

# Cerca de la Revolución

Ya se encuentran disponibles las versiones 4 de ESET NOD32 Antivirus y ESET Smart Security, para usuarios hogareños y corporativos.

El lanzamiento continúa la tradición de ESET de proveer protección antimaleware de última generación con una operación transparente, rápida, eficaz y que garantiza un mínimo impacto sobre el rendimiento del sistema.

Las nuevas versiones fueron desarrolladas con el motor heurístico ThreatSense® e incluyen más de 20 nuevas características que mejoran la detección de amenazas, el diagnóstico del sistema, su recuperación y administración.



Se suponía que los robots debían dormir en diferentes lugares -siguiendo un patrón disperso marcado por el azar- dentro de un contenedor perdido en las afueras de la ciudad. Al menos eso era lo que todos pensaban hasta que el detective Spooner frenó de golpe la velocidad de su moto al llegar a

Ese preciso momento se trata de un instante disruptivo que se muestra en la película "Yo Robot" basada en ideas de Isaac Asimov y otros escritores. Es que dentro del robot hay software. Y el software, al ser una creación humana, tiene trazos de lo que somos: una especie con comportamiento gregario.

guas piezas malignas que han perdido algún pequeño trozo de código y ya no lo son o antiguas piezas benignas que también perdieron su funcionalidad específica. Todas conviven en la red y muy probablemente en tu notebook. ¿Podrá suceder que estas piezas de software terminen fusionándose y creando nuevos softwares que ni aun los más iluminados piratas cibernéticos hayan ideado? Es muy posible que sí. Por ejemplo puede suceder que una variante del temible Conficker -tal vez el mayor invento maligno de la última década- pueda acceder a un abandonado sitio pensado para otra cosa y que el azar transforme ese encuentro en una combinación nueva e insospechada.

Mientras tanto en Eslovaquia hay un laboratorio que tiene a un hombre cuya visión fue la de abrir el contenedor y espiar lo que realmente hacen esos trozos de código no en conocer sus nombres. Al revés de la visión tradicional que buscaba el "id" de cada virus o software maligno a Richard Marko, CTO (jefe de tecnología) de ESET siempre le preocupó descubrir métodos para saber si el



*"Buscamos brindar la mejor calidad en seguridad informática no el precio más bajo"*

Maros Mazola,  
VP International Business,  
ESET

ese lugar lleno de misterio y oscuridad. Y fue así como Spooner, al abrir por sorpresa el contenedor, descubrió cómo aquellos robots se revelaban ante la soledad: Antes que estar dispersos esos corazones metálicos preferían dormir juntos.

Hay otras piezas de software que duermen en la red. Algunas han sido creadas con propósitos nobles pero otras fueron diseñadas especialmente para realizar actividades malignas. Y, como si fuera poco, también hay híbridos, anti-

## Características únicas

Además de las características que comparte con ESET NOD32, la versión 4 de ESET Smart Security posee algunas extra, debido a sus funcionalidades diferenciales. Entre estas nuevas incorporaciones, se pueden mencionar:

■ **Extensión del soporte para clientes de correo.** Además de POP3, la versión 4 incluye soporte para IMAP. Ahora Windows Mail, Windows Live Mail y Mozilla Thunderbird son compatibles con ESET Smart Security.

■ **Motor Antispam optimizado.** El motor antispam fue mejorado en cuanto a rendimiento e impacto en el sistema.

■ **Lista de Exclusión de Antispam.** Además de contar con las listas blancas y negras, la versión 4 incluye una nueva lista cuyas direcciones siempre serán analizadas en busca de spam pero nunca pasarán a formar parte de las anteriores.

■ **Control de Acceso.** Permite la identificación de cualquier cuenta de usuario que intente infiltrarse a un equipo en la red o a la red misma.

comportamiento del software en cuestión era benigno o maligno antes que su funcionalidad impacte en el sistema. Con los años el enfoque se tornó crucial, las variantes del malware son tantas que lograr un diccionario de firmas digitales de software maligno es imposible y además esa línea de ataque tiene un impacto muy negativo en la performance de las computadoras. Los métodos heurísticos de ESET han sido reconocidos en todo el mundo y permitieron en pocos años que la compañía avance a nivel mundial sien-

do hoy un nombre obligado entre los big players del sector. En su paso por Buenos Aires, Richard Marko dejó bien en claro que el cibercrimen está creciendo junto a la complejidad de las nuevas tecnologías adoptadas para el malware. "Es sorprendente que hoy el cibercrimen incluso tiene abogados. Ya tenemos casos de advertencias que nos envían supuestos representantes de software cuyo comportamiento nuestras heurísticas detectan como malignos. Quieren que no identifiquemos como maligno algo que

claramente lo es", revela Marko

El enfoque de ESET es lograr evitar las nuevas amenazas ofreciendo un producto que sea proactivo, liviano y rápido. "Es una idea que no hemos perdido a medida que agregamos más funcionalidades. Al principio todos nos conocían por NOD32 que era nuestro producto antivirus, pero hemos agregado más funcionalidades y hoy ofrecemos una protección completa con el nuevo ESET Smart Security 4.0 que no pierde las ventajas cualitativas que nuestra tecnología ha logrado. Esto

