Estrategia multicapa y proactiva de protección contra spyware en entornos corporativos

Tecnología antispyware
premiada por PC World US

PC WORLD
Best
BUY

Platinum Internet Security 2005
PC World US - October 2005

Panda Software

www.pandasoftware.es

Índice

¿Cómo definimos y clasificamos el spyware?

En la actualidad existe bastante confusión en la industria con respecto a la definición de spyware y a los tipos concretos de amenazas dentro de esta categoría. Tanto las consultoras Gartner e IDC, como los fabricantes de soluciones de seguridad informática, ofrecen distintas definiciones, lo que está causando bastantes quebraderos de cabeza en el sector, sobre todo por la forma en que cada fabricante denominamos a cada ejemplar detectado.

Antes de proseguir se hace necesario definir qué entendemos en Panda Software por **spyware. A veces nos referimos a este tipo de software también con el nombre de** *spybot* **o** *tracking software.*

Spyware son programas engañosos que realizan determinadas actividades en el PC sin obtener el apropiado consentimiento del usuario para su instalación. El spyware puede recopilar información personal y/o cambiar la configuración del navegador de Internet, entre otros comportamientos. Para Panda, el spyware es un tipo de *malware*[1].

Además de resultar molesto para el usuario, el spyware causa una variedad de efectos en el PC, que pueden ir desde la degradación del rendimiento del PC hasta la violación de la privacidad personal.

El **spyware** es desarrollado por empresas que buscan obtener beneficios económicos por medios poco ortodoxos. La información que recoge el **spyware** es utilizada por las propias empresas o es vendida a terceros. Según las últimas estimaciones, el volumen de negocio generado por este tipo de prácticas alcanza los 2.000 millones de dólares US[2] en concepto de beneficios por año, cantidad más que atractiva para programadores y compañías, en muchos casos, sin escrúpulos.

Uno de los asuntos más polémicos en relación al spyware es la categorización de otra amenaza que en principio es distinta, el **adware, como si fuera spyware.**

Adware es una palabra inglesa que nace de la contracción de las palabras *Advertising Software*, es decir, programas que muestran anuncios. Se denomina **adware** al *software* **que muestra publicidad, empleando cualquier tipo de medio**: ventanas emergentes, banners, cambios en la página de inicio o de búsqueda del navegador, etc. La publicidad está asociada a productos y/o servicios ofrecidos por los propios creadores o por terceros.

El **adware puede ser instalado con el consentimiento del usuario y su plena conciencia, pero en ocasiones no es así**. Si se instala con el conocimiento y consentimiento del usuario, en Panda lo categorizamos y detectamos como **adware.** En el caso de que su instalación se realice **sin el consentimiento ni conocimiento del usuario, en Panda** lo consideramos **spyware.**

Esta diferenciación es muy importante, dado que en determinadas ocasiones se cataloga **adware legal** como **spyware,** lo que causa las protestas de compañías que están actuando de buena fe al desarrollar y distribuir este tipo de software.

1. **Malware:** es todo aquel documento o aplicación capaz de causar perjuicios al PC del usuario.
2. Disponible en http://blogs.zdnet.com/BTL/?p=1341

Clasificación

Existen diversas amenazas a la privacidad y a la confidencialidad dentro de los entornos corporativos y domésticos a las que nos referimos como **spyware.**

Así, dentro de la categoría del spyware, encontramos los siguientes tipos de amenazas:

- **Tracking software o Trackware:** son programas que realizan inventarios de las aplicaciones instaladas, rastreo de itinerarios del usuario, etc. Para ello, guardan todas las búsquedas realizadas en el buscador que colocan como página de inicio, o introducen capturadores de teclado (keyloggers), que registran todas las pulsaciones de teclas realizadas.

  - **Tracking Cookies:** un tipo de Tracking Software son las Tracking Cookies. Las cookies son unos pequeños archivos de texto utilizados por servidores y navegadores Web para almacenar y recuperar información acerca de sus visitantes. Sin embargo, existe un tipo de cookie maliciosa llamado Tracking Cookie que suele ser empleada por programas espía para recopilar información. En Panda las detectamos como Cookies.

