Dispositivos portátiles: fugas de información y otros riesgos

Todos los usuarios de sistemas de información son plenamente conscientes de la aparición de dispositivos portátiles de almacenamiento en distintas formas y con distintas medidas de capacidad. Su popularización, sin embargo, introduce problemas de seguridad en la infraestructura de las organizaciones y son un riesgo a la confidencialidad de la información que manejan ya que éstos pueden utilizarse tanto para transportar, de forma subrepticia, gran cantidad de información fuera de la organización, como para introducir código malicioso dentro de ésta.

Javier Fernández-Sanguino

La demanda del mercado informático en la disponibilidad de, por un lado, dispositivos portátiles para todo tipo de usos y, por otro lado, de la existencia de *buses* universales de comunicación a los que conectar estos dispositivos, ha creado un mercado explosivo de dispositivos de almacenamiento que, mes a mes, incrementan su capacidad de almacenamiento y reducen su tamaño.

Los dispositivos de almacenamiento masivo compactos están teniendo una aplicación en muchas aplicaciones de la informática personal: reproductores de música, cámaras digitales, reproductores de vídeo, e incluso, teléfonos móviles. Todos ellos utilizan tecnologías similares (discos *flash*) con distintos nombres: *Compact Flash (CF)*, *Unidades Flash*, *Memory Stick*, *Microdrives, Mini Card*, *Multi Media Card* (MMC), *Secure Digital* (SD), *Smartmedia,* y *XD-Picture Card*.

Por otro lado, la introducción de *buses* universales para la conexión de dispositivos portátiles como son el estándar *Universal Serial Bus* (USB) y el estándar Firewire (*IEEE 1394*) en los ordenadores personales ha llevado a la proliferación de dispositivos que utilizan estas interfaces, entre ellos, de nuevo, dispositivos de almacenamiento. Debido a la limitación de capacidad de los basados en tecnología *flash,* han proliferado en el mercado de consumo los denominados "discos duros externos" que no son sino discos duros de consumo y tamaño reducido que ofrecen una capacidad de almacenamiento muy superior a los compactos. En la actualidad es posible encontrar, a precios razonables, discos duros USB de 500 GB y Firewire de 1.000GB.

La proliferación de estos dispositivos y las economías de escala llevan a que sufran una continua reducción de precio al tiempo que se ve incrementada su capacidad.

Riesgos asociados a los dispositivos de almacenamiento

La disponibilidad de esta capacidad de almacenamiento en un dispositivo pequeño hace posible que un empleado interno o un intruso los pueda utilizar para:

a) Extraer información de la empresa y transportarla fuera de ésta.

b) Introducir programas no autorizados desde el exterior (potencialmente maliciosos), con, en algunos casos, ejecución de código automática sin intervención del usuario.

c) Comprometer el equipo a través del arranque de un dispositivo desde la BIOS.

d) "Atacar" al sistema operativo a través de controladores de dispositivos maliciosos o mal programados.

Los tres primeros riesgos no son nuevos; evidentemente, ya existían asociados a cualquier dispositivo de almacenamiento externo (como los disquetes o CDs) integrados en los PCs que, en el caso del tercer riesgo descrito, puede utilizarse para arrancar el sistema. Pero el nivel de riesgo de estos nuevos dispositivos es mucho mayor. No es comparable la cantidad de información que se puede transportar en un disquete flexible o un CD-Rom grabado a la que se puede transportar hoy en día con una unidad de disco portátil, la diferencia es de varios órdenes de magnitud. Si comparáramos los discos portátiles con discos DVD-Rom se podría ver que una persona puede, hoy en día, transportar el equivalente a más de 60 DVDs en un dispositivo que cabe en la palma de una mano o en el bolsillo de su chaqueta.

Asociados a los dispositivos portátiles está el riesgo de instalación de controladores maliciosos o la malversación de controladores con deficiencias que puedan llevar a comprometer el equipo en el que se instalan.

También, una de las circunstancias que hace que el riesgo se vea incrementado es debido a la proliferación de memorias USB portátiles y a su uso en las organizaciones dando (y recibiendo) memorias USB para intercambiar documentos, incluso con personal externo. Aquellos que manejan memorias USB con asiduidad no son habitualmente conscientes de que existen memorias modificadas que pueden hacer creer al sistema operativo (Windows) que son un dispositivo de sólo lectura. Así, cuando éstas se conecten a un equipo el código de que dispongan se ejecutará automáticamente a menos que se haya deshabilitado esta función de forma global. A diferencia de los medios de sólo lectura, que sólo podrían propagar código malicioso, un atacante podría disponer de un dispositivo USB que copie de forma automática y "silenciosa", al ser insertado, todos los contenidos del ordenador al que se ha conectado, dejando en el propio dispositivo USB (por ejemplo, en una carpeta oculta) toda la información recuperada sin que el usuario que lo ha utilizado sea consciente de ello.

