

¿Abrirá Microsoft su Protección para el parche del kernel a desarrolladores de aplicaciones de seguridad independientes?

El juego de ping-pong entre Microsoft y los desarrolladores de aplicaciones de seguridad parece haber terminado la semana pasada, cuando Microsoft anunció su intención de compartir el código fuente de su mecanismo de seguridad, conocido como Protección para el parche del kernel (KPP, *Kernel Patch Protection*).

La Protección para el parche del kernel, también conocido como PatchGuard, es una nueva medida de seguridad introducida por Microsoft en el sistema operativo Windows Vista x64. Su finalidad es prevenir que códigos maliciosos reemplacen parte del núcleo de Windows con uno propio, y así vulnerar el sistema operativo. Sin embargo, un efecto secundario desafortunado de esta implementación, es que crea limitaciones a los desarrolladores de aplicaciones de seguridad independientes, confirmadas por los investigadores de seguridad de todas partes del mundo.

Anticipadamente, en julio de 2006, Agnitum, junto con su proveedor asociado Sunbelt, plantearon su preocupación por la [introducción de la Protección para el parche del kernel](#).

Grandes proveedores como Symantec y McAfee presentaron las mismas inquietudes más tarde.

Como consecuencia de esto, la Comisión Europea emitió una advertencia a Microsoft de no dejar a los competidores fuera del mercado de los programas de seguridad.

La comisión consultó a distintos desarrolladores de aplicaciones de seguridad acerca de los inconvenientes que podrían tener con Vista, y ha confirmado que tomará acciones si cree que Microsoft quebranta las leyes antimonopolio.

Sin otra elección, Microsoft evidentemente decidió dar un paso atrás, al menos oficialmente.

El viernes 13 de octubre, la empresa informó que modificaría la protección para el parche del kernel, para permitir que las aplicaciones creadas por los desarrolladores independientes atravesasen esta medida de seguridad.

Así, también brindarían a los usuarios finales, la posibilidad de elegir su programa de seguridad preferido.

Para hacer esto, Microsoft crearía una Interfaz de programación de aplicaciones (API), que permita a los desarrolladores acceder al núcleo del sistema operativo, y desactivar el Centro de seguridad en Vista.

Esto ciertamente sonó alentador. Microsoft, después de todo, decidió hacer cambios al verse acorralado en una esquina por la Comisión Europea y los principales proveedores de seguridad.

Pero, ya que Windows Vista está próximo a desembarcar en algunas semanas, no dispondremos del tiempo necesario para brindar a los usuarios una cantidad significativa de herramientas de seguridad, para que hagan su elección.

Presumo, que también deberíamos tomar nota del día en que Microsoft hizo este anuncio: viernes 13, una fecha no acorde para las buenas noticias en el transcurso de la historia. Porque, ¿cuál fue la novedad del día? Según TechWeb:

"Microsoft no implementará las API para PatchGuard en la primera edición de Vista, pero las lanzará con el primer Service Pack (Paquete de mantenimiento).

Por lo general, Microsoft desarrolla un Service Pack inicial después de 12 a 18 meses a partir del lanzamiento de un sistema operativo."

Hemos contactado a Microsoft para intentar ponernos de acuerdo. Tenemos confianza. Desde el punto de vista de Agnitum, Microsoft ha tomado una decisión positiva, pero aún no tenemos las API para analizarlas.

Y por supuesto, los perdedores más grandes aquí van a ser los usuarios.

A menos que Microsoft cumpla con su anuncio original de tener disponibles APIs para la Protección del parche del kernel, esta semana. Lo más probable es que Vista se comercialice con una "alternativa" de soluciones de seguridad de un solo desarrollador: Microsoft.

Una compañía no precisamente aclamada por su atención a la seguridad de los ordenadores.

Cuando tengamos nuevas noticias de Microsoft, le informaremos. ¡Permanezca sintonizado!