



Managed VirusScan Plus AntiSpyware

**Una combinación vencedora para los
proveedores de servicios**

Índice

Introducción	3
Actualización de mercado	3
¿Qué es <i>spyware</i>?	4
El efecto comercial de los virus y programas espías sobre los usuarios de banda ancha y las PyMES	4
Creación de una solución gestionada contra virus y programas espías utilizando McAfee	6
Resumen	7

Una combinación vencedora para los proveedores de servicios

Introducción

En 2005, el precio y la disponibilidad del acceso a Internet en alta velocidad por banda ancha a cable o xDSL alcanzaron un punto comercialmente aceptable tanto para pequeñas empresas como para el mercado residencial/consumidor. La percepción y penetración de la banda ancha en el mercado aumentó considerablemente en toda Europa y Norteamérica.

La capacidad de acceder a Internet y conducir comunicaciones de negocios en alta velocidad a través de enlaces de banda ancha es negativamente afectada por el constante aumento del número de programas malintencionados capaces de diseminarse de forma rápida y fácil entre computadoras personales (PC) conectadas a Internet. Empresas y residencias se están dando cuenta que, a menos que tomen precauciones adecuadas, los datos y la información personal almacenados en sus PC, además de la máquina en sí, no estarán seguros.

Eso les brinda a los proveedores de servicios (SP) y proveedores de acceso a Internet (ISP) una gran oportunidad de ofrecer a sus clientes servicios de seguridad como un servicio de valor agregado que genera ingresos.

Este artículo discute la oportunidad que tienen los SP de implementar la solución McAfee® Managed VirusScan® plus AntiSpyware como un servicio de seguridad que:

- Genera un ingreso promedio anual más elevado por usuario (ARPU) suscriptor de banda ancha
- Protege automáticamente su base de clientes contra todas las formas de programas potencialmente indeseables (PUP)
- Crea servicios diferenciados en el mercado que reducen la rotación de clientes, aumentando el número de suscripciones
- Aumenta el nivel de satisfacción de los clientes, eliminando de las PC los programas desconocidos e indeseables que consumen ancho de banda y dejan las aplicaciones más lentas
- Reduce el número de llamadas de auxilio de los clientes y los gastos operacionales con la mesa de ayuda

- Permite que el administrador genere informes detallando los tipos de PUP que atacaron a los usuarios finales y el éxito de las aplicaciones de seguridad en el combate a las amenazas

Actualización de mercado

La mayor conectividad por banda ancha de las PC con las redes de empresas y con Internet llevó al aumento de la sofisticación de los programas espías y de otros PUP. Esta nueva y más siniestra amenaza es capaz de transferirse de una máquina a la otra, ya sea instalándose automáticamente en las *desktops*, o persuadiendo a un usuario inocente a descargar la aplicación como parte de un adjunto invisible o aparentemente inocente de alguna otra forma de información.

El aumento de la velocidad de la conexión por banda ancha permite que los programas espías se instalen en una PC “blanco” antes que el usuario siquiera sospeche de alguna violación de seguridad. Algunos usuarios pueden darse cuenta de que sus computadoras fueron infectadas sólo cuando las aplicaciones ya no operan normalmente, cuando archivos son excluidos o corrompidos, o cuando la banda se vuelve muy lenta. En algunos casos, los PUP interceptan y copian información bancaria privada que, más tarde, permiten el acceso fraudulento a las cuentas bancarias de los usuarios. El usuario quizás ni se dé cuenta de que su computadora está infectada y, posiblemente, controlada por otra persona.

Las máquinas desprotegidas conectadas con Internet por banda ancha están expuestas a innumerables amenazas que pueden infectar al azar o a través de un ataque coordinado dirigido. Entre dichas amenazas están las siguientes:

- *Worms*
- Troyanos y PUP/programas espías/*bots*
- *Exploits* de desborde de buffer
- *Exploits* de elevación de derechos
- *Backdoors*
- *Rootkits*
- *Exploits* de HTTP

El efecto de los virus sobre las computadoras es ampliamente conocido.¹

¹ Para ver una explicación más detallada sobre dichas amenazas, lea *Un breve historial de los Programas Malintencionados: Una nota educativa para Proveedores de Servicios*, de McAfee.

