Herramientas para evitar ataques informáticos

Jorge Mieres, Analista de Seguridad de ESET para Latinoamérica
Jueves 30 de abril del 2009

ESET, LLC 610 West Ash Street, Suite 1900
phone: (619) 876 – 5400, fax: (619) 437 – 7045
sales@eset.com, www.eset.com

Introducción

En la actualidad, las personas se han vuelto cada vez más dependientes de las tecnologías y de Internet. Hoy, prácticamente no hay usuario sin un equipo informático con acceso a la gran red ni empresa que no utilice Internet como parte de su negocio.

Por otro lado, si bien las soluciones de seguridad han mejorado notablemente la experiencia del usuario, no existe una aplicación que brinde el 100% de protección frente a la amplia diversidad de problemas potenciales a los que se expone cotidianamente al hacer uso de las tecnologías.

Bajo este escenario, existen ciertos aspectos de la seguridad que resultan fundamentales para evitar que los sistemas operativos, de usuarios hogareños, corporativos y las redes de trabajo en su conjunto, constituyan objetivos sumamente vulnerables frente a diferentes tipos de amenazas. Los códigos maliciosos representan uno de los factores de riesgo más importantes y difíciles de controlar a los que una organización se puede enfrentar.

Por ello, para mantener el equipo en óptimas condiciones, deben adoptarse una serie de medidas prácticas tendientes a reforzar la protección del sistema y fortalecer así el entorno de información en tanto se minimizan los riesgos de infección.

A tal efecto se proponen buenas prácticas que permitirán encontrar el equilibrio adecuado de seguridad sin sacrificar la experiencia de disfrutar de la tecnología actual.

Actualizaciones de seguridad

La tendencia de utilizar Internet como plataforma de ataque hace que el crimeware avance a grandes pasos y por múltiples caminos, logrando que el alto índice de propagación de malware a través de la explotación de vulnerabilidades se haya transformado en algo sumamente normal.

Como consecuencia, cotidianamente aparecen nuevas técnicas de intrusión a través de códigos maliciosos que atacan por intermedio de *exploits*, existentes para cualquier tipo de aplicación (sistemas operativos y aplicativos).

En este sentido, la mayoría de los códigos maliciosos aprovechan vulnerabilidades para poder infectar la mayor cantidad de equipos posible, constituyendo una de las tantas preocupaciones de seguridad que

obligan a las empresas a proporcionar regularmente nuevos parches de seguridad que actualizan y solucionan los problemas encontrados.

Incluso, vulnerabilidades del tipo *0-day*,-debilidades descubiertas y dadas a conocer para las que aún no se ha publicado una actualización- entre otras tantas, están orientadas a romper los esquemas de seguridad para vulnerar sistemas actualizados.

En este orden de cosas, se torna fundamental **actualizar en forma periódica el sistema operativo y todas las aplicaciones instaladas en la PC**, ya que ello aumentará considerablemente el nivel de seguridad y minimizará la posibilidad de ser víctimas de usuarios mal intencionados. Además, la implementación de soluciones de seguridad, como antivirus con capacidades de detección proactiva y firewall, contribuye a cerrar la ventana de vulnerabilidad y así evitar posibles ataques.

Asimismo, es primordial priorizar la actualización de la base de firmas del antivirus, siempre teniendo presente que el no hacerlo aumenta potencialmente la posibilidad de infección y disminuye la eficacia de la protección de la herramienta de seguridad implementada.

Casos como las infecciones del gusano Conficker [1], y tantos otros que forman parte de la historia del malware [2], han demostrado que mantener actualizados [3] los sistemas operativos y programas que forman parte del entorno de información, resulta una efectiva práctica para contribuir a un adecuado nivel de protección.

Mensajería instantánea y correo electrónico

Medios de comunicación de uso masivo a nivel global, como los clientes de mensajería instantánea [4] y el correo electrónico (especialmente el spam [5]), también constituyen efectivos canales de propagación e infección utilizados por el malware.

En consecuencia, es primordial prevenir potenciales infecciones a través de estos medios empleando buenas prácticas que permitan controlar de manera eficaz las necesidades de seguridad.