- **Spybot o Troyanos espía:** Existe una gran variedad de troyanos espía, cada cual más peligroso y todos ellos destinados al robo de información sensible. Estos troyanos están programados para actuar de forma automatizada y activarse o realizar determinadas acciones cuando reciben las órdenes pertinentes de sus creadores. Algunos de ellos se especializan en la obtención de datos financieros, mientras que otros buscan claves para el uso fraudulento de software pirateado. Otros se centran en el robo de nombres de usuarios y contraseñas de sistemas así como en las credenciales de acceso a servicios web o de correo[3]. En Panda los detectamos como troyanos.

Atendiendo a su **comportamiento** una vez instalados, los podemos denominar **Hijackers** (literalmente, secuestradores) cuando modifican información del usuario, como por ejemplo la página de inicio y de búsqueda del navegador, alteran los resultados de las búsquedas realizadas, etc.

Y, según su **forma de activarse,** podemos diferenciar entre:

- **BHO** (Browser Helper Object): son pluggins de los navegadores. Suelen ser cargados al pulsar un enlace de una página maliciosa visitada, y se ejecutarán cada vez que se abra el navegador. Pueden aparecer visibles como barras de herramientas del navegador, o permanecer ocultos mientras realizan una serie de operaciones sin conocimiento del usuario.

- Otras formas de activación que coinciden son las utilizadas por virus y troyanos

3. Recientemente ha habido una noticia relacionada con un caso de troyanos espía en Israel, disponible en http://iblnews.com/noticias/05/128888.html.

Algunas publicaciones y sitios web de referencia incluyen, dentro de la categoría de **spyware,** otro tipo de amenazas y/o comportamientos que estrictamente no realizan las mismas acciones en los sistemas. Así, las siguientes amenazas no son consideradas, desde el punto de vista de Panda, dentro de la categoría de **spyware**:

- **Keyloggers:** los keyloggers son más un comportamiento asociado a un virus, a un gusano o a un troyano que una amenaza en sí misma. Así, las amenazas que tienen este comportamiento asociado capturan todo lo que hace un usuario en el teclado y lo guardan en un archivo que, posteriormente, puede ser enviado a un tercero sin conocimiento ni consentimiento del usuario. Bugbear.B es un ejemplo de un gusano que lleva asociado este tipo de comportamiento.

- **Dialers:** son programas que, sin el consentimiento del usuario, cortan la conexión telefónica que se está utilizando en ese momento (la que permite el acceso a Internet, mediante el marcado de un determinado número de teléfono) y establece otra, marcando un número de teléfono de tarificación especial. Los dialers sólo afectan a usuarios con conexiones a Internet vía módem o dial-up. No afectan, por lo tanto, a los usuarios que se conectan a Internet vía ADSL, cable u otro tipo de conexiones distintas al dial-up o módem. Si un usuario con módem es afectado por un dialer, experimentará un **notable aumento del importe de su factura telefónica**.

Spyware: ¿cómo llega al ordenador del usuario?

Existen diferentes vías de entrada de spyware en el ordenador:

- Un **troyano** los descarga de Internet y los instala.

- Cuando se accede a una página web, y dependiendo de la configuración de seguridad del navegador, se solicita permiso para instalar un determinado **control ActiveX**, procedente de una fuente poco fiable o insegura. Si el usuario acepta, se instalan.

- Cuando se visita una página web que incluye código que explota una determinada vulnerabilidad. Si el ordenador es vulnerable, el malware se descarga y ejecuta automáticamente, sin necesidad de intervención del usuario.

- A veces, están ocultos en la **instalación de programas** aparentemente inocuos, descargados de Internet y con licencias *shareware* o *freeware*.

Spyware son programas engañosos que realizan determinadas actividades en el PC sin obtener el apropiado consentimiento del usuario para su instalación. El spyware puede recopilar información personal y/o cambiar la configuración del navegador de Internet, entre otros comportamientos.

Además de resultar molesto para el usuario, el spyware causa una variedad de efectos en el PC, que pueden ir desde la degradación del rendimiento del PC hasta la violación de la privacidad personal.

