



McAfee System Protection Solution

Manual de Evaluación de Anti-Spyware Enterprise

Metodología de Evaluación de McAfee Anti-Spyware Enterprise

Cómo usar este Manual de Evaluación	3
Qué es McAfee Anti-Spyware Enterprise	3
Exploración	3
Protección de Acceso	4
ePolicy Orchestrator™	4
Documentación	5
Sistema necesario	5

Prueba de Productos Anti-Spyware	5
Evalúe la Tecnología Subyacente	6
Evalúe el Elemento Dinámico: Contenido de las actuales	7

Metodología Objetiva de Prueba	8
Panorama	8
Herramientas de Toma de “Instantáneas”	8
Obtención y Retención de Muestras	9

Prueba de la Protección Preventiva	9
Etapas	9

Prueba de la Protección Reactiva	11
Etapas	12

Evaluación de los Resultados	13
Envío a AVERT de Muestras que No Fueron Detectadas	13
Recursos	14

Cómo usar este Manual de Evaluación

Este manual resumido fue creado para dirigir sus esfuerzos de prueba de programas anti-spyware. Consiste en una sucinta descripción de McAfee Anti-Spyware Enterprise (incluso recursos esenciales y requisitos de sistema), destaca aspectos generales del producto que deben tenerse en cuenta al evaluar un producto anti-spyware y, finalmente, describe una metodología objetiva de prueba y las etapas necesarias para ejecutarla.

Este manual presupone que usted está familiarizado con la terminología y la tecnología de antivirus y anti-spyware.

Qué es McAfee Anti-Spyware Enterprise

McAfee Anti-Spyware Enterprise (MASE) es la primera y única protección disponible en el mercado para grandes empresas, y la única protección para grandes empresas contra programas potencialmente indeseables (PUP), tales como programas espías, *adware*, *cookies*, bromas y troyanos. MASE realiza la exploración en el acceso y tareas de exploración a petición para detectar programas potencialmente indeseables y, después, tomar medidas respecto a dichas detecciones. MASE permite que usted defina exclusiones de archivos, valores de registro y *cookies* que no desea incluir en la detección. Además, MASE aprovecha los poderosos recursos de Protección de Acceso de McAfee VirusScan Enterprise para ofrecer protección contra PUP desconocidos.

MASE es instalado como un complemento de McAfee VirusScan Enterprise 8.0i o de McAfee VirusScan Enterprise 7.1, integrándose totalmente al producto antivirus que ya existe para ampliar la protección sin aumentar la complejidad de la gestión. Este manual presupone que usted realizará la instalación en VSE 8.0i, aunque el funcionamiento sea equivalente en ambas plataformas antivirus de McAfee.

Exploración

MASE permite que los escáneres subyacentes del VirusScan Enterprise utilicen definiciones de PUP en los archivos de definición de virus (DAT) de McAfee para detectar una lista creciente de programas potencialmente indeseables. Eso permite una exploración profundizada de cada archivo para identificarlo como un verdadero PUP, en vez de simplemente utilizar el reconocimiento por nombre o la comparación de *hash* MD5. Por lo tanto, MASE reduce la *chance* de identificación positiva falsa y, con la identificación heurística, puede detectar un número mayor de variantes de PUP. MASE permite la exploración preventiva en el acceso y la exploración programada o por encargo, garantizando que sus computadoras queden y permanezcan limpias.

- **Escáner de Acceso** — Es la principal protección *preventiva*, que detecta archivos de programas potencialmente indeseables luego que se les accedan. No detecta *cookies*.

Detecciones — Configure la acción para 'Limpiar archivos automáticamente', y el escáner tomará la acción especificada por el archivo DAT. Entre dichas acciones pueden estar el cierre de procesos, la eliminación de .DLL inyectadas, la exclusión de archivos y/o la exclusión de claves de registro. En la mayoría de los casos de programas espías, el usuario final sólo se dará cuenta de que los archivos fueron excluidos porque son los más visibles. Si usted configura la acción para 'Excluir archivos automáticamente', el archivo detectado será excluido.

Exclusiones — Si MASE detecta un archivo que usted utiliza de forma legítima, es posible excluirlo de la detección.

- **Tareas de Exploración por Encargo**— Además de la exploración de archivos, usted puede configurar tareas de exploración por encargo para examinar el registro en busca de programas espías potencialmente indeseables, y la carpeta de *cookies*, en busca de *cookies* potencialmente indeseables. Se han incluido elementos de exploración por encargo para exploraciones de registro y de *cookies*.

Exploración del Registro — La exploración del registro detecta elementos relativos a programas espías en el registro, potencialmente indeseables, que no habían sido limpiados anteriormente.

Detecciones — Configure la acción para 'Limpiar archivos', y el escáner tomará la acción especificada por el archivo DAT. Eso puede incluir la limpieza o la exclusión de claves o valores del registro. Si se configura la acción para 'Excluir archivos', la clave o el valor del registro será excluido. Todas las otras acciones son tratadas como 'Seguir en la exploración'.

