

Estudio de la Seguridad del Windows Vista

Introducción:

El presente texto surge del estudio del **Windows Vista Community Technical Preview Build 5365 (64 Bits)**.

Windows Vista introduce varias barreras adicionales de seguridad que intentan prevenir ataques al kernel. Las modificaciones implementadas en el Kernel reducen drásticamente los “frentes de ataque” para los hackers / crackers.

Pero a pesar de los intentos de Microsoft por mejorar la seguridad de su sistema, este sigue teniendo algunos bugs conocidos y lo que resulta más alarmante es que se están descubriendo nuevos bugs resultantes de implementar código nuevo en el Kernel.

Windows Vista introduce nuevas medidas de seguridad (con respecto a las versiones anteriores del Windows), pero la mayoría de estas “revolucionarias y nuevas medidas” para asegurar el Kernel ya están implementadas en otros sistemas operativos más maduros como GNU/Linux o el Mac OS X.

Algunas de esas medidas son:

- Firma Digital de Drivers
- PatchGuard
- Chequeos de Integridad en el modo Kernel
- Uso del TPM para asegurar opcionalmente el booteo
- Modo restringido en el acceso a la memoria física



El Kernel del Windows Vista versión de 64 bits se llama **NTOSKRNL.exe**.

El responsable de chequear la integridad de las firmas digitales de los drivers de booteo es WINLOAD.EXE.

Por otra parte el mismo Kernel (NTOSKRNL.exe) es el responsable de la verificación de los drivers del sistema.

Los chequeos de integridad y de seguridad en tiempo de ejecución son controlados por PatchGuard y CI.dll.

Firmas de los Drivers

La idea de firmar digitalmente los drivers surge a partir de las conocidas vulnerabilidades en el XP que al explotarlas permiten la instalación de rootkits como si fueran drivers del sistema.

Como solución a este tipo de inconvenientes, el Windows Vista de 64Bits exige que todos los drivers estén firmados digitalmente.

Al requerir que los drivers estén firmados por entidades seguras (como **VeriSign**) vuelve muy complicada la instalación de rootkits utilizando métodos como los descritos anteriormente.

En la teoría ésta parece una gran solución, pero igualmente se puede saltar esta medida de seguridad de maneras muy simples...

Antes que nada hay que aclarar que se puede deshabilitar la opción de que Vista requiera la firma digital en los drivers. Por lo tanto, si se deshabilita esta opción el sistema queda expuesto a las mismas vulnerabilidades del XP.

Suponiendo que no se deshabilite y el sistema requiera la firma digital, cabe la posibilidad de que cualquiera puede registrarse y obtener una firma digital legítimamente y así “burlar” esta medida de seguridad e instalar todo el código malicioso que quiera.

Hay otro método aún más simple, que empleados de empresas de sistemas publiquen certificados robados en Internet permitiendo que cualquier programador use esas firmas y hacerse pasar por una empresa certificada.

Obviamente, estas formas de conseguir tan fácilmente firmas digitales vuelven insignificante la exigencia de pedir que todos los drivers estén firmados digitalmente.

PatchGuard

PatchGuard fue diseñado para prevenir el parcheo del Kernel del Windows Vista. PatchGuard chequea y valida periódicamente (de forma aleatoria cada 5 o 10 minutos) ciertas estructuras críticas del sistema. Si se llegara a detectar una modificación, aparece la famosa “pantalla azul de la muerte” (al mejor estilo del Windows 98).

A diferencia de las Firmas Digitales de los drivers y de los chequeos de integridad, PatchGuard no se puede deshabilitar

Modo restringido en el acceso a la memoria física

Deshabilitando el acceso a la memoria física, se reduce drásticamente la posibilidad de insertar código malicioso en el Kernel. Esto se implementó en el Service Pack 1 del Windows 2003 y continúa la misma implementación en el Windows Vista.

Así y todo se puede saltar esta protección, por ejemplo, usando la instrucción CALL FAR para obtener acceso al Kernel.

Integridad del código

CI.dll protege al Windows Vista verificando que los binarios del sistema no hayan sido modificados y asegurándose de que no haya drivers “no firmados” ejecutándose en modo Kernel.

CI se ejecuta en el arranque del sistema y verifica los binarios comparándolos con las firmas de los mismos almacenadas en el sistema.

CI.dll es parte de la plataforma DRM, no hay forma de remover CI.dll, si el usuario llegara a eliminar esta dll NTOSKRNL fallaría al cargarse. Si el usuario intenta remover dicha dll de la lista de imports del NTOSKRNL provoca que el WINLOAD.EXE (el Loader del Vista) rechace cargarlo ya que la firma digital no coincidiría porque el Kernel ha sido modificado.