Por lo tanto, es una amenaza más de Internet capaz de causar perjuicio al ordenador del usuario y se engloba dentro de la categoría de malware. Y, como tal, la tecnología necesaria para detectarlo, bloquearlo y/o eliminarlo debe estar integrada junto a la que se utiliza con otro tipo de malware, como virus, gusanos, troyanos, dialers, etc.

La percepción de las empresas del spyware

El spyware es uno de los problemas de seguridad más extendidos. Según Microsoft, aproximadamente un 50% de todos las caídas de sistemas o aplicaciones (crashes) reportados por su herramienta *Dr. Watson* son causados por el spyware. Además, el spyware ocupa 7 de los 10 tipos de incidencias más comunes. Según datos presentados también por Microsoft, en empresas como Dell, HP o IBM el spyware causa aproximadamente un 30% de las llamadas de soporte. En el caso de Dell, el spyware es la incidencia número uno, con unos costes de soporte de unos $2,5 millones anuales.

Otros datos reveladores: según un reciente informe elaborado por las empresas Webroot y Earthlink, hay software espía instalado en 9 de cada 10 ordenadores.

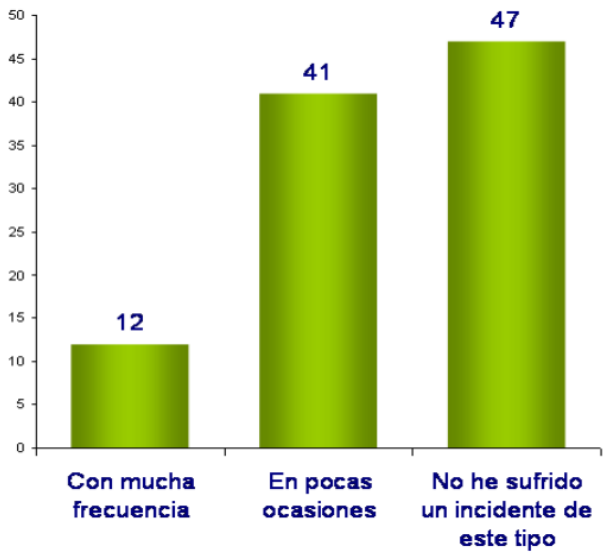
Es decir, el 90% de los usuarios encuestados se encuentra afectado por este tipo de malware. Además, la media de spyware instalado en cada uno de los equipos analizados es de 25 ejemplares[4].

Por su parte, según los datos recogidos por la solución antivirus online y gratuita de Panda Software, Panda ActiveScan -cuya nueva versión detecta spyware-, encontró que el 84% del total de malware instalado en los ordenadores es software espía.

Según Forrester, una encuesta reciente realizada a 3.750 usuarios de Norteamérica ha revelado que sólo el 55% de los encuestados sabe lo que es el spyware y que sólo el 40% utiliza una aplicación antispyware más de una vez al mes[5].

Las empresas están realmente preocupadas por el problema del spyware, como demuestra los resultados de una encuesta internacional realizada por Panda Software a través de su sitio web[6], cuyas principales conclusiones son las siguientes:

- ¿Con qué frecuencia su PC ha resultado afectado por spyware?