La solución es instalar programas antivirus de una empresa de seguridad líder de mercado, como McAfee. En los últimos meses, los usuarios de banda ancha fueron molestados por dos nuevas formas de PUP: programas espías y *adware*. Los PUP reducen la velocidad de la conexión de banda ancha a una velocidad de banda estrecha, brindándoles a los *hackers* acceso total a los datos personales de los usuarios y el control sobre sus PC.

IDC calcula que un 67 por ciento de todas las computadoras están infectadas por algún tipo de *spyware*.²

¿Qué es *spyware*?

Spyware es el término que se usa para designar los programas que logran entrar en la máquina de un usuario y realizan funciones indeseables tales como exhibición de propaganda, secuestro de navegación, captura de teclado y actividades similares. De forma más general, el término fue creado para indicar cualquier programa instalado de forma subrepticia en la PC de un usuario sin su permiso explícito. (Es por eso que McAfee describe la categoría general de programas que incluye *adware* y programas espías como “programas potencialmente indeseables”). La mayoría de los programas espías llega a la PC del usuario empaquetada u oculta en alguna otra forma de *software* que el usuario realmente desea descargar e instalar, o a través de la visita inocente de un usuario a una página Web sin saber que contiene *scripts* que se descargan automáticamente luego de la apertura de la página.

No todos los PUP son malintencionados. Algunos PUP, aunque sean una pequeña minoría actualmente, pueden ser instalados por una empresa legítima para alguna finalidad bienintencionada. Sin embargo, un PUP se define como CUALQUIER programa que un usuario de computadoras que se preocupe razonablemente con la seguridad o la privacidad pueda querer saber que existe en su máquina y, en la mayoría de los casos, eliminar. Aunque algunos hayan sido creados para uso profesional legítimo, los PUP pueden alterar el estado de seguridad de las computadoras donde están instalados y, por lo tanto, la mayoría de los usuarios quiere estar consciente de su presencia.

Los principales tipos de PUP son:

Programas espías: programas cuya función principal es transmitir información personal de un usuario, sin su conocimiento y consentimiento explícitos, a terceros. Los programas espías normalmente vienen incluidos como componentes ocultos de programas gratis o compartidos (*shareware*) que se pueden descargar desde Internet sin ningún costo. Los programas espías se están convirtiendo rápidamente en uno de los mayores problemas asociados a la conexión de las computadoras con Internet. Los programas espías son, a menudo, usados por las empresas para monitorear secretamente los hábitos de navegación y de compras de un usuario en Internet y recopilar secretamente información personal que les permita crear anuncios personalizados (*adware*) dirigidos a los usuarios a través de *e-mail* y ventanas instantáneas (*pop-ups*) indeseables. Algunos programas espías monitorean el teclado del usuario para identificar y posteriormente capturar logins, números de tarjeta de crédito y

contraseñas, información que, en otro momento, se puede enviar secretamente por *e-mail* a un atacante, sin que lo sepa el usuario.

Adware: programa cuya principal función es obtener lucros a través de la exhibición de anuncios dirigidos al usuario de la computadora donde está instalado. Dichos lucros lo pueden obtener el proveedor o sus socios. Eso no significa necesariamente que se recopilará o que transmitirá alguna información personal como parte de la función del programa, aunque, a menudo, eso realmente ocurra.

Discador: programa que redirige las conexiones con Internet a otro lugar que no sea el proveedor de acceso usual del usuario, para hacerle pagar tarifas de un proveedor de contenido, fabricante u otros terceros.

Herramientas de administración remota: programas creados para permitir que un administrador bienintencionado controle una máquina a distancia. En las manos de otras personas que no sean el legítimo propietario o el administrador, las herramientas de administración remota son una gran amenaza a la seguridad.

