

Los seis mitos más importantes sobre la Protección para el parche del kernel, disipados

La última iniciativa de Microsoft, la Protección para el parche del kernel (KPP, *Kernel Patch Protection*), ha generado un gran debate.

El camino elegido para proteger el núcleo de Windows, ha causado la aparición de muchas sugerencias y opiniones controvertidas. Como desarrollador de seguridad independiente (ISV, *Independent Security Vendor*), Agnitum se ve seriamente afectado por los pasos realizados por Microsoft, y no puede permanecer silenciosamente al margen.

A continuación presentamos nuestras consideraciones al respecto.

En principio, es bastante comprensible que Microsoft haya decidido implementar la Protección para el parche del kernel en su nueva generación de sistemas operativos.

La seguridad de Windows, ciertamente necesita una mejora.

También estamos de acuerdo en que, debido a la creciente ola de aplicaciones maliciosas, y la llegada de nuevas amenazas informáticas, como los *Rootkits* y los ataques relacionados, existe una necesidad urgente de hacer algo para enfrentar el peligro. El núcleo es el corazón del sistema operativo, y creemos que protegerlo sólidamente y evitar que sea sabotado, es un paso beneficioso en la dirección correcta, antes de dedicarse a otras cuestiones.

Sin embargo, al aislar el núcleo de los accesos externos, Microsoft ha impedido que Agnitum, y los demás desarrolladores de seguridad independientes, puedan monitorizar y controlar áreas y objetos críticos en un ordenador personal.

Como consecuencia, se ve reducida la protección de los usuarios, que afrontan técnicas de piratería cada vez más elaboradas y peligrosas.

Al no permitirnos una integración íntima con el núcleo, no podemos asegurar más la protección total contra comportamientos anormales o ilegítimos de los programas, ni resguardar nuestros propios productos adecuadamente contra sabotajes.

Dicho esto, un argumento lógico como “ustedes no pueden brindar más una protección completa, mientras que otros desarrolladores sí pueden hacerlo, de modo que la gente simplemente tendría que elegir otro producto de seguridad” parecería una respuesta razonable.

Sin embargo, la realidad interfiere.

Ni Microsoft, ni otras empresas de seguridad, logran proteger a los usuarios de sistemas de 64 bits tan confiablemente como lo están haciendo con los entornos de 32 bits. Microsoft no puede, a pesar de ofrecer cierta seguridad básica con productos como el cortafuegos integrado en Windows Vista.

Los desarrolladores de seguridad independientes tampoco pueden, porque no tienen la posibilidad de integrarse estrechamente al sistema, impedimento que no les permite incorporar funcionalidades que prohíban las operaciones de códigos maliciosos sofisticados.

Por ejemplo, Agnitum es el ganador de las pruebas de terminación de cortafuegos ([Firewall Termination Tests](#)), pero no puede extender este nivel de protección a Windows 64-bit debido a las limitaciones generadas por la Protección para el parche del kernel. Este es sólo uno entre varios ejemplos del impacto que producen los obstáculos impuestos por el aislamiento del núcleo del sistema operativo.

Específicamente, hay seis mitos con respecto a la Protección para el parche del kernel, que argumentan que la decisión de Microsoft de acorazar el núcleo, es completamente beneficiosa para los usuarios.

Nosotros no tenemos la misma opinión:

- **Tesis 1:**

“Permanentemente, Microsoft ha puesto reparos y desalentado el uso de modificaciones no documentadas en el kernel.

Siempre ha instado a los desarrolladores de seguridad independientes a abandonar las prácticas de acceso al núcleo, y a utilizar, en cambio, otras herramientas diseñadas por Microsoft”.

En esta jugada de equipar Windows x64 con la Protección para el parche del kernel, Microsoft se ha olvidado de negociar y acordar con sus socios los mecanismos exactos de la implementación de PatchGuard.

