

## La Protección para el parche del kernel ha sido vulnerada... otra vez

Una vez más, aún antes que Vista salga a la venta, PatchGuard ha sido vulnerado. Esto demuestra, nuevamente, que depender sólo de Microsoft para proteger a los usuarios que utilizan la versión x64 de Windows Vista, definitivamente no va a funcionar.

Como he comentado en este espacio [anteriormente](#), esto es como colocar la misma cerradura en todas las casas del mundo, y esperar que mantenga a todos los ladrones afuera.

Cuando los delincuentes informáticos descubren cómo violar y eludir la Protección para el parche del kernel (KPP, *Kernel Patch Protection*), automáticamente todos los usuarios quedan desprotegidos y afrontarán el mayor riesgo de seguridad concebible.

Dependerán exclusivamente de la habilidad de Microsoft para tapar los agujeros que dejó abiertos en Vista, mediante parches semanales, mensuales y fuera de término, que a menudo tienen un retraso de días con respecto a los delincuentes informáticos.

En la conferencia Black Hat en agosto de 2006, los expertos en programas maliciosos encontraron una manera de violar el núcleo de Vista. Como respuesta, Microsoft se vió obligado a enmendar la Protección para el parche del kernel.

Esta semana, [eWeek](#) y otras agencias de noticias, informaron que la Protección para el parche del kernel había sido vulnerada otra vez. En esta oportunidad, Authentium, la empresa desarrolladora de aplicaciones de seguridad, anunció que una nueva versión de su producto Authentium ESP Enterprise Platform puede eludir la Protección para el parche del kernel de Vista x64.

Microsoft reaccionó violentamente ante la [noticia](#), y confirmó que lanzará una solución, siguiendo el habitual proceso del Centro de respuestas de seguridad de Microsoft (MSRC, Microsoft Security Response Center). Esto significa que virtualmente todos los usuarios de Vista x64 serán vulnerables hasta que la empresa de Redmond emita ese parche.

Destaquemos la ironía en esta situación. Se supone que PatchGuard vuelva invulnerable a Vista x64, pero Microsoft tuvo que ponerle un parche, por segunda vez, ¡incluso antes que Vista salga oficialmente al mercado!

Ese no debería ser el precio a pagar por los usuarios, para preservar su seguridad.

Hay una expresión popular que dice "El camino al infierno está lleno de buenas intenciones". Precisamente, esto es lo que está sucediendo con la decisión de Microsoft de "mejorar" la seguridad de sus sistemas operativos, impidiendo que soluciones robustas, de desarrolladores independientes, interaccionen con Vista.

### **Mikhail Penkovsky**

Director de ventas en Agnitum Ltd.

27 de octubre de 2006