El último de los riesgos mencionados sí es nuevo y deriva del hecho de que, en principio, un dispositivo conectado a un *bus* estándar se trata con un controlador (*driver*) específico desarrollado, en algunas ocasiones, por el fabricante del sistema operativo y, en otras, por empresas externas. Aunque los dispositivos de almacenamiento masivo pueden funcionar con un controlador genérico, algunos dispositivos específicos (cámaras, PDAs, reproductores de música, etc.) pueden requerir para su correcto funcionamiento un controlador desarrollado por el fabricante del hardware. Así, el controlador de dispositivos, en algunos casos, estará incluido dentro del sistema operativo y, en otros casos, se provee a través de un medio externo adicional (como pueda ser un CD-Rom o un componente descargable desde Internet).

Cabe destacar que el desarrollo de estos controladores de dispositivo no suele ser tan estricto como el desarrollo de otras áreas del sistema operativo (máxime si la compañía que lo desarrolla no es la misma) y puede estar sujeto a vulnerabilidades que puedan aprovecharse simplemente con que el usuario introduzca un dispositivo modificado.

Por tanto, asociados a estos dispositivos portátiles está el riesgo de instalación de controladores maliciosos o la malversación de controladores con deficiencias que puedan llevar a comprometer el equipo en el que se instalan. En ambos casos, los fallos de seguridad de un controlador suponen el compromiso del sistema, ya que éste se ejecuta en el núcleo del sistema operativo, con máximos privilegios.

Este es un problema emergente y aunque aún no ha sido aprovechado como vector de ataque puede convertirse en uno en un futuro. Personal de la empresa SPI Dynamics **[1]** y, posteriormente, un técnico de Internet Security Systems **[2]** han hecho públicas vulnerabilidades de controladores de dispositivos de Windows (en las versiones 98, ME, 2000, XP y 2003). Las distintas vulnerabilidades descubiertas por SPI Dynamics están identificadas globalmente como CAN-2005-2388 (BID-14376) y están, en el momento de escribir estas líneas, aún sin arreglar.

Aunque no se ha publicado ningún análisis de los controladores de dispositivos disponibles en el sistema operativo Windows, como muestra puede ser útil el análisis del código fuente del núcleo de Linux 2.6.9 (5.5 millones de líneas de código) realizado por Coverity. Este análisis determinó que el 53 por ciento de los problemas de seguridad detectados se encontraban en los controladores

de dispositivos siendo la calidad de éstos (número de errores por línea de código) inferior a la calidad del núcleo base **[3]**.

Funcionamiento del acceso a dispositivos de almacenamiento masivo

Para entender los distintos riesgos de los dispositivos portátiles es útil describir el funcionamiento del sistema operativo cuando se intenta hacer uso de este tipo de dispositivos. Se van a describir dos ejemplos distintos de funcionamiento, por un lado para el entorno de escritorio de Windows (2000, XP y 2003) y por otro, para el entorno de escritorio de las distribuciones basadas en Linux.

En el caso de Windows (en las versiones ME, 2000, XP y 2003), las operaciones que se producen al conectar un dispositivo son las que se muestran en la **figura 1 [4][5][6]**.

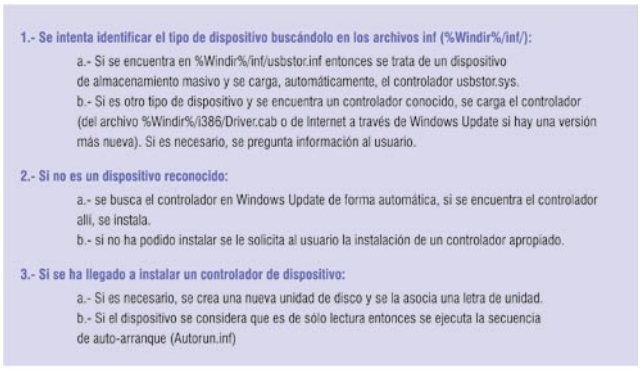

Figura 1. Operaciones al conectar un dispositivo en sistemas Windows

Así, el proceso es, en la mayoría de los casos, automático. Se puede configurar, a través de la política de seguridad del equipo (o la política del dominio): quién puede instalar nuevos controladores (el valor por omisión es el grupo de Administradores), si se permite o no la instalación de controladores no firmados (el valor por omisión es permitir la instalación pero avisar al usuario), si se descargan nuevos controladores desde Windows Update (el valor por omisión es el que se permite). Además, en Windows XP SP2 es posible controlar (a través del registro, no a través de una política) si se permite acceso de escritura al dispositivo.