Los desarrolladores independientes que históricamente confiaban en Microsoft, para obtener un informe detallado y completo de sus nuevas características, esta vez recibieron un baldazo de agua fría: la empresa de Redmond falla, y no ofrece ninguna alternativa factible para especificar las modificaciones que han incrementado las defensas de Windows. Si bien Microsoft, supuestamente, desalentaría el uso de Interfaces de programación de aplicaciones no oficiales, el hecho es que “modificaciones del sistema no documentadas, ni soportadas” existen en cada iteración de Windows.

Después de muchas discusiones, Microsoft ahora ofrece la posibilidad de abordar la Protección para el parche del kernel, poniendo a disposición de los desarrolladores de seguridad independientes unas interfaces de programación de aplicaciones suplementarias.

Este es un ofrecimiento gracioso, pues, en principio, nunca tuvimos la oportunidad de trabajar con dichas interfaces, pues todavía son inexistentes.

Y, suponiendo que podamos analizar las interfaces prometidas, que Microsoft asegura que distribuirá (tal vez en 18 meses, incluida en el primer paquete de mantenimiento para Windows Vista), no creemos que estas permitan que Agnitum ni otros desarrolladores aseguren Windows adecuadamente, al nivel esperado por los usuarios.

De acuerdo a los rumores, las Interfaces de programación de aplicaciones prometidas no posibilitarán el nivel de control que los desarrolladores han tenido para acceder directamente al núcleo.

En general, si la historia sirve como indicador, Microsoft tiene una opinión muy distinta con respecto a lo que los desarrolladores necesitan para proteger a los usuarios de Windows, en contraposición a lo que la experiencia nos indica que es indispensable, para brindar los niveles de protección que los usuarios de Windows realmente merecen.

En este aspecto, creemos que Microsoft debería haber trabajado junto a los desarrolladores de seguridad independientes, antes de tomar una decisión unilateral para impedir el acceso al núcleo del sistema operativo.

¿Qué habrá que hacer para adaptar nuestros productos con las interfaces de programación de aplicaciones propuestas?

No lo sabemos.

Microsoft todavía tiene que anunciar la liberación de las interfaces, y ofrecer detalles.

Estamos esperando el primer paquete de mantenimiento, que no será emitido antes del año 2008.

Si Microsoft quiere, podría retrasar esa entrega seis meses, o un año más, y distribuir solamente parches semanales interinos.

- **Tesis 2:**

“Microsoft está ofreciendo a los desarrolladores de seguridad independientes todos los instrumentos necesarios, y en ningún momento quiso sofocar la competencia.

Además, la Protección para el parche del kernel no es algo nuevo, y su intención es bloquear sólo el acceso de delincuentes informáticos al núcleo del sistema operativo”.

Sí, es cierto que la Protección para el parche del kernel existía desde el lanzamiento de los primeros Windows x64, pero era mucho más débil y accesible, comparada con lo que Microsoft propone en Vista x64.

Microsoft continúa diciéndonos que los desarrolladores de seguridad no necesitan mantener una interacción con el núcleo del sistema para ofrecer una protección sólida.

Sin embargo, de acuerdo a nuestras investigaciones y las pruebas realizadas, sabemos que esa afirmación dista mucho de ser real.

Específicamente, con Outpost, no podremos brindar el mismo nivel de defensa para Windows x64, como lo hicimos con la versión de 32 bits, en dos aspectos fundamentales:

1. **Autodefensa: que asegura que el código malicioso no puede desactivar Outpost.**

La protección que el cortafuegos se brinda a sí mismo, dependerá de la Protección para el parche del kernel en los entornos de 64 bits.

Si algún código malicioso eludiera la defensa de Windows, y se instalara en el nivel del núcleo, todo el sistema estaría comprometido, sin importar qué utilidades de seguridad tiene el usuario.

2. **Los mecanismos para evitar fugas de información, que controlan el comportamiento de las aplicaciones en un ordenador personal.**

La Protección para el parche del kernel evita que Outpost verifique que la interacción entre los programas y el sistema operativo sea legítima.

En Windows x32, el módulo de Control Anti-Leak se instala a nivel del núcleo, para asegurar la protección total contra las técnicas de fuga de información conocidas.