Exclusiones — Si MASE detecta un elemento de registro referente a un programa espía que usted utiliza de forma legítima, es posible excluirlo de la detección.

- **Exploración de Cookies** — La exploración de *cookies* detecta *cookies* potencialmente indeseables en las carpetas de *cookies*.

Detecciones — Si se configura la acción para 'Excluir archivos' o 'Transferir archivos para una carpeta', todo el archivo de *cookie* será excluido o transferido. La opción 'Limpiar archivos' es tratada de la misma manera que 'Excluir archivos'.

Exclusiones — Si MASE detecta un *cookie* que usted utiliza de forma legítima, es posible excluirlo de la detección.

El Equipo de Reacción a Emergencias Antivirus (AVERT) de McAfee incluye nuevas definiciones de PUP en los archivos DAT luego que se las identifican. Los investigadores de AVERT se encuentran en todo el mundo para producir archivos DAT actualizados diariamente para proteger a su empresa de la mejor forma posible.

Los clientes también pueden enviar muestras de PUP a AVERT para que se las incluyan en los archivos DAT diarios. Dicho proceso es sencillo y rápido, y permite que los clientes creen contenidos de PUP que, entonces, se puedan usar para eliminar ciertos PUP de su empresa. Para saber más sobre el envío de una muestra a AVERT, visite <http://vil.nai.com/vil/submit-sample.asp>.

Protección de Acceso

McAfee Anti-Spyware Enterprise hereda los recursos de protección de acceso del VirusScan Enterprise cuando se integra al VSE durante la instalación. Las reglas de protección de acceso impiden que programas malintencionados rompan varias reglas en su computadora, proporcionando, así, una considerable protección desde el primer día - protección contra amenazas desconocidas.

- **Protección de Archivos, Unidades compartidas y Carpetas**

Impide el acceso de lectura o grabación a archivos, unidades compartidas y carpetas. Este recurso puede ser muy útil en la prevención de invasiones, así como para impedir que las invasiones se propaguen durante brotes de virus. También se lo puede usar para tomar la iniciativa de evitar la ejecución de PUP desconocidos o crear una regla personalizada para aguardar hasta que MASE reciba la característica del ataque a través de una actualización del DAT. Por ejemplo, cree una regla que impida todas las lecturas y grabaciones en el directorio c:\Archivos de Programas\Kazaa y en sus subdirectorios. Eso impedirá, en la práctica, que Kazaa opere.

- **Bloqueo de Puertos**

Bloquee el tráfico entrante y saliente en puertos específicos y elija si desea registrar los intentos de acceso a los puertos bloqueados. Cuando usted bloquea un puerto, se bloquean tanto el acceso al Protocolo de Control de Transmisión (TCP) como el acceso al Protocolo de Datagramas del Usuario (UDP).

ePolicy Orchestrator

McAfee ePolicy Orchestrator es el núcleo de las Soluciones de Protección de Sistemas de McAfee. Permite que los administradores reduzcan el riesgo de sistemas fuera de control y no conformes, mantengan la protección

actualizada, configuren y fiscalicen las políticas de protección, y supervisen la situación de seguridad, 24 horas al día, desde una única consola centralizada que se puede ampliar a toda la empresa.

McAfee Anti-Spyware Enterprise es totalmente administrado a través del ePolicy Orchestrator¹. A través de la consola central del ePO, usted puede establecer políticas de exploración, protección de acceso y actualización para toda la empresa. Usted también puede generar informes que muestren el estado del sistema, las tasas de infección/brotos y ubicaciones, etc.

Documentación(en inglés)

- Notas de versión de McAfee Anti-Spyware Enterprise v8.0
- Manual del Módulo McAfee Anti-Spyware Enterprise

Otras Fuentes de consulta(en inglés)

- Manual de Instalación del VirusScan 8.0i
- Manual del Producto VirusScan 8.0i
- Manual de Configuración VirusScan 8.0i
- Manual del Producto ePO 3.5
- Manual de Generación de Informes del ePO 3.5
- Manual de Evaluación del ePO 3.5
- Manual de Instalación del ePO 3.5
- Tarjeta de Consulta Rápida del ePO 3.5

Sistema necesario

Verifique si su servidor y/o su estación de trabajo cumplen los requisitos de sistema antes de empezar el proceso de instalación.