Decodificador de contraseñas: programas creados para permitir que un usuario legítimo o administrador recupere las contraseñas perdidas u olvidadas de cuentas o archivos de datos. En las manos de un atacante, dichas mismas herramientas permiten el acceso a información confidencial y representan una amenaza a la seguridad y la privacidad.

Bromas: programas sin ningún contenido o uso malintencionado y que no afectan al estado de seguridad o privacidad, pero puede alarmar o molestar a un usuario.

De la misma forma que se utiliza normalmente el término *antivirus* para referirse a programas que combaten no sólo virus, sino también *worms* y otras formas de programas malintencionados, el término *spyware* se utiliza cada vez más para referirse a los PUP de forma genérica, aunque la función de diversos PUP pueda ser distinta.

El efecto comercial de los virus y programas espías sobre los usuarios de banda ancha y las PyMES

Empresas y consumidores que ya sufrieron ataques de virus están confusos, frustrados y enojados con los efectos de los programas espías y virus que infectan sus computadoras. Muchos se enojan con el hecho de que su novísima y costosísima computadora de vanguardia, conectada con Internet por la más reciente tecnología de banda ancha, se comporta como su lenta PC antigua, o con el hecho de que la conexión de alta velocidad que promete su proveedor parece tan lenta como su vieja conexión telefónica. Los usuarios cuyas máquinas están infectadas luchan para controlar su patrimonio de informática e inundan las mesas de ayuda de los proveedores de servicios con llamadas y reclamaciones coléricas.

² IDC, *Análisis de Mercado: Proyecciones y análisis sobre Programas Espías en el mundo entre 2004 y 2008: Pesadillas con Gestión de Seguridad y Sistemas*, noviembre de 2004.

Los flujos de ingresos de los proveedores de servicios caen por causa del aumento de los costos de soporte y posible pérdida de ingresos motivada por la insatisfacción de los clientes. Para los proveedores de servicios que cobran por capacidad de descarga de gigabits en vez de una suscripción fija, los ingresos caen porque los clientes no tienen total control sobre sus recursos y no son capaces de acceder a Internet e iniciar descargas que generan ingresos.

Antivirus y anti-spyware son una oportunidad de generación de ingresos para los proveedores de servicios

La solución sirve para que los usuarios se protejan con programas antivirus y anti-spyware disponibles en el mercado. A pesar de la amenaza, los usuarios comerciales y las pequeñas empresas no cuentan, a menudo, con el conocimiento y la voluntad para gestionar la seguridad de sus computadoras y, a fin de cuentas, quieren que los problemas creados por los programas malintencionados y los programas espías sean solucionados por terceros.

Existe una oportunidad para que los proveedores de servicios atiendan a dicha necesidad y tomen la iniciativa de brindarles a las empresas pequeñas y medianas (PyMES) un servicio automatizado de seguridad que proteja a los clientes, sin que se den cuenta, contra dichas amenazas, y, al mismo tiempo, identifique y elimine con seguridad los archivos infectados y los PUP.

Eso se puede hacer con soluciones que reúnen antivirus y anti-spyware para máquinas conectadas con la VPN gestionada de una PyMES o conectadas a través de una conexión de banda ancha, e incluidas en el costo básico del servicio, o como un servicio opcional de valor agregado para las empresas pequeñas y medianas que ya son sus clientes.

El proveedor de servicios puede aprovechar una nueva fuente de ingresos minoristas y diferenciar sus servicios con respecto a la competencia. Además, el proveedor de servicios puede reducir sus costos operativos y de soporte, además de reducir la rotación de clientes a través del aumento de su satisfacción y del aumento de la fidelidad a los productos³.

Recientemente, IDC divulgó que el segmento que más rápidamente crece en el mercado de antivirus es el segmento de soluciones gestionadas de seguridad, cuyo valor crecerá hasta superar los US\$417 millones en 2008.⁴

¿Qué necesita el cliente en una solución antivirus y anti-spyware?

