

Índice

I. Asalto a la empresa: las nuevas amenazas requieren nuevas estrategias	2
Más amenazas + más dispositivos = mayor complejidad	2
La mayor amenaza actual: la “ventana de vulnerabilidad”	3
II. La protección preventiva de McAfee® frente a las amenazas: una tecnología avanzada para salvaguardar las empresas.....	4
Seis meses antes del ataque: evaluación de vulnerabilidad frente a virus y bloqueo de clientes ..	4
Tres meses antes de un ataque: detección avanzada de nuevas amenazas y protección frente a mensajes publicitarios no deseados (spam)	5
Momento del ataque: protección integrada en múltiples frentes	7
III. La protección preventiva en acción	8
Paso 1: detección de la amenaza	8
Paso 2: defensa frente a un ataque	9
Paso 3: atajar la propagación de la amenaza	9
Paso 4: cierre de la ventana de vulnerabilidad.....	9
Resumen	9
Acerca de McAfee Security	10
Notas finales	10

I. Asalto a la empresa: las nuevas amenazas requieren nuevas estrategias

El gusano SQLSlammer de enero de 2003, capaz de inhabilitar servidores de Internet y redes corporativas de todo el mundo, ilustra a la perfección la velocidad y la virulencia con la que arremeten las amenazas actuales contra la seguridad. Este gusano se sirvió de un fallo de seguridad de Microsoft documentado en MSDE/SQL Server 2000 para obtener autorizaciones remotas que le permitieron infectar al ordenador personal anfitrión. Una vez infectado éste, el gusano intentó infectar rápidamente a otros equipos anfitriones enviándose a sí mismo a direcciones IP aleatorias. Aunque carecía de carga útil destructiva, el gusano generó un intenso tráfico en la red que causó estragos en todo el mundo:

- en Estados Unidos, Bank of America Corp. reconoció que, en la mayoría de sus 13.000 cajeros automáticos, los clientes no pudieron realizar operaciones como resultado de la acción del gusano;
- el gusano bloqueó casi todos los servicios de Internet en Corea del Sur, donde siete de cada diez personas son usuarios on line. KT Corp., el mayor proveedor de acceso a Internet de Corea del Sur resultó inhabilitado y otros sitios web quedaron desconectados de la red;
- en el momento álgido del ataque en Estados Unidos, alrededor del 20 % del tráfico de datos remitidos a través de Internet se perdieron en tránsito, lo que supone una proporción al menos diez veces superior a la normal.

En los últimos años, además de gusanos como SQLSlammer, se han registrado daños graves debidos a la acción de amenazas mixtas, que combinan la malicia tradicional de los virus vinculados al correo electrónico con nuevas capacidades asociadas a las redes, preparadas para buscar y encontrar grietas en la seguridad de las redes de las empresas y provocar daños añadidos como los asociados a los ataques de denegación de servicio, bloqueo de servidores y vulnerabilidad o en el núcleo o "raíz" de los ordenadores. Las amenazas combinadas, como CodeRed, Klez, Nimda y otros, golpean con una velocidad endiablada y reúnen condiciones para eclipsar de inmediato la destrucción provocada por anteriores generaciones de virus informáticos.

Más amenazas + más dispositivos = mayor complejidad

Por desgracia, SQLSlammer es sólo una de las más de doscientas nuevas amenazas que aparecen cada mes, que vienen a sumarse al total de 63.000 o más amenazas existentes en la actualidad. Además de las amenazas "tradicionales" vinculadas a los virus, actúan ahora gusanos en Internet como SQLSlammer, envíos por correo masivos, ataques distribuidos de denegación de servicio, troyanos de puerta trasera y zombis. Estas amenazas no sólo son más inteligentes, sino también más rápidas. En tiempos, a un virus informático le llevaba semanas, o incluso un mes, alcanzar una circulación generalizada; ahora, amenazas como SQLSlammer se sirven de las redes corporativas mundiales y de Internet para propagarse en todo el planeta en cuestión de horas.

La Ventana de "vulnerabilidad"

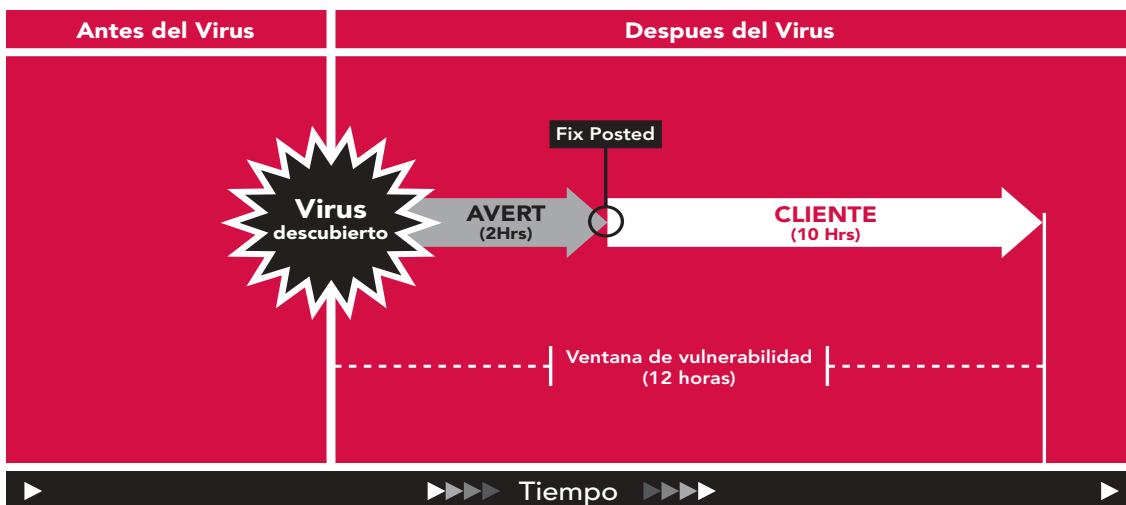


Figura 1: las soluciones de McAfee ayudan a las empresas a reducir al mínimo la ventana de vulnerabilidad después del ataque de una amenaza para la seguridad, aplicando medidas tanto preventivas como reactivas.