Cabe destacar que los privilegios necesarios para la instalación de nuevos controladores sólo se aplican al usuario que hace uso de un dispositivo si el controlador no se puede cargar de forma automática. Es decir: si está disponible en el sistema, está firmado, se instala sin errores y no requiere la intervención del usuario se cargará en el sistema independientemente de los privilegios que tenga el usuario que tiene abierta la sesión.

En general, es necesario que un usuario tenga una sesión abierta en el sistema para que entre en funcionamiento la carga de controladores pero, sin embargo, en Windows 2003 se ha modificado este comportamiento haciendo posible que los controladores se carguen antes de la entrada de un usuario (en el proceso de *logon*) si se inserta un dispositivo nuevo.

En el caso de los sistemas operativos que utilizan el núcleo de Linux el proceso es distinto. Las operaciones que se producen cuando se conecta un dispositivo se muestran en la **figura 2.**

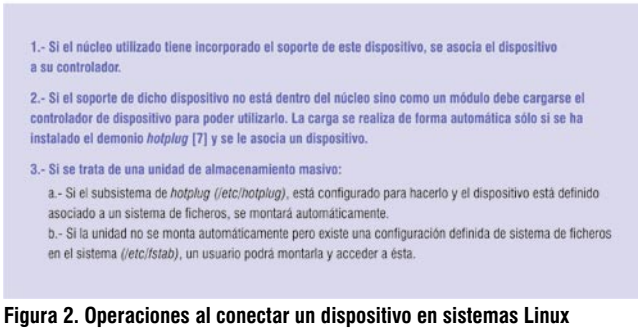

Figura 2. Operaciones al conectar un dispositivo en sistemas Linux

En las distribuciones de Linux no está (aún) estandarizado el sistema de interfaz con el usuario a la hora de introducir dispositivos, aunque se está desarrollando una capa de abstracción para el entorno de escritorio denominado HAL **[8]**.

En cualquier caso, los privilegios necesarios dependerán de la configuración del sistema operativo. En el caso de que no se haya configurado un montaje automático ni se haya definido el sistema de ficheros en el sistema como un sistema de ficheros que puede montar un usuario cualquiera, el único que podrá montar la unidad será el usuario *root*. Como vemos, no se ha incorporado la posibilidad de descargar controladores a través de Internet.

Prevención de riesgos asociados a la instalación de dispositivos

Los responsables de seguridad tienen dificultades para gestionar el riesgo asociado a los dispositivos móviles, al haberse convertido en algo de uso común y cotidiano. Una vez se ha creado una cultura corporativa de que el uso de este tipo de dispositivos está permitido, es difícil luchar contra ésta e intentar poner límites a su utilización. Sin embargo, es preciso hacerlo si se quieren evitar fugas importantes de información. Para ello resulta necesario, por un lado, concienciar a los usuarios de los riesgos asociados a estos dispositivos e implementar las medidas de control del puesto de usuario para impedir su mala utilización.

En el caso de sistemas Windows se pueden tomar distintas medidas para controlar el uso de dispositivos simplemente impidiendo que usuarios no privilegiados instalen nuevos controladores de dispositivos. Esto no impedirá, sin embargo, que puedan utilizar dispositivos para los que los controladores ya estén disponibles en el sistema. Para controlar este caso se puede bloquear el acceso al archivo con la descripción de controladores disponibles (*Layout.pnf*) o al archivo que contienen los controladores (*Driver.cab*) de forma que el equipo no tenga acceso de lectura a este fichero. Para bloquear el acceso en el sistema pero permitir que los administradores puedan instalar dispositivos es necesario mover estos ficheros fuera del sistema (a una unidad de red) y dar permisos al grupo de administradores. Esto impediría que se pueda extraer de ellos los controladores disponibles para dispositivos pre-instalados. Nótese que no basta con cambiar permisos locales, dado que el servicio "*Plug and Play*" se ejecuta como usuario SYSTEM en el equipo local.

Para el caso específico de los dispositivos de almacenamiento masivo USB (que se cargarían sin intervención del usuario y sin necesidad de tener privilegios especiales), se pueden tomar distintas medidas:

- Deshabilitar la carga de dispositivos USB, bien modificando el registro o bien eliminando el controlador del sistema para que éste no pueda cargarse.
- Modificar la lista de dispositivos "reconocidos" como dispositivos de almacenamiento masivo modificando la lista definida en *usbstor.inf*, para que sólo un conjunto de dispositivos autorizados puedan hacer que se cargue de forma automática el controlador *usbstor.sys.*
- Deshabilitar la carga de controladores desde Internet.
- Bloquear el acceso de escritura a dispositivos de almacenamiento modificando la clave del registro. Esta alternativa sólo es posible en sistemas Windows XP SP2 (KB-555443).