Al pensar en cómo crear e implementar una solución antivirus y anti-spyware gestionada para usuarios comerciales y profesionales, el proveedor de servicios debe comprender las necesidades del usuario profesional:

- El usuario final no se debe dar cuenta⁵ de la presencia de la solución antivirus y anti-spyware
- El cliente quiere simplemente usar su red por completo (PC/servidor) sin ninguna interrupción de operación
- El usuario quiere la tranquilidad de saber que está protegido contra ataques e infecciones de programas malintencionados y que su información personal y la información de su empresa están protegidas
- Los usuarios que se suscriben al servicio exigen protección actualizada con muy poca interacción de ellos mismos
- Los usuarios necesitan una alta velocidad de procesamiento contra virus y programas espías que no deje sus PC/servidores más lentos

Eso significa que, para brindar dicho servicio automatizado, el proveedor de servicios debe diseñar una solución capaz de

1. Ofrecer e instalar la protección antivirus al usuario final de una forma que el cliente no necesite involucrarse profundamente en el proceso.
2. Encontrar una solución antivirus que opere en la mayoría de las máquinas de la base instalada sin afectar a la operación eficaz de dichas máquinas. (Específicamente, el *software* antivirus y anti-spyware no debe consumir mucha memoria de las PC, debe ser compatible con la mayoría de las computadoras, debe operar con rapidez suficiente y no debe causar conflictos con ningún otro programa usado por el usuario final en la PC. Además, el *software* antivirus y anti-spyware debe ser capaz de desinstalar cualquier otro *software* antivirus y anti-spyware instalado anteriormente en la PC, o debe ser capaz de operar junto con otro *software*).
3. Asegurar que la protección contra virus y programas espías esté siempre actualizada, es decir, que, a intervalos regulares, el SP sea capaz de enviar a la PC del usuario final las protecciones más recientes contra los virus identificados, alertar al *software* antivirus y anti-spyware residente sobre actualizaciones urgentes y de alta prioridad e iniciar una descarga automática, o permitir que el usuario final configure de forma sencilla, simple y clara su computadora para que puede elegir cuándo se deben descargar las actualizaciones.

³ Por ejemplo, al firmar un nuevo contrato de 12 meses para la provisión de "servicios de protección de datos/seguridad gestionada" con una PyME, el cliente se involucra en una nueva relación extendida de largo plazo con el proveedor de servicios. Dicho contrato efectivamente protege el flujo existente de ingresos y genera un nuevo flujo. Cuanto más servicios de valor agregado el proveedor de servicios logra convencer al cliente a adquirir, menor será la probabilidad (y mayor la dificultad) de que el cliente cancele algún servicio, aunque sean los que no se provean más a precios competitivos de mercado.

⁴ IDC, *Proyección del Mercado Mundial de Antivirus entre 2004 y 2008 y Participación de Mercado de los Proveedores en 2003*, agosto de 2004

⁵ El SP puede optar por informar al usuario final o al administrador de sistemas sobre la detección de un PUP, brindándole al usuario/administrador la opción de excluir o no el programa. Eso es necesario, pues algunos PUP pueden ser intencionalmente instalados en una red por un administrador de sistemas, y la exclusión deliberada de dicho programa puede desactivar procesos de negocios necesarios y esenciales.

4. Gestionar el tamaño de las descargas de actualizaciones, para reducir el tiempo de procesamiento necesario en la PC del usuario final y hacer que las descargas se realicen en segundo plano sin que el usuario se dé cuenta. Eso también reduce el uso del ancho de banda capaz de afectar el enlace de acceso del cliente a Internet. En resumen, las actualizaciones antivirus deben ser pequeñas, así como el tamaño de la solución instalada en la PC del usuario final.
5. Desde el punto de vista del cliente, no existe diferencia entre *spam*, PUP o virus. Todo eso es igual, pues causan dificultades al cliente, reducen el tiempo de uso efectivo de las computadoras y son increíblemente frustrantes o molestos. Para reaccionar a eso, el proveedor de servicios debe pensar en la mejor forma de enfrentar todas esas amenazas con una única oferta de seguridad, o en la mejor forma de reunir económicamente varias soluciones de seguridad, para que el cliente permanezca protegido de la forma más eficaz, lucrativa y sencilla posible.
6. Un servicio gestionado y automatizado debe permitir que los administradores monitoricen el desempeño de la solución antivirus y anti-*spyware* en la organización, y emitan informes de diagnóstico que muestren cuáles PC fueron atacadas por programas malintencionados y cuándo/cómo combatió a la amenaza la solución antivirus y anti-*spyware*. Dicha información ayuda a los gerentes de red a monitorizar el nivel de amenaza a sus organizaciones y planificar estrategias futuras de seguridad. Esos informes también permiten que los gerentes de red justifiquen el presupuesto que se utilizó en las medidas de seguridad. Donde se necesiten informes, el servicio debe implementar una solución antivirus y anti-*spyware* que brinde autonomía a los dirigentes de seguridad/gerentes de TI del cliente.