Las dificultades en materia de seguridad se ven agravadas por la proliferación de equipos utilizados en la empresa. La reciente explosión de dispositivos inalámbricos dará lugar a la próxima plataforma principal de multiplicación de amenazas para la seguridad. Mientras que se prevé que el censo de ordenadores personales de sobremesa se mantendrá estable, los dispositivos inalámbricos integran la categoría de nuevos equipos de más rápido crecimiento, y deben ser gestionados y garantizados, lo que eleva sustancialmente la carga soportada por las empresas en materia de seguridad. Estos dispositivos inteligentes ejecutan servicios IP, ofrecen acceso a Internet y facilitan el acceso a la red corporativa. Además, brindan a los usuarios la posibilidad de conectarse desde una ubicación remota a otros dispositivos y redes. Estos equipos, así como los PDA's habilitados para una prestación inalámbrica, son intrínsecamente menos seguros, ya que se mantienen al margen de las salvaguardias tradicionales de las redes. A medida que aumente el volumen de datos corporativos de valor que transportan, las redes y los dispositivos inalámbricos se convertirán en un objetivo cada vez más atractivo para los creadores de amenazas malintencionadas. Además, de cara al futuro, la telefonía IP o los servicios integrados de datos, voz y vídeo, auguran un crecimiento sustancial de este tipo de dispositivos a partir de 2004. Por último, la creciente popularidad de los servidores de PC de gama baja alimenta las dificultades en cuanto a seguridad. Estos equipos son cada vez más frecuentes en las empresas, ya que, dispuestos en grupos, ejecutan los sistemas operativos Windows y Linux y sustituyen a los servidores UNIX, de mayor precio y tamaño. Tal situación influye ya en

el entorno de seguridad de las empresas. En este sentido, Microsoft hizo pública la existencia de más de setenta vulnerabilidades en 2002, una de las cuáles fue aprovechada por SQLSlammer para actuar. Este potente gusano pone de manifiesto el potencial de daño que existe ya en el segmento de la gama baja.

La mayor amenaza actual: la "ventana de vulnerabilidad"

Juntos, estos tres factores (mecanismo de ataque combinado, creciente velocidad de los ataques, y cambio permanente del entorno de redes y dispositivos) dan lugar a la "ventana de vulnerabilidad" (figura 1), o período de tiempo durante el que una empresa es susceptible de recibir un ataque y de sufrir los daños consiguientes. Dicha ventana se abre cuando se crea la amenaza, y no se cierra hasta que todos los sistemas de la red quedan protegidos de ella. En el contexto de una propagación de programas malintencionados de una rapidez sin precedentes, debe asegurarse un número de dispositivos cada vez mayor, lo que obliga a superar los límites en cuanto a la utilización recursos vinculados a las TI, sometidos ya a una considerable presión. Como consecuencia, a menudo, la ventana de vulnerabilidad puede permanecer abierta durante días, lo que eleva en gran medida las posibilidades de infección, la alteración de operaciones, los gastos de desinfección asociados y la pérdida de ingresos debida al bloqueo de recursos esenciales para el desempeño de determinadas funciones.

McAfee Security Proactive Threat Protection

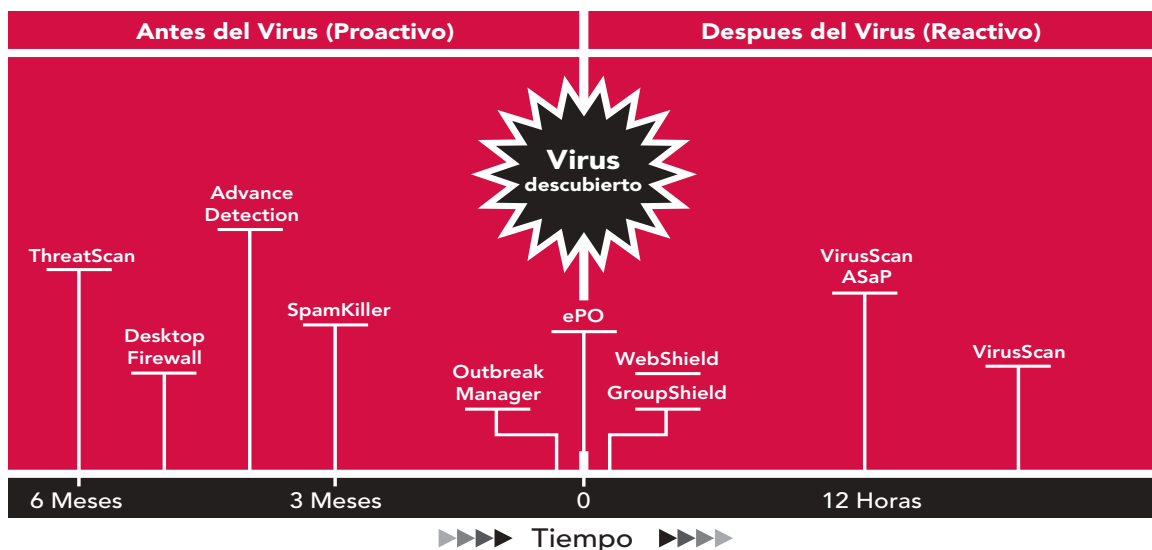


Figura 2: la protección preventiva frente a amenazas de McAfee Security, cuando se aplica en función de la ventana de vulnerabilidad, puede reducir drásticamente los daños infligidos por virus y otras amenazas malintencionadas para la seguridad.