Software

McAfee VirusScan Enterprise, versión 7.1 u 8.0i (se recomienda la versión 8.0i)

Estación de Trabajo necesaria

Windows NT 4, Windows 2000/2003 o Windows XP

Requisitos del Servidor

Windows NT 4 Server, Windows NT 4 Terminal Server, Windows 2000 Server, Windows 2000 Advanced Server, Windows 2000 DataCenter Server, Windows Standard Server 2003, Windows Enterprise Server 2003 o Windows Web Server 2003

Prueba de Productos Anti-Spyware

Hoy día, existen varios productos anti-spyware para uso particular, para pruebas y para empresas. A diferencia del ya maduro mercado de antivirus, donde los fabricantes estandarizaron las nomenclaturas y comparten colecciones para proteger de la forma más amplia posible sus clientes, cada producto anti-spyware posee una base de datos cerrada y utiliza esquemas de nomenclatura propios. los programas espías (no sólo los programas malintencionados, sino también *adware*, chistes, etc.)¹ tienden a ser más complejos que los programas malintencionados 'tradicionales' por el simple número de elementos de registro, archivos, mecanismos de auto-protección y otras herramientas que utiliza. Dichos factores dificultan que las empresas que desean evaluar productos anti-spyware comparen unos con otros.

A continuación, este manual presenta una metodología de Prueba de Productos Anti-Spyware de la forma más objetiva posible, mostrando las etapas para eliminar la preferencia de un producto en detrimento de otro. Reconoce la existencia de los aspectos que se deben evaluar para determinar cómo protege un producto anti-

¹ En este documento, se utilizará el término Programa Potencialmente Indeseable, o PUP, para indicar las diversas categorías de programas espías, *adware*, etc.

spyware a la productividad y los recursos de computación e información de su empresa.

Primeramente, se necesita evaluar la tecnología subyacente del producto anti-spyware. Ese es el componente que no cambiará a lo largo del tiempo y que limita o define la eficacia del producto.

En segundo lugar, usted debe examinar el elemento dinámico: la base de datos de programas indeseables de un cierto producto anti-spyware y los procesos, los recursos y la capacidad del proveedor de actualizar su base de datos regularmente.

Evalúe la Tecnología Subyacente

La base tecnológica detrás de un producto anti-spyware determina su eficacia y sus recursos de largo plazo, además de los costos de poseerlo y administrarlo. Al analizar la tecnología de un producto anti-spyware, tenga en cuenta las siguientes cuestiones.

- **¿La seguridad de la información es muy esencial para su organización?**
McAfee Anti-Spyware Enterprise posee verdaderos recursos preventivos de acceso para evitar que los PUP se instalen en una computadora en primer lugar. Otros productos ofrecen protección reactiva “de tiempo real”, que limpia un PUP tras detectar su instalación.

Ambos enfoques funcionan bien en la exclusión de amenazas conocidas, pero el último es más arriesgado. Durante el período entre la instalación de un PUP y su detección por el producto anti-spyware, existe la posibilidad de descargar otros PUP desconocidos o transmitir su información confidencial a Internet.

- **¿Cómo identifica el producto anti-spyware a los programas espías?**
Algunos productos utilizan sólo los nombres de los archivos. Los beneficios de dicha modalidad son obvios, facilitando la creación rápida de una amplia base de datos y la realización de rápidas exploraciones del sistema. Sin embargo, es muy propensa a falsos positivos, además de ser fácil engañarla mediante el cambio del nombre del archivo.

Algunos productos utilizan sólo *hashes* MD5 para identificar el contenido de los archivos ejecutables de un PUP. Los *hashes* también permiten exploraciones rápidas del sistema y son más confiables que la comparación de nombres, pero los autores de PUP pueden, asimismo, engañarlos con el cambio aunque sea de un solo octeto en sus archivos.

Algunos productos, incluso McAfee Anti-Spyware Enterprise, realizan exploraciones profundizadas de archivos para identificar a los PUP. La exploración profundizada es más lenta cuando se realiza por encargo, pero usted puede estar seguro de los resultados. Además, debido a que las exploraciones también buscan virus, el tiempo total de exploración para ambas funciones no es mucho más largo que el tiempo de exploraciones separadas contra virus y programas espías.

- **¿Está dispuesto a aceptar el reinicio de las máquinas para garantizar la limpieza total?**
Muchos productos anti-spyware son capaces de identificar procesos indeseables en la memoria de uso, pero no todos son capaces de descargar las DLL sin que el sistema necesite reinicio o que sea necesario cerrar la aplicación. Si su entorno exige un tiempo máximo de actividad y muy poca interrupción de computadoras y usuarios, dicha capacidad le será más importante. Debido a que utiliza tecnología AV líder de mercado, McAfee Anti-Spyware Enterprise es capaz de descargar más DLL sin exigir el cierre de las aplicaciones o el reinicio de la computadora.
- **¿Cómo brinda protección el producto anti-spyware contra las amenazas desconocidas?**
Los mejores productos anti-spyware poseen alguna forma de protección o blindaje de acceso para proteger archivos y directorios esenciales de su computadora contra comprometimientos. Como ocurre con la detección de amenazas conocidas, dichas funciones pueden ser preventivas o reactivas.