Creación de una solución gestionada contra virus y programas espías utilizando a McAfee

McAfee integró su solución Managed VirusScan líder de mercado a su tecnología anti-*spyware* de vanguardia. Los proveedores de servicios pueden implementar una única solución para brindarles a las empresas pequeñas y medianas la mejor protección contra todas las formas de programas malintencionados y espías.

La solución Managed VirusScan plus AntiSpyware se provee fácilmente a las empresas pequeñas y medianas a través del proveedor de servicios. La solución les brinda a los administradores de sistemas la autonomía que necesitan para implementar con agilidad una solución eficaz y unificada contra virus y programas espías para los clientes. Permite que un único administrador de sistemas instale el *software* licenciado de McAfee en varios nodos y los administre desde un punto centralizado, sin intervención del usuario.

A través de una interfaz sencilla e intuitiva, el administrador de la PyME, o un proveedor de servicios que administre la red en nombre de la PyME, es capaz de generar informes que detallen la actividad de protección contra virus y *spyware*. Cada computadora protegida transfiere información al servidor hospedado por McAfee.

Informes detallados exhiben el *status* de momento de las computadoras protegidas, de las detecciones o de los brotes.

Los administradores pueden usar los recursos avanzados del servicio para crear grupos de usuarios, establecer políticas para grupos y exhibir datos de informes de una forma significativa para la empresa, sin la inversión adicional de instalar una máquina servidora en la propia empresa. La solución Managed VirusScan plus AntiSpyware fue diseñada para varias situaciones de implementación y varios procesos de provisión distintos, lo cual permite que los proveedores de servicios la pongan a disposición de forma rápida y fácil a las PyMES que ya son clientes hace algún tiempo o hace poco tiempo. Entre esos procesos están los siguientes:

- Un programa de proveedor de servicios afiliado
- Un Portal de socio, listo para uso, que les permita a los proveedores de servicios recibir rápidamente las órdenes de los clientes, utilizando las aplicaciones y el conocimiento de McAfee para llevar la solución al cliente
- Una solución de Nivel Uno para socios que permita a los proveedores de servicios recibir órdenes de los clientes y hacer disponible la solución desde su propio Centro de Operaciones de Red (NOC) hospedado
- Una solución de Nivel Dos para socios que permita a los proveedores de servicios recibir órdenes de los clientes y utilizar el Centro de Operaciones de Red de McAfee para hacer disponible la solución a los clientes

Para aumentar la eficacia de la distribución de las actualizaciones de *software* en toda la empresa, la solución McAfee Managed VirusScan plus AntiSpyware cuenta con la Tecnología Rumor, un mecanismo patentado de actualización de antivirus que no requiere conexión directa con Internet.

El *software* de instalación es pequeño (6 MB), y es rápido y fácil de distribuir, además de ahorrar el ancho de banda de la red.

La solución se puede implementar para un único usuario o para miles, según la necesidad, aunque la implementación típica sea dirigida a los clientes del proveedor de servicios que posea cien nodos como máximo.

