



Los intrusos y sus herramientas: ¿De qué manera McAfee Enterccept protege los servidores?

White Paper del McAfee Enterccept

Los invasores y sus herramientas: De qué manera McAfee Enterecept protege los servidores

White Paper del McAfee Enterecept

Índice

I. El set de herramientas de los intrusos	3
1. <i>Worms</i>	3
2. Explotaciones de 'buffer overflow'	3
3. Explotaciones de elevación de privilegio	4
4. Troyanos	4
5. <i>Backdoors</i>	4
6. <i>Rootkits</i>	5
7. Explotaciones de HTTP	5
II. McAfee Enterecept protege sus servidores	5
1. McAfee Enterecept Standard Edition	6
2. McAfee Enterecept Web Server Edition	6
3. McAfee Enterecept Database Edition	7
III. Resumen: ¿Cómo McAfee Enterecept bloquea las herramientas de los intrusos?	8

Los invasores y sus herramientas: De qué manera McAfee Enterecept protege los servidores

White Paper del McAfee Enterecept

Ataques contra servidores son responsables por miles de millones de dólares en daños, anualmente. ¿Cómo suceden esos ataques? ¿Qué pueden hacer las empresas para evitarlos? Este documento pretende responder esas preguntas explicando los métodos más comunes utilizados para afectar a los servidores y cómo McAfee® Enterecept® impide que tales ataques sean exitosos.

I. El set de herramientas del intrusos

Actualmente, existen muchas herramientas y métodos de ataque disponibles para los intrusos. Entre los ataques más comunes a servidores, están:

- Worms
- Explotaciones de 'buffer overflow'
- Explotaciones de elevación de privilegios
- Troyanos
- Rootkits
- Backdoors
- Explotaciones de HTTP

Es esencial comprender cada uno de esos métodos de ataque para poder combatirlos.

1. Worms

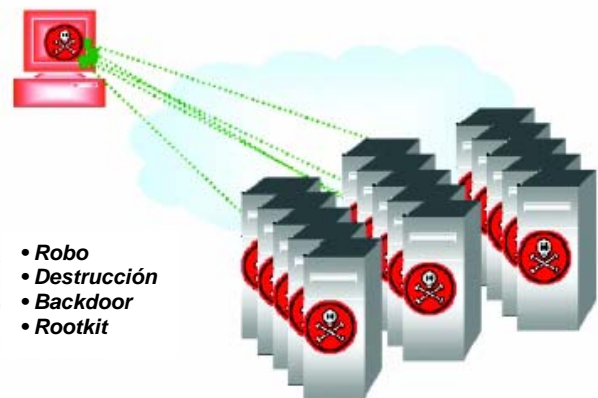
Worms son programas mal intencionados que se diseminan automáticamente, de manera diferente a los virus que precisan de intervención humana para propagarse (por ejemplo, insertar un disquete infectado en la computadora, hacer clic dos veces en un adjunto de *email*, etc.). *Worms* recientes, como Code Red y Nimda, causaron daños de miles de millones de dólares, gastos en limpieza y pérdida de negocios. Los intrusos ahora están usando los *worms* con mucho más frecuencia, pues ellos también pueden causar grandes daños, rápidamente.

Los *worms* son muy peligrosos por varios motivos. En primer lugar, se diseminan con mucha rapidez. El Code Red infectó más de 100.000 máquinas en 24 horas. En segundo lugar, si el *worm* consigue obtener privilegios suficientes, generalmente puede ejecutar cualquier actividad mal intencionada deseada por el invasor. En tercer lugar, pueden ser desarrollados más fácilmente, pues hay programas de creación de *worms* disponibles en Internet.

Un *worm* tiene tres partes principales:

- **Vulnerabilidad**—La “brecha” que el *worm* explota para obtener acceso al sistema
- **Mecanismo de propagación**—El método usado por el *worm* para comunicarse con sus víctimas
- **Carga mal intencionada**—El daño real causado por el *worm* al afectar el sistema

Esas tres partes cambian de *worm* a *worm*, pero todos ellos tienen esos tres elementos.



