Seguridad en Windows 7

Autor: Sebastián Bortnik, Analista en Seguridad de ESET para Latinoamérica
Fecha: Jueves 03 de Diciembre del 2009

ESET, LLC 610 West Ash Street, Suite 1900
phone: (619) 876 – 5400, fax: (619) 437 – 7045
sales@eset.com, www.eset.com

Índice

Introducción

Windows 7 es la nueva versión del sistema operativo de Microsoft, lanzada al mercado el 22 de octubre de 2009. Aunque la versión anterior es Windows Vista, la llegada de esta nueva versión pretende que finalmente los usuarios abandonen Windows XP, el sistema operativo más utilizado del mercado, aún habiendo transcurrido ocho años desde su primera versión. El propio Microsoft confirma su intención en el sitio web oficial de Windows 7 [1]: "*sabemos que ama Windows XP*".

Disponible en cuatro versiones distintas (Starter, Home, Professional y Ultimate), las estimaciones indican que en su primer mes de vida, Windows 7 ha tenido una positiva recepción del público, con más ventas en el período que su versión anterior, Windows Vista [2].

Pero, ¿cuáles son las novedades respecto a la seguridad de Windows 7? En el presente documento se analizarán los principales aspectos de la seguridad del nuevo sistema operativo de Microsoft. El presente artículo cuenta con dos secciones. En "Mejoras de Seguridad" se describirán cuáles son las principales características del sistema operativo que brindan mayor seguridad a los usuarios (y su información) y, en el caso que corresponda, cuál es su impacto ante los códigos maliciosos. Posteriormente, en "Malware en Windows 7" se analizará el comportamiento de códigos maliciosos ejecutados en un sistema con la nueva versión del sistema operativo.

Mejoras de Seguridad

User Access Control

El UAC (Control de Acceso a Usuarios) es la funcionalidad que permite controlar los privilegios de los usuarios que hacen uso del sistema cuando se ejecutan tareas administrativas que accedan o modifiquen archivos críticos del sistema.

En contraposición con Windows XP, en donde se instala por defecto una cuenta de usuario con permisos administrativos (e irrestrictos) al sistema; UAC ofrece una capa de protección importante, denegando la ejecución de tareas que pueden ser maliciosas o indeseadas, sin la autorización del usuario.

Aunque fue introducido en Windows Vista, se han realizado una serie de modificaciones en esta nueva versión del sistema operativo. Debido al gran salto que implicó para los usuarios la incorporación de esta funcionalidad, la misma recibió muchas críticas por su claro impacto en la usabilidad del sistema. Por tal

motivo, Microsoft ha introducido algunos cambios en esta nueva versión. En las configuraciones por defecto:

- UAC no se activará cuando el sistema detecte que los permisos fueron solicitados por el mouse o el teclado. Sólo se activará cuando identifique la necesidad de tareas administrativas por parte de procesos o acciones automatizadas.
- Permisos administrativos solicitados por aplicaciones firmadas a través de un certificado digital, tampoco activarán el UAC.

En otras palabras, Windows 7 ha moderado el Control de Acceso a Usuarios, equilibrando la relación seguridad/usabilidad, en función de los pedidos de los propios usuarios para no recibir tantas alertas durante el uso de la computadora. Cabe destacar que el UAC puede configurarse para alertar ante todo tipo de acceso administrativo al sistema, y es recomendable hacerlo.

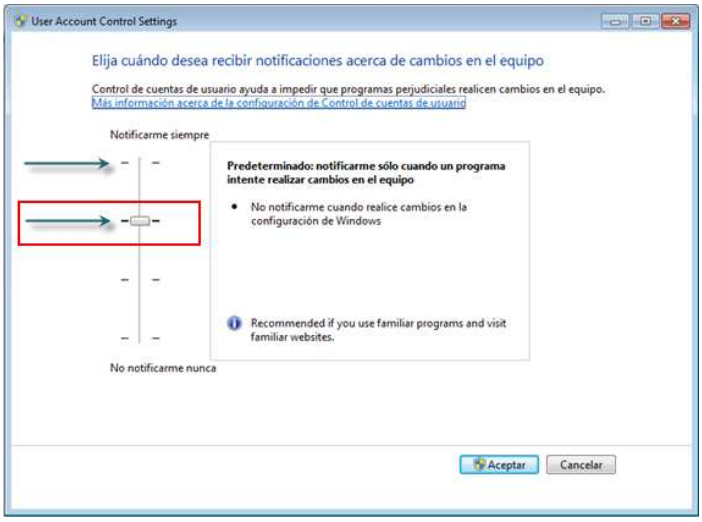

Imagen 1 – UAC configurado por defecto

El UAC es una característica de seguridad de mucha utilidad para la prevención de códigos maliciosos. Por ejemplo, familias de troyanos como *Win32/Qhost*, que intentan utilizar técnicas de pharming local [3] modificando el archivo *hosts* del sistema, no podrán realizar sus tareas sin la autorización del usuario, si es que éste tiene correctamente configurado el Control de Acceso a Usuarios. Esto es extensible a otras familias de códigos maliciosos que modifican archivos del administrador del sistema (no el entorno del usuario).

