# USB: otra vía para la entrada de los virus informáticos

Desde hace apenas dos años, la calidad y variedad de los dispositivos de almacenamiento USB ha crecido extraordinariamente y su abaratamiento ha posibilitado su uso masivo. Si a esto se agrega su funcionalidad, tanto para los usuarios hogareños como los corporativos, es fácil percatarse de que este periférico es indispensable para todos.

De hecho, la tecnología de almacenamiento con interfaz USB ha evolucionado para ofrecerle al usuario mayores funcionalidades, como es el caso de aquellos que tienen incorporada la tecnología U3 **www.u3.com**.

La tecnología U3 permite la ejecución de aplicaciones directamente desde el dispositivo de almacenamiento USB y sin dejar rastro alguno en un equipo.

Esta tecnología, a diferencia de la que posee un dispositivo de almacenamiento USB tradicional, cuenta con dos particiones: la primera y principal es para el sistema operativo, un medio de almacenamiento extraíble; la otra, una partición muy pequeña, se considera como una unidad de CD-ROM; es aquí donde precisamente se encuentra el punto al que queremos llegar.

Windows XP con SP2 tiene una función de ejecución automática habilitada por *Default*, por lo que el solo hecho de insertar este dispositivo en la ranura USB, y sin ningún tipo de intervención por parte del usuario, lanzará el menú y permitirá el acceso a las aplicaciones.

Cuando insertamos un dispositivo no U3, en un sistema con *Microsoft Windows XP*, este se reconoce como una unidad de almacenamiento extraíble, y luego mediante un *pop-up* se consulta al usuario qué acciones desea que ejecute en relación con ese medio.

Esta acción, realizada con el fin de ayudar al usuario a tomar una decisión sobre cuál de las acciones del menú elegir, es aprovechada por los creadores de programas malignos para violar la seguridad de nuestros sistemas. El atacante entonces creará y colocará en el dispositivo un fichero *autorun*:

icon=start.ico “AQUI EL íCONO QUE DESEAMOS QUE MUESTRE”
open=start.bat
action=Click “OK” to install USB flash drive drivers “AQUí EL MENSAJE ASOCIADO”
shell\open\command=start.bat
o tan sencillo como este otro:
[Autorun]
open=setup.exe
icon=setup.exe,0

En cualquiera de los dos casos, el resultado es correr un fichero, no importa su nombre, y ejecutar un programa cuya función es crearnos problemas en la PC. Y son muchos los

que han caído inocentemente con este proceder. Para resolver esta vulnerabilidad es necesario deshabilitar dos opciones que el sistema habilita por defecto:

*Primero*: ir a *Panel de control* - opciones de carpeta - ver y marcar donde dice: *Mostrar todos los archivos y carpetas ocultos* (estos archivos siempre están ocultos).

*Segundo*: en menú de inicio - ejecutar y escribir *gpedit.msc*, y en la ventana que se abra seleccionar en *Directiva Equipo Local - Plantillas de administración - sistema - desactivar reproducción automática* - clic derecho - *propiedades* y en la ventana que se abre marcar en *habilitada* y debajo seleccionar todas las unidades y aceptar los cambios que sólo tendrán efecto cuando se reinicie la *PC.DptoInfraestructura*.

***Trabajo procesado por el licenciado Ramón Orlando Bello Hernández.***