Revista de Comunicación Vivat Academia
ISSN: 1575-2844 · DOI: http://dx.doi.org/10.15178/va.2003.43.38-43
Marzo 2003 · Año VI · nº 43 · pp. 38-43

DATOS PRIVADOS EN DISCOS DUROS DE SEGUNDA MANO

PRIVATE DATA ON SECOND-HAND HARD DRIVES

Xavier Caballé: http://www.hispasec.com
xavi@hispasec.com

CURRÍCULUM VITAE

Programador y analista de sistemas de la empresa española de consultoría y programación Hispasec (www.hispasec.com). Especializado en redes y sistemas de protección de usuarios ante infecciones virales.

RESUMEN

La adquisición de discos duros de segunda mano por Internet se realiza cada vez más con mayor normalidad. El problema es que más de la mitad de estos discos permiten recuperar archivos que contienen información privada, desde datos médicos o cartas de amor, hasta números de tarjetas de crédito. El mercado de compra/ venta de equipos con varios años de antigüedad es muy importante.

PALABRAS CLAVE

Disco duro - Segunda mano - Información

ABSTRACT

The acquisition of second-hand hard drives over the Internet is increasingly being performed more normally. The problem is that over half of these discs can retrieve files containing private information from medical records or love letters to credit card numbers. The market purchase / sale of equipment with several years of seniority is very important.

KEY WORDS

Hard drive - Used (second hand) - Information

TEXTO:

Durante los dos últimos años, dos estudiantes del MIT han adquirido discos de segunda mano a través de subastas en Internet y tiendas de segunda mano. De un total de 129 discos adquiridos y operativos, fue posible recuperar archivos en un total de 69. Y de éstos, en 49 había información "privada": datos médicos, cartas de amor, pornografía y más de 5.000 números de tarjetas de crédito.

Esto puede poner los pelos de punta al indicar que, según algunas estimaciones, durante el año 2002 un total de 150.000 discos duros fueron "jubilados". Si bien la mayoría de estos discos retirados acaban en la papelera, un porcentaje significativo de los mismos pasa al mercado de segunda mano.

Hoy en día los en los discos duros de todos nosotros tenemos almacenada una gran cantidad de información altamente sensible, que bajo ningún concepto deseamos

ISSN: 1575-2844 · DOI: http://dx.doi.org/10.15178/va.2003.43.38-43

pueda llegar a manos de cualquier otra persona. Cuando borramos un archivo, en realidad lo que hacemos es indicarle al sistema operativo que lo marque como borrado y que su espacio en el disco pase a ser reutilizable. Pero los datos del archivo continúan en el disco hasta que no son sobrescritos. De la misma forma, formatear un disco no siempre borra los datos. Con el fin de hacer la operación lo más breve posible, en muchas ocasiones sólo se rescriben las cabeceras de los sectores del disco.

Es un hecho que, cada vez con más frecuencia (y no siempre de forma debidamente justificada), la vida operativa de los ordenadores personales se acorta. Por eso no es extraño que, llegado el momento de la ampliación o cambio, deseemos recuperar algo de la inversión efectuada procediendo a la subasta o venta del equipo antiguo. En el caso de las empresas, la situación todavía es más común. Hoy en día no es nada raro que las medianas y grandes empresas, en lugar de adquirir directamente los ordenadores tengan su parque de informática personal bajo leasing o renting. Por tanto, pasado el período de vida, estos equipos son devueltos a la empresa arrendataria. Un destino tradicional de estos equipos procedentes del leasing/renting es, al igual que sucede con los particulares, que pasen a propiedad de empresas especializadas en subastas o venta de equipos a precio de saldo.

Hoy en día existe un importante mercado de venta de equipos con dos/tres años de antigüedad que se nutre, precisamente, de los equipos que han finalizado su periodo de vida en las medianas y grandes empresas.

El estudio efectuado por los dos estudiantes del MIT se realiza a partir de discos que proceden de subastas en Internet o tiendas de segunda mano. Durante un período de dos años, se adquirieron un total de 158 discos duros, de los cuales 129 eran operativos. En el momento de recibir cada disco, se conectaban a un ordenador ejecutando FreeBSD 4.4 y se realizaba una copia, bloque a bloque del disco duro en un archivo imagen (mediante la utilidad dd del sistema operativo). Al finalizar la