En el caso de sistemas Linux es más sencillo ya que es posible:

- Deshabilitar el servicio *hotplug* para desactivar la carga automática de dispositivos (en Windows no se puede parar el servicio *Plug and Play* sin inhabilitar gran parte del sistema)
- Modificar la configuración del servicio para que no monte automáticamente dispositivos de almacenamiento
- Modificar la configuración de los permisos de montaje para usuarios impidiendo el montaje de dispositivos en el sistema de ficheros o limitando las operaciones que se pueden hacer con éstos (solo lectura, sin permisos de ejecución, etc.)

Análisis forense del uso de dispositivos portátiles

En algunas organizaciones puede llegar a darse el siguiente escenario de fuga de información:

- Un usuario de la organización abandona su estación de trabajo sin bloquearla (salvapantallas con contraseña).
- Un atacante accede físicamente al puesto de usuario con un dispositivo portátil y extrae datos de la estación de trabajo y los recursos de red a los que tiene acceso el usuario, realiza una copia masiva y abandona la estación.
- El usuario vuelve a su estación de trabajo tras el período de descanso y detecta algo que le hace sospechar que alguien ha utilizado su sistema

(porque hay una aplicación que él no ha lanzado, porque hay un mensaje del sistema de que se ha introducido y desconectado un dispositivo, etc.).

¿Cómo es posible saber si se ha producido un robo de información? ¿Cómo saber qué información ha sido sustraída?

En sistemas Windows el análisis forense con la información proporcionada por el propio sistema operativo de la conexión y desconexión de dispositivos es difícil **[9]**. El problema es que, *a priori*, parece no haber una forma para determinar si en un equipo se ha instalado o no un dispositivo USB. Por ejemplo, cuando se inserta un dispositivo no aparece ningún registro en los ficheros de registro habituales (de aplicación, sistema o seguridad).

La información de conexión de dispositivos se debe buscar, sin embargo en el registro almacenado en el fichero *Setupapi.log*. En este archivo se encontrarán los registros indicando si se ha introducido un dispositivo (y cargado su controlador asociado) y cuál es su identificador y número de serie. Además, la conexión de cualquier dispositivo USB almacena información en las claves de registro del sistema, donde se guarda una clave por cada dispositivo conectado. Aunque las herramientas de tratamiento del registro de Windows ordinarias (regedit.exe, regedt32.exe, reg.exe...) no proporcionan información de tiempo, sí que se guarda la fecha de modificación para las claves del registro (pero no para los valores) y se puede obtener esta información con otras herramientas.

Sin embargo, esta información sólo se modifica la primera vez que se conecta un dispositivo. Las conexiones sucesivas de un mismo dispositivo para el que ya se han determinado los controladores a utilizar y se ha introducido en el registro no introducen cambios que puedan trazarse en los cambios de configuración. Sólo un análisis forense de la información de acceso a ficheros (letra de unidad asignada, últimos ficheros accedidos desde el explorador de archivos, los "documentos recientes", etc.) podría hacer posible reconstruir cuándo se ha conectado un dispositivo y para qué se ha utilizado (uso dado a un dispositivo conectado al equipo).

En este caso se trata de una diferencia importante del caso de sistemas Linux, en el que los eventos de conexión de dispositivos se registran en el Syslog del sistema, pudiéndose recuperar trazas de los momentos exactos en los que se han conectado.

Software para el control de uso de dispositivos

La modificación de decenas o cientos de estaciones de trabajo para controlar la carga de dispositivos es, sin embargo, una tarea tediosa que requiere de la modificación de los puestos de usuario. Como hemos visto, en Windows se tiene que elegir entre introducir una política permisiva (se permite instalar cualquier dispositivo) o restrictiva (no se permite instalar ninguno, aunque esté en el sistema). La "tercera vía" es una opción consistente en la revisión de todos los controladores de dispositivos proporcionados por el sistema operativo para eliminar aquellos no autorizados en el entorno corporativo.