DRM son todas las tecnologías orientadas a ejercer restricciones sobre los usuarios de un sistema, por comisión de los poseedores de derechos de autor e independientemente de la voluntad de uso del usuario del sistema

OTRAS VULNERABILIDADES

Deshabilitar el firmado de los drivers y el CI

Estas restricciones se pueden saltar simplemente parcheando los ejecutables y deshabilitando el chequeo. Para cargar drivers “sin firmar” en tiempo de ejecución, el Kernel (NTOSKRNL.exe) debe ser parcheado. Pero como al parchear el Kernel winload.exe rechazara ejecutarlo (porque fue modificado el Kernel), también hay que parchear WINLOAD.exe.

Windows Resource Protection (WRP) setea ACLs en los archivos del sistema, por lo tanto no pueden ser modificados por los administradores.

Los pasos para evadir WRP son:

- 1- Habilitar el privilegio **SeTakeOwnership**
- 2- Tomar el control del archivo protegido del WRP o de la llave de registro

Esto se puede hacer usando las Apis **AdjustTokenPrivileges** y **SetNamedSecurityInfo**.

Luego de efectuar estos pasos, los Administradores ya pueden parchear NTOSKRNL.exe y WINLOAD.exe

Posibles vulnerabilidades en los Protocolos de Red

Windows Vista maneja varios protocolos de red desde el Kernel. Esto es un gran problema, ya que si se llegara a descubrir una vulnerabilidad en los drivers de red, esa vulnerabilidad permitiría que un atacante remoto tome control total del sistema.

Microsoft optó por reescribir la pila de protocolo IP en Vista para dotarlo de soporte nativo a Ipv4 e Ipv6 para aumentar el rendimiento y simplificar su desarrollo y mantenimiento.

Pero al reescribir el código Microsoft volvió a cometer los mismos errores que cometió en otras versiones de Windows; y además se han introducido nuevos errores de programación que dan lugar también a nuevos BUGs.

Symantec a partir de varios informes basados en esta temática afirma que las primeras pilas IP del Windows XP eran más seguras que la pila implementada actualmente en el Windows Vista.

Conclusiones

Los cambios y medidas de seguridad aplicadas al Kernel del Windows Vista están orientadas a prevenir la inyección de código malicioso y para establecer una “cadena de confianza” en el booteo del Vista antes de que las aplicaciones sean ejecutadas.

Pero como se expuso anteriormente estas medidas no son del todo efectivas, ya que es posible deshabilitar el chequeo de las firmas digitales de los drivers y de la integridad del código (CI.dll) parcheando los binarios.

Microsoft en su afán de asegurar su nuevo sistema (o por lo menos de dar sensación de que es más seguro que los anteriores) llevo a que el Windows Vista nos interroge continuamente sobre las acciones que efectuamos.

Aparecen continuas y molestas advertencias en el system tray en forma de popups (Windows Defender, Windows Update, Windows Firewall, etc), que bombardearán al usuario y que a mi entender son contraproducentes. Es probable que al principio el usuario haga caso y lea cada mensaje que aparezca, pero al cabo de un tiempo se va a cansar y no les va a prestar mas atención.

Como todavía no se implemento ningún tipo de filtro inteligente, el sistema pregunta por casi todo lo que se haga.

El mejor ejemplo de esto es que para poder borrar un acceso directo del escritorio, en el Windows Vista se requieren 7 molestos pasos!!

Esto deja en evidencia que Microsoft en vez de preocuparse realmente por crear un sistema seguro, delega –ocultamente- la responsabilidad de la seguridad del sistema al usuario final, teniendo éste que confirmar todo lo que haga y asumiendo indirectamente la responsabilidad de la seguridad del sistema.

Lo único rescatable de todo esto, es que por primera vez Microsoft cambia su política de solo priorizar la facilidad de uso y el tener “un entorno lindo y amigable”; por la seguridad del sistema ya desde sus bases. Esto se puede observar al ver la actitud que tuvo Microsoft en la convención de **BlackHat 2006**, en la cual distribuyó copias de la Beta del Windows Vista para que los Hackers intenten descubrir y explotar fallos en el sistema... y obviamente, lo lograron! Para más información entrar en <http://www.kriptopolis.org/node/2688>

Todavía Microsoft tiene la posibilidad de cambiar la pila de protocolos del Windows Vista y de asegurar aun mas su sistema y de implementar nuevas medidas para que no se puedan saltar tan fácilmente las protecciones del nuevo Kernel. Y también de “pulir” las molestas advertencias y preguntas que hace al usuario desde el system tray.

Así que solo nos resta esperar a que se mejoren estas cosas y que se implementen en la versión final del tan esperado Windows Vista...