2. Explotaciones de 'buffer overflow'

Actualmente, las explotaciones de 'buffer overflow' es uno de los mayores problemas en la seguridad computacional. Todas las aplicaciones poseen buffers que contienen datos. Tales buffers tienen un tamaño fijo. Si el invasor envía datos en demasía para uno de esos buffers, éste “desborda”. Entonces, el servidor ejecuta los datos “desbordados” como un programa. Ese programa puede realizar varias cosas: desde enviar contraseñas a Rusia hasta cambiar archivos del sistema; instalar *backdoors*, etc., dependiendo de cuáles datos el invasor envió al buffer.

Los programadores pueden impedir ese ataque al chequear el volumen de los datos enviados antes de almacenarlos en el buffer. Si hubiese un volumen muy grande de datos se informa un error. Lamentablemente, muchos programadores se olvidan de verificar el volumen de los datos antes de salvarlos en un buffer. Así, las aplicaciones contienen una gran cantidad de “buffers no verificados”, vulnerables a ataques.

Los invasores y sus herramientas: De qué manera McAfee Enterecept protege los servidores

White Paper del McAfee Enterecept

Microsoft ya publicó por lo menos cinco boletines en los últimos seis meses sobre buffers no-verificados existentes en sus productos. Cuando un proveedor (Microsoft®, entre otros) lanza un *patch* para impedir esos desbordamientos de buffer potenciales, el *patch* simplemente adiciona un código que verifica el volumen de los datos antes de salvarlos en el buffer. De esa forma, si hubiese un *patch* disponible, impedirá el desborde del buffer.

“[En 2001] hubo un aumento de 33% en el número de empresas afectadas por ataques de ‘buffer overflow’...”

Encuesta de mercado realizada en 2001 por la revista Information Security

Las explotaciones de ‘buffer overflow’ son problemas serios debido a los siguientes factores:

- Son muy comunes. Se sabe que cientos de buffers no-verificados pueden ser aprovechados por los *hackers* y, lamentablemente, se descubren otros a todo momento. Más de un 50% de los consultores de la CERT lidian con explotaciones de ‘buffer overflow’.
- Son fáciles de usar. Cualquier persona (incluso niños de diez años de edad y “Script Kiddies”) puede descargar un código para ataque de ‘buffer overflow’ y seguir una “receta” sencilla para ejecutarlo, es decir, no hay necesidad de contar con un conocimiento técnico avanzado.
- Son muy potentes. En varios casos, el código mal intencionado ejecutado para causar un ‘buffer overflow’ tiene privilegios de administrador, por lo tanto puede hacer lo que quiera en el servidor.

3. Explotaciones de elevación de privilegio

Las explotaciones de elevación de privilegios conceden derechos de acceso a nivel administrador, a usuarios que antes no tenían tal privilegio. Por ejemplo, hay una cuenta en todos los servidores Windows NT y 2000 denominada “Invitado”. Como patrón, esa cuenta no exige contraseña. Cualquier persona puede realizar logon en el servidor utilizando la cuenta “Invitado” y usar una explotación común de elevación de privilegios denominada “GetAdmin” para lograr el derecho de acceso de administrador al sistema. Hay varias explotaciones de elevación de privilegio, como HackDLL. Son bastante útiles, pues permiten que cualquier usuario con derecho de acceso, de cualquier nivel en el sistema, eleve sus privilegios fácilmente y realice cualquier actividad.

4. Troyanos

En la conocida historia del caballo de Troya los intrusos usaron algo que parecía inofensivo (un enorme caballo de madera) para atacar una ciudad protegida. De la misma forma, los Troyanos del universo de la seguridad parecen ser programas inofensivos, pero atacan al sistema de las computadoras.

Normalmente, los intrusos sustituyen archivos esenciales al sistema y/o programas por versiones mal intencionadas. Cuando esos programas son ejecutados, elaboran actividades destructivas y los usuarios no tienen como evitarlo.

Por ejemplo, un invasor puede sustituir una de las DLL (*Dynamically Linked Library*) del sistema operativo Windows® por una versión mal intencionada. Las DLL son archivos de programa llamados por el Windows para realizar varias tareas. El invasor puede sustituir una de esas DLL por un caballo de Troya que hace todo lo que la DLL normal hace y un poco más. Ese “un poco más” puede significar varias cosas, desde reformatear el disco duro hasta hurtar números de tarjetas de crédito, etc.