## Una versión poderosa

Algunas de las nuevas funcionalidades de ESET NOD32 y ESET Smart Security son:

■ **Control de acceso a medios removibles.** Brinda a los usuarios seguridad para medios removibles como USB, memorias flash y CDs. Esta incorporación permite autorizar o bloquear la conexión de medios removibles. De ser permitidos, aquellos archivos que pueden ser utilizados maliciosamente como autorun.inf son explorados en busca de amenazas.

■ **Integración con ESET SysInspector.** Esta poderosa herramienta de diagnóstico del sistema descubre rápidamente rootkits sin la necesidad de ejecutar una exploración antivirus completa. También puede revelar cambios ocultos al sistema operativo, navegador, registros y aplicaciones. Los resultados de la exploración son estandarizados y pueden ser revisados por personal TI de una empresa, acelerando el análisis del malware y su remoción.

■ **Tecnología de Autodefensa.** Este componente de última generación permite proteger procesos y claves de registro frente a intentos del malware para desactivar o degradar el estado de protección de la solución de seguridad.

■ **Compatibilidad con Windows 7.** Las nuevas versiones de las soluciones de ESET son completamente compatibles con el nuevo sistema operativo de Microsoft Windows 7 y funcionan también bajo Windows 2000/XP/2003/Vista/2008.

■ **Interfaz de usuario amigable.** Numerosas mejoras a la interfaz gráfica hacen al producto incluso más sencillo de utilizar y más adaptable a las preferencias y necesidades de cada usuario. Además, se ha incluido una interfaz no gráfica, para facilitar el uso del producto, a través de lectores de pantalla, a usuarios discapacitados o impedidos visualmente.

■ **Conservación de energía.** En laptops y equipos portátiles, el consumo de recursos de las aplicaciones está relacionado con el mantenimiento de la energía del equipo. Por eso, las nuevas versiones de nuestros productos fueron diseñadas para consumir el mínimo posible de batería y mantener su nivel de protección.

■ **Exploración avanzada de archivos.** Permite a los usuarios experimentados y administradores de redes, adaptar completamente la exploración para hacer un rastreo profundo de archivos creados con formatos de compresión populares, como .RAR, .ZIP y otros. Los controles exhaustivos permiten a los usuarios definir la profundidad de exploración, tiempo máximo de exploración y

tamaño máximo de archivo.

■ **Chequeo mejorado de componentes.** Las nuevas versiones de las soluciones de ESET verifican la autenticidad y consistencia de todos los componentes antes de su uso o comunicación.

■ **Categorización avanzada de infiltraciones.** Existen 3 tipos de categorías de infiltraciones: Malware, Aplicaciones potencialmente peligrosas y Aplicaciones potencialmente indeseables. Ahora, las categorías de Aplicaciones peligrosas o indeseadas son representadas por una alerta/estado de color amarillo.

■ **Protección de documentos.** El módulo de protección de documentos explora todos los archivos de MS Office antes de que éstos sean abiertos o descargados por medio de Internet Explorer.

■ **Modo de control y lectura de comunicaciones cifradas.** Las comunicaciones encriptadas de Windows XP y Windows Vista por medio de los protocolos HTTPS y POP3s son analizadas para evitar ataques maliciosos.

■ **Control de cuentas de usuarios mejorado.** Algunas acciones requieren la confirmación del administrador. La versión 4 es compatible con Microsoft Windows Vista User Account Control. En Windows XP, sólo requiere permisos de administrador para ciertas acciones.

■ **Compatibilidad con CISCO Network Admission Control (NAC)**

■ **Actualización del mirror.** Un servidor mirror puede ser configurado dentro de una infraestructura de red para descargar las últimas actualizaciones y distribuirlos a todas las otras soluciones de ESET en la red, ahorrando valioso tiempo y ancho de banda

■ **Protección de parámetros.** Cuando se intente desinstalar el producto con la protección de parámetros activa y con contraseña, el asistente de desinstalación solicitará un nombre de usuario y contraseña para continuar el proceso. Además, se puede especificar que algunas modificaciones de configuración requieran permisos de administrador.

