o de modificaciones desconocidas a malware conocido. El análisis estático escanea el código en busca de señales de comandos sospechosos asociados al malware, mientras el análisis dinámico examina el código de la máquina que el archivo puede intentar ejecutar, en respuesta a "llamadas" imitadas con "respuestas" probables para determinar si el código es seguro o no.

LISTA BLANCA ANTIPHISING

En ataques de phising extremadamente nuevos, en los que solo un número reducido de usuarios se ha visto afectado, la tecnología de Kaspersky Lab puede buscar evidencia adicional de actividad sospechosa, como vocabulario, formas de escritura o secuencia ilegible de símbolos. Esto se suma al enfoque más tradicional y dirigido por bases de datos descrito anteriormente.

Las amenazas basadas en phishing son el punto de partida para muchas de las amenazas avanzadas más recientes y extremadamente peligrosas.

SISTEMA DE PREVENCIÓN DE INTRUSIONES BASADO EN HOST (HIPS)

HIPS de Kaspersky Lab agrega un nivel adicional de protección, que detecta y administra las solicitudes y las actividades sospechosas, para prevenir que se inicien las amenazas. HIPS ayuda a controlar la forma en que las aplicaciones se comportan, ya que establece niveles de confianza tras el análisis inicial. Estos niveles definen cuáles son los recursos que se pueden usar, a qué tipo de datos se puede acceder o cuáles se pueden modificar, etc. Restringe la ejecución de programas potencialmente peligrosos sin que afecte el rendimiento de las aplicaciones autorizadas y seguras. Una aplicación que no es confiable no tendrá permitido realizar nada, incluido el inicio.

CONTROL DE APLICACIONES Y LISTA BLANCA

El Control de aplicaciones bloquea o permite aplicaciones especificadas por el administrador. El enfoque de Kaspersky Lab se basa en listas blancas dinámicas; listas continuamente actualizadas de aplicaciones y categorías de software de confianza que solo se pueden ejecutar si se cumple con determinadas reglas y políticas. Kaspersky Lab cuenta con un laboratorio de listas blancas y una base de datos dedicados con más de mil millones de archivos, lo que significa un crecimiento de un millón por día.

El control de aplicaciones y las listas blancas reducen los riesgos planteados por las amenazas que aún no conocemos; la mayoría del malware se presenta como un archivo ejecutable fuera de toda lista blanca. Las organizaciones que adoptan este enfoque (y las tecnologías de apoyo) pueden evitar que se ejecute cualquier archivo malicioso, sin la necesidad de identificar ni saber qué son esos archivos en realidad.

KASPERSKY SECURITY NETWORK

En la práctica, un laboratorio global basado en la nube, Kaspersky Security Network detecta, analiza y administra amenazas conocidas, desconocidas y nuevas, así como los orígenes de ataques en línea en cuestión de segundos; y lleva esa inteligencia directamente a los sistemas de los clientes.

Con datos anónimos en tiempo real de 60 millones de sensores de endpoint a nivel mundial, cada archivo que pasa por los sistemas protegidos de Kaspersky Lab es analizado según la inteligencia de amenaza pertinente. Los mismos datos garantizan que se lleve a cabo el plan de acción más adecuado; en conjunto con los demás componentes del motor de Kaspersky Lab, Kaspersky Security Network habilita la protección contra amenazas desconocidas antes de que las firmas estén disponibles (las respuestas tradicionales basadas en firmas pueden tomar horas, pero a Kaspersky Security Network le lleva alrededor de 40 segundos).

DETECCIÓN DE AMENAZAS AVANZADAS

Su archivo se descargó e inició; las tecnologías de Kaspersky Lab escanearon, analizaron, aplicaron inteligencia y lo bloquearon o lo permitieron según las amenazas conocidas y desconocidas.

¿Pero qué ocurre con las amenazas avanzadas?

Las tecnologías de detección de amenazas avanzadas de Kaspersky Lab están diseñadas para detectar y bloquear las amenazas avanzadas con una variedad de mecanismos de conducta proactivos y sofisticados que controlan las conductas de procesamiento, localizan patrones sospechosos, bloquean actividades maliciosas y revierten los cambios dañinos, incluido Cryptors.

Demos un vistazo...

SYSTEM WATCHER

Monitorea y recopila los datos de la aplicación y de otras actividades importantes del sistema por medio de actividades de seguimiento de las actividades y el discernimiento de los patrones de comportamiento. Esta información se proporciona a los demás componentes de la protección Kaspersky Lab que hemos descrito. Cualquier actividad que responda a los patrones de amenaza se aborda según las políticas establecidas por el administrador, o bien, se utiliza la configuración predeterminada, lo que permite terminar el proceso malicioso y ponerlo en cuarentena para analizarlo más tarde.