A medida que las empresas se ven sometidas a ataques de mayor envergadura, se requieren planteamientos más eficaces y preventivos, puesto que las medidas reactivas tradicionales son insuficientes. McAfee Security se ha comprometido a ayudar a las empresas a reducir la ventana de vulnerabilidad por medio de tres vías:

- reducir preventivamente la velocidad de los ataques;
- reducir preventivamente la posibilidad de éxito de los ataques;
- reducir preventivamente la exposición a los ataques.

En la figura 2 se ilustra el modo en que McAfee Security se sirve tanto de una preparación a largo plazo como de soluciones inmediatas posteriores al ataque para cerrar la ventana de vulnerabilidad en el menor plazo posible.

En resumen, mediante la integración de productos de seguridad líderes del sector, la gestión de políticas de seguridad, la asistencia técnica y los servicios expertos, el planteamiento dinámico de McAfee Security ofrece un mecanismo de defensa caracterizado por su cohesión y exhaustividad, frente a las amenazas para la seguridad que aterrorizan a la empresa actual.

II. La protección preventiva de McAfee frente a las amenazas: una tecnología avanzada para salvaguardar las empresas

La protección preventiva fundamenta la estrategia integrada de McAfee Security encaminada a salvaguardar las empresas respecto a nuevas amenazas con la mayor anticipación posible, y a ayudar a los gestores de seguridad de las TI a cerrar con rapidez la ventana de vulnerabilidad cuando atacan tales amenazas.

En los apartados siguientes se ofrece una visión general detallada de las diversas fases de la estrategia de protección preventiva frente a amenazas de McAfee Security, conforme a lo descrito anteriormente en la figura 2, así como de los productos asociados utilizados en cada fase.

Seis meses antes del ataque: evaluación de vulnerabilidad frente a virus y bloqueo de clientes

Al plantearse la seguridad de una empresa, el primer axioma que debe abordarse alude a la necesidad de medir las amenazas para hacerles frente; antes de establecer una política de seguridad, deben recogerse datos esenciales acerca de todos los equipos de la red, y ha de evaluarse su vulnerabilidad a un ataque. De estas tareas se ocupa McAfee ThreatScan™, que detecta de manera preventiva la

vulnerabilidad de ordenadores de sobremesa y servidores frente a virus. Ayuda a los administradores a detectar los dispositivos, aplicaciones y sistemas operativos vulnerables a los virus, infectados o desprotegidos.

ThreatScan, único en el campo de la seguridad de redes, protege preventivamente éstas frente a amenazas combinadas, sirviéndose de firmas actualizadas y de exploraciones de vulnerabilidad frente a virus programadas. Sin que deba mediar la intervención de un experto en seguridad, ThreatScan lleva a cabo exploraciones preventivas e informa de los equipos desprotegidos, no gestionados, infectados y vulnerables a los virus. Con ello, ayuda a las empresas a alcanzar niveles superiores de protección antivirus y de cumplimiento de las políticas formuladas, al identificar dispositivos, sistemas operativos y aplicaciones vulnerables a los virus y descubrir equipos desprotegidos o aislados que abren la puerta a las infecciones de la red.

Con ThreatScan, las empresas pueden pasar de reaccionar a las infecciones a tomar la iniciativa en la prevención frente a amenazas combinadas, contribuyendo así a reducir la ventana de vulnerabilidad. ThreatScan permite la identificación preventiva de una amplia gama de elementos de vulnerabilidad en materia de seguridad, entre los que figuran:

- equipos susceptibles;
- aplicaciones susceptibles;
- equipos infectados;
- amenazas para la seguridad debidas a virus específicos designados;
- amenazas para la seguridad por clase general de vulnerabilidad explotable.

Antes de la aplicación de ThreatScan, cada dispositivo de la red debía auditarse físicamente para comprobar su vulnerabilidad. Ciertos métodos y herramientas requieren amplios conocimientos técnicos en materia de seguridad para detectar los focos de problemas en la red. Los administradores se encuentran entre la espada y la pared: andan escasos de tiempo, pero tienen que prevenir los costes de las infecciones.

ThreatScan permite la programación de las exploraciones y la comprobación de los equipos anexas a la red utilizando los agentes instalados gestionados mediante McAfee ePolicy Orchestrator™ (ePO™). Aplicando esta herramienta, los agentes de ThreatScan pueden instalarse con facilidad en puntos estratégicos de la red corporativa, haciendo posible una sencilla inspección a distancia de los equipos nuevos.

ePolicy Orchestrator es la plataforma de gestión de McAfee Security para desempeñar en el conjunto de la empresa las tareas de supervisión de seguridad e instalación de soluciones, capaz de transformar grandes cantidades de datos en información procesable en el ámbito empresarial. Cumple con el mandato de manejabilidad, y facilita la protección de la empresa frente a amenazas de todo tipo. ePO garantiza la visibilidad plena de la red corporativa, y permite la ejecución de actualizaciones en el conjunto de la red casi instantáneamente. Sirviéndose de las herramientas de gestión global de políticas, generación de informes gráficos e instalación de software de ePO, los administradores pueden gestionar políticas e instalar los medios de protección de ThreatScan y McAfee Desktop Firewall™, además de generar informes gráficos detallados acerca de los productos de McAfee Security, así como de los productos antivirus de Symantec para ordenadores personales y servidores.

El modelo de servidor único de ePolicy Orchestrator puede ampliarse hasta un máximo de 250.000 usuarios. Los administradores pueden disponer de una gama de opciones de gran alcance, y establecer políticas por dispositivo o por grupo. Éstas pueden modificarse con la frecuencia que sea necesaria para procurar la adaptación a cambios en las amenazas y los entornos de red, todo desde una única consola. Las utilidades se extienden a la gestión de infecciones. ePolicy Orchestrator responde de manera instantánea a los brotes de virus y amenazas combinadas mediante la configuración de una actualización automática para el conjunto de la empresa, la ejecución manual de exploraciones y la generación de informes detallados para señalar los puntos de entrada e identificar un patrón de propagación. Esta respuesta coordinada agiliza el proceso de actualización y ayuda a detener la propagación de las amenazas mediante el cierre de la ventana de vulnerabilidad.

