

## ¡Encontraron una nueva vulnerabilidad en Windows!

eWeek informa que “un código detallado que se aprovecha de una vulnerabilidad de seguridad en Windows XP, ha sido publicado en Internet, y ofrece a los delincuentes informáticos una serie de instrucciones para desactivar el cortafuegos integrado en el sistema operativo.”

Esto **NO** afecta a los usuarios de Outpost Firewall Pro. Hicimos la prueba. El código malicioso no logra interrumpir la ejecución de Outpost, que continúa protegiendo eficazmente el sistema.

Aquí está la ironía. En realidad, esta nueva vulnerabilidad no disminuye la seguridad de los usuarios de Windows XP, pues todo aquel que dependa del cortafuegos integrado en este sistema operativo ya está completamente desprotegido.

El cortafuegos incluido en Windows XP no brinda protección de los datos salientes. Esto significa, que los usuarios que confían en él, no tienen manera de prevenir que publicidad no solicitada (*Adware*), falsificación de sitios (*Phishing*), programas espía (*Spyware*), troyanos y aplicaciones maliciosas roben información personal de sus ordenadores.

El cortafuegos de Windows XP tampoco logra superar ninguno de los 18 análisis independientes de fuga, documentados en <http://www.firewallleaktester.com/>.

La mayoría de los programas cortafuegos de desarrolladores independientes pueden bloquear, por lo menos, la mitad de estas pruebas. Por otro lado, Outpost Firewall Pro 4.0 fue el único producto que aprobó todos los análisis de fuga de la lista.

También debemos destacar, que estas pruebas confirman que Outpost es la aplicación que mejor se protege, a sí misma, de los ataques directos y brutales, que pueden inhabilitar, interrumpir y desactivar a otros cortafuegos menos potentes.

Las tecnologías de autodefensa incluidas en Outpost, previenen que sea desactivado por virus, troyanos o programas espía.

Outpost analiza continuamente sus archivos en el disco duro, al igual que las entradas en el registro, el estado de la memoria y los servicios en ejecución, para bloquear cualquier intento de modificación proveniente de aplicaciones maliciosas.

☑ Consulte el documento [Outpost Firewall y las pruebas de fuga](#), para más información sobre este tema y analizar cómo Outpost aprueba todas las verificaciones efectuadas.

**Igor Pankov,**  
Gerente de mercado de productos en Agnitum Ltd.  
02-Noviembre-2006