5. Backdoors

Cuando un invasor consigue derechos de acceso en el nivel de la raíz en un servidor (por ejemplo, usando una explotación de ‘buffer overflow’ o de elevación de privilegios), hará dos cosas:

1. Instalar un *backdoor*
2. Ocultar sus rastros

Los *backdoors* permiten que los intrusos accedan remotamente a un sistema, en el futuro. Por ejemplo, el invasor puede haber aprovechado un determinado fallo en la seguridad para obtener derechos de acceso al nivel de la raíz. Sin embargo, con el tiempo, se puede sanar aquel fallo de seguridad e impedir que el invasor acceda al sistema nuevamente. Para evitar que se impidan en el futuro, los intrusos instalan *backdoors*. Estos pueden tomar diversas formas, pero todos permiten que el invasor acceda al servidor nuevamente sin tener que pasar por los procedimientos patrón de logon o tener que repetir el mismo ataque.

Los invasores y sus herramientas: De qué manera McAfee Enterecept protege los servidores

White Paper del McAfee Enterecept

Varios *worms* instalan *backdoors* como parte de su carga mal intencionada. El Code Red II, por ejemplo, instaló un *backdoor* que proporcionaba acceso a las unidades C y D del servidor de la Web afectado, a partir de cualquier lugar en Internet. Otros *backdoors* comunes son el Netbus y el BackOrifice, los cuales permiten que los intrusos controlen remotamente el servidor afectado.

6. Rootkits

Los *rootkits* son usados para ocultar los rastros del invasor. Si el invasor instala un *backdoor* u otro programa mal intencionado, el administrador del sistema puede percibir un nuevo programa y suprimirlo, impidiendo que el *hacker* acceda al sistema, en el futuro. El objetivo de un *rootkit* es disfrazar la existencia de programas mal intencionados en un sistema.

Al sustituir ciertos programas del sistema por versiones modificadas, los *rootkits* enmascaran la presencia de *backdoors* o de otros programas mal intencionados. Por ejemplo, el programa UNIX "ls" imprime una lista de directorios del sistema de archivos. Normalmente, eso permitiría que el administrador del sistema viese los archivos dejados por el invasor. El *rootkit* instala una versión modificada del "ls" que exhibe todos los archivos y programas en el directorio, excepto el *backdoor* o cualquier otro archivo dejado por el invasor. Eso oculta con eficacia las pruebas de que el sistema fue afectado. Generalmente, los *rootkits* sustituyen el "ls" y otros diversos programas del sistema operativo para ocultar rastros.

7. Explotaciones de HTTP

Las explotaciones de HTTP involucran el uso de una aplicación del servidor de la Web para la ejecución de actividades mal intencionadas. Tales ataques son muy comunes y están creciendo en popularidad, ya que, en general, los *firewalls* bloquean la mayor parte del tráfico de Internet para mantenerlo alejado de los servidores corporativos. No obstante, el tráfico HTTP, utilizado para la navegación en la Web casi siempre pasa libremente por los *firewalls*. Así, los intrusos tienen una línea directa con el servidor de la Web. Si fuese posible hacer que el servidor de la Web ejecute actividades mal intencionadas, los recursos que, de otra manera no estarían disponibles, podrán ser accedidos.

Nuevas explotaciones de HTTP aparecen con bastante frecuencia. Entre algunas de ellas están las vulnerabilidades Unicode Directory Traversal Exploit y Double Hex Encoding Exploit. La primera usa secuencias de caracteres como ".../..." para acceder a directorios que están fuera del directorio normal Webroot, en el cual es almacenado el contenido de la Web. Dado que la mayoría de los servidores de la Web bloquea los URL que contienen "...", los intrusos esquivan esa protección usando Unicode o codificaciones hexadecimales para representar el patrón "...". Al digitar en un navegador de la Web una secuencia de caracteres elaborada para realizar un ataque, los intrusos pueden acceder a otros directorios en el servidor de la Web. Esos otros directorios pueden contener informaciones confidenciales, contraseñas u otros archivos secretos.

Cuando se utiliza una explotación de http, los intrusos pueden acceder a tales archivos fácilmente por medio de un navegador de la Web patrón. Otras explotaciones de HTTP permiten que los intrusos ejecuten programas, cambien informaciones del sistema y llaves de registro de acceso y ejecuten otras actividades mal intencionadas.