El controlador que intercepta el funcionamiento del archivo para el componente antimalware de Kaspersky, además, reúne la información de los cambios realizados al registro, mientras el firewall recopila los datos sobre la actividad de las aplicaciones en la red. Toda esta información se entrega a System Watcher que, a su vez, cuenta con su propio módulo capaz de reaccionar a eventos complejos del sistema, como la instalación de controladores.

Se bloquean las acciones maliciosas y los patrones de comportamiento destructivo que indiquen un malware.

AUTOMATIC EXPLOIT PREVENTION (AEP)

Esta tecnología apunta específicamente a malware que ataca las vulnerabilidades del software. Ya que se desarrolló por medio de un análisis profundo de las funciones y comportamientos de los ataques más generalizados, la tecnología resultante es capaz de identificar los patrones de comportamiento característicos de los ataques y evitar que completen su proceso.

AEP actúa como una malla de seguridad, una capa adicional de seguridad que complementa las otras tecnologías de Kaspersky Lab. Funciona en conjunto con System Watcher de Kaspersky Lab.

REVERSIÓN

Este seguimiento continuo y detallado de los sistemas permite una funcionalidad de reversión increíblemente precisa, lo que limita el impacto de cualquier infección y devuelve los sistemas a sus parámetros seguros anteriores. Los mecanismos de reversión se pueden actualizar y funcionan con archivos creados y modificados que se pueden ejecutar, modificaciones MBR, importantes archivos de Windows y claves de registro.

DENEGACIÓN PREDETERMINADA

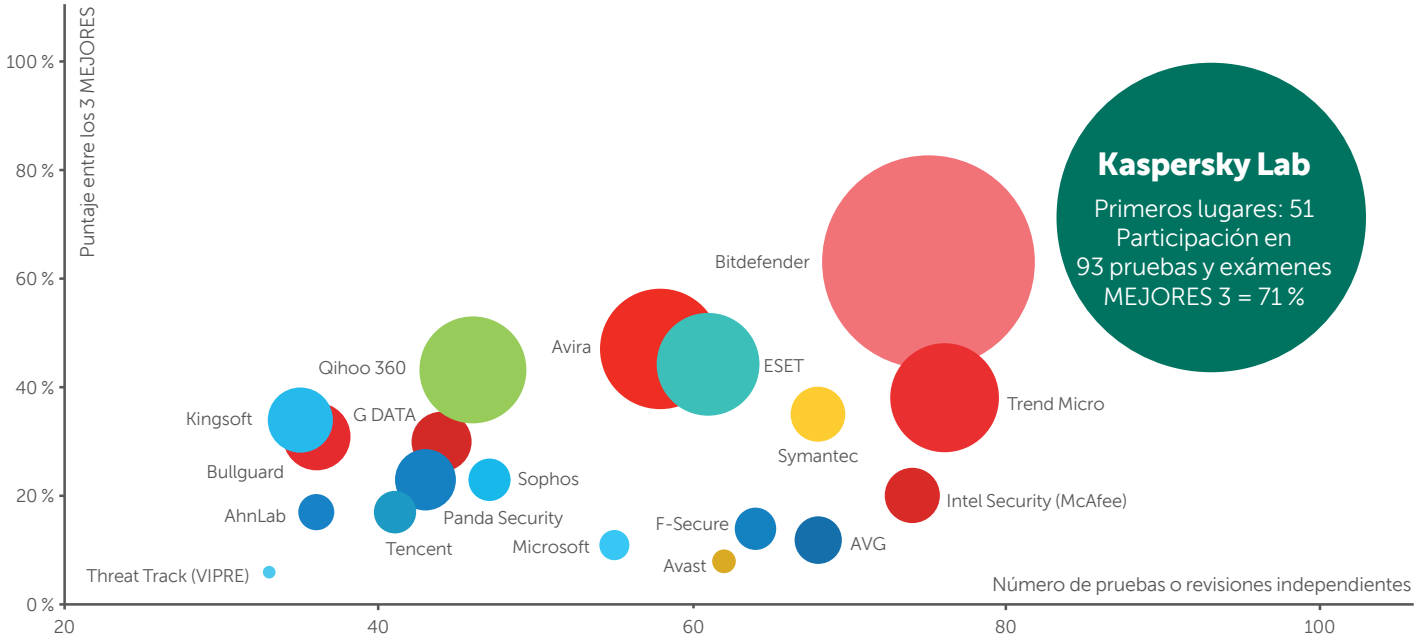
Considerada cada vez más como la posición de seguridad más eficaz para adoptar contra las amenazas avanzadas y en constante evolución. Simplemente bloquea la ejecución de todas las aplicaciones en cualquier estación de trabajo, a menos que el administrador las permita explícitamente.