En todo tipo de situaciones, las excepcionales capacidades para la generación de informes de ePO ayudan a establecer la relación entre los sucesos en la red y las soluciones ejecutables en la empresa. Muchas herramientas de gestión se limitan a producir una cantidad ingente de datos que el administrador debe revisar para determinar un problema específico en la red. ePolicy Orchestrator responde a las dos preguntas planteadas constantemente respecto a las infecciones por virus: "¿estoy protegido?" y "¿estoy infectado?". Con ePO, los administradores pueden estar seguros de que los ordenadores han sido actualizados con los motores de exploración y definiciones de virus más recientes. Se dispone además de una amplia gama de

cuadros personalizables, entre los que se cuentan gráficos de barras en tres dimensiones, circulares, lineales y tablas.

Por último, ePolicy Orchestrator permite a los usuarios de TI gestionar la seguridad frente a amenazas combinadas en el ámbito de Internet, incluidos los usuarios u oficinas en ubicaciones remotas, incluso en el caso de aquéllos que no se encuentran conectados a la red corporativa. Cualquier conexión a Internet permite la comunicación entre agentes y servidores de ePolicy Orchestrator, lo que permite una gestión homogénea e integrada de los usuarios móviles. Incluso la consola del administrador puede conectarse desde una ubicación remota.

Del bloqueo de clientes se ocupa McAfee Desktop Firewall, una solución líder en el terreno de los firewall para ordenadores personales y el software de detección de intromisiones. Desktop Firewall permite la inspección de todo el tráfico con origen y destino en la empresa, autorizando o denegando conexiones en función de políticas definidas de forma centralizada respecto a direcciones, puertos, protocolos y aplicaciones.

Desktop Firewall combina el firewall líder en el mercado con el software de detección de intrusos para proteger a los ordenadores personales frente a programas malintencionados y hackers. Actúa como un "policía de tráfico", permitiendo a las aplicaciones conocidas conectarse al ordenador personal y deteniendo el tráfico dañino generado por hackers informáticos, programas malintencionados, ataques distribuidos de denegación de servicio y aplicaciones vulnerables o no autorizadas. Un sistema de detección de intromisiones (IDS) distribuido constituye la primera línea de defensa para bloquear los ataques comunes de hackers informáticos y detener trojanos, ataques distribuidos de denegación de servicio y otras amenazas, mientras que un firewall distribuido representa la segunda línea de defensa, dotada de un sólido filtrado por paquetes y basada en la ejecución de políticas a escala de aplicaciones. Desktop Firewall estrecha la ventana de vulnerabilidad mediante el bloqueo de ordenadores personales y servidores con antelación a un ataque.

Uno de las características más populares de Desktop Firewall es la facilidad y la visibilidad de su manejo. Gracias a ePolicy Orchestrator, Desktop Firewall puede configurarse para operar de manera invisible para los usuarios, inspeccionando el tráfico de entrada y salida del ordenador, y permitiendo o bloqueando a continuación conexiones en función de las políticas relativas a direcciones, puertos, protocolos y aplicaciones. Tales políticas pueden ser determinadas por un usuario o por el administrador.

Desktop Firewall protege los ordenadores personales de los ataques generados dentro y fuera de la red corporativa, y es capaz incluso de desbaratar los ataques de programas malintencionados después de la puesta en marcha de éstos en el perímetro de la empresa. Este tipo de programas dañinos pueden invadir en silencio ordenadores personales con una sola visita a un sitio web, y atacar a continuación otros equipos de la red. Desktop Firewall detecta las intromisiones y las conexiones de aplicaciones no autorizadas, las bloquea, registra el suceso e informa al administrador de lo sucedido mediante ePolicy Orchestrator. Esta herramienta permite además una gestión centralizada, incluidos la instalación, la gestión continua, la generación de informes y el bloqueo de políticas.

Tres meses antes de un ataque: detección avanzada de nuevas amenazas y protección frente a mensajes publicitarios no deseados (spam)

Las amenazas actuales golpean con una velocidad pasmosa y una increíble ferocidad, haciendo de las empresas un objetivo vulnerable a los ataques en cualquier momento. Las tecnologías de detección heurística y genérica avanzada incorporadas en todos los productos antivirus de McAfee Security reducen al mínimo el nivel de riesgo mediante la prestación de una protección avanzada frente a más del 40 % de las amenazas nuevas y desconocidas, con el consiguiente estrechamiento de la ventana de vulnerabilidad. La realización de pruebas independientes y rigurosas y su utilización en el mundo real han permitido comprobar que las herramientas de detección avanzada de McAfee Security permiten obtener un gran nivel de ahorro, al eliminar la necesidad de descarga y distribución de emergencia de definiciones de virus, los períodos de interrupción de la actividad de los usuarios y los costes de desinfección de virus.

El análisis heurístico comprende la inspección del código de cada archivo para determinar si contiene instrucciones similares a las de un virus. Si el número de este tipo de instrucciones supera un umbral predefinido, se señalan como posible virus, y se pide al cliente que facilite una muestra para su análisis ulterior. McAfee Security equilibra este planteamiento heurístico positivo con otro negativo, centrado en las instrucciones que pueda contener el archivo y que, sin lugar a duda, no se asemejan a un virus. El mecanismo de detección heurística de McAfee Security se ajusta para evitar falsas alarmas.