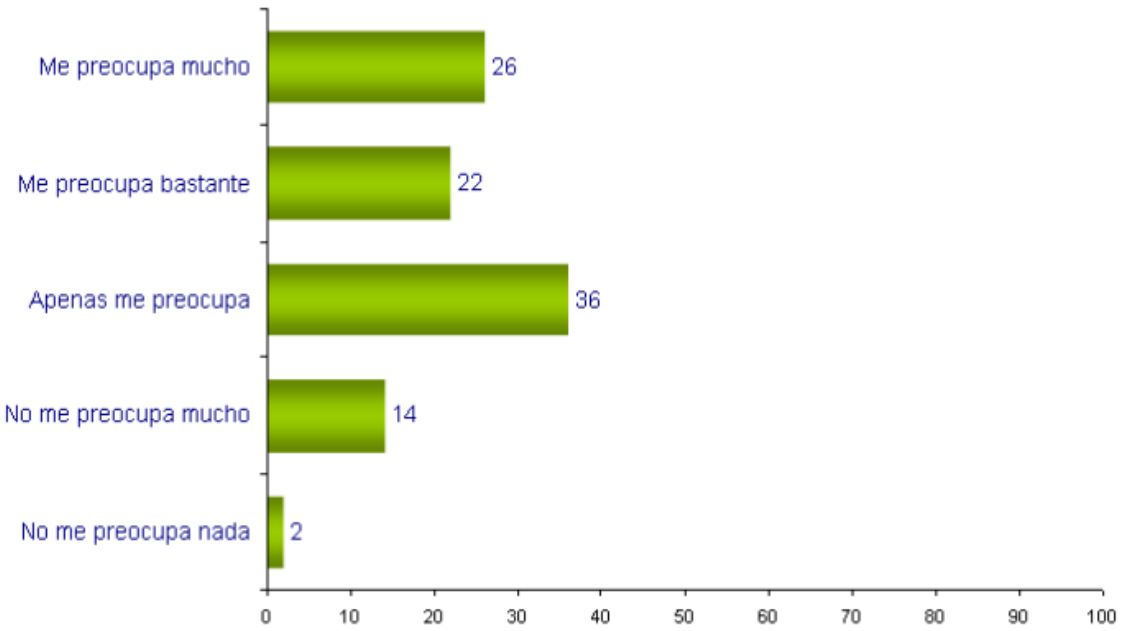


4. Disponible en:http://www.webroot.com/company/pressmedia/pressreleases /20040804-spywarereport

5. D. LOPEZ, Maribel: “Spyware Threat goes unchecked". Abril 2005. Forrester.

6. Encuesta realizada a 1.000 empresas en mayo de 2005 a través de www.pandasoftware.com.

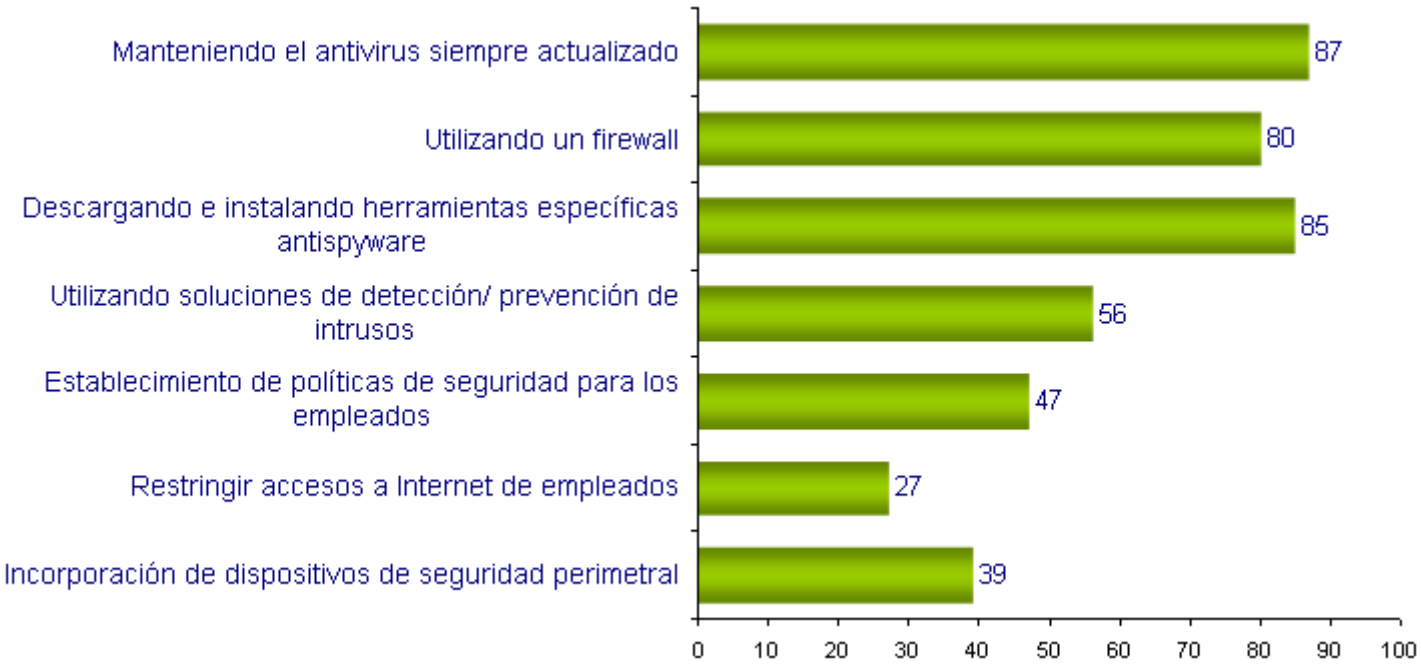
- ¿Hasta qué punto le preocupa el spyware?