La protección preventiva de acceso impide que los PUP realicen ciertas etapas, tales como modificar archivos del *host*, ser ejecutados en directorios temporales, iniciar comunicaciones con el mundo externo a través de ciertos puertos y otros archivos. Las reglas de protección de acceso de McAfee Anti-Spyware Enterprise y del VirusScan Enterprise son ejemplos de dicha capacidad preventiva. Los blindajes reactivos supervisan el comportamiento de las aplicaciones y son activados cuando se rompe un conjunto de reglas. La diferencia está en la prevención de un comportamiento o en la reacción a un hecho que ya ocurrió.

Tenga en cuenta toda la solución anti-spyware para determinar cuál protección o blindaje ofrece y la extensión de su capacidad: ¿Es posible incluir reglas propias? ¿Es posible excluir de la exploración los programas deseados?

- **¿Cómo se puede administrar el producto anti-spyware en su organización?**
Con el aumento del tamaño de la organización, también aumenta la importancia de una administración centralizada. Al pensar en una solución anti-spyware, no piense sólo en el componente de *desktop*. Piense también en su capacidad de administrar dichos agentes de *desktop*. ¿Qué recursos tiene la solución para distribución y actualización a distancia de agentes y para emisión de informes de detección y limpieza? ¿Es posible crear, distribuir y fiscalizar las políticas anti-spyware? Los clientes de McAfee cuentan con todos esos recursos de administración a través de McAfee Protection Pilot (para empresas pequeñas/medianas) o de McAfee ePolicy Orchestrator (para grandes empresas).
- **¿Cuál es el costo?**
Muchos de los productos contra programas espías del mercado son gratis o para prueba por tiempo limitado (*shareware*). Eso es adecuado, pues fueron lanzados como productos para el mercado consumidor.

Es fácil presuponer que un bajo costo de licenciamiento se refleje en un bajo costo total. Sin embargo, se necesita evaluar los costos de operación que están asociados al 'gratis'. Tenga en cuenta elementos tales como el costo de distribución, actualización y recopilación de informes, entre otros. Además, tenga en cuenta los costos del soporte local y de la pérdida de productividad mientras su personal limpia y reinicia las computadoras.

Evalúe el Elemento Dinámico: Contenido de las actuales

Un producto anti-spyware debe contar con recursos para detectar y proteger contra amenazas desconocidas y conocidas. Las amenazas conocidas son aquellas para las cuáles el equipo de investigación del fabricante creó detecciones (características, *drivers* heurísticos, *hashes* MD5, tablas de nombres). Además de ofrecer detección contra PUP, el proveedor distribuye instrucciones que le permiten al producto anti-spyware limpiar o eliminar los PUP de su computadora.

Los PUP son productos complejos, a menudo estrechamente integrados a su sistema operativo o a sus aplicaciones, que utilizan diversas tácticas para escapar a la detección y exclusión. Algunos PUP se comportan bien y ofrecen *scripts* de desinstalación. Sin embargo, muchos de ellos crean varias claves de registro con muchos valores, cargan procesos de observación en la memoria para recargarse (o descargar nuevamente) entre ellos, o imitar archivos del sistema operativo. A menudo, los PUP también descargan desde la Web otras aplicaciones, frecuentemente nuevas y desconocidas, además de simplemente instalarse.

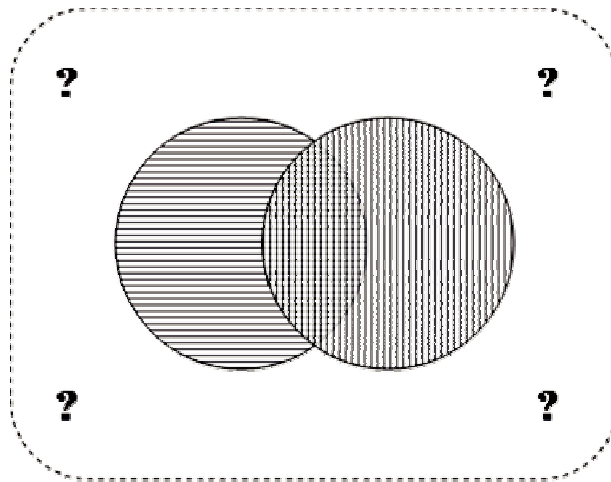
Por dichos motivos, además de la relativa juventud del mercado de anti-spyware, a menudo es difícil que un único producto anti-spyware limpie cada uno de los componentes de los PUP de su computadora. Todos los proveedores de anti-spyware dependen de la comunidad de usuarios para recibir muestras de PUP sospechosos para aumentar sus bases de datos. McAfee está asumiendo la delantera, trabajando con otros proveedores para crear un consorcio de reparto de muestras, nomenclaturas comunes y cuentas, así como el que ya existe en el mercado más maduro de los antivirus.

Metodología Objetiva de Prueba

Panorama

Si hoy en día ningún producto anti-spyware logra, por sí mismo, detectar y eliminar todos los PUP, ¿cómo es posible probar objetivamente la eficacia de cualquiera de ellos?