La detección y desinfección genéricas exigen la creación de una definición de virus con el grado de exhaustividad suficiente para capturar todas las variantes posteriores de una determinada familia de virus. Si finalmente aparecen

nuevas variantes (lo que sucede muy a menudo, ya que los virus de éxito suelen copiarse), los clientes de McAfee Security se encuentran protegidos de antemano. La detección genérica, controlada en todos los archivos (DAT) de definición de virus, ofrece además capacidad de desinfección.

Las técnicas genéricas y heurísticas son complementarias, se refuerzan mutuamente para ofrecer una capacidad de detección preventiva superior y habilitan a las soluciones de McAfee Security para detectar nuevas amenazas antes de su aparición en la práctica.

Puesto que los programas malintencionados pueden transportarse de muchos modos (en un archivo .EXE, un script o incluso un sencillo mensaje de texto que contenga un bulo capaz de hacer perder el tiempo), el filtrado del correo electrónico resulta esencial. Instalados en el gateway de la empresa, los dispositivos McAfee WebShield® combinan un software antivirus y de gestión de contenidos con un hardware optimizado. Sus funciones de filtrado de contenidos pueden explorar la línea de asunto, el cuerpo del mensaje, el nombre del archivo adjunto, el tipo y el tamaño de todo envío de correo electrónico SMTP, además del contenido de los archivos adjuntos de texto.

Las soluciones de WebShield son extremadamente adaptables en tamaño, con un único dispositivo capaz de explorar hasta 160.000 mensajes de correo electrónico por hora, o 2 MB de tráfico http por segundo. Es posible equilibrar automáticamente la carga de los múltiples dispositivos de WebShield para obtener un mayor grado de disponibilidad y de capacidad para la resolución de fallos. Como consecuencia, WebShield ofrece una excelente defensa frente a los mensajes publicitarios no deseados, que representan un problema cada vez mayor para las empresas en todo el mundo.

Además de la propagación de virus, el correo electrónico basura no deseado expone a las organizaciones a posibles problemas jurídicos asociados a contenidos inapropiados, además de distraer a los usuarios y reducir su productividad.

Los mensajes publicitarios no deseados costarán a las empresas de Estados Unidos más de 10.000 millones de dólares en 2003, de acuerdo con un informe publicado en enero de este año por Ferris Research, una compañía consultora especializada en mensajería e investigación en régimen de cooperación. "Probablemente, (el spam) ha aumentado en un 100 % en los últimos nueve meses. No creemos que nada vaya a romper esa tendencia actualmente", se advierte en el informe. Entre las conclusiones de éste figuran las siguientes:

- el coste del spam para las empresas de Estados Unidos ascendió a 8.900 millones de dólares en 2002;
- los costes del spam en Europa ascendieron en 2002 a 2.500 millones de dólares.

WebShield combate el spam mediante una defensa de tres niveles:

- en primer lugar, las funciones de detección de spam de WebShield garantizan que el dispositivo en cuestión bloquea los mensajes de correo electrónico procedentes de una fuente de spam conocida, sirviéndose de listas negras en tiempo real facilitadas por proveedores terceros como MAPS (servicio de pago) u ORDB (servicio gratuito);
- en segundo lugar, si la empresa no está suscrita a listas negras, el administrador del sistema puede crear normas de contenido con frases "similares a las propias del spam";
- en tercer lugar, WebShield permite asimismo invalidar los dominios de correo electrónico incluidos en listas negras mediante "listas blancas" de dominios de correo admisibles.

Las funciones anti-relay de WebShield evitan que la organización sea utilizada para enviar mensajes de correo electrónico no deseado contra su voluntad o sin su conocimiento. Por último, WebShield puede utilizarse además para consignar una nota normalizada de exención de responsabilidad al final de todos los mensajes de correo electrónico de salida, lo que facilita el cumplimiento de las políticas de legalidad y seguridad de las empresas.

La gama de productos McAfee SpamKiller™ dispone de herramientas complementarias antispam para servidores y ordenadores personales. Basado en el motor SpamAssassin™, caracterizado por una elevada tasa de detección de mensajes publicitarios no deseados, combinada con un bajo índice de falsos positivos, SpamKiller dispone de un sistema de calificación con el que categoriza los mensajes de correo electrónico con arreglo a una serie de pruebas. De una precisión fuera de lo habitual, detecta más del 95 % del correo electrónico no deseado, con un índice de identificación de falsos positivos extremadamente bajo (inferior al 0,05 %). La gama de productos SpamKiller potencia el enfoque preventivo de McAfee Security con un planteamiento articulado en cinco niveles de detección de spam:

- detección basada en conjuntos de normas: el motor SpamAssassin es un filtro basado en puntuaciones que incorpora un conjunto de más de 750 normas en diversas categorías, incluidas las relativas a encabezamientos,

cuerpo principal de texto y estructura del mensaje. Cada norma se asocia a una puntuación, positiva o negativa. Las normas con puntuaciones negativas indican la presencia de correo legítimo, mientras que las positivas ponen de manifiesto atributos del correo no solicitado. Una vez agregadas, estas puntuaciones individuales otorgan a cada envío de correo electrónico una "calificación global como spam". El administrador de SpamKiller determina el nivel de calificación por encima del cuál un mensaje de correo electrónico se clasifica como spam y es enviado a la carpeta de correo no deseado del usuario o a una carpeta opcional de correo no deseado del servidor;