Previamente configurado como un sistema de exploración en el acceso, Managed VirusScan plus AntiSpyware detecta inmediatamente las actividades de programas espías y supervisa las posibles fuentes de virus, incluso disquetes, CD-ROM, descargas desde Internet, adjuntos de *e-mail*, servidores accedidos, archivos compartidos y servicios remotos. Se pueden iniciar exploraciones completas del sistema o se pueden someter archivos individuales a la exploración cuando se necesite. Con la configuración de políticas por la Web, el administrador de sistemas puede seleccionar cuándo se realizarán las otras exploraciones, definir excepciones para los archivos que NO se deben someter a la exploración, y especificar la frecuencia con la cual la solución verificará la existencia de actualizaciones de antivirus y anti-*spyware*.

Actualizaciones de antivirus y anti-spyware

La solución McAfee Managed Virus plus AntiSpyware sigue eficaz tras la instalación, garantizando que se descarguen automáticamente y de forma imperceptible las nuevas actualizaciones de *software* en cada PC administrada por el servicio. Tras la instalación, el *software* está configurado para buscar actualizaciones automáticamente cinco minutos tras la inicialización y, después, a cada doce horas, si la computadora del usuario permanece conectada con Internet. Sin embargo, el administrador de sistemas puede configurar el intervalo de actualización para 4, 8, 12, 16 o 24 horas. (Nota: Aunque Managed VirusScan plus AntiSpyware se actualice automáticamente, el usuario final también puede verificar nuevas actualizaciones en el servidor del NOC, para lo cual basta realizar una exploración de la computadora cuando lo necesite).

Si ocurre un brote

Cuando McAfee AVERT™ identifica un brote de virus, lanza un DAT de brote, que es un archivo especial de actualización de un virus indicado como un virus de importancia mediana o alta. Cuando McAfee lanza un archivo DAT de brote, un socio proveedor de servicios/operador de telecomunicaciones que hospede su propio NOC recibe automáticamente dicho archivo y lo redistribuye para llevar protección inmediata a sus clientes. Los clientes de un socio proveedor de servicios/operador de telecomunicaciones que utiliza el NOC de McAfee para la distribución recibirán el archivo DAT de brote hasta una hora tras su lanzamiento.

Quédescese tranquilo con los mayores expertos del mercado — AVERT — de guardia 24 horas al día

Cuando los proveedores de servicios eligen una solución que utiliza la tecnología McAfee VirusScan plus AntiSpyware, pueden quedarse tranquilos: su protección antivirus y anti-spyware será suministrada por el líder de mercado en la detección y solución de los problemas causados por los programas malintencionados.

La familia McAfee VirusScan de soluciones antivirus y anti-spyware es parte de una gama de servicios gestionados que cuentan con el apoyo de McAfee AVERT, el más importante centro de investigación antivirus del mundo. Con un equipo central de investigación que posee más de 50 años de experiencia combinada en antivirus, AVERT consulta clientes, usuarios de computadoras, autoridades federales y países extranjeros en busca de opiniones especializadas. Formada por tres equipos integrados que trabajan juntos para proveer servicios y soporte contra virus, análisis de virus e investigación avanzada contra virus, AVERT ayuda a los usuarios a trabajar de forma más segura, investigando las amenazas más recientes y descubriendo amenazas que puedan surgir en el futuro.

Resumen

El aumento de la comprensión de la conexión por banda ancha y de las comunicaciones de alta velocidad entre empresas llevó a un notable aumento en el número de pequeñas empresas que sufren los efectos de los ataques de programas malintencionados, programas espías y *adware*.

Eso les brinda a los proveedores de servicios una excelente oportunidad de ofrecer a las empresas un servicio gestionado de seguridad contra ataques de programas malintencionados y programas espías. El servicio se puede ofrecer como un componente de un servicio combinado de VPN/DSL segura, o como un servicio incremental opcional de valor agregado.

Este artículo buscó presentar la solución de *software* McAfee Managed VirusScan plus AntiSpyware y demostrar cómo pueden implementarla los proveedores de servicios para aumentar los ingresos y la fidelidad de los clientes con la oferta de una única solución integrada capaz de brindar protección máxima, imperceptiblemente, a su base de clientes de PyMES.