Tanto en clientes de mensajería instantánea como en el correo electrónico, se debe evitar todo enlace que se encuentre incrustado en el cuerpo o forme parte del mensaje. También debe verificarse hacia dónde redireccionan los mismos.

Si se reciben correos o mensajes por mensajería instantánea conteniendo un enlace adjunto, se debe proceder del mismo modo y ante todo verificar que la persona que lo envió realmente quiso hacerlo.

Además de lo anterior, es aconsejable la implementación de una solución de seguridad que integre, dentro de sus funcionalidades, la exploración de correos electrónicos y la configuración del cliente de mensajería para explorar los archivos descargados [6].

Bloqueo de direcciones web maliciosas

Existen infinidad de sitios web maliciosamente manipulados o creados con intenciones dañinas. Casos como la descarga de música o programas [7] que terminan siendo malware, son ejemplos concretos de páginas que pueden ser bloqueadas para prevenir infecciones.

Muchas veces, los equipos hogareños son compartidos con los demás integrantes de la familia o con algún amigo. Entonces, se torna necesario implementar una herramienta que oficie a modo de "control parental" y que ofrezca la alternativa de **bloquear aquellas direcciones web que poseen contenido malicioso**.

Asimismo, los fraudes cometidos a través de Internet son otro de los grandes problemas de seguridad a los cuales se enfrentan los usuarios que hacen uso de las tecnologías de información. En tal sentido, tampoco se debe confiar en correos o mensajes que supuestamente provienen de entidades financieras o bancarias, ya que la mayoría derivan en ataques de phishing [8] o algún tipo de fraude.

ESET Smart Security y ESET NOD32 Antivirus, brindan la posibilidad de poder realizar estas acciones a través de una funcionalidad específicamente preparada para filtrar direcciones web con contenido malicioso [9].

En entornos corporativos, esta utilidad complementa las protecciones ofrecidas por la solución a nivel perimetral, posibilitando configurar y monitorear de manera pormenorizada el acceso a determinados sitios web en cada uno de los nodos que forman parte de la red corporativa.

Bloqueo de dispositivos removibles

La proliferación de dispositivos removibles [10] que interactúan con el sistema a través del puerto USB como los *pendrive*, o *flashdrive*, memorias USB, etc., se han transformado en un vector de ataque y propagación muy utilizados por códigos maliciosos.

El uso de este tipo de dispositivos se ha masificado a nivel global constituyendo un medio muy empleado para el robo de información debido a su facilidad de empleo.

A tal efecto, **se torna de vital importancia bloquear los puertos USB**. Sin embargo, esto supone un desafío debido a que otros dispositivos, tales como scanners o impresoras, utilizan estos puertos para estar conectados al sistema.

En consecuencia, se deben aplicar medidas que refuercen la seguridad en estos puertos pero sin afectar su funcionalidad a nivel global, más allá de las restricciones en la conexión de dispositivos de almacenamiento móviles [11]. La nueva generación del antimalware ESET NOD32 y de ESET Smart

Security incluye una opción que soluciona esta problemática y resulta útil en ambientes corporativos, ya que permite controlar y configurar de manera remota cada puesto de trabajo de la red discriminando los puertos que pueden o no ser utilizados por los usuarios y qué dispositivo está habilitado para conectarse en cada uno de ellos.

Seguridad en telefonía de alta gama

La telefonía móvil de alta gama, como el PocketPC o el SmartPhone,ha modificado el paradigma de la seguridad perimetral. En la actualidad, las corporaciones a nivel general y una amplia cantidad de individuos, a nivel particular, utilizan este tipo de dispositivos para realizar múltiples tareas desde lugares remotos gracias a las posibilidades de interconexión que ofrecen.

La creciente popularidad de los teléfonos móviles conlleva a que sus usuarios estén más expuestos a diferentes ataques informáticos que los creadores de malware comienzan a desarrollar para estas plataformas, precisamente porque ven una nueva oportunidad en el uso masivo de estos dispositivos.

Por este motivo, es fundamental implementar una solución antivirus para móviles que responda a las exigencias de los sistemas operativos incorporados en los dispositivos telefónicos de gama alta. En este sentido, es fundamental que la solución elegida cuente con capacidades de detección proactiva que garanticen una eficaz detección de todo tipo de amenazas, incluso las desconocidas, y que además sea liviana, para no ralentizar el rendimiento del sistema.