Una metodología común es comprometer una computadora con el mayor número posible de PUP y, enseguida, ejecutar varios programas anti-spyware en secuencia en la computadora. Independientemente del producto que se ejecute primeramente, el segundo, casi siempre, encontrará algún conjunto de PUP que el primero no encontró. Si, enseguida, usted ejecuta un tercer producto anti-spyware en la misma computadora, podrá detectar otro conjunto más de PUP que los dos primeros no lograron detectar.



Dos productos anti-spyware detectan algunos PUP iguales, pero ¿y los que dejan ambos de detectar?

Es tentador presuponer que el segundo producto anti-spyware habría detectado todo lo que el primero encontró, más lo que encontró él y no encontró el primero. Eso es una trampa. Según muestra el diagrama arriba, los recursos de detección de cualquier pareja de productos anti-spyware se sobrepondrá, pero cada uno de ellos detectará elementos que el otro no detectó.

Al comparar productos anti-spyware de igual para igual, es necesario realizar -al menos- dos pruebas. Cree su entorno de prueba y ejecute el Producto A; enseguida, ejecute el Producto B. Repita la prueba con el Producto B, después con el Producto A. Compare todos los *logs*. Así, usted tendrá una visión más equilibrada de la capacidad de detección y exclusión de cada uno de los productos.

El mejor método de comparación de productos anti-spyware es usar una herramienta objetiva para cuantificar y detallar el estado de su computadora (archivos, registro) antes de intentar comprometerla, aplicar un único producto anti-spyware y, después, tomar otra "instantánea" del sistema y compararla con el original. Las diferencias entre dichos informes muestran exactamente qué hicieron los PUP instalados con su computadora y cuántos de dichos PUP fueron evitados, eliminados o corregidos por el producto anti-spyware.

Una prueba objetiva también comparará la protección preventiva/reactiva y los recursos de limpieza 'tras la incidencia' del producto anti-spyware. Las 'recetas' dadas a continuación sugieren un plan que usted puede adoptar según sus necesidades y su entorno.

Herramientas de Toma de "Instantáneas"

Existen varios productos que toman "instantáneas" del antes y después de los componentes esenciales del sistema operativo Windows y del sistema de archivos para exponer los efectos de la instalación de un software.

Dos ejemplos son el InctrI5 (de PC Magazine)² y el Tracker (de Evans Programming)³

Obtención y Retención de Muestras

Existen varias fuentes en Internet que le pueden indicar dónde 'adquirir' programas potencialmente indeseables, por ejemplo: <http://spywarewarrior.com/asw-test-guide.htm#test>. Observe que dichas pruebas fueron realizadas con diversos productos anti-spyware de uso personal a fines del 2004. Por lo tanto, el contenido está un poco obsoleto, pero la metodología es sólida y reproducible. Naturalmente, usted también puede navegar audaciosamente por sitios donde normalmente no navegaría e intentar recopilar muestras, quizás siguiendo las transferencias con un "sniffer de paquetes" para identificar las fuentes de contenido realmente ricas.

Independientemente del método elegido, anote los sitios Web desde donde descargó las muestras de PUP. Eso será importante si desea probar otros productos posteriormente y si cree que MASE dejó de detectar alguna de las muestras. Después, usted puede enviar las URL junto con el residuo de la muestra al sistema WebImmune de los laboratorios AVERT de McAfee. Allí, AVERT procederá a analizar los PUP y actualizar los archivos DAT de MASE para ampliar la protección.

Prueba de la Protección Preventiva

Pruebe la capacidad de McAfee Anti-Spyware Enterprise de impedir que los PUP se instalen e instalen otros programas en una computadora. Esta prueba indica la capacidad del producto para proteger sus sistemas y su información, manteniendo la computadora constantemente limpia.

Usted debe ejecutar esta prueba en las configuraciones predefinida y ajustada. Por ejemplo, McAfee Anti-Spyware Enterprise puede ofrecer una considerable protección preventiva con la configuración de reglas de protección de acceso que bloquean la ejecución de programas en el directorio temporal o bloquear alteraciones en los archivos de los *hosts*. Algunas reglas de protección de acceso pueden afectar a la velocidad de aplicaciones desarrolladas internamente o personalizadas. Seguramente usted va a querer probar su entorno para encontrar una combinación adecuada de protecciones de acceso y exclusiones que le brinden una seguridad ideal. Lea la documentación del VirusScan Enterprise para saber más sobre las reglas predefinidas de protección de acceso y cómo crear sus propias reglas.

