

¿Terminará Microsoft la competencia por la seguridad en Internet, en el año 2008?

Al igual que muchos desarrolladores de seguridad en Internet, hemos estado vigilando atentamente las últimas acciones de Microsoft con respecto a la Protección para el parche del kernel (*KPP, Kernel Patch Protection*).

Nuestra conclusión, seguramente es la misma que han obtenido varios colegas: la promesa de Microsoft de lanzar su Interfaz de programación de aplicaciones (API) producirá un efecto escaso o nulo, sobre una situación que muchos expertos en seguridad ya denominan "eliminando la competencia en el mercado de la seguridad en Internet".

Halloween* se acerca, pero nuestra opinión es que las perspectivas de los usuarios finales, que dependen de la seguridad que brinda Microsoft, son mucho más escalofrantes.

📅 Halloween es una fiesta que se celebra en gran parte del mundo occidental, sobre todo en los países anglosajones, la noche del 31 de octubre, víspera del Día de Todos Los Santos (1 de noviembre).

La historia oficial

Ya en julio de 2006, anticipamos nuestra preocupación [acerca de la implementación 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 alternativa posible, 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 atravesaran 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 API, que permitiría a los desarrolladores acceder al núcleo del sistema operativo, y desactivar el Centro de seguridad en Vista.

Los hechos reales

La semana pasada, según la información emitida por *TechWeb* y *eWeek*, entre otros, supimos que Microsoft no implementará las API para *PatchGuard* en la primera edición de Vista, sino que planea lanzarlas con su primer *Service Pack* (Paquete de mantenimiento).

Esto promete ser una larga espera, pues por lo general, Microsoft desarrolla un *Service Pack* unos 12 a 18 meses después del lanzamiento de un sistema operativo.

Consecuencias

¿Por qué es tan riesgoso utilizar KPP, en vez de una solución de seguridad alternativa, para proteger el kernel en los ordenadores con Vista x64?

Analicemos la siguiente analogía. En la actualidad, cada casa tiene una cerradura diferente en su puerta principal. De la misma manera, los usuarios pueden utilizar el producto de seguridad que deseen para proteger sus ordenadores.

Ahora, imaginemos qué sucedería si todas las casas de una ciudad fueran obligadas a colocar exactamente la misma cerradura en su puerta de acceso. En cuanto un ladrón descubriese cómo abrir esa traba, podría entrar libremente y robar en cualquier edificio.

La seguridad de Windows 64-bits, con *PatchGuard*, sería similar a la situación descrita.

Esto no es precisamente una película mala, de ciencia ficción.

Muchos expertos en programas maliciosos, que participaron en la conferencia Black Hat de agosto de 2006, vieron una presentación que demostraba la forma de vulnerar el núcleo de Vista. Después de este hecho, Microsoft se vio obligado a modificar su Protección para el parche del kernel.

¿Cómo podría inspirar confianza KPP? ¿Cómo es posible que proteja mejor a los usuarios?

Si es que aún no está ocurriendo, todos los delincuentes informáticos apuntarán a la protección para el parche del kernel. Si Microsoft continúa en esta dirección, la única protección que tendrán los usuarios de sistemas operativos de 64-bits, dependerá exclusivamente de la velocidad con la que la empresa de Redmond sea capaz de emitir parches de seguridad.

Si los hechos históricos sirven como indicador válido, estamos en vísperas de una larga serie de “parches del martes” (*Patch Tuesday*).*

📅 *Patch Tuesday* es el segundo martes de cada mes, día en que Microsoft publica sus parches de seguridad.

¿Por qué está haciendo esto Microsoft?

Creemos que Microsoft está ejecutando una serie de pasos lógicos con la intención de eliminar la competencia, y ganar una significativa porción del mercado de las aplicaciones de seguridad.

La clásica colección de libros *Competitive Strategy (Estrategias competitivas)*, escritos por Michael E. Porter, aconsejan que uno de los mejores métodos para asegurarse una posición en el mercado, es crear barreras tecnológicas que no permitan que los competidores accedan al mismo.

Como los ordenadores x64 apenas comenzaron a penetrar en el mercado, también tiene sentido que Microsoft enfoque su atención a este segmento. Claramente, están esperando menos objeciones de sus competidores en este aspecto, pues tomará un par de años más para la mayoría de los usuarios migrar a x64.

Hasta este momento, aún no está claro si la estrategia de Microsoft con respecto a Vista x64 y la implementación de la protección para el parche de seguridad es legal. La Comisión Europea, y otros cuerpos legislativos están trabajando en ello.

Lo que realmente nos molesta como desarrolladores de seguridad, es que Microsoft está abusando de su poder para hacer que todos los usuarios dependan solamente de ellos para asegurar sus sistemas.

Cada “parche del martes” prueba nuevamente que una alternativa de un solo proveedor, no es de ningún modo una alternativa.

Cuando se trata de seguridad, esto es particularmente verdadero. La protección para el parche del kernel presentada por Microsoft, ya ha sido vulnerada. Va a ser atacada continuamente, y quebrantada una y otra vez.

¿Qué deberían hacer los usuarios?

Nuestra mejor recomendación hasta el momento es no cambiar al modelo de 64-bits utilizando **Windows Vista**, hasta que Microsoft brinde a los desarrolladores de seguridad independientes la posibilidad de ofrecer a los clientes varias opciones para elegir el sistema de seguridad que utilizarán.