

Reto Forense Episodio III - Resumen Técnico

José Salvador González Rivera

Puebla, México / Marzo 2006

Introducción

La idea de este resumen técnico es realizar investigación sobre un sistema comprometido para el concurso "Reto Forense Episodio III". El escenario básico a entender es el siguiente:

El administrador de sistemas de una pequeña empresa ha notado que existe una cuenta que él no creó en su sistema de ERP, por lo que sospecha de algún ingreso no autorizado, del que desconoce el alcance. El sistema en que se ejecuta la aplicación es un servidor Windows 2003, cuya principal función era proporcionar acceso al sistema ERP a través de la Web. Hace poco tiempo que habían migrado al uso de este servidor.

Según el administrador, trataba de mantener el sistema actualizado por lo que no sabe cómo pudieron ingresar a su sistema. Sin embargo, también mencionó que más de una persona tiene acceso a cuentas privilegiadas en el sistema y aceptó que ocupaban a veces estas cuentas para labores no sólo administrativas, sino también personales o para aplicaciones que no requerían ningún tipo de privilegio para ejecutarse.

Objetivos

El objetivo principal es determinar si existió un ingreso no autorizado, cómo ocurrió y el alcance del daño al sistema e información.

Evidencias

Se cuenta únicamente con la imagen del servidor Windows, sin más información adicional.

Herramientas utilizadas

El sistema operativo que utilicé fue *WindowsXP* por la única razón que es mi sistema operativo de escritorio y se pueden aprovechar sus utilerías; ya instalados tenía *TheCleaner* (AntiTrojans) y *Norton Antivirus*. Utilicé *MountImage Pro* (versión de prueba) para montar la imagen y *Cygwin* para trabajar bajo un entorno similar a Linux y aprovechar el uso de sus comandos de manera gratuita. También usé el programa gratuito *PC Inspector File Recovery* para la recuperación de archivos borrados y *QuickViewPlus* (versión de prueba) para la visualización de archivos sin abrirlos. Adicionalmente busqué y encontré *Windows Registry File Viewer* el cual es un programa gratuito para ver archivos del registro de *Windows* y *hfind/sfind/galleta* de Foundstone los cuales son *software* gratuito. No utilicé *suites* específicas para análisis forense, sino más bien, comandos y programas ordinarios.

Análisis Forense

Esta es la primera vez que realizo un análisis forense por lo que busqué un método que me llevara de la mano, por lo que revisé el documento *Forensic Examination of Digital Evidence* del **NIJ** (U.S. National Institute of Justice) que consiste en:

- Preparar un directorio independiente para almacenar datos recuperados o extraídos.
- Extracción de información física (búsqueda de palabras clave) y lógica (recuperación y extracción).
- Análisis de datos de interés, aplicaciones, programas ocultos, código malicioso, etc.
- Conclusión del análisis.

El documento puede encontrarse en la dirección: <http://www.ojp.usdoj.gov/nij>

Nota: En el transcurso del análisis, favor de poner atención al tipo de *prompt* ya que puede mostrar un comando en *cygwin* (\$) como también en *cmd* (c:\>)

Archivos de Imagen

Terminé de obtener las imágenes del sistema comprometido de la siguiente dirección:

<http://pgp.rediris.es:16000/reto3.0/>

Procedí inmediatamente a verificar las sumas de verificación *md5*:

```
$ md5sum windows2003.img.gz.a?
c972863f5584a95f1d5ff350d972b48d *windows2003.img.gz.aa
b7a57c513a0abl8914f63cc927d8b4e0 *windows2003.img.gz.ab
42ef380cf64ddfc956dbf6acf63a174c *windows2003.img.gz.ac
4fc8381404fef912ae77f61244128643 *windows2003.img.gz.ad
fba13b0f9cddf1a83b4d244c2987811f *windows2003.img.gz.ae
4fa323705ee2064415c2854b8abef502 *windows2003.img.gz.af
490e34026f2aaf91604b9e84896def16 *windows2003.img.gz.ag
```

Comparados con las sumas *md5* proporcionadas por UNAM-CERT / RedIris se tiene la seguridad que mantienen su integridad y no fueron alteradas o modificadas en el tránsito. Procedí a descomprimir los archivos para formar la imagen completa:

```
$ cat windows2003.img.gz.a? | gunzip -d > windows2003.img
```