II. McAfee Enterecept protege sus servidores

McAfee Enterecept protege los servidores contra los tipos de ataque mencionados arriba y contra varios otros, incluso nuevos ataques aún no publicados. Un análisis de la arquitectura y de las varias capas de protección de McAfee Enterecept muestra cómo el producto bloquea tales ataques.

McAfee Enterecept está directamente ligado al sistema operativo interceptando llamadas del sistema antes de ser ejecutadas. Si la denominada fuese clasificada como un ataque, McAfee Enterecept la bloquea, en caso contrario, se puede concluir normalmente.

McAfee Enterecept está disponible en tres versiones de agente: Standard Edition, Web Server Edition y Database Edition. Las versiones Web Server y Database Editions incluyen todas las funcionalidades de la versión Standard Edition juntamente con recursos adicionales específicos para impedir ataques contra servidores de la Web o servidores de banco de datos.

Los invasores y sus herramientas: De qué manera McAfee Enterecept protege los servidores

White Paper del McAfee Enterecept

1. McAfee Enterecept Standard Edition

McAfee Enterecept Standard Edition protege la parte más importante de cualquier servidor: el sistema operativo. Todos los usuarios y programas acceden al servidor por el sistema operativo.

Protege recursos

La versión Standard Edition protege los recursos del sistema (bibliotecas, archivos, directorios, cuentas de usuario) impidiendo que se cambien. Esa protección es extremadamente valiosa, ya que los Troyanos, *rootkits* y *backdoors* cambian los recursos del sistema para poder instalarse. Al impedir el cambio de esos recursos, McAfee Enterecept Standard Edition evita la instalación de esas herramientas de invasión.

Impide las explotaciones de elevación de privilegio

La versión Standard Edition también impide que los ataques de elevación de privilegios sean exitosos. Los ataques de elevación de privilegios son bastante comunes, pues les ofrecen a los usuarios comunes derechos de acceso de usuario avanzado (raíz o administrador) en el servidor. McAfee Enterecept Standard Edition previene que tales ataques tengan éxito bloqueando el acceso a archivos y recursos necesarios para cambiar los niveles de privilegio. Hasta las elevaciones de privilegios nuevas, aún no publicadas, pueden ser impedidas sin el conocimiento de la explotación específica. Eso es posible porque todas las explotaciones de elevación de privilegios cambian los accesos de los usuarios y McAfee Enterecept las impide.

Previene contra explotaciones de 'buffer overflow'

En la actualidad, las explotaciones de 'buffer overflow' son el método más común de atacar los servidores. Esos ataques pueden ser bajados y ejecutados fácilmente por intrusos con poco conocimiento, también denominados de "Script Kiddies". Más de 60% de los consultores de la CERT lidian con explotaciones de 'buffer overflow', por lo tanto, impedir esas explotaciones comunes es esencial. McAfee Enterecept Standard Edition es capaz de determinar si el código que ha de ser ejecutado por el SO es proveniente de una aplicación normal o de un 'buffer overflow'. Si es proveniente de una aplicación común, McAfee Enterecept permitirá su ejecución. Si es proveniente de un 'buffer overflow', será bloqueado, y la explotación no tendrá éxito.

De esa manera, McAfee Enterecept impide que un 'buffer overflow' afecte el servidor. Esa protección es extremadamente importante, por tanto evita los métodos más comunes de ataque contra los servidores.

Ataques conocidos

Lo más importante es que McAfee Enterecept puede impedir los ataques mencionados anteriormente utilizando la tecnología de reglas conductuales, en vez de depender apenas de firmas individuales. Esa tecnología permite que McAfee Enterecept detenga ataques nuevos, aún desconocidos, sin necesidad de actualizar las firmas del producto. Por ejemplo, las reglas de McAfee Enterecept para impedir el éxito de las explotaciones de 'buffer overflow' no están relacionadas a una aplicación o a una firma específica. En vez de ello, McAfee Enterecept puede impedir esas explotaciones, independientemente de la aplicación o buffer involucrado. Del mismo modo, la protección de recursos de McAfee Enterecept protege contra ataques nuevos y antiguos, conocidos o no.