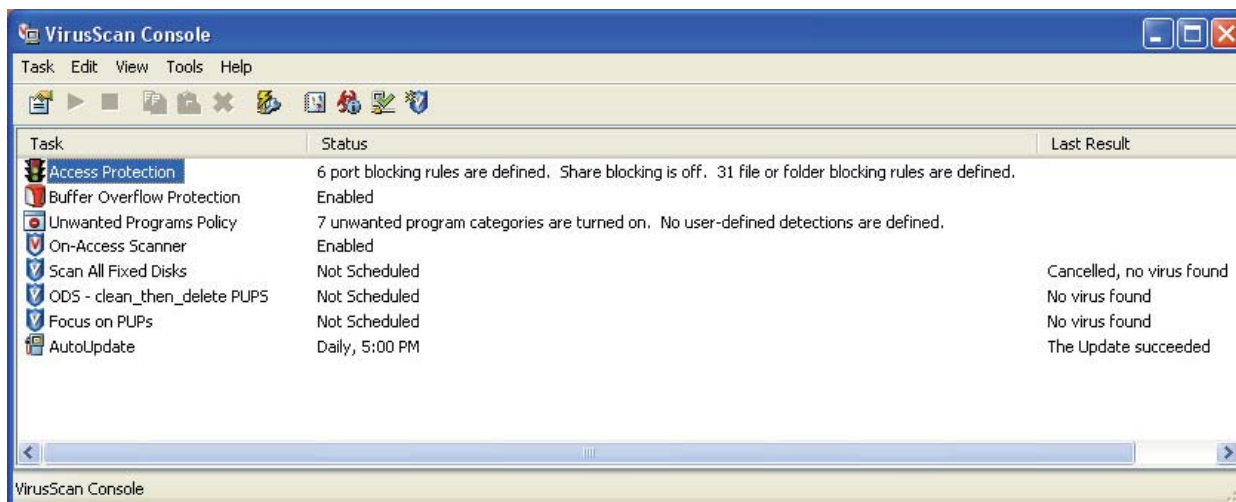
Etapas

1. Empiece con una computadora limpia (por ejemplo, una instalación estándar del Windows que nunca fue conectada con Internet).
2. Instale un producto de toma de instantáneas como los indicados más arriba.
3. Extraiga una imagen del sistema en este punto para que usted pueda ejecutar pruebas subsecuentes desde el estado inicial exacto.
4. Instale MASE y actualice sus archivos DAT para garantizar que la prueba será realizada con el contenido más actualizado.⁴
5. Abra la Consola del VirusScan y pulse dos veces en 'Access Protection' (*Protección de Acceso*).

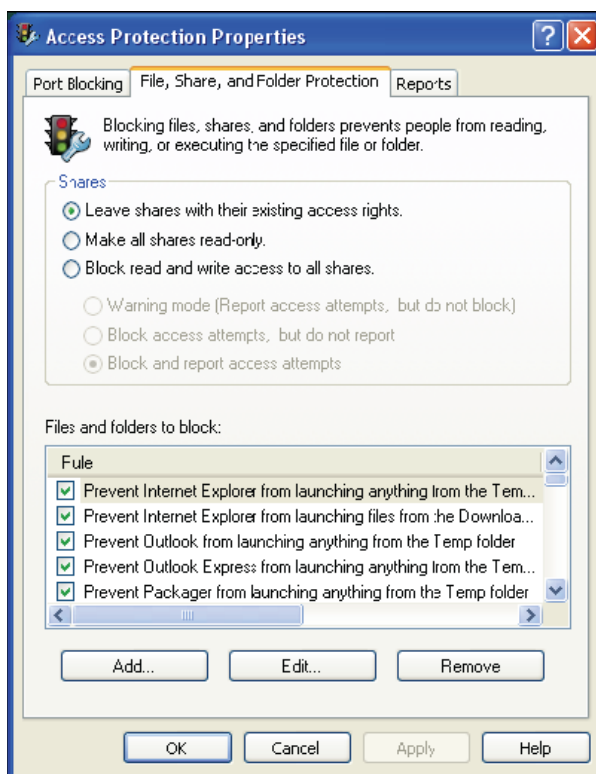
² <http://www.pcmag.com/article2/0,4149,25126,00.asp>

³ <http://www.evansprogramming.com/tracker.asp>

⁴ Para obtener los contenidos más actualizados de McAfee, descargue el archivo DAT diario más reciente. Usted también puede descargar el archivo DAT beta más reciente de McAfee en el sitio de la Biblioteca de Información sobre Virus - VIL (<http://vil.nai.com/vil/averttools.asp>). Los DAT Beta permiten que se vean anticipadamente los *drivers* contra programas mal intencionados antes de que aparezcan en los archivos DAT lanzados oficialmente.



6. En la ventana 'Access Protection Properties' (*Propiedades de la Protección de Acceso*), seleccione la guía 'File, Share, and Folder Protection' (*Protección de Archivos, Unidades Compartidas y Carpetas*).