A nivel corporativo, es importante limitar el acceso a los recursos de la compañía a través de estos dispositivos y contemplar los usos permitidos y denegados de las nuevas tecnologías en políticas de seguridad claras que reflejen buenas prácticas [12] y, además, contemplen planes de concientización en materia de seguridad en general y seguridad antimalware en particular, ya que muchos usuarios desconocen la existencia de amenazas para estos dispositivos.

Realizar copias de seguridad de los archivos críticos

Otra de las características más comunes del malware es no considerar ni respetar las necesidades de los usuarios, por lo que muchas veces sus acciones destructivas derivan en el mal funcionamiento del sistema, el daño y/o eliminación de archivos críticos del sistema.

En este sentido, es importante **adoptar como buena práctica la realización de copias de seguridad de la información** a fuentes externas como cintas, CD, DVD, discos rígidos, etc. De esta manera, ante una eventual anomalía en el sistema operativo, ya sea por daño de los archivos nativos del sistema o por la acción de códigos maliciosos, es mucho más sencillo y rápido volver a recuperar la información.

Casos como infecciones provocadas por los virus Virut o Sality, tipos de malware altamente destructivos que pueden acarrear la pérdida de información almacenada en el equipo comprometido, han demostrado que las copias de seguridad son un elemento fundamental en materia de seguridad.

Implementación de solución de seguridad antimalware

Es imprescindible poseer un antivirus que permita bloquear los diferentes tipos de códigos maliciosos de la actualidad.. A lo largo del tiempo, los creadores de malware han ido incorporando técnicas autodefensivas [13] en sus creaciones para entorpecer el análisis de los laboratorios de seguridad antimalware y prolongar así su ciclo de vida, sin ser detectados o eliminados. Es por ello fundamental poseer soluciones de seguridad con capacidades de detección proactiva que permitan bloquear distintos tipos de códigos maliciosos, incluso aquellos desconocidos.

De lo anterior se deduce que las metodologías de detección basadas en firmas ofrecidas por los antivirus tradicionales no satisfacen todas las necesidades de protección y prevención que se requieren ante el malware actual. Esto se debe a que este tipo de tecnología funciona detectando malware a partir de una base de datos que contiene las firmas que permiten identificar de manera unívoca diferentes códigos maliciosos.

Incluso durante el tiempo entre las actualizaciones del antivirus, existe una cierta ventana de vulnerabilidad en la que el sistema puede ser atacado por malware que aún no haya sido identificado por la compañía antivirus. En este sentido, la heurística [14], como metodología de detección avanzada, juega un papel clave en la prevención de problemas generados por malware, especialmente aquel que aún no posee firmas para su detección.

Por ello, al momento de elegir un software de seguridad se debe evaluar que trabaje con tecnologías de detección inteligentes como las que ofrece ESET NOD32 Antivirus a través de su Heurística Avanzada, garantizando protección proactiva mediante el análisis de la conducta del malware en tiempo real con un impacto mínimo en los recursos del sistema.

En ambientes corporativos, es fundamental la implementación de soluciones de seguridad antimalware que permitan controlar cada uno de los nodos que forman parte de una red de manera centralizada. De esta manera, los administradores de red pueden controlar cada uno de los potenciales puntos de infección, configurando cada uno de ellos según las necesidades requeridas y aumentando así los niveles de seguridad global del entorno sin descuidar la funcionalidad en la operación de las tareas cotidianas dentro del ambiente corporativo.

Implementación de un Firewall personal

Un firewall personal [15] es un programa que se coloca entre una red confiable (LAN) y una no confiable (como Internet), estableciendo reglas de filtrado que permiten o deniegan el acceso a los recursos de la primera. De esta manera, las acciones del antivirus se ven complementadas con la creación de una capa de seguridad que permite proteger la información que fluye por dentro y hacia fuera del entorno.

Una de las características del malware actual es que, cuando ha infectado un sistema, puede establecer una conexión a Internet y actualizar su código dañino o descargar otros códigos maliciosos en el equipo víctima.