Para enfrentar esta barrera de seguridad, los creadores de códigos maliciosos seguramente utilizarán la Ingeniería Social como principal técnica: si el usuario desea ejecutar el archivo, él mismo autorizará la

ejecución del mismo en el sistema. Además, en las versiones Beta de Windows 7 existieron pruebas de concepto para "engañar" al UAC (en su configuración por defecto), simulando que acciones de procesos automáticos aparenten ser ejecutados por el usuario (mouse y teclado). Aunque esta vulnerabilidad ya fue reparada en la versión final de Windows 7, la explotación de vulnerabilidades (en caso que apareciera una nueva) será un factor de provecho por el malware.

El fin del Autorun: Autoplay

La ejecución automática de archivos ante la conexión de dispositivos USB (o similares), también conocida como *Autorun*, ha sido una de las funcionalidades más aprovechadas por creadores de malware para infectar sistemas. Diversos gusanos han utilizado estos dispositivos como método de propagación. Desde el gusano Conficker [4] hasta otra gran cantidad de variantes (identificadas genéricamente por ESET NOD32 como *INF/Autorun* y *Win32/Autorun*) que han ocupado los primeros puestos en los *rankings* de detección realizados mensualmente por ESET Latinoamérica.

Luego de haber liberado parches para deshabilitar el *Autorun* en las versiones anteriores del sistema operativo [5], Microsoft ha decido eliminar por defecto la ejecución automática de dispositivos USB en Windows 7, suplantándola por una nueva funcionalidad: *Autoplay*. Básicamente, ésta consiste en que sólo los dispositivos ópticos, tales como CD o DVD, utilizarán la opción de ejecutar automáticamente archivos al ser insertados. Otro tipo de medios, como dispositivos USB, tarjetas de memoria, u otros; no contarán con esta alternativa, visualizando el usuario solo las opciones principales de navegación, tal como se muestra en la siguiente imagen:

Imagen 2 – Autoplay en dispositivos USB

Como ya se mencionó, esta funcionalidad tendrá un alto impacto en todos los códigos maliciosos (específicamente gusanos) que utilizaban los dispositivos USB como método de propagación.

Cabe destacar que existen ciertas metodologías para continuar explotando este vector de ataque, por ejemplo simulando que el dispositivo USB es en realidad un medio CD o DVD, tal como indica el blog de Microsoft sobre Windows 7 [6]. También serán vulnerables aquellos usuarios que deshabiliten el *Autoplay*.

Biometric Framework

La funcionalidad *Windows Biometric Framework* (WBF) es una adición a Windows 7 que ofrece soporte para la utilización de dispositivos biométricos de lectura de huellas dactilares.

Aunque esta funcionalidad parece no tener impacto directo en los códigos maliciosos, cabe destacar que la utilización de contraseñas fuertes es una práctica de gran importancia para versiones anteriores de Windows [7], y que debe seguir siendo considerada para cualquier sistema que requiera clave de acceso.

Sin embargo, en tanto y en cuanto se comiencen a utilizar soportes de *login* que no requieran usuario y contraseña, los usuarios podrán tener una capa de protección ante códigos maliciosos diseñados para robar claves de acceso, como *Win32/Mebroot*,.

Malware en Windows 7

Aunque, como se mencionó en la sección anterior, muchas familias de códigos maliciosos verán afectada su propagación con las nuevas características de seguridad de Windows 7; otras aún siguen funcionando en la nueva versión del sistema operativo. Se describen a continuación los principales vectores de ataque que continúan vigentes.

Ingeniería Social, y las medidas de siempre

En pos de la usabilidad, Windows 7 continúa ocultando las extensiones de los archivos. Esta característica, junto con la utilización de archivos como ocultos, puede ser utilizada por códigos maliciosos para engañar al usuario y lograr la ejecución. Esta medida puede ser considerada controversial, ya que mantiene un vector de ataque de sencilla remediación. Al igual que en las versiones anteriores del sistema operativo, el usuario puede configurar el sistema para ver las extensiones de todos los archivos.

Particularmente los troyanos serán los códigos maliciosos que aprovecharán en mayor medida estas características.

También el malware del tipo rogue, que hace un amplio uso de la Ingeniería Social, podrá ser ejecutado en Windows 7, y por lo tanto es de esperarse que su tasa de crecimiento continúe en ascenso con la nueva versión del sistema operativo, así como ya lo ha demostrado en algunos de otro tipo como Mac OS X. En la siguiente imagen se muestra un sistema infectado con la amenaza detectada por ESET NOD32 como *Win32/Adware.VirusAlarmPro*.