copia, se intentaba montar el disco mediante diversos sistemas de archivo. Si se podía montar el archivo, se copiaban todos los archivos reconocidos con tar y se procedía al análisis de estos archivos. En total, los dos estudiantes del MIT obtuvieron 75 GB de datos (71 GB correspondían a las imágenes de particiones recuperadas y 3,7 GB eran archivos tar comprimidos). Los datos obtenidos son apabullantes. Del total de discos adquiridos, únicamente 12 (un 9%) habían pasado por un proceso de limpieza para garantizar el borrado de la información. 83 discos (64%) contenían particiones FAT16 o FAT32 directamente accesibles. El resto, 46 discos no contenían ninguna partición que pudiera ser accedida. De los 83 discos con particiones, 51 aparentemente habían sido formateados ya que no había ningún archivo. Otros seis discos si bien habían sido formateados, disponían de los archivos del sistema operativo (DOS o Windows) necesarios para arrancar la máquina. Pero en los discos no formateados también fue posible encontrar datos. Entre los 46 discos sin particiones, en 30 se pudo extraer información leyendo los diversos sectores del disco. Una vez identificados los discos, se procedió a recuperar los archivos: 675 documentos DOC, 274 hojas de cálculo XLS, 20 bases de mensajes PST, 566 presentaciones PPT. Algunos de estos archivos almacenaban datos especialmente sensibles: documentos de una empresa referentes al personal, una carta a un médico quejándose del tratamiento recibido para curar un cáncer, plantillas de fax de un hospital para niños, cartas de amor, imágenes pornográficas...

Para profundizar todavía más, se escribió un programa que rastreaba los discos en busca de datos de tarjetas de crédito (series de números que se ajustan al formato de las tarjetas de crédito y que son reconocidos como tales mediante el algoritmo de verificación). Entre todos los discos, en 42 de ellos se obtuvieron números aparentemente válidos de tarjetas de crédito. Uno de estos discos, contenía un gran número de tarjetas de crédito (más de 2.800 números). El análisis más detallado del mismo llega a la conclusión que el disco pertenecía a un cajero automático. Otro disco duro almacenaba los números de más de 3.700 tarjetas de crédito dentro de lo

ISSN: 1575-2844 · DOI: http://dx.doi.org/10.15178/va.2003.43.38-43

que se asemejaba a un archivo log. En otro caso, la tarjeta de crédito estaba dentro de un archivo procedente de la memoria caché del navegador web. Existen un gran número de herramientas útiles cuando se intenta recuperar los datos que una vez estuvieron almacenados en un disco. En el apartado de "Más información" incluimos los enlaces a diversas herramientas, como TestDisk (una herramienta para acceder a los datos de particiones borradas, con soporte para particiones FAT, FAT32, Linux, NTFS, BeFS, NetWare...) y The Coroner's Toolkit (un conjunto de utilidades para investigaciones forenses que se puede utilizar para acceder a datos borrados). También incluimos los enlaces de AutoClave, un sistema para el borrado seguro de los datos del disco duro y un par de comparativas de diversas herramientas para el borrado seguro de los datos. Otra alternativa es el cifrado de los datos. Algunos sistemas operativos, como Windows 2000/XP, incorporan de serie la posibilidad de cifrar los datos almacenados en el disco. También PGP permite crear discos virtuales cuyo contenido está permanentemente cifrado. De esta forma, si alguien dispone de acceso al disco, a pesar de que pueda recuperar los datos, lo tendrá muy difícil para poder visualizar la información.

CONCLUSIÓN

Las conclusiones que se obtiene de todo este estudio es que antes de deshacerse de un disco duro, hay que tomar una serie de medidas adecuadas para garantizar que los datos almacenados en su interior son totalmente borrados. Las recomendaciones que se realizan son:

* Los usuarios deben conocer las técnicas necesarias para el borrado seguro de la información.

* Las organizaciones deben establecer políticas para el borrado de todos los sistemas de almacenamientos que son vendidos, destruidos o devueltos al fabricante. Como

ejemplo, en el apartado de más información incluimos las recomendaciones que realiza al respecto la NASA.

* Los fabricantes de sistemas operativos deberían incluir herramientas de sistema para el borrado seguro de los datos.

* En el futuro, los sistemas operativos deberían realizar la operación de borrado seguro de forma automática.

* Siempre que sea posible, es conveniente utilizar sistemas de archivos que incorporen funciones de cifrado.

* Los fabricantes de discos deben facilitar herramientas para garantizar la confidencialidad de los datos almacenados.

Más información en:

NASA Office of Inspector General - Protect Yourself and NASA Before Getting Rid of That Old Home Computer
http://www.hq.nasa.gov/office/oig/hq/identity.html

Security: File wiping
http://www.stack.nl/~galactus/remailers/index-wipe.html

Wipe - Secure File Wiping Utility for Linux
http://www.heidi.ie/eraser

TestDisk - Herramienta para recuperación de particiones borradas
http://www.cgsecurity.org/index.html?testdisk.html

ISSN: 1575-2844 · DOI: http://dx.doi.org/10.15178/va.2003.43.38-43