SecureSelect

McAfee Enterecept ofrece tres modos de seguridad:

SecureSelect™ Warning Mode, SecureSelect Protection Mode y SecureSelect Vault Mode. Cada modo ofrece más seguridad que el anterior. Los clientes comienzan las implementaciones de McAfee Enterecept en el Warning Mode, después avanzan para el Protection Mode y para el Vault Mode, a medida que van adaptando y refinando su instalación del McAfee Enterecept.

2. McAfee Enterecept Web Server Edition

Las capas del WSE (McAfee Enterecept Web Server Edition) son:

Filtración de HTTP

McAfee Enterecept Web Server Edition incluye una capa de filtración de HTTP que intercepta solicitudes HTTP después de ser descifradas y decodificadas (no importa si fueron criptografiadas por SSL, Unicode o hex), pero antes de que el servidor de la Web las ejecute. McAfee Enterecept usa firmas en esa capa para detectar ataques contra el servidor de la Web y otras vulnerabilidades. La importancia de esa filtración fue comprobada durante los recientes ataques de los *worms* Code Red y Nimda.

Los invasores y sus herramientas: De qué manera McAfee Enterecept protege los servidores

White Paper del McAfee Enterecept

McAfee Enterecept bloqueó los dos *worms* en la capa de HTTP, antes que se tuviese conocimiento de ellos. No fue necesaria ninguna actualización de firma, pues la filtración de HTTP del McAfee Enterecept protege contra las solicitudes normales que los *worms* usaron para intentar penetrar en el servidor de la Web. Ni el Code Red ni el Nimda infectaron servidores protegidos por McAfee Enterecept Web Server Edition. Esa capa es el lugar principal para detener ataques, ya que esos ataques se bloquean mucho antes de que el servidor los ejecute.

Protección de servidores de la Web

McAfee Enterecept también utiliza Protección de Servidores de la Web para impedir que los ataques conocidos y desconocidos cambien el contenido de la Web o usen el servidor de la Web como una herramienta de ataque. McAfee Enterecept instala la aplicación del servidor de la Web, sus archivos y recursos en un recipiente altamente protegido. Si el servidor de la Web intenta acceder a cualesquier recurso fuera del recipiente, McAfee Enterecept bloquea el intento. Del mismo modo, si cualquier otro usuario o proceso intenta acceder o alterar los archivos o recursos contenidos en el recipiente, McAfee Enterecept bloquea ese acceso, también.

McAfee Enterecept protege definiendo un conjunto de reglas de comportamiento para el servidor de la Web. Si el servidor de la Web intenta hacer algo diferente del comportamiento definido, se bloquea el intento. Eso permite que McAfee Enterecept proteja contra ataques desconocidos, que aún no fueron publicados. En vez de concentrarse solamente en abordajes que utilizan firmas, como los proveedores de IDS tradicionales, McAfee Enterecept usa reglas de conducta para identificar el comportamiento conocido y adecuado. Cuando se crea un nuevo ataque, viola, por definición, las reglas de McAfee Enterecept que establecen el comportamiento apropiado y será bloqueado.

Los abordajes basados en firma se concentran en cómo funciona el ataque, intentando detectar ciertas secuencias de caracteres u otras informaciones de identificación. Ese abordaje funciona, hasta cierto punto, para ataques conocidos. Sin embargo, si el invasor hace cambios mínimos en cómo funciona el ataque, las firmas grabadas no lo detectarán.

Al contrario, McAfee Enterecept se concentra en lo que el ataque hace. Puesto que si el invasor altera la manera cómo el ataque es realizado, lo que hace no cambia: el ataque realiza actividades mal intencionadas.

La tecnología de reglas de comportamiento de McAfee Enterecept identifica tentativas de ejecutar actividades mal intencionadas impidiendo que tengan éxito. Ese abordaje protege los usuarios contra ataques desconocidos aún no publicados.

Incluye capas de protección de McAfee Enterecept Standard Edition

WSE incluye todos los recursos de la Standard Edition, así como niveles adicionales de protección, creados específicamente para servidores de la Web.