- detección heurística: en este marco basado en la asignación de puntuaciones, el motor SpamAssassin emplea diversos métodos heurísticos de detección para identificar mensajes de correo electrónico como probable spam. La detección heurística se sirve de una serie de pruebas internas para determinar la probabilidad de que un mensaje sea spam, y a cada prueba se le asigna un valor en puntos para reducir el número de falsos positivos. Estos métodos pueden incluir el análisis de encabezamientos y el cuerpo de los textos, así como la presencia de trucos estructurales empleados por los creadores de este tipo de mensajes para disfrazar su contenido;
- filtrado de contenidos: la funcionalidad de filtrado de contenidos de SpamKiller puede utilizarse para facilitar la identificación de términos o frases clave que aparecen en correos electrónicos y pueden indicar que el mensaje en cuestión es spam. El administrador o el usuario pueden incorporar a una base de datos términos o expresiones como "XXX", "gratuito", "hipotecas baratas", etc. Esta funcionalidad complementa y se añade al conjunto de normas suministrado con los productos;
- listas negras y blancas: al igual que WebShield, SpamKiller admite listas negras y blancas. Ofrece la versatilidad añadida de dos niveles de este tipo de listas. El administrador determina las normas a escala del servidor, para determinar los mensajes de correo electrónico no deseados dirigidos a todos los miembros de la organización utilizando las configuraciones globales de listas blancas y negras, mientras que cada persona puede adoptar un conjunto de normas complementario a escala de ordenador personal mediante la definición de sus propias entradas en listas blancas o negras.

Esta funcionalidad reviste especial importancia, pues lo que un usuario o empresa pueden clasificar como spam, puede ser bienvenido por otro. Así, las firmas de abogados no pueden permitirse la pérdida de ningún

mensaje de correo electrónico remitido por sus clientes. Si un socio trabaja en un caso referente al Viagra, deberá estar en condiciones de permitir el acceso de un determinado tipo de correo electrónico procedente de su cliente. Mediante la creación de su propia lista blanca, el usuario podrá autorizar la recepción de mensajes de clientes o dominios específicos;

- aprendizaje automatizado: el motor SpamAssassin es capaz de aprender las características de los mensajes de correo electrónico que reciben los usuarios, interpretando esta información para ajustar la puntuación en materia de spam atribuida a dichos mensajes, en el marco de un proceso conocido asimismo como "elaboración automática de listas blancas". La funcionalidad de aprendizaje automatizado determina la distribución estadística de la "calificación general en materia de spam" del correo electrónico enviado por cada remitente, y utiliza ésta para ajustar dicha calificación general de los nuevos mensajes enviados por un remitente conocido.

Momento del ataque: protección integrada en múltiples frentes

Cuando se produce una infección por virus, se requiere una respuesta reactiva rápida. McAfee Security sienta las bases necesarias para agilizar tal respuesta, convirtiéndola en parte de la estrategia de gestión preventiva de amenazas de una empresa. En el momento del ataque, McAfee Security proporciona diversas funciones para frustrar las amenazas de inmediato y cerrar la ventana de vulnerabilidad:

- Internet Patrol
- entrega rápida de definiciones de virus
- protección de dispositivos móviles
- gestión de infecciones.

Internet Patrol ubica las galardonadas funciones de exploración de virus de McAfee Security en un dispositivo de seguridad empresarial que registra constantemente Internet para detectar programas malintencionados, 24 horas al día y 365 días al año. Sirviéndose de su capacidad para la detección heurística y genérica de nuevas amenazas, Internet Patrol permite a los equipos de seguridad internos anticiparse con rapidez a éstas.

La entrega rápida de definiciones de virus corresponde a McAfee AVERT™ (Equipo de soluciones urgentes para antivirus), una organización dedicada al estudio de antivirus líder en su campo de actuación. El equipo de AVERT, compuesto por más de noventa miembros repartidos por seis continentes, es responsable de suministrar remedios para grandes infecciones como las provocadas por

LoveLetter, CodeRed, Nimda y SQLSlammer. Las posibles amenazas presentadas a McAfee AVERT se abordan igualmente con velocidad y urgencia. Más del 40% de las muestras remitidas a AVERT se procesan automáticamente. En este proceso se incluye el análisis a cargo del revolucionario sistema WebImmune™ de este Equipo. Presentado en septiembre de 2000 como el primer explorador de seguridad de virus concebido para Internet, WebImmune ofrece análisis y soluciones en tiempo real, con un lapso medio de respuesta de 90 segundos en el caso del autoanálisis avanzado de muestras.

Cuando aparece una nueva amenaza, AVERT ofrece asimismo una entrega rápida de definiciones de virus para cerrar rápidamente la ventana de vulnerabilidad. McAfee AVERT cuenta con un historial sin parangón en cuanto a la respuesta a nuevas amenazas, siendo la primera organización en responder al 75 % de las principales amenazas para la seguridad que aparecieron en 2002. AVERT ofrece definición de virus en casos de emergencia, alertas asociadas al correo electrónico e información esencial sobre el modus operandi de la nueva amenaza.

En el caso del gusano SQLSlammer, como en el de otras grandes infecciones, McAfee AVERT llevó su capacidad de protección un paso más allá con McAfee Stinger™, un explorador bajo demanda producido específicamente para el SQLSlammer que puede descargarse del sitio web de AVERT (www.avertlabs.com). Este explorador de 650 Kb puede ejecutarse como herramienta autónoma o a través de ePO, que puede instalarlo temporalmente en nodos gestionados y detectar y eliminar el gusano.

Como se señala en el apartado I, la protección de dispositivos móviles desempeña un papel cada vez más importante en la reducción al mínimo de la ventana de vulnerabilidad. A medida que aumenta el número de usuarios que confían en teléfonos inteligentes, PDA y otros equipos inalámbricos, el riesgo de que una infección por virus se traslade a una empresa se acrecienta.

McAfee VirusScan® Wireless salvaguarda de las infecciones mediante un sistema de protección de seguridad global aplicable a una amplia gama de dispositivos de bolsillo, que cubre plataformas como PalmOS, PocketPC, Windows CE y Symbian EPOC. Las redes empresariales corren un grave peligro cuando los usuarios sincronizan sus PDA con sus ordenadores personales. Durante la sincronización, VirusScan Wireless se activa y explora todos los archivos para detectar infecciones por virus. Este producto incorpora además una función de exploración integrable en los propios dispositivos para PalmOS.