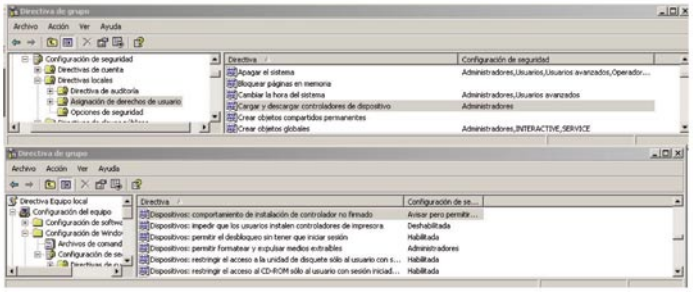

Figura 3. Configuración de políticas asociadas a dispositivos Windows

Para cubrir este hueco han surgido distintas soluciones software en el mercado para el control de dispositivos en entornos Windows. Las más conocidas son DeviceLock de Smartline, DeviceShield de Layton Technology, DeviceWall de Centennial Software, Safend Protector/Auditory USB Port Protector/Auditor de Safend, Sanctuary DeviceControl de Securewave y la plataforma Onigma del fabricante del mismo nombre.

En general, las soluciones de control de dispositivos tienen características similares y permiten:

- Controlar qué usuarios o grupos pueden acceder a los distintos dispositivos del sistema (CD-ROMs, USB, FireWire, WiFi, Bluetooth...), pudiendo establecer perfiles de uso en función del día y hora.
- Gestionar desde una consola centralizada.
- Auditar la actividad de uso de los dispositivos, bien con registros propios o enviando eventos al gestor de eventos de Windows, para disponer de una traza de auditoría.
- Realizar un despliegue de forma automática sobre equipos a través de las políticas de grupo de un directorio activo.

Algunos funcionan como servicio del sistema (lo que significa que un administrador local puede detenerlos) y otros como controladores en el núcleo. Algunos de estos productos también permiten la generación de códigos de desbloqueo temporal de forma que si un usuario no está en la oficina puede solicitar por teléfono un código temporal para acceder a un dispositivo que necesita utilizar como parte de su trabajo.

El coste de adquisición de este tipo de agentes de control no es excesivamente elevado, las licencias de un solo puesto rondan los 20-30 euros reduciéndose a 5-10 euros en el caso de instalaciones de más de 1.000 puestos.

Conclusiones

Los dispositivos portátiles suponen un riesgo no controlado hoy en día en la mayoría de las organizaciones, a pesar de disponer de herramientas, tanto en los propios sistemas operativos como las disponibles de aplicaciones de terceros para limitar y auditar su utilización, y reducir, por tanto su riesgo.

La aparición de nuevos tipos de dispositivos (como las memorias USB con capacidad de ejecución automática), el dramático incremento de su capacidad y la confianza y casualidad con la que se hace uso de este tipo de dispositivos no hace sino agravar el problema. A medio plazo las organizaciones tendrán que plantearse introducir políticas, so pena de exponerse a aparecer en las noticias como otra de las empresas que ha sufrido un robo importante de información interna o de sufrir las consecuencias de la sustracción masiva de información confidencial. ■

Javier Fernández-Sanguino
División de Seguridad,
GERMINUS
jfernandez@germinus.com

REFERENCIAS

[1] "Plug and Root", the USB key to the kingdom. David Barrall y David Dewey, SPI Dynamics, conferencias Black Hat, USA julio 2005 (disponible en http://www.blackhat.com/presentations/bh-usa-05/BH_US_05-Barrall-Dewey.pdf)

[2] *USB and CardBus (and some oddball PCMCIA) DMA security*, David Maynor, X-Force Advanced R&D, Internet Security Systems, conferencias CanSecWest/core05 (disponible en https://www.cansecwest.com/resources.html)

[3] Linux Kernel Security Report, Andy Chou, Bryan Fulton y Seth Hallern, Coverity, septiembre 2005.

[4] USB Storage - FAQ for Driver and Hardware Developers, Microsoft, octubre 2004. (disponible en http://www.microsoft.com/whdc/device/storage/usbfaq.mspx)

[5] Device Installation FAQ, Microsoft, octubre 2004 (disponible en http://www.microsoft.com/whdc/driver/install/installFAQ.mspx).

[6] Windows 2003 Technical Reference: How Device Drivers Work, Microsoft. marzo 2003 (disponible en http://technet2.microsoft.com/WindowsServer/en/Library/2e81a334-ece5-4210-815a-6a2ea33f61151033.mspx)

[7] Hotplug, http://linux-hotplug.sourceforge.net/ http://www.kernel.org/pub/linux/utils/kernel/hotplug/udev.html

[8] Preguntas frecuentes sobre HAL, http://freedesktop.org/wiki/Software_2fHalFAQ

[9] USB Storage Devices on Windows XP Systems, Harlan Carvey, MITRE corporation, 2005.