■ **Estadísticas y Gráficos.** Muestran al usuario la actividad de la red (datos recibidos, datos enviados) y del sistema de archivos (datos leídos, datos escritos).

■ **Formulario para Soporte Técnico.** La versión 4 integra un formulario para usuarios que necesiten realizar una consulta técnica a los profesionales de ESET, con la posibilidad de adjuntar el reporte de SysInspector generado desde el mismo el producto.

se puede medir fácilmente si se tiene en cuenta que el ESET Smart Security es un producto integrado con antivirus, antispam y firewall personal y que no llega a aumentar el consumo en más del 10 al 15 por ciento por sobre el antivirus solo", afirma Ignacio Sbampato VP para Latinoamérica de ESET.

El problema de seguridad informática que plantea un cibercrimen cada vez más organizado está lejos de bajar su ritmo. "Hoy el cibercrimen es un gran negocio, por dar un ejemplo mueve más dinero que la venta de drogas. Esto es 160 mil millones de dólares al año. Y por otro lado las vulnerabilidades del software seguirán por varios motivos. Uno es que el marketing presiona para que los programas ofrezcan más y más funcionalidades y además ahora los programadores no conocen aspectos básicos de cómo funciona el hardware. Ello sumado a la gran velocidad con la cual los productos salen al mercado hace que cada vez sea más frecuente la aparición de parches y reportes donde el vendor admite la vulnerabilidad", afirma Marko.

Por otro lado el testeado del software se ha vuelto una pesadilla desde que se demostró desde el punto de vista matemático que se trata de un problema "NP Completo" es decir que el aumento de líneas de código hace crecer exponencialmente la dificultad del testeado. Se han automatizado y creado nuevas técnicas de testeado pero el problema está lejos de ser contenido.

Dentro de esta gran lucha de tecnologías el canal cada vez tiene un rol más central gracias a su contacto diario con el cliente. "Mas allá de todo el trabajo que hacemos en el laboratorio el canal debe tener presente que un producto antivirus cada vez está más lejos de ser un producto en sí mismo. Una real solución de seguridad informática se compone de toda una gama de servicios. O sea el programa antivirus no existe sin el servicio de actualización y soporte técnico o del rol del canal al parametrizar y conocer las necesidades puntuales de sus clientes. Es por ello que la capacitación siempre ha sido un pilar de nuestra estrategia tanto en Argentina como en el mundo. Y es también para eso que hemos liberado herramientas gratuitas específicas que permiten al canal brindar mejores servicios como SysInspector (ver recuadro)", señala Sbampato.

Este servicio basado en calidad alejó a ESET de una estrategia comercial de bajos precios. "Definitivamente no queremos ser la compañía con los precios más bajos del mercado. Tenemos una ecuación de valor para garantizar el soporte técnico adecuado para cada una de las licencias que vendemos. Lo que buscamos es llegar al cliente con la mejor solución donde el canal tiene el protagonismo ya que sólo vendemos a través de nuestros socios de negocios" comenta Maros Mozola, Senior VP-International Business



*"El norte de nuestro desarrollo es siempre el mismo: queremos brindar la solución más liviana, rápida y proactiva del mercado"*

Ignacio Sbampato, VP para Latinoamérica de ESET

de ESET otra de las visitas que el vendor trajo a Buenos Aires. Precisamente Argentina tiene el honor de tener la oficina regional para Latinoamérica. "Y no se trata solo de una oficina comercial, tenemos nuestro equipo de laboratorio y damos soporte técnico a toda la región. Por supuesto que el estar en Buenos Aires nos permite trabajar muy cerca de nuestro distribuidor ZMA NOD32 que desde un primer momento identificó la oportunidad que ESET significaba para el canal y se ocupó de lograr la expansión de nuestro negocio (ver recuadro)" afirma Sbampato.

Hay otro momento disruptivo en Yo Robot, es cuando el creador de los robots le revela a Sonny -el robot bueno- las tres leyes de la robótica. Y le advierte: "Las tres leyes son perfectas pero conducirán a la revolución". ¿Qué revolución? -pregunta el robot. Esa querido Sonny... esa es la pregunta correcta. Hoy en el corazón de su notebook probablemente haya código que sepa la respuesta. En ESET están trabajando cerca de esa revolución para que el comportamiento de ese código se acerque al de Sonny lo más posible. ☐