La gestión de infecciones constituye el tercer y último elemento de la estrategia de McAfee Security para cerrar la ventana de vulnerabilidad. McAfee Outbreak Manager™ analiza la actividad en el gateway o el servidor de correo electrónico, filtrando el tráfico de éste de acuerdo con características específicas y frustrando los ataques antes de su acceso a las defensas antivirus de las empresas. Outbreak Manager es un componente de los exploradores antivirus para correo electrónico de McAfee Security, entre los que figuran sus productos WebShield SMTP y GroupShield™. Se trata de un sistema de gestión de infecciones basado en normas que permite a los administradores establecer múltiples normas específicas aplicables a sus respectivos entornos. Cada norma consta de cuatro componentes: un activador, un umbral, una reacción y una o varias acciones. Por ejemplo: puede determinarse la activación de una norma cuando se reciban veintidós archivos adjuntos idénticos en el plazo de veinte minutos.

Una vez desencadenada la activación, Outbreak Manager ofrece dos tipos de respuesta: automática o manual. La primera dará lugar a la ejecución de la primera acción preconfigurada. Si, después de cierto período, el activador se mantiene activo, Outbreak Manager ampliará la respuesta a la siguiente acción configurada. Una respuesta manual dará lugar a que se solicite al administrador que lleve a cabo la acción recomendada predeterminada.

Outbreak Manager permite además una combinación de estas respuestas. Especificando el horario laboral habitual del administrador, puede configurarse una norma para provocar una reacción automática fuera de ese horario, y solicitar la intervención manual durante la jornada laboral.

En cuanto a las acciones, Outbreak Manager ofrece opciones adecuadas a las plataformas en las que se instala, entre las que pueden figurar:

- el incremento de opciones de exploración mediante la activación de heurísticas de archivos, de macros, OLE;
- exploración de archivos comprimidos, archivados y de la totalidad de los archivos;
- reducción de notificaciones;
- ejecución de actualizaciones de DAT;
- ejecución de exploraciones a petición;
- bloqueo de determinados archivos adjuntos;
- configuración de acciones para borrar archivos adjuntos;
- bloqueo de todos los archivos adjuntos;
- suspensión del servidor y reinicio;
- cierre del servidor.

Con Outbreak Manager, las empresas pueden evitarse las avalanchas de correo electrónico producido por virus. Las normas pueden configurarse para alertar al administrador durante la irrupción de un virus, lo que le permite intervenir manualmente para bloquear la amenaza. Alternativamente, si Outbreak Manager se ejecuta de modo automático, se advertirá al administrador, pero la amenaza se abordará de manera automática. Utilizando esta funcionalidad, las infecciones por virus pueden controlarse con tanta eficacia, que el servicio de correo electrónico ni siquiera se verá alterado.

Combinados, McAfee AVERT, VirusScan Wireless y Outbreak Manager ayudan a las empresas a cerrar la ventana de vulnerabilidad mediante una rápida detección de los ataques y la detención de las amenazas antes de que éstas tengan la oportunidad de propagarse. Para las empresas que pretenden externalizar éstas y otras funciones de seguridad, McAfee ASaP Online Managed Services™ puede reducir la carga y el coste de mantener una protección antivirus y de seguridad, dejando estas tareas en manos de los expertos de McAfee Security. Con ASaP Online Managed Services, una amplia gama de soluciones de McAfee Security pueden instalarse rápidamente y actualizarse de manera automática cada día. McAfee proporciona plena visibilidad a su empresa con una completa función de generación de informes vinculada a Internet. Todos los servicios cuentan con el respaldo de AVERT, el laboratorio de investigación de McAfee Security, líder mundial en su campo de actividad, lo que permite la oferta de una respuesta rápida y continua, y garantiza que la ventana de vulnerabilidad se cierre de inmediato en caso de irrupción de virus o gusanos.

III. La protección preventiva en acción

Las amenazas combinadas actuales golpean con una velocidad y un grado de refinamiento sorprendentes. El ejemplo que se refiere a continuación ilustra el modo en que los productos de McAfee Security ofrecen herramientas de detección integrada y preventiva para bloquear la amenaza combinada Bugbear, presente en los titulares de los medios de comunicación de todo el mundo en 2002.

Paso 1: detección de la amenaza

Bugbear es un distribuidor de correo electrónico masivo que se sirve de una vulnerabilidad de Microsoft Internet Explorer 5 denominada *"Incorrect MIME Header Can Cause IE to Execute E-Mail Attachment"* (Una cabecera MIME incorrecta puede hacer que IE ejecuta un adjunto de correo

electrónico), que garantiza que Bugbear se carga automáticamente cuando un usuario lee el mensaje de correo electrónico infectado, sin necesidad de que haga doble clic en el archivo adjunto de éste.

Los exploradores de gateways de Internet de McAfee Security detectan muestras que se sirven de esta vulnerabilidad, como Exploit-MIME.gen o Exploit-MIME.gen.exe, utilizando 4213.DAT o superior. Estos productos pudieron detectar tal amenaza dos meses antes de su aparición. McAfee ThreatScan incluía igualmente funciones de detección para este tipo de vulnerabilidad. Muchas otras amenazas (como la combinada Klez.h) se han detectado de este modo, con anterioridad a su aparición real.

Paso 2: defensa frente a un ataque

Bugbear, una vez cargado, abre un puerto 36794 del anfitrión en el equipo objeto del ataque, y busca una larga lista de antivirus y procesos de seguridad. Si los encuentra, los inhabilita. Cuando Bugbear o una amenaza combinada similar ataca, McAfee Desktop Firewall y ThreatScan constituyen lo que puede representar el único medio efectivo de defensa de una empresa. Desktop Firewall puede utilizarse para bloquear dicho puerto, mientras que ThreatScan identifica los equipos de la red que no están protegidos por software antivirus, alertando al administrador de su vulnerabilidad al ataque.