- ¿Considera peligroso el spyware?

■ ¿Sabe qué efectos puede provocar en su empresa el spyware?

■ ¿Sabe qué medidas tomar para combatir el spyware?



Sin embargo, el instalar protecciones específicas para cada amenaza, como para el spyware, en un PC no tiene tantas ventajas como pueden percibir los usuarios. Sería como decir, por ejemplo, que los usuarios necesitan un software contra virus, otro contra gusanos, otro contra troyanos, etc., cuando, en realidad, las ventajas de tener una solución global son mayores.

Si contasen con una suite de seguridad antimalware tendrían como ventajas la gestión centralizada desde un único interfaz, desde el cual el usuario puede manejar y configurar todas las protecciones conociendo un solo producto, no distintos de varios fabricantes. Además, no tendrían que hacer desembolsos parciales por cada protección, dado que las suites de seguridad son más económicas que la suma de los gastos parciales.

Y, por último, el consumo de recursos en memoria sería menor, dado que no se abrirían distintos procesos en paralelo (varios programas ejecutándose a la vez), sino que sería sólo uno el que estaría protegiendo activamente el PC evitando, de esta manera, ralentizaciones, bloqueos, etc.

El spyware representa una clara amenaza para los usuarios, según se desprenden de varios estudios de Forrester, Webroot, Panda, etc. Los entornos empresariales sienten la necesidad de sentirse protegidos de forma eficaz frente a la proliferación de spyware.

El que el usuario, bien doméstico o bien corporativo, cuente en su PC con soluciones específicas para cada tipo de amenaza, como contra el spyware, se traduce en una falta de comodidad y eficacia (al tener que aprender, manejar y configurar distintos productos a la vez), en una pérdida económica (al tener que hacer un desembolso económico por cada uno de ellos) y en un aumento del consumo de recursos del ordenador (al tener varios procesos en paralelo ejecutándose en memoria).

Mantener productos específicos contra cada tipo de amenaza sería como decir, por ejemplo, que los usuarios necesitan un software contra virus, otro contra gusanos, otro contra troyanos, etc.

Soluciones de Panda Software: estrategia integrada y multicapa contra el spyware

Según la directora de Research de Gartner, Avivah Litan, publicado por PCAuthorithy[7], el que los programas antispyware se basen sólo en ficheros de firmas explica su falta de efectividad:

"La falta de efectividad viene del hecho de que muchos programas están basados en ficheros de firmas. Las compañías antispyware, como los antivirus, debe crear firmas digitales para detectar y, entonces, borrar cada nuevo ejemplar de spyware. Hay un período de latencia aquí, un espacio desde que un nuevo spyware aparece hasta que la firma es creada."

En la actualidad, las soluciones específicas contra el spyware no son suficientes para detener a este tipo de malware. La cada vez más frecuente aparición de ejemplares híbridos o el uso de vías de propagación tipo gusanos, troyanos, controles ActiveX, etc., precisa de la utilización de varias tecnologías para detectar tanto los medios de distribución como el propio spyware.