La cual, vuelvo a comprobar su integridad que obviamente, debe coincidir con la suma *md5* proporcionado por UNAM-CERT / RedIris:

```
$ md5sum windows2003.img
062cf5d1ccd000e20cf4c006f2f6ccea4 *windows2003.img
```

Para determinar que tipo de archivo es, utilicé el comando *file* el cual nos dice que es un archivo de imagen con todos sus parámetros:

```
$ file windows2003.img
windows2003.img: x86 boot sector, code offset 0x52, OEM-ID "NTFS      ",
sectors/cluster 8, reserved sectors 0, Media descriptor 0xf8, heads 255,
hidden sectors 63, dos < 4.0 BootSector (0x80)
```

Por esta razón para *montarlo* en el sistema utilicé *Moun Image Pro*, primero compruebo que utiliza un sistema de archivo NTFS:

```
C:\Archivos de programa\Mount Image Pro>mip view j:\reto\windows2003.img
Mount Image Pro 1.05

Disk Capacity   : 10233342 sectors (4996 MB)
Number Of Files : 1

  Type      Size      Path
  ----      -
  RAW      10233342  j:\reto\windows2003.img

Partitions      :
  #      Start Sector      Length in sectors      Type
  --      -
  0              0      10233342 ( 4996 MB)  NTFS
```

Y procedo a montarlo en la unidad Z en modo de solo-lectura (default):

```
C:\Archivos de programa\Mount Image Pro>mip open * j:\reto\windows2003.img /L:Z
Mount Image Pro 1.05

Started the Virtual Disk Driver.
Virtual Disk 0
Access Type      : Read-Only
Disk Capacity    : 10233342 sectors (4996 MB)
Number Of Files  : 1
```

Type	Size	Path
RAW	10233342	j:\reto\windows2003.img

Partitions		:		
#	Start Sector	Length in sectors	Type	
z:	0	0	10233342 (4996 MB) NTFS

En Cygwin asigno a `/cygdrive/z` directamente a `/z` por comodidad:

```
$ mount -c /
```

Extracción de Información

Versión del Sistema Operativo

El nombre de un archivo es subjetivo y no revela precisamente su contenido, por lo que para estar seguros de la versión del sistema operativo a analizar, revisé la estructura de directorios y la ubicación del registro de Windows:

```
$ ls /z/windows/system32/config/system
/z/windows/system32/config/system
```

La ruta `\windows\system32\config` es el directorio por default donde Windows XP y 2003 almacenan su registro, a diferencia de otros sistemas por ejemplo Windows NT (`\winnt\system32\config\system`) o Windows 98 (`\windows\system.dat`). También verifiqué el archivo `boot.ini`:

```
$ cat /z/boot.ini
[boot loader]
timeout=30
default=multi(0)disk(0)rdisk(0)partition(1)\WINDOWS
[operating systems]
multi(0)disk(0)rdisk(0)partition(1)\WINDOWS="Windows Server 2003, Enterprise"
/noexecute=optout /fastdetect
```

Donde se puede apreciar que la única partición NTFS arranca un *Server 2003* versión *Enterprise*. Además, a convenir por su estructura de directorios (`/Program Files`) y por el idioma del contrato de licencia (`/windows/system32/eula.txt`) es la versión en inglés (de evaluación por 180 días).

Listado de archivos

La primera extracción que hice fue el listado de archivos con su respectiva información:

```
$ find /z/ -printf "%m;%Ax;%AT;%Tx;%TT;%Cx;%CT;%s;%p\n" > /j/reto/archivos.txt
```

Donde:

- %m** = Permisos tipo Unix.
- %Ax** = Fecha de acceso
- %AT** = Hora de acceso
- %Tx** = Fecha de modificación
- %TT** = Hora de modificación
- %Cx** = Fecha de cambios
- %CT** = Hora de cambios
- %s** = Tamaño
- %p** = Nombre del archivo

Este listado lo guardé como referencia en el transcurso de la investigación y lo incluyo como anexo a este documento. Incluyendo también los archivos ocultos detectados con *hfind*:

```
J:\reto>hfind z:\ > ocultos.txt
```