En contraposición a esto, en el entorno de 64 bits, esta protección no será tan poderosa, pues es imposible instalar controladores a nivel del kernel, y Microsoft no ofrece ninguna alternativa.

Estas herramientas de seguridad actualmente protegen a los usuarios de Outpost con Windows x32, contra técnicas avanzadas de obtención de datos con fines maliciosos.

Outpost es el único cortafuegos que supera exitosamente las 32 pruebas de fuga independientes (puede ver información al respecto en http://www.outpost-es.com/pressroom_docs_ofp/OFPvsLeakTests.html), mientras que Microsoft dejaría a los usuarios de Windows x64 desprotegidos y expuestos.

Recordemos también que Microsoft es el autor del sistema operativo.

Si la empresa puede construir sus propios métodos de acceso e interfaces de programación de aplicaciones privadas, para sus funciones de monitorización y control, los desarrolladores de seguridad independientes tendrán que escribir código auxiliar, si pretenden agregar facultades de protección que interaccionen con las llamadas de los programas e intercepten comandos hostiles en el nivel del núcleo, antes que estos sean ejecutados por las aplicaciones maliciosas.

Como Microsoft es el creador del kernel, puede sustituir funciones específicas del mismo, con su código propietario, que no es conocido, ni estará disponible para los desarrolladores independientes, y que elude potencialmente, la necesidad de acceder directamente al núcleo con el fin de ofrecer protección.

Al respecto, Microsoft sencillamente no necesita tomarse el trabajo de insertar desvíos e interceptores en el sistema, sino que puede incorporar todos los filtros que desee, directamente en su propio código.

Los desvíos son necesarios para los componentes de los desarrolladores independientes, que no tienen el permiso de Microsoft para modificar el código.

- **Tesis 3:**

“Vista, con la Protección para el parche del kernel, es más seguro que cualquier otra versión de Windows. Incluso si el acceso al núcleo tuviera que permitirse a los desarrolladores de seguridad seleccionados, esto no mejoraría la situación, y eventualmente podría empeorarla. Nosotros brindaremos el soporte necesario a través de otras herramientas, como las interfaces de programación de aplicaciones, y mini filtros”.

Las interfaces de programación de aplicaciones son ampliamente publicitadas, pero todavía no se ha visto mucho de ellas.

En segundo lugar, como ya hemos mencionado anteriormente, Microsoft no pondrá a nuestra disposición estas interfaces hasta el lanzamiento del primer paquete de mantenimiento, Service Pack 1, para Vista. Históricamente, este proceso tarda entre 12 y 18 meses, y prolongará el período de desprotección de Vista, que será vulnerable a ataques, y los usuarios estarán expuestos a las fallas de Microsoft.

Durante este lapso de tiempo, Microsoft monopolizará todas las ofertas de seguridad disponibles para los usuarios.

También es importante destacar, que con la Protección para el parche del kernel, si se detectan modificaciones en el núcleo de Windows x64, el sistema “se suicida”, detonando la función de apagado de emergencia de la Pantalla azul de la muerte (BSOD, *Blue Screen of Dead*).

Este método para apagar el sistema se inicia cuando Windows trata de verificar la integridad del núcleo, que no coincide con el momento en que se realizó el intento por escribir en el kernel.

Por lo tanto, una vez activada, la Protección para el parche del kernel hará que los usuarios pierdan datos no guardados, y, en el peor de los casos, pone en riesgo la integridad de Windows, que podría dejar de funcionar las próximas oportunidades.

Con respecto a este tema, imaginemos que Vista está ejecutando una operación de defragmentación programada, cuando se activa la Protección para el parche del kernel.

Esto causaría el colapso del sistema operativo, y sería asombroso que Windows se las ingenie para iniciarse nuevamente.

Esto no tiene la apariencia de protección al usuario.

En cambio, se asemeja cada vez más a un método para vengarse de los intentos de corromper el núcleo, haciendo estallar Windows. ¿Qué le parecerá la idea al servicio de atención al cliente?