Además, la mayoría de las soluciones antispyware del mercado son reactivas, es decir, sólo detectan spyware mediante ficheros de firmas. Ninguna, en estos momentos, detecta spyware de forma proactiva ni tienen la capacidad de devolver el ordenador a su configuración inicial borrando cualquier rastro que hubiera podido dejar en registros, temporales, etc. Muchas de ellas, además, no tienen residente. Esto quiere decir que el análisis tiene que hacerlo el usuario bajo demanda cuando se acuerda, lo que puede provocar que la aplicación no bloquea el spyware antes de que se instale, sino que lo desinfecta una vez el software está instalado en el PC.

Panda Software dispone de soluciones de protección que integran diferentes tecnologías de detección. De esta manera se conforman como verdaderas soluciones antimalware, que utilizan un sistema u otro según el tipo de amenazas. Así, Panda Software cuenta con tecnologías capaces de detectar y eliminar eficazmente spyware:

- **Tecnología de detección de spyware basada en firmas.** Esta tecnología, de naturaleza reactiva, está presente en todos las soluciones de Panda Software. Con ella, se detecta y elimina spyware conocido. Sin embargo, la eficacia de la misma depende de la capacidad de identificación y de elaboración de vacunas contra los nuevos ejemplares de software espía. Dado que Panda Software cuenta con personal dedicado exclusivamente a ello, la detección de spyware por firmas de sus soluciones puede considerarse como una de las mejores que puedan encontrarse actualmente.

- Gracias a las **Tecnologías TruPrevent™**, que cada vez que detectan un nuevo spyware lo envía a **PandaLabs** para que lo identifiquen y faciliten la nueva vacuna a todos los clientes, nuestra tecnología reactiva es una de las más rápidas en ofrecer soluciones contra nuevos ejemplares de spyware. **PandaLabs,** el laboratorio de malware de Panda Software, tiene el mejor tiempo de reacción a la hora de proporcionar protección completa frente a nuevas amenazas, tal y como certifica www.av-test.org, laboratorio de Andreas Marx.

7. Disponible en: www.pcauthority.com.au/news.aspx?ClaNID=18269

- Mediante el motor de limpieza y restauración de configuración original **SmartClean.** En el caso de que el usuario tuviera spyware en su PC, este motor limpia todos los rastros que hubiera podido dejar y restaura las configuraciones originales que tenía el ordenador antes de haber sido afectado por el programa malicioso.

- **Tecnología antimalware proactiva:** representada por las **Tecnologías TruPrevent™**. Son un conjunto de tecnologías diseñadas para hacer frente a amenazas desconocidas, capaces de determinar por sí mismas y sin necesidad de conocerlo previamente, si un archivo o proceso puede ser dañino para el sistema. En caso afirmativo, estas tecnologías bloquean el proceso potencialmente dañino al menos hasta que la posible amenaza haya sido analizada en profundidad. Actúan como una línea de defensa adicional, que impide que un nuevo riesgo de seguridad pueda dañar los sistemas antes de que se dispongan de los medios adecuados para luchar frente a él. Estas tecnologías son capaces de detectar todo tipo de malware, incluyendo spyware. Las **Tecnologías TruPrevent™** se encuentran en constante evolución, de forma que cada vez van ampliando sus capacidades y perfeccionando su funcionamiento. Así, recientemente se ha incorporado a ellas una nueva tecnología de análisis “genético” de malware que integra técnicas de correlación de firmas genéticas digitales e inspección profunda de código (Deep code inspection). Esta tecnología se ha mostrado extremadamente eficaz frente al spyware.

- **Tecnologías de filtrado web:** Panda Software ofrece soluciones que incorporan la tecnología más avanzada de filtrado web gracias a su alianza con Cobion/ISS, enfocadas específicamente al bloqueo de spyware. Concretamente, en gateways esta tecnología categoriza más de veinte millones de direcciones web, incluyendo aquellas desde la que se esté descargando spyware. De esta manera, no solamente se evita la entrada de spyware en la red, sino que se refuerza el cumplimiento de las políticas de seguridad establecidas por la empresa en cuanto al uso de Internet por parte de los empleados.

Con las mencionadas tecnologías, Panda Software ha desarrollado diferentes productos que integran varias de ellas según las necesidades de protección de cada elemento concreto de la red.

