

Agnitum analiza las últimas iniciativas en seguridad por parte de Microsoft Parte II: Conclusiones

Expertos en seguridad advierten una mayor amenaza en los desarrolladores de programas de seguridad que en la existencia de los propios *hackers*, debido a la presentación, por parte de Microsoft, de la tecnología denominada **Protección para el parche del Kernel** (*Kernel Patch Protection*).

Introducción

Después de un exhaustivo análisis de las nuevas medidas de seguridad presentadas por Microsoft, bajo la denominación de **Protección para el parche del Kernel**, los expertos en seguridad de Agnitum concluyeron que este intento para mejorar la seguridad, podría ser en realidad, un cambio para impedir o bloquear el uso de programas de protección de terceros bajo los sistemas operativos Windows, dificultando la compatibilidad entre los mismos y que ocasionará poca o ningún tipo de amenaza para los piratas informáticos.

Las conclusiones claves del análisis incluyen:

- Este parche imposibilita, a los desarrolladores de programas de seguridad, la instalación de alguna protección a nivel Kernel, una vía que los programadores utilizan para asegurar el resguardo de las aplicaciones contra programas maliciosos.
- Si ciertas versiones del Kernel están en uso, este parche de protección no evita que los *hackers* apliquen ingeniería inversa a ciertas áreas de código específico en el sistema operativo, para así obtener otra vez, el acceso no autorizado al Kernel.
- Si un programa de seguridad de terceros pudiera instalarse y trabajar bajo este entorno, de ese mismo modo, también desarrolladores independientes podrían, de forma similar, aplicar ingeniería inversa para el acceso al Kernel del sistema operativo, con lo cual, se haría más difícil la instalación y el mantenimiento de productos que puedan asegurar una mejor protección para Windows y sus usuarios.

Alexey Belkin, arquitecto en jefe de programas de Agnitum, expresa enfáticamente: “Como desarrolladores de Outpost Firewall Pro, tenemos que instalar a nivel Kernel y al referirnos al problema potencial que encontramos al vernos imposibilitados de instalar Outpost en las nuevas versiones de Windows, hemos descubierto que es posible atravesar las nuevas medidas de seguridad presentadas por Microsoft – sólo si utilizamos las mismas técnicas que los *hackers*. Esto es un gran agujero abierto. Si nosotros descubrimos esto, entonces los *hackers* también lo descubrirán, y utilizarán ese mismo agujero para instalar programas maliciosos.”

Este parche intenta proporcionar una mejor protección para las actividades de bajo nivel del sistema, como las operaciones de archivos y registro del Kernel de Windows, el nivel más profundo de las operaciones del sistema operativo. (http://www.microsoft.com/whdc/driver/Kernel/64bitpatch_FAQ.msp).

Cualquier programa que tenga acceso al Kernel puede, por ejemplo, esconder una carpeta en el disco duro y procurar que sea imposible eliminarla utilizando las herramientas más comunes de Windows.

Si los programas maliciosos pueden modificar el Kernel de Windows, para esconderse, y así robar información, los desarrolladores de programas de seguridad también necesitan de un acceso al Kernel para proporcionar protección al ordenador.

Forzar a los desarrolladores independientes a actuar como *hackers*, les da ventajas a los verdaderos *hackers*, ya que no necesitan someterse al análisis de compatibilidad y calidad que requieren los legítimos desarrolladores.

Por otra parte, Mikhail Penkovsky (Vicepresidente de ventas y mercadeo de Agnitum) agrega: “Microsoft ha hecho un movimiento lógico con este intento para proteger Windows de los ataques de tipo *rootkit*”.

“Desafortunadamente esto no resuelve el problema, y hace mucho más difícil para los desarrolladores independientes la tarea de hacer sus programas totalmente compatibles con Windows.

Nadie sabe con certeza si Microsoft ha hecho esto intencionalmente, pero nosotros no podemos evitar la sospecha de que esta acción puede haber sido diseñada para obligar a los usuarios a confiar solamente en Microsoft para la seguridad de Windows. Si las experiencias pasadas sirven de algo, las soluciones en seguridad de terceros tienden a ser más robustas y proporcionan una mejor protección para los usuarios, quienes serán los más perjudicados si se comprueba nuestra duda.”

En las versiones de 64-bit y Windows Vista, la protección del parche resguardará al Kernel de cambios legítimos. Esto implicará que ningún desarrollador independiente, de programas de seguridad, podrá instalar nada que utilice las funciones del Kernel con una codificación legítima. Pero los *hackers* aún pueden sentirse libres de aplicar ingeniería inversa, a su manera, para poder implantar un ataque de tipo *rootkit*, utilizando métodos menos legítimos.

Continúa diciendo Penkovsky: "El problema yace en el hecho que estos métodos menos legítimos sólo funcionarán para versiones específicas del Kernel de Windows, y si los desarrolladores independientes de los programas legítimos se ven forzados a tomar esta vía con cada actualización seria del sistema operativo, también tendrán que hacer cambios en los métodos de instalación. Será una pesadilla para los desarrolladores, mientras que para los *hackers* presentará poco o ningún problema, ya que ellos no tendrán que mantener un ciento por ciento de compatibilidad. Y las mejoras de un programa malicioso son mucho más fáciles de codificar que las mejoras de un programa de seguridad".