Y, lo que es aún más importante, no incrementa la seguridad, pues el código malicioso podría haberse ejecutado cómodamente entre las etapas de apagado, realizando las tareas para las que fue programado, y esto incluye el envío de información confidencial, o la distribución de mensajes de correo electrónico de forma masiva.

- **Tesis 4:**

“La protección para el parche del kernel es perfecta, y eliminará el código malicioso del núcleo. Su función es reforzar los sistemas Windows x64, instantáneamente”.

Esto es broma, ¿verdad? ¿Existe alguien que espere, seriamente, aplicaciones “perfectas” de Microsoft?

La verdad es, que hay informes publicados que documentan que los investigadores de seguridad ya han vulnerado la Protección para el parche del kernel, aún antes del lanzamiento de Windows Vista. Pensemos en las consecuencias que esto tiene, pues es una manera de telegrafiar a los delincuentes informáticos la fragilidad de esta protección.

Parece bastante obvio que este sistema será vulnerado rápidamente, y no precisamente por los chicos buenos. Microsoft debería saber que está erigiendo un blanco enorme.

Tan pronto como se descubra la forma ilegítima de atravesar la Protección para el parche del kernel, cualquier programador de código malicioso la utilizará en sus obras, para abrir el camino a su propagación y perjudicar a los usuarios.

Y, si Microsoft continúa lanzando actualizaciones para la Protección para el parche del kernel, de la misma manera en que programa la emisión de sus parches, las aplicaciones maliciosas permanecerán en el sistema durante varios meses.

Los desarrolladores de seguridad, por otro lado, no tienen la suerte de permitirse este lujo.

Nuestros productos no pueden ser incompatibles o inestables en las versiones emparchadas de Windows. No pueden ser la causa de las pantallas azules, mientras Microsoft lucha por reparar y enmendar la Protección para el parche del kernel una y otra vez, al mismo tiempo que nosotros modificamos nuestras aplicaciones, para que se acomoden a estas actualizaciones.

Microsoft nos confina a pelear contra programas maliciosos conocidos, utilizando solamente mini filtros “autorizados”.

Potencialmente, no seremos siquiera capaces de proteger nuestros propios productos contra el sabotaje de las aplicaciones maliciosas, mientras esperamos que Microsoft haga algo con respecto a los últimos agujeros de seguridad descubiertos en la Protección para el parche del kernel.

- **Tesis 5:**

“Microsoft no recurre a la manipulación del núcleo del sistema operativo, utiliza soluciones documentadas para proteger a sus usuarios”.

Microsoft puede implementar modificaciones del código por cuenta propia, agregando las funcionalidades que desee de acuerdo a sus necesidades.

No hay obligación de modificar el núcleo, porque Microsoft afirma que estos cambios sólo le sirven a aquellos que no están satisfechos con las utilidades tradicionales.

Eso es genial, si queremos un kernel que ya está fallado, y es vulnerable a que los delincuentes informáticos vuelvan a atacarlo.

No es lo que nosotros deseamos, precisamente.

- **Tesis 6:**

“Microsoft no puede ofrecer excepciones a la Protección para el parche del kernel para las aplicaciones legítimas.

Además, el proceso para distinguir el código bueno del malo, es demasiado complicado para nosotros”.

En realidad la Protección para el parche del kernel puede desactivarse a voluntad.

Esto ocurre, por ejemplo, cuando Windows se ejecuta en modo seguro.

Desafortunadamente, al no distinguir entre lo bueno y lo malo, Microsoft ha ahorrado muchísimo tiempo en el proceso de evaluación, auditoría, y subvención de las exclusiones para la Protección para el parche del kernel.

Simultáneamente, también ha establecido nuevos obstáculos que limitan a los desarrolladores de seguridad independientes, en un territorio al que Microsoft apunta para incrementar sus propios ingresos.

🔍 La Protección para el parche del kernel monitoriza si el código del núcleo del sistema operativo, o sus recursos clave han sido modificados.

Ayuda a evitar este tipo de ataques, que modifican las estructuras y el código del núcleo para manipular sus funcionalidades.

Igor Pankov

Gerente, en Agnitum, de mercado de productos.

11-Noviembre-2006