Soluciones de Panda Software

La protección eficaz contra el spyware en una empresa debería contemplar las instalación de tecnologías específicas para detectar este tipo de malware en las pasarelas de Internet y en las estaciones de trabajo.

Los gateways son una parte clave en la protección frente al spyware, ya que es la vía de entrada principal de este malware en la red. La implementación de tecnología antispyware en este punto evita las consecuencias de que los usuarios puedan hacer llamadas a sitios web o servidores que son susceptibles de descargar spyware. Además, si a esta tecnología se une otra, capaz de filtrar direcciones web a las que los usuarios de una red pueden acceder, se consigue reforzar la política de seguridad de la empresa.

Por su parte, la instalación de tecnología antispyware en las estaciones de trabajo es fundamental, debido a la propia naturaleza del spyware, cuyo objetivo principal es recopilar datos referentes a los hábitos de navegación de los usuarios. Dicha información puede ser conseguida con más facilidad en las estaciones de trabajo que en cualquier otro punto de la red, por lo que un spyware tratará de instalarse en dicha capa.

Panda Software cuenta con las siguientes soluciones para la defensa de pasarelas de Internet y estaciones de trabajo:

- Protección del servidor de Internet con *Panda Gatedefender Serie 8000:* Appliance de alto rendimiento que combina flexibilidad, escalabilidad y facilidad de uso gracias a sus diferentes módulos integrados: la mejor tecnología antimalware, el antispam de MailShell y el Filtrado de URL proporcionados por Cobion. La familia de appliances *GateDefender,* con sus tres modelos (8050, 8100 y 8200), se adaptan prácticamente a cualquier tamaño de empresa. El modelo más alto de gama, 8200, proporciona un rendimiento de su motor antimalware (virus, spyware, troyanos, etc.) HTTP de 80 a 350 Mbps, dependiendo del tráfico. Además del escaneo HTTP, proporciona un gran rendimiento en el análisis de mensajes por hora en sus módulos antimalware y antispam, alcanzando entre 120.000 y 300.000 (más de 1,5 millones sólo el módulo antivirus), dependiendo del tráfico. *GateDefender* incluye tecnología de filtrado web, de forma que impide el acceso a aquellas direcciones desde la que se esté descargando spyware.

- Protección para estaciones de trabajo: *ClientShield con* **Tecnologías TruPrevent™**. Esta solución antimalware integrada bloquea spam y protege contra hackers, spyware, dialers, hoaxes, jokes, etc. ClientShield proporciona a las compañías una capa adicional de seguridad gracias a sus **Tecnologías TruPrevent™**. Estas tecnologías proactivas detectan y bloquean malware desconocido, incluyendo spyware.

Tecnología antispyware premiada por PC World Us[8]

Platinum Internet Security 2005
PC World US - Octubre 2005

Platinum Internet Security 2005, ha sido analizado frente a otras suites de seguridad como Norton Internet Security 2005 Anti-Spyware Edition y Zone Labs Internet Security 6.0 y ante productos específicamente diseñados para la lucha contra el spyware como McAfee Antispyware 2005, Trend Micro Anti-Spyware 3.0, y Microsoft Windows AntiSpyware Beta 1.06.615, resultando mejor que todos ellos en la eliminación de spyware:

:"De las tres suites (analizadas) "todo en uno", recomendamos Panda Platinum Internet Security 2005 de Panda Software (50$). Nuestra selección como Best Buy de entre las suites, Panda ha conseguido el mayor ratio de eliminación de spyware de las tres y el segundo más alto entre el resto de productos, eliminando el 86 por ciento de los componentes de spyware. Panda también eliminó el spyware sin obligarnos a tomar decisiones caso por caso".

100% de los procesos en ejecución eliminados

"Una medición clave del software anti-spyware es su habilidad de eliminar procesos de spyware que están ejecutándose activamente en memoria; este tipo de procesos representan una porción del total de los componentes de spyware mencionados anteriormente. Panda fue el único programa que eliminó el 100 de los procesos en ejecución."