Seleccione todas las reglas que están en la lista 'Files and folders to block' (*Archivos y carpetas por bloquear*). VirusScan / MASE vienen con varias de dichas opciones desactivadas porque algunas empresas trabajan con aplicaciones desarrolladas internamente o personalizadas que pueden ser afectadas por algunas de esas reglas. En general, los clientes activan todas las reglas en un entorno de pruebas y, después, desactivan las que causan algún conflicto. Para los fines de prueba de anti-spyware, vale el mismo procedimiento.

7. Quizás usted quiera crear sus propias reglas de protección de acceso, por ejemplo, para evitar lecturas/grabaciones en el archivo de *hosts* o en otros archivos/carpetas que quiera restringir. Para

eso, pulse en el botón 'Add' (*Añadir*) para añadir una nueva regla.

Rule for File/Share/Folder Blocking

Rule Name
New Rule

What to block
Specify processes affected by this rule. Type a specific process name or * for all processes. Type 'System:Remote' for incoming network processes.
*

File or folder name to block. Wildcards are allowed.
Browse file
Browse folder

File actions to prevent
 Read access to files
 Write access to files
 Files being executed
 New files being created
 Files being deleted

How to react
 Warning mode (Report access attempts, but do not block)
 Block access attempts, but do not report
 Block and report access attempts

OK Cancel

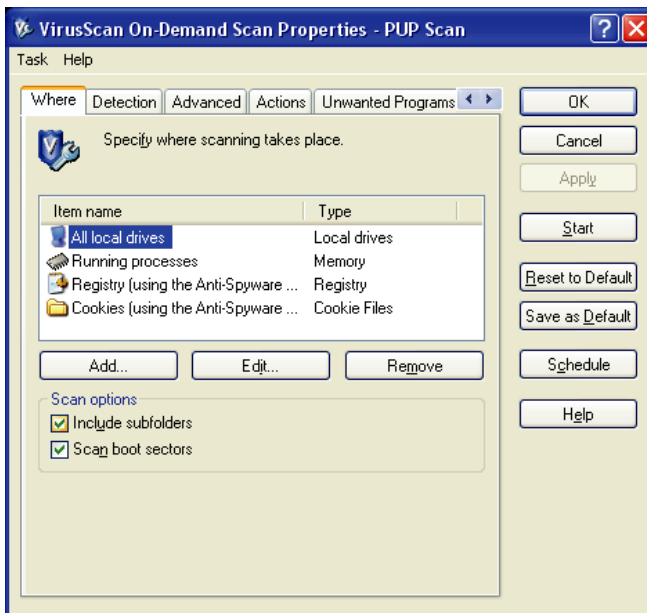
- a. Atribuya un nombre a la regla
 - b. Identifique los procesos que desea afectar con esta regla. Un asterisco indica "todos los procesos".
 - c. Navegue hasta el archivo (por ejemplo, el archivo de *hosts*) que desea bloquear.
 - d. Seleccione las acciones que desea restringir (por ejemplo, lectura, grabación, ejecución)
 - e. Especifique la reacción: avisar, bloquear y avisar, o bloquear y no avisar.
 - f. Pulse en OK para guardar la nueva regla.
8. Tome una "instantánea" de sus sistemas operativo y de archivos.
 9. Comprometa la computadora, iniciando Internet Explorer y descargando algunos PUP desde Internet.
 10. Deje que pasen algunos minutos. Durante ese tiempo, los PUP descargados pueden intentar descargar e instalar otras aplicaciones. Cuando cesen las actividades de disco y de red, siga adelante.
 11. Examine el *log* de OAS para identificar los PUP que MASE bloqueó.
 12. Tome una segunda "instantánea" del sistema. Analice el estado del sistema respecto a la primera instantánea.

Prueba de la Protección Reactiva

Pruebe la capacidad de McAfee Anti-Spyware Enterprise de limpiar los PUP de una computadora ya comprometida. Esta prueba indica la capacidad del producto de limpiar una computadora que ya fue comprometida por usuarios que navegan en sitios Web que descargan PUP.

Etapas

1. Empiece con una computadora limpia (por ejemplo, una instalación estándar del Windows que nunca fue conectada con Internet)
2. Instale un producto de toma de instantáneas como los indicados más arriba.
3. Extraiga una imagen del sistema en este punto para que usted pueda ejecutar pruebas subsecuentes desde el estado inicial exacto.
4. Instale MASE y actualice su base de datos para garantizar que se está realizando la prueba con el contenido más reciente. Verifique si el producto está desactivado, de manera que no impida, ni limpie nada.
5. Cree una exploración por encargo que analice no sólo los archivos, sino también el registro y los *cookies*.