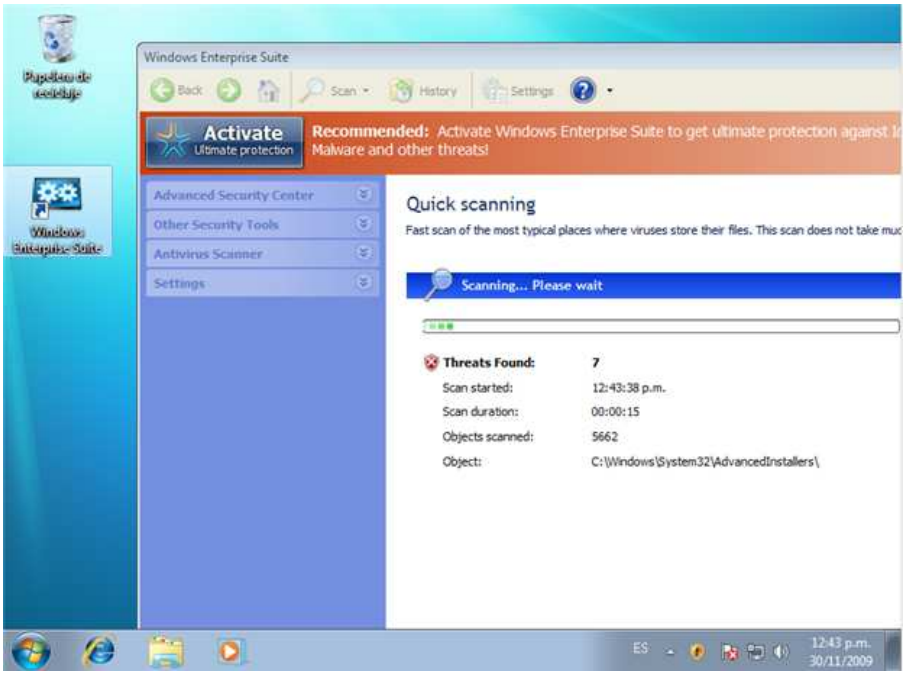

Imagen 3 – Rogue ejecutado en Windows 7

Explotación de vulnerabilidades

Independientemente de cualquier mejora de seguridad, la aparición de vulnerabilidades es siempre un vector de ataque que puede ser utilizado por gusanos para su propagación. Por lo tanto, a medida que aparezcan vulnerabilidades en el nuevo sistema operativo, aparecerán los *exploits* y, en consecuencia y de ser aplicable, gusanos que aprovechen los mismos para infectar sistemas [8].

Ante la explotación de una vulnerabilidad que permita ejecutar un código remoto, las medidas de seguridad antes expuestas no serán aplicables y un gusano de este tipo podrá ejecutar las acciones que desee, incluso si éstas son críticas o administrativas. Una epidemia como la ocurrida con el gusano Conficker [4] podría ocurrir en Windows 7, siempre y cuando los usuarios no sean conscientes de la importancia que las actualizaciones de seguridad tienen [9].

Infección del entorno del usuario

Así como el UAC previene la ejecución de tareas administrativas, que por lo general infectan, alteran o modifican archivos del sistema; ciertos códigos maliciosos no necesitan de estos recursos para lograr su cometido. Particularmente se destacan aquellos malware del tipo bot, diseñados para convertir a los sistemas en equipos zombis, y que por lo general sólo necesitan ejecutarse al inicio de sesión. Es decir, sólo necesitan alterar el entorno del usuario, sin necesidad de permisos administrativos (sobre todo el sistema).

Códigos maliciosos como las familias *Win32/Zbot* o *Win32/Agent* pueden ser ejecutados en esta versión del sistema operativo. Algunas variantes de estos fueron probadas con éxito sobre la versión lanzada de Windows 7.

Conclusión

En las secciones anteriores se detalló que ciertos códigos maliciosos no podrán ser ejecutados con las nuevas características de seguridad de Windows 7, mientras que otros sí podrán hacerlo. Independientemente de la selección realizada, en la cual se identificaron las principales familias en cada categoría, cabe destacar que existe una regla general: el lanzamiento de una nueva versión del sistema operativo logrará que ciertos códigos maliciosos sean controlados y otros no.

Este análisis radica sobre las familias de malware ya conocidas, pero es relevante destacar que, conforme los usuarios comiencen a utilizar Windows 7, nuevas familias de malware pueden aparecer, siendo destinadas únicamente a esta nueva versión y con nuevos vectores de ataque hasta el momento no explotados.

De todas maneras, vale destacar los esfuerzos de Microsoft por mejorar la seguridad de su sistema operativo, así como también recordar la importancia de mantener sus sistemas protegidos con soluciones de seguridad con capacidades de detección proactivas, combinadas además con las buenas prácticas y la concientización de los usuarios.

Referencias

[1] http://windows.microsoft.com/es-ES/windows7/products/why-choose?os=winxp

[2] http://www.npd.com/press/releases/press_091105a.html

[3] http://www.eset-la.com/centro-amenazas/videos-educativos/1997-pharming-local

[4] http://www.eset-la.com/centro-amenazas/2241-conficker-numeros

[5] http://blogs.eset-la.com/laboratorio/2009/08/29/elimina-autorun-dispositivos-usb/

[6] http://blogs.msdn.com/e7/archive/2009/04/27/improvements-to-autoplay.aspx

[7] http://www.eset-la.com/centro-amenazas/2037-seguridad-contrasenas

[8] http://blogs.eset-la.com/laboratorio/2009/11/16/vulnerabilidad-0-day-windows7/

[9] http://www.eset-la.com/centro-amenazas/1996-importancia-actualizaciones