

Aspectos positivos y negativos de la seguridad en Vista 64 bits

Microsoft lanzó el sistema operativo Windows Vista hace casi un año.

En el periodo previo a este suceso, Bill Gates se comprometió a hacer de la seguridad la prioridad número uno de la compañía para este nuevo sistema.

La intención era que, al escribir un código seguro desde el diseño hasta la implementación, el sistema operativo fuese impenetrable para los códigos maliciosos más sofisticados y los ataques de intrusión remota que tanto habían acechado a su predecesor, Windows XP.

Microsoft pasó cinco años creando un sistema operativo desde cero.

Cuando llegó el momento de ponerlo a la venta, a fines de enero de 2007, ya llevaban dos años de atraso en relación a los planes originales.

Durante ese periodo de dos años, los fabricantes de dispositivos físicos comenzaron a lanzar componentes que permitían que los ordenadores ejecutaran códigos de 64 bits en los sistemas operativos compatibles.

En respuesta a la creciente demanda de esta nueva capacidad informática de 64 bits, Microsoft dividió el proceso de desarrollo de Vista en dos versiones diferentes: una de 32 bits (x-86) y una de 64 bits (x-64).

Los sistemas de 64 bits brindan más beneficios que los modelos x-86, en cuanto a desempeño y a la posibilidad de expansión. Esto también afecta a la forma de implementar la seguridad, y ese será el tema central de este documento.

Beneficio Nº 1

Prevención total de ejecución de datos (DEP, *Full Data Execution Prevention*)

La prevención de ejecución de datos, aprovecha determinadas características de los procesadores modernos, para definir algunas regiones de la memoria y marcar que estas no contienen bits de datos ejecutables.

De esta forma, evita que el código sea ejecutado desde dichas zonas.

Esta funcionalidad evita que los códigos maliciosos se aprovechen de las situaciones de desbordamiento de la memoria intermedia, que se presentan cuando un proceso llegó a los límites de la memoria asignada e intenta escribir en las regiones adyacentes, que ya están siendo usadas por otros procesos.

La prevención de ejecución de datos en las plataformas de 64 bits, permite proteger a nivel físico todos los programas y servicios en ejecución.

En cambio, en los sistemas de 32 bits, esta opción solo está habilitada para programas y servicios esenciales, o que permiten activar esta característica.

Beneficio Nº 2

Protección contra el emparchado del *kernel* (KPP, *Kernel Patch Protection*)

También conocido como **PatchGuard**, la protección contra el emparchado del *kernel* es una medida que impide que cualquier programa modifique directamente la memoria del núcleo del sistema operativo Windows.

Microsoft ha insistido por años que no debería estar permitido que las aplicaciones de desarrolladores independientes realicen ningún tipo de modificación en el núcleo.

De hecho, eliminó toda posibilidad de acceso al mismo en las últimas versiones 64 bits de Windows XP y Vista.

Esta jugada fue pensada para minimizar el impacto potencial de los códigos maliciosos sofisticados, como los *rootkits* que trabajan en modo núcleo.

Estos actúan emparchando el *kernel* (esto es, modificando las estructuras del núcleo de forma tal que los nuevos datos que se incorporan no puedan ser registrados o reconocidos por el sistema) con la finalidad de ocultarse y permanecer en el sistema de esta manera.

Si bien esta estrategia estaba genuinamente destinada a aumentar la protección del sistema, sellando el núcleo contra alteraciones externas, resultó muy costosa para los desarrolladores de aplicaciones de seguridad, que dependían de la posibilidad de realizar este tipo de modificaciones para solucionar ciertas debilidades del sistema operativo.

Como se descubrió posteriormente, la forma de actuar de la protección contra el emparchado del *kernel* no resulta un verdadero impedimento para los códigos maliciosos más tenaces.

Como solo revisa la integridad del núcleo ocasionalmente, es vulnerable a modificaciones ilegales durante los intervalos de inactividad.

Además, una vez que se detecta una alteración en el núcleo, el sistema inicia un cierre de sesión de emergencia, haciendo que los usuarios pierdan toda la información que no haya sido guardada.

Por supuesto, los piratas informáticos y los investigadores de seguridad han encontrado formas de sortear la protección contra el empatchado del *kernel*.