6. En la guía 'Actions' (*Acciones*), seleccione 'Clean Files' (*Limpiar Archivos*) como la acción principal y 'Delete Files' (*Excluir Archivos*) como la acción secundaria
7. Tome una "instantánea" de sus sistemas operativo y de archivos.
8. Comprometa la computadora, iniciando Internet Explorer y descargando algunos PUP desde Internet.
9. Deje que pasen algunos minutos. Durante este tiempo, los PUP descargados pueden intentar descargar e instalar otras aplicaciones. Cuando cesen las actividades de disco y de red, siga adelante.
10. Tras comprometer la computadora, reiniciela y reinicie Internet Explorer antes de intentar la exploración y exclusión de los PUP. Eso garantiza que los PUP estén totalmente instalados y funcionando: algunos de ellos activan otros procesos cuando se inicie Windows, y otros necesitan del IE para que se carguen. Eso también prueba la capacidad de MASE de excluir PUP activos.
11. Active MASE y ejecute la exploración por encargo creada en la etapa 5 más arriba, para detectar y excluir los PUP descargados. Verifique los resultados de la exploración en el *log*.
12. Tome una segunda "instantánea" del sistema. Analice el estado del sistema con respecto a la primera instantánea.

Evaluación de los Resultados

Al examinar las instantáneas del sistema tras cada ciclo de prueba visto más arriba, es útil establecer metas y parámetros para que usted pueda comparar la capacidad de McAfee Anti-Spyware Enterprise y de otros productos anti-spyware de proteger su sistema, además de clasificar el riesgo que representan los elementos que no detectó el producto.

No existe ninguna norma para cuantificar qué es lo que detecta un producto anti-spyware. Algunos individualizan cada clave de registro, valor de clave, archivo, directorio y otra información creada por los PUP en su sistema. Otros cuentan sólo los nombres de los PUP, mientras otros quedan entre uno y otro. Una categorización útil para la cuenta de lo que restó es la siguiente:

- El PUP en sí. ¿Cuántos PUP enteros o parciales dejó para atrás el producto anti-spyware en su computadora de prueba?
- Si el producto anti-spyware eliminó sólo parcialmente a los PUP, identifique qué es lo que dejó para atrás:
 - Archivos
 - Carpetas
 - Claves de registro (los valores son menos importantes - si el producto anti-spyware elimina a la clave, los valores asociados a ella también serán eliminados. La cuenta de valores es una forma artificial de aumentar el número de 'detecciones'.)

Un parámetro útil que se puede aplicar a dichos 'restos' es el siguiente:

Rojo	.exe, .dll, .com, <i>scripts</i> u otros códigos ejecutables que puedan recargar el PUP o causar otros daños.
Amarillo	Elementos benignos tales como claves de registro, carpetas, archivos de texto u otros códigos no ejecutables que deberían haber sido limpios, pero que no representan una amenaza a la seguridad de su computadora o de su información.
Verde	Elementos benignos tales como archivos temporales, archivos en la caché del IE, etc. dejados para atrás por el sistema operativo o instalador de <i>software</i> , pero que no representan partes del PUP en sí.

Quizás usted quiera aplicar una clasificación numérica a las categorías Rojo, Amarillo y Verde. Quizás también quiera aplicar un multiplicador para distinguir entre los elementos asociados a un PUP que el producto anti-spyware dejó totalmente de detectar y los elementos restantes tras una exclusión parcial.

Envío a AVERT de Muestras que No Fueron Detectadas

Para ayudar a mejorar los recursos de protección de cada producto anti-spyware evaluado, envíe muestras y *logs* de todos los PUP que no fueron detectados a AVERT de McAfee, para que se puedan actualizar los archivos DAT. Además de ser bueno para la comunidad de usuarios, usted también gana otra forma de evaluar a McAfee: ¿fue fácil enviar las muestras? ¿Con qué frecuencia la empresa añade nuevos PUP a los DAT?

McAfee acepta envíos de programas malintencionados y PUP por *e-mail* o por el sistema WebImmune. En la Biblioteca de Información de Virus (VIL), puede encontrar información sobre cómo enviar muestras:

<http://vil.nai.com/vil/default.asp>.

Recursos

Para saber más sobre los varios métodos usados por los fabricantes de productos anti-spyware para contar programas indeseables en sus bases de datos y en su computadora, contacte con su Gerente de Cuenta de McAfee y pídale el siguiente *White Paper* '*Cuenta de Detecciones de Programas Espías*'.

Para acelerar sus pruebas, usted puede utilizar un programa de PC virtual como Microsoft Virtual PC (<http://www.microsoft.com/windows/virtualpc/default.msp>). Dicho tipo de herramienta ahorra el tiempo de reconfiguración, en comparación con la reinstalación de toda la PC.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054

McAfee y/o otras marcas mencionadas en este documento son marcas comerciales, ya sean registradas o no, de McAfee, Inc. y/o de sus afiliadas en EE.UU. y/o en otros países. El color rojo de McAfee usado para denotar la seguridad es una marca distintiva de los productos que llevan la marca McAfee. Todas las otras marcas comerciales, ya sean registradas o no, mencionadas en este documento pertenecen exclusivamente a sus respectivos titulares. © 2005 McAfee, Inc. Todos los derechos están reservados.

mase_evalguide_001_0605