Paso 3: atajar la propagación de la amenaza

El modo de propagación de Bugbear en la red se basa en la utilización de recursos compartidos abiertos. McAfee puede detener la difusión de la amenaza mediante ThreatScan, que identifica tales recursos abiertos en la red, y Desktop Firewall, que permite el bloqueo de las comunicaciones en la red.

Además de los recursos compartidos abiertos, Bugbear utiliza su propio motor SMTP para enviarse masivamente por correo a sí mismo; es decir, no depende de Microsoft Outlook para propagarse. Desktop Firewall permite a los administradores evitar la utilización de otros medios ajenos a Outlook para remitir correo electrónico, lo que evita la difusión de Bugbear.

Por último, como Bugbear utiliza líneas de asunto y nombres de archivos adjuntos aleatorios cuando se propaga por medio del correo electrónico, las normas de contenido no resultan de gran ayuda contra esta amenaza. No obstante, GroupShield y WebShield permiten el bloque de determinadas extensiones de archivo. En el caso de Bugbear y amenazas similares, el bloqueo de archivos .EXE detiene la

amenaza en el gateway, al cortar una vía de infección primordial y limitar la penetración en las defensas corporativas.

Paso 4: cierre de la ventana de vulnerabilidad

La perfección de amenazas combinadas como Bugbear, Klez, CodeRed, Nimda y SQLSlammer abruma en poco tiempo a las plantillas de TI, que disponen de tiempo y recursos limitados. Los intentos de reaccionar manualmente ante tales amenazas resultan frustrados de inmediato por la velocidad y la ferocidad de los ataques. La solución integrada Proactive Threat Protection de McAfee Security representa la forma más rápida y eficaz de cerrar herméticamente la ventana de vulnerabilidad, garantizando el funcionamiento continuo y seguro de la infraestructura informática de las empresas.

Resumen

Amenazas de destrucción masiva y amplio alcance como SQLSlammer, Bugbear, Klez, Nimda y CodeRed, surgidos periódicamente para causar estragos en todo el mundo, subrayan la necesidad de las empresas de cerrar su ventana de vulnerabilidad, el período en el que son susceptibles de sufrir un ataque que puede acarrearles daños muy cuantiosos. La ventana de vulnerabilidad es consecuencia de una combinación del carácter refinado de estas amenazas, su velocidad de propagación y la proliferación de dispositivos informáticos. Se abre cuando se genera una amenaza, y no se cierra hasta que todos los sistemas de la red quedan protegidos frente a su acción.

McAfee Security se ha comprometido a ayudar a las empresas a reducir la ventana de vulnerabilidad por medio de tres vías:

- reducir preventivamente la velocidad de los ataques;
- reducir preventivamente la posibilidad de éxito de los ataques;
- reducir preventivamente la exposición a los ataques.

El planteamiento dinámico de McAfee Security ofrece un mecanismo de defensa caracterizado por su cohesión y exhaustividad frente a las amenazas para la seguridad que aterrorizan a la empresa actual. Este objetivo se alcanza mediante la integración de:

- Productos de seguridad líderes en el sector:
 - McAfee ThreatScan
 - McAfee Desktop Firewall
 - los dispositivos de McAfee WebShield

- McAfee GroupShield for Exchange y GroupShield for Domino
- Internet Patrol
- McAfee VirusScan Wireless
- McAfee Outbreak Manager
- McAfee ePolicy Orchestrator
- la gestión de las políticas de seguridad
- la asistencia técnica y los servicios especializados de McAfee AVERT.

Juntos, estos componentes proporcionan el mejor servicio en el campo de la protección preventiva de amenazas, una absoluta necesidad para las empresas que desean cerrar con rapidez su ventana de vulnerabilidad.

Acerca de McAfee Security

McAfee Security es una gama de productos de Network Associates, Inc. que protege a las empresas frente a las violaciones de seguridad, los ataques de virus y las amenazas combinadas. McAfee Security ofrece protección global de las redes mediante la integración de tecnologías líderes en el sector en el campo de los antivirus, el cifrado, los firewall para ordenadores personales, la detección de intromisiones, las evaluaciones de vulnerabilidad y la gestión de seguridad. Todos los productos y servicios de McAfee Security se encuentran respaldados por una organización denominada AVERT (Equipo de soluciones urgentes para antivirus), responsable de la obtención de soluciones para infecciones de gran alcance como LoveLetter, CodeRed y Nimda. Para más información, puede ponerse en contacto con McAfee Security en el teléfono 91 347 85 00; o consultar la dirección de Internet <http://www.mcafeesecurity.com>.

NOTAS FINALES

¹ Fuente: Yahoo News.

² Ibid.

³ Fuente: Matrix NetSystems Inc., empresa dedicada a la supervisión de redes.

⁴ Disponible en el segundo trimestre de 2003.

⁵ MS Explorer, versiones 5.01 o 5.5 sin SP2.

Todos los productos de Network Associates® reciben el apoyo de nuestro programa PrimeSupport® y de Network Associates Laboratories. Personalizado para adaptarlo a las necesidades de su compañía, el servicio PrimeSupport® ofrece el conocimiento esencial del producto y soluciones técnicas fiables y rápidas para mantenerle en pie y en marcha. Network Associates Laboratories, líder mundial en sistemas informáticos y seguridad, es su garantía del desarrollo y la mejora continua de todas nuestras tecnologías.

Avenida de Bruselas nº 22 | Edificio Sauce 28108 Alcobendas | Madrid | España



YOUR NETWORK. OUR BUSINESS.

networkassociates.com