8. Disponible en: www.pcworld.com/reviews/article/0,aid,122496,pg,1,00.asp

Facilidad de uso

"Cuando hablamos de facilidad de uso, la suite de Panda fue de la más alta calidad, eliminando el adware y el spyware detectado sin esperar al input del usuario. También se puede cambiar la configuración por defecto para tomar una decisión caso por caso".

El reconocimiento de PCMagazine US

La prestigiosa revista PCMagazine US[9] ha publicado recientemente los resultados de un estudio de la efectividad de los productos actuales antispyware. De los productos de Panda afirma:

"Fue la más exitosa suite de seguridad a la hora de limpiar y detectar spyware".

En dicha comparativa, se evaluó Platinum Internet Security 2005 contra otras suites de seguridad del Mercado y productos específicos antispyware.

La tecnología antispyware de Panda está disponible, de forma gratuita para los clientes, en todo el catálogo de productos. Así, grandes empresas, pymes, negocios y profesionales y usuarios domesticos están protegidos contra spyware.

Las soluciones de Panda Software integran distintas tecnologías para combatir el spyware:

- **mediante ficheros de firmas o tecnologías reactivas, utilizando su motor SmartClean para limpiar los posibles rastros dejados por este tipo de amenaza**
- **mediante las Tecnologías TruPrevent™ , de detección y de bloqueo proactivo**
- **mediante la utilización de tecnologías de Filtrado Web**

Combinándolas, Panda ofrece la mejor estrategia de protección integral multicapa contra el spyware, tanto a nivel de pasarela de Internet como de estaciones de trabajo y para todo tipo de usuarios: grandes empresas, pymes, SOHO y usuarios domésticos. Y se integran en los productos de forma gratuita y sin coste adicional.

Así, las soluciones de Panda son muy superiores en detección, bloqueo y/o desinfección del spyware al resto de suites de seguridad del mercado, así como frente a soluciones específicas, según ha confirmado PC World US y PCMagazine US.

De la tecnología antispyware de Panda, PC World US ha dicho: "Cuando hablamos de facilidad de uso, la suite de Panda fue de la más alta calidad, eliminando el adware y el spyware detectado sin esperar al input del usuario."

8. Disponible en: www.pcmag.com/article2/0,1759,1754437,00.asp

Consejos para evitar el spyware

Uno de los principales problemas de la defensa frente al spyware es que suele propagarse desde sitios web que los usuarios visitan voluntariamente -y en más de una ocasión-, o mediante la instalación de aplicaciones informaticas que, en principio, pueden resultar atractivas. Esto conlleva que los usuarios hagan caso omiso a las políticas de seguridad establecidas por la empresa, y que deban utilizarse medios tecnológicos para combatir la amenaza del software espía. Así, una adecuada defensa contra el spyware en una red corporativa debería contemplar los siguientes aspectos:

- Instalacion de soluciones de seguridad que integren diferentes tecnologías:
  - Detección de spyware conocido por archivos de firmas de virus (tecnologías reactivas).
  - Detección de spyware desconocido mediante análisis de comportamiento (tecnologías proactiva).
  - Filtrado web, que impida las visitas a sitios web desde donde puede descargarse spyware.
- Implante una estrategia de protección por capas en su red. Para el spyware debería reforzarse dicha protección especialmente en los puntos de conexión a Internet y en las estaciones de trabajo. Los puntos de conexión a Internet son una parte clave en la protección frente al software espía, ya que es la vía de entrada principal de este malware en la red. Por su parte, la instalación de tecnología antispyware en las estaciones de trabajo es fundamental, debido a la propia naturaleza del spyware, cuyo objetivo principal es recopilar datos referentes a los hábitos de navegación de los usuarios.
- Informe a los usuarios de la red sobre las vías de entrada del spyware en los ordenadores. Uno de los principales peligros del spyware es el desconocimiento que los usuarios muestran sobre el mismo, sobre todo en cuanto a sus efectos y vías de propagación.

Y, ante cualquier duda, siempre puede utilizar la solución on-line y gratuita Panda ActiveScan que, en sólo unos minutos, analizará el PC y detectará los posibles ejemplares de spyware que pueda encontrar. ActiveScan puede ser utilizado desde: www.activescan.com.