A medida que Microsoft agrega parches para fortalecer su KPP, surgen ejemplos que muestran cómo algunas personas han superado exitosamente las últimas correcciones, confirmando así sus limitaciones para impedir intrusiones graves a nivel del núcleo.

En respuesta al pedido de los desarrolladores de aplicaciones de seguridad, que solicitaban una manera viable de acceder al núcleo para proteger a los usuarios, Microsoft accedió a proporcionar una interfaz de programación de aplicaciones (API, *Application Programming Interface*) a quienes estuvieran debidamente calificados, y Agnitum pertenece a ese grupo.

Esta API estará disponible en el paquete de mantenimiento SP1 (*Service Pack 1*) de Windows Vista, que actualmente se encuentra en fase beta y cuyo lanzamiento se ha anunciado para los primeros meses del año 2008.

Beneficio nº 3

Firma de los controladores

La firma de los controladores es otro cambio controvertido, aunque importante, realizado por Microsoft.

Esta característica demanda que todos los controladores que trabajan sobre el núcleo estén firmados digitalmente.

Esto, desafortunadamente, no es de mucha ayuda al momento de combatir los códigos maliciosos más sofisticados.

El problema radica en que un desarrollador de aplicaciones alguna vez confiable y certificado que se vuelve deshonesto (al igual que un trabajador disgustado, o aquel que después de dejar su empleo aún posea un certificado digital expedido a nombre de la compañía donde prestaba sus servicios), puede autenticar el controlador con su firma personal, y liberar así un código malicioso.

Tan pronto como esto ocurre, el controlador puede cargarse sin restricciones en los sistemas de los usuarios, y trabajar sobre Vista 64 bits, tal como fue diseñado.

Obviamente, la autoridad que lo emitió, o el propio Microsoft (como en este [ejemplo](#) reciente), puede revocar el certificado y de esta manera deshabilitar el controlador.

Este proceso, sin embargo, insuere tiempo, y los usuarios continuarán en riesgo mientras el controlador permanezca activo.

Otra debilidad de esta propuesta es que un simple parámetro de línea de comandos puede deshabilitar completamente las firmas en Vista 64, acción que resultaría bastante sencilla para un código malicioso.

Beneficio Nº 4

Verificación de la integridad de los códigos durante el inicio del sistema

Cuando el ordenador carga el sistema operativo, se verifica la autenticidad de cada código binario usado durante este proceso (programas ejecutables, controladores y otros códigos de programas). Este procedimiento asegura que estos elementos no fueron modificados y el sistema está limpio.

Los códigos se verifican buscando sus firmas en los catálogos del sistema.

Durante el inicio de sesión en Windows Vista, el programa que carga el sistema operativo revisa la integridad del núcleo, la capa de abstracción de dispositivos (HAL, *Hardware Abstraction Layer*) y los discos de inicio, protegiendo de forma confiable al ordenador contra la infiltración de códigos maliciosos, no autorizados o defectuosos.

Resumen

A pesar del progreso hecho por Microsoft para fortalecer su versión de Vista 64 bits, las vulnerabilidades que afectaban a los sistemas x-86 siguen aplicándose a los sistemas x-64. Y los expertos creen que esta situación llegó para quedarse.

Una revisión de la historia de las [vulnerabilidades documentadas](#) de Windows Vista revela que ambos sistemas son igualmente susceptibles a los códigos maliciosos programados para aprovecharse de cualquier vulnerabilidad que puedan detectar.

Este [informe](#) de Microsoft es un ejemplo de ello.

Conclusión

¿Qué significan entonces estas mejoras del sistema 64 bits para los usuarios que utilizan Windows Vista?

En la mayoría de los casos, los cambios son para mejor y están bien diseñados, a pesar de que a veces hay falencias en cuanto a su implementación.

El primer paquete de mantenimiento y la interfaz de programación de aplicaciones ayudarán en gran medida a nivelar el campo de juego entre Microsoft y las compañías desarrolladoras de soluciones de seguridad.

Mientras tanto, el usuario deberá continuar tomando recaudos eficaces en cuanto a la seguridad, contando con aplicaciones antivirus y contra programas espía de desarrolladores independientes, además de cortafuegos y otras herramientas de protección, que suelen ser más poderosas y flexibles que sus equivalentes integrados en Vista.