

Agnitum analiza las últimas iniciativas en seguridad por parte de Microsoft Parte I: Algunas cuestiones técnicas

La protección para el parche del kernel, de Microsoft, pone en peligro a los desarrolladores independientes de programas de seguridad

Introducción

Las nuevas medidas de seguridad, introducidas por Microsoft con el nombre de **Protección para el parche del kernel** (*Kernel Patch Protection*), están siendo presentadas como la forma de brindar un nuevo nivel de protección a los usuarios. Estas medidas serán provistas mediante una combinación entre programas de seguridad de Microsoft y el diseño del kernel del sistema operativo Windows.


Los expertos en seguridad de Agnitum han analizado estas nuevas medidas y opinan, con fundamento, que realmente causarán **más daños que beneficios, por dos razones primarias:**

- Será más complicado para las compañías independientes, desarrolladoras de programas de seguridad, instalar y mantener sus aplicaciones en ordenadores con Windows. En algunas circunstancias, la protección para el parche del kernel puede, incluso, bloquear la instalación de sus programas de seguridad.
- Será más fácil para los piratas compartir y utilizar esta nueva tecnología que para los desarrolladores de aplicaciones legítimas.

Antecedentes técnicos

Para brindar una protección proactiva, las soluciones de programas de seguridad deben obtener el control de las actividades del sistema a bajo nivel, tales como operaciones con archivos y en el registro.

Para lograr este nivel de control, un enfoque utiliza una API* documentada provista por Microsoft. Sin embargo, esta API no permite a los proveedores de programas independientes controlar la actividad del sistema de manera preventiva y rápida. Limita el control sobre las operaciones con archivos y en el registro, como por ejemplo, la modificación de la memoria utilizada por los procesos, al mismo tiempo que impone una serie de otras restricciones. Esto no ayuda a los proveedores de programas independientes a brindar una protección al sistema utilizando interfaces nativas.

 **API:** (*Application Program Interface*, Parte del sistema operativo que provee, a las aplicaciones, una interfaz de uso común.)

Un enfoque alternativo, requiere una modificación o reemplazo de código o estructuras críticas en el kernel del sistema operativo Microsoft Windows utilizando llamadas internas al sistema, denominadas creación de parches del kernel. Básicamente, la creación de parches del kernel ignora el código real del kernel de Windows e invoca código de terceros. No obstante, este enfoque abre Windows a los ataques por parte de código malicioso de terceros, así como también intentos legítimos para ampliar la funcionalidad de Windows.

Uno de los enfoques más utilizados para implementar la protección proactiva tiene que ver con el cambio y control de la tabla de despachos de servicios (*SDT, Service Dispatch Table*), utilizada por el sistema operativo para transferir el control desde el modo usuario al kernel (modo del sistema en bajo nivel). Algunas veces, los desarrolladores aplican un parche en el kernel cambiando el número de servicio en la *SDT*. De esta forma, cuando se realiza una llamada para invocar un servicio del sistema, se llama al código de terceros en lugar del código del kernel.

Por lo general, los proveedores de seguridad, incluyendo Agnitum, utilizan este enfoque. A diferencia de otras técnicas sugeridas por Microsoft, esta alternativa permite a los programas de terceros proteger el sistema operativo obteniendo control total sobre las operaciones con archivos y en el registro.

Sin embargo, Microsoft, prefiere que los desarrolladores no utilicen esta opción. De hecho, la compañía ha indicado, en las versiones x64 de Windows, que se debe evitar el redireccionamiento que incluya punteros *SDT* de 32-bits.

Lamentablemente, esto no representa ningún problema para los piratas, dado que existen áreas sin utilizar en el código del kernel, que pueden usarse para crear los llamados *conectores*.

En teoría, la tecnología **Windows Patch Guard** debería interrumpir este proceso después de realizar una verificación del espacio en memoria, pero los piratas ya saben cómo desactivar esta protección.