Denegación predeterminada significa que todas las variedades de malware nuevo y basado en archivos se bloquean automáticamente, incluso los ataques dirigidos.

UN PEQUEÑO CAMBIO PUEDE HACER UNA GRAN DIFERENCIA

Como hemos visto, incluso un solo punto porcentual adicional en la tasa de detección puede traducirse en cientos de miles de elementos de malware introducidos ilegalmente a través de las redes. También hemos visto cómo las "redes" de mitigación, detección y análisis adicionales de Kaspersky Lab pueden atrapar amenazas desconocidas e incluso avanzadas antes de que hagan su trabajo.

KASPERSKY LAB: LA MEJOR PROTECCIÓN EN LA INDUSTRIA*



Resultados de pruebas independientes demuestran de forma consistente que Kaspersky Lab ofrece la mejor protección de la industria. Solo en el año 2014, participamos en 93 pruebas y exámenes independientes. Logramos 51 veces el primer lugar y quedamos entre los tres primeros, primeros lugares el 71% de las veces, todo un record. Esa es solo una de las razones por la que los OEM, incluidos Microsoft, Cisco Meraki, Juniper Networks y Alcatel Lucent, confían en que Kaspersky Lab les proporcione la seguridad que buscan para sus productos.

Todas las tecnologías de seguridad de Kaspersky Lab se desarrollan y mantienen internamente, desde la misma base de códigos, lo que quiere decir que todas se integran fácilmente entre sí, por lo que se logra una plataforma multicapas que es mejor que la suma de sus partes. Este nivel de integración también se traduce en un mejor rendimiento, actualizaciones más rápidas y una mirada y sensación unificadas en todas las soluciones, lo que le da tiempo para concentrarse en lo que mejor sabe hacer, mientras Kaspersky Lab se ocupa de la seguridad.

*Notas:
De acuerdo con el resumen de los resultados de pruebas independientes en 2014 en productos para empresas, consumidores y dispositivos móviles.

En el resumen se incluyen las pruebas realizadas por los siguientes laboratorios de pruebas independientes y revistas:
AV-Comparatives, AV-Test, Dennis Technology Labs, MRG Effitas, NSS Labs, PC Security Labs, VirusBulletin
El tamaño de la burbuja refleja la cantidad de veces que alcanzó el primer lugar.

EMPIECE AHORA MISMO: PRUEBA GRATUITA DE 30 DÍAS

Descubra cómo nuestra seguridad premium puede proteger a su empresa contra el malware y los delitos cibernéticos con una prueba sin compromiso.

Visite **kaspersky.com/trials** hoy para descargar las versiones de producto completo y evaluar qué tan satisfactoriamente estas protegen su infraestructura de TI, endpoints y datos confidenciales de la empresa.

OBTENGA SU PRUEBA GRATUITA HOY

ÚNASE A LA CONVERSACIÓN

#Securebiz

Véanos en YouTube

Denos un "Me gusta" 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 proveedor privado de soluciones de protección de endpoints más grande del mundo. La empresa se encuentra entre los mejores cuatro proveedores del mundo de soluciones de seguridad para usuarios de endpoints.* Durante sus más de 17 años de historia, Kaspersky Lab ha innovado en seguridad de TI y proporcionado las soluciones de seguridad digital más efectivas para empresas grandes, pequeñas y medianas, y para consumidores finales. Kaspersky Lab, con su empresa base registrada en el Reino Unido, opera actualmente en casi 200 países y territorios del mundo, y brinda protección a 400 millones de usuarios alrededor del globo. Conozca más en www.kaspersky.com.

* La empresa obtuvo el cuarto puesto en la clasificación de IDC de Ingresos en seguridad de endpoints en todo el mundo por proveedor en 2013. La clasificación se publicó en el informe de IDC "Worldwide Endpoint Security 2014-2018 Forecast and 2013 Vendor Shares" (IDC #250210, agosto de 2014) (Pronóstico mundial de seguridad de endpoints 2014-2018 y cuota por proveedor 2013, IDC #250210, agosto de 2014). En el informe se clasificó a los proveedores de software de acuerdo con los ingresos procedentes de la venta de soluciones de seguridad de endpoints durante 2013.

Kaspersky.com/business
#Securebiz