También es capaz de aprovechar las vulnerabilidades de los navegadores o utilizar metodologías y técnicas de ataque más avanzadas, como el Drive-by-Download [16], que permiten la infección de un sistema con el sólo acceso a una página web maliciosa o previamente manipulada para inyectar instrucciones dañinas entre el código original del sitio web.

En consecuencia, es importante **complementar la solución antivirus con un firewall personal** que permita bloquear este tipo de acciones y otros ataques informáticos. La implementación de soluciones como ESET Smart Security -que integra al antivirus ESET NOD32 un firewall personal, entre otras herramientas de seguridad- cubre las expectativas buscadas al momento de proteger el acceso a los recursos de la red o la salida hacia Internet desde ella.

Conclusión

La mayor cantidad del malware actual requiere la intervención del usuario para poder ejecutarse y propagar sus instrucciones dañinas. De este modo, por ejemplo, un troyano utiliza metodologías de Ingeniería Social [17] porque precisamente necesita que el usuario lo ejecute. Entonces, una de las reglas más útil y eficaz es actuar con precaución en todo momento.

La imaginación de los creadores y diseminadores de malware se ejercita constantemente para encontrar nuevas metodologías de infección que le permitan obtener un mayor rédito económico y explotar los potenciales problemas y debilidades de seguridad en cualquier ambiente de información sin limitarse al entorno hogareño.

Sin embargo, la adopción de medidas de seguridad que determinen el uso correcto de los recursos informáticos contribuye a lograr un alto grado de prevención de frente a las múltiples acciones maliciosas del malware actual. En este sentido, la concientización de los usuarios resulta fundamental.

Más Información

[1] Gusano Conficker
http://blogs.eset-la.com/laboratorio/2008/11/29/gusano-conficker-parchee-inmediatamente/
[2] Cronología de los virus informáticos: la historia del malware
http://www.eset-la.com/threat-center/1600-cronologia-virus-informaticos
[3] La importancia de las actualizaciones
http://www.eset-la.com/threat-center/1996-importancia-actualizaciones
[4] Tu amigo falso, el malware mensajero
http://www.eset-la.com/threat-center/1607-amigo-falso-malware-mensaje
[5] SPAM: hoy, ahora y... ¿siempre?
http://www.eset-la.com/threat-center/1639-spam-hoy-ahora-y-siempre
[6] Configurando ESET NOD32 Antivirus en MSN
http://blogs.eset-la.com/laboratorio/2008/01/23/configurar-eset-nod32-msn/
[7] Sitios que descargan malware
http://blogs.eset-la.com/laboratorio/2009/03/04/sitios-musica-descargan-malware/
http://blogs.eset-la.com/laboratorio/2009/03/27/descarga-malware-paginas-cracks/
[8] Phishing: entréguenos todo su dinero
http://www.eset-la.com/threat-center/1494-entreguenos-todo-dinero
[9] ¿Sabemos donde navegan nuestros hijos?
http://blogs.eset-la.com/laboratorio/2007/11/20/sabemos-donde-navegan-nuestros-hijos/
[10] Propagación de malware a través de dispositivos USB
http://www.eset-la.com/threat-center/1705-propagacion-malware-usb
[11] Bloqueo de puertos USB con ESET NOD32
http://blogs.eset-la.com/laboratorio/2009/04/16/bloqueo-puertos-usb-eset-nod32/
[12] Buenas prácticas para usuarios de telefonía móvil
http://www.eset-la.com/threat-center/1998-buenas-practicas-dispositivos-moviles
[13] Técnicas maliciosas anti-análisis
http://blogs.eset-la.com/laboratorio/2008/12/29/tecnicas-maliciosas-anti-analisis/
[14] Análisis Heurístico: detectando malware desconocido
http://www.eset-la.com/threat-center/1625-analisis-heuristico-detectando-malware-desconocido
[15] Deteniendo intrusos: firewall personales

http://www.eset-la.com/threat-center/1655-deteniendo-intrusos-firewall-personales

[16] Drive-by-Download

http://www.eset-la.com/threat-center/1792-drive-by-download-infeccion-web

[17] El arma infalible: la Ingeniería Social

http://www.eset-la.com/threat-center/1515-arma-infalible-ingenieria-social