Llega la protección para el parche del kernel

En una actualización reciente, Microsoft eliminó la posibilidad de los desarrolladores de cambiar, de manera legítima, el número de servicio en la *SDT*, generando la llamada protección para el parche del kernel, para las versiones basadas en x64 de Windows Server 2003 SP1, Windows XP y versiones posteriores de Windows para sistemas basados en x64.

Microsoft cree que esta protección preserva el código y las estructuras críticas en el kernel de Windows, e impide la modificación proveniente de código o datos desconocidos.

Además, almacena y verifica, de manera periódica, las sumas de áreas específicas de memoria del kernel (componentes de red). Si la verificación de la suma no coincide, el resultado es la temida pantalla azul de la muerte (*BSOD*, *Blue Screen of Death*). De acuerdo con Microsoft, esta técnica debería evitar la modificación de la *SDT* y frustrar los intentos de infiltración de una serie de *rootkits*.

La investigación, por parte de expertos de seguridad de Agnitum, determinó que en la práctica, la protección para el parche del kernel no evita que los piratas apliquen ingeniería inversa en áreas específicas de código del sistema operativo para volver a adquirir las capacidades deseadas.

Si bien sí desactiva la compatibilidad con versiones futuras del kernel, el aseguramiento de la calidad no es una gran preocupación para la mayoría de desarrolladores de código malicioso.

¿Dónde coloca esto a los desarrolladores independientes de programas de seguridad?

Microsoft parece decir que es suficiente utilizar sólo las herramientas de protección integradas y estándar. Agnitum y otros desarrolladores de seguridad independientes, no coinciden con esta postura.

Las soluciones de seguridad de terceros crean un nivel de protección adicional necesario, y por lo tanto, contar con una variedad de estas herramientas disponibles beneficia al usuario, al mismo tiempo que perjudica a los piratas.

Dicho de otra forma, es mucho más difícil para los desarrolladores de código con fines delictivos, adaptar código malicioso para diferentes mecanismos de protección de múltiples proveedores, que atacar una solución de un único proveedor que pretende ser una solución universal.

Limita a los desarrolladores independientes

A partir de la implementación de la protección para el parche del kernel, los desarrolladores independientes se enfrentan a dos alternativas:

- Utilizar la API legítima provista por Microsoft y no poder implementar una protección proactiva en el sistema.
- Utilizar métodos *oscuros*, es decir, utilizar las técnicas de los piratas para competir con Microsoft y reforzar un entorno equitativo de competencia.

La protección para el parche del kernel complica la vida de los desarrolladores de *rootkits*. Pero estos pueden utilizar técnicas rápidas e ilegítimas, porque no tienen que preocuparse de la compatibilidad con el sistema existente y el resto de las aplicaciones.

Además, ¿tiene sentido mostrar la pantalla azul de la muerte como forma de defenderse contra *rootkits*?

Con la solución propuesta por Microsoft, un *rootkit*, que previamente podía detectarse y erradicarse con un buen programa antivirus, ahora detendrá el sistema y mostrará la temida pantalla azul. El mismo resultado ocurrirá después de la instalación de un programa de seguridad que no sea compatible con la tecnología de protección para el parche del kernel.

Los expertos en seguridad de Agnitum, creen que esta jugada de Microsoft está diseñada para obligar a los usuarios a depender únicamente de Microsoft para la seguridad de Windows, eliminando así la opción de utilizar soluciones de terceros que, si se tienen en cuenta las experiencias anteriores, probablemente sean más potentes y brinden una mejor protección que las ofrecidas por el mismísimo Microsoft.

Creemos que Microsoft les debe a los usuarios una mejor solución.

Para más referencias, consulte:

http://www.microsoft.com/whdc/driver/kernel/64bitpatch_FAQ.msp

<http://support.microsoft.com/kb/914784>

Igor Pankov,
Agnitum Ltd