3. McAfee Enterecept Database Edition

Las capas de McAfee Enterecept Database Edition son:

Protección contra inyección de SQL

Ese recurso de McAfee Enterecept Database Edition protege contra una amenaza común a la seguridad del banco de datos: las técnicas de inclusión de código SQL. Con la inserción de instrucciones SQL bien elaboradas en campos de datos de una aplicación vulnerable, los intrusos pueden acceder a datos restringidos, como números de tarjeta de crédito, pueden excluir datos particulares, cambiar datos y hasta atacar otras computadoras en la red del servidor de bancos de datos. McAfee Enterecept Database Edition impide ataques de inyección de SQL con la validación de consultas SQL antes de ser procesadas por el mecanismo del banco de datos. Así, se rechazan los intentos mal intencionados de inyección de SQL y se preserva la integridad del banco de datos.

Prevención contra ataques específicos

Este recurso impide que los intrusos perjudiquen el banco de datos. Se sabe de decenas de ataques creados para impedir el funcionamiento de y/o para comprometer servidores de bancos de datos. Con el uso de la tecnología de Interceptación de SQL, McAfee Enterecept bloquea tales ataques antes que puedan causar cualquier daño al banco de datos.

Protección de banco de datos

Protege bancos de datos y datos contra acceso no autorizado. Esa protección garantiza que cualquier proceso que vaya más allá del propio banco de datos no pueda acceder al ambiente de ejecución, a los datos o a las configuraciones del banco de datos. Además de ello, el banco de datos queda impedido de acceder a recursos que no le correspondan. Eso impide que los intrusos usen el banco de datos para iniciar ataques contra otros objetivos.

Los invasores y sus herramientas: De qué manera McAfee Enterecept protege los servidores

White Paper del McAfee Enterecept

Por lo tanto, la protección de bancos de datos actúa como una capa protectora para las operaciones evitando tanto la penetración externa como el uso mal intencionado del servidor de banco de datos. El resultado de ello es que se bloquean tanto los ataques conocidos como los desconocidos en tiempo real, antes de afectar al servidor de banco de datos y causar daños. Los intrusos potenciales no consiguen acceder ni modificar parámetros operacionales—aunque consigan privilegios de acceso al servidor.

III. Resumen: Cómo McAfee Enterecept bloquea las herramientas de los intrusos

- **Worms**—McAfee Enterecept impide que un *worm* infecte un servidor bloqueando su tentativa de explorar vulnerabilidades en el servidor.
- **Explotaciones de 'buffer overflow'**— McAfee Enterecept bloquea la ejecución de códigos provenientes de 'buffer overflow' impidiendo que el servidor sea afectado.
- **Explotaciones de elevación de privilegios**— McAfee Enterecept detiene las explotaciones de elevación de privilegios utilizando la capa de Protección de Recursos que impide el cambio de los recursos del sistema.
- **Troyanos, rootkits y backdoors**— McAfee Enterecept impide que esas herramientas de ataque comunes comprometan los servidores bloqueando la alteración de recursos del sistema. Visto que los Troyanos, *rootkits* y *backdoors* son todas tentativas de modificar recursos del sistema, McAfee Enterecept impide su instalación.
- **Explotaciones de HTTP**—La capa de filtración de HTTP de McAfee Enterecept impide que las explotaciones de HTTP tengan éxito al bloquear solicitudes HTTP mal intencionadas.



Todos los productos de Network Associates® cuentan con el respaldo de nuestro programa PrimeSupport® y de los Laboratorios de Network Associates. Proyectados para adecuarse a las necesidades de la empresa, los servicios de PrimeSupport ofrecen el conocimiento de producto y las soluciones técnicas rápidas y fiables necesarias para mantenerlo en plena actividad. Los Laboratorios de Network Associates, líderes mundiales en sistemas de información y seguridad, son la garantía del desarrollo y refinamiento continuo de todas nuestras tecnologías.

Network Associates, McAfee, Enterecept y PrimeSupport son marcas comerciales, registradas o no, de Network Associates, Inc. y/o de sus afiliadas en EE.UU. y/o en otros países. Los productos que llevan la marca Sniffer® son producidos apenas por Network Associates, Inc. Todas las otras marcas comerciales, registradas o no, mencionadas en este documento pertenecen exclusivamente a sus respectivos propietarios. ©2003 Networks Associates Technology, Inc. Todos los derechos reservados. 6-avd-ent-tools-001-1003