Registro de Windows

En la carpeta `\windows\system32\config` se encuentran intactos los archivos de registro del sistema operativo, así como las bitácoras del sistema que pueden verse con *Event Viewer*.

```
$ file /z/WINDOWS/system32/config/*
/z/WINDOWS/system32/config/AppEvent.Evt: data
/z/WINDOWS/system32/config/DnsEvent.Evt: data
/z/WINDOWS/system32/config/SAM: Windows NT registry file
/z/WINDOWS/system32/config/SAM.LOG: Windows NT registry file
/z/WINDOWS/system32/config/SECURITY: Windows NT registry file
/z/WINDOWS/system32/config/SECURITY.LOG: Windows NT registry file
/z/WINDOWS/system32/config/SecEvent.Evt: data
/z/WINDOWS/system32/config/SysEvent.Evt: data
/z/WINDOWS/system32/config/TempKey.LOG: Windows NT registry file
/z/WINDOWS/system32/config/default: Windows NT registry file
/z/WINDOWS/system32/config/default.LOG: Windows NT registry file
/z/WINDOWS/system32/config/default.sav: Windows NT registry file
/z/WINDOWS/system32/config/software: Windows NT registry file
/z/WINDOWS/system32/config/software.LOG: Windows NT registry file
/z/WINDOWS/system32/config/software.sav: Windows NT registry file
/z/WINDOWS/system32/config/system: Windows NT registry file
/z/WINDOWS/system32/config/system.LOG: Windows NT registry file
/z/WINDOWS/system32/config/system.sav: Windows NT registry file
/z/WINDOWS/system32/config/systemprofile: directory
/z/WINDOWS/system32/config/userdiff: Windows NT registry file
/z/WINDOWS/system32/config/userdiff.LOG: Windows NT registry file
```

Programas Instalados en Windows

Debido a que no se tuvo acceso al equipo antes de ser apagado para recolectar datos *en-caliente* (solo se cuenta con la imagen del disco), no es posible saber que programas estaban corriendo. Tampoco le veo sentido intentar reconstruir el servidor en una máquina virtual pues la información volátil ya se perdió. Solo queda ver que programas están o estaban instalados y registrados por el sistema operativo, a través de la clave del registro *Uninstall*, debido a que los programas que se instalan y registran en Windows crean una entrada en esta llave:

Archivo de registro:	<code>\windows\system32\config\software</code>
Llave de registro:	<code>Microsoft\Windows\CurrentVersion\Uninstall</code>

AddressBook	Pertenece a Windows 2003
Branding	Pertenece a Windows 2003
Connection Manager	Pertenece a Windows 2003
DirectAnimation	Pertenece a Windows 2003
DirectDrawEx	Pertenece a Windows 2003
DXM_Runtime	Pertenece a Windows 2003
Fontcore	Pertenece a Windows 2003
ICW	Pertenece a Windows 2003
IE40	Pertenece a Windows 2003
IE4Data	Pertenece a Windows 2003
IE5BAKEX	Pertenece a Windows 2003
IEData	Pertenece a Windows 2003
KB890046	Parche corresponde al boletín MS05-032
KB896358	Parche corresponde al boletín MS05-026
KB896422	Parche corresponde al boletín MS05-027
KB896424	Parche corresponde al boletín MS05-053
KB896428	Parche corresponde al boletín MS05-033

KB896688	Parche corresponde al boletin MS05-052
KB896727	Parche corresponde al boletin MS05-038
KB899587	Parche corresponde al boletin MS05-042
KB899589	Parche corresponde al boletin MS05-046
KB901017	Parche corresponde al boletin MS05-048
KB901214	Parche corresponde al boletin MS05-036
KB902400	Parche corresponde al boletin MS05-051
KB903235	Parche corresponde al boletin MS05-037
KB905414	Parche corresponde al boletin MS05-045
KB908519	Parche corresponde al boletin MS06-001
MobileOptionPack	Perteneciente a Windows 2003
Mozilla Firefox (1.5.01)	C:\Program Files\Mozilla FireFox\firefox.exe
Mplayer2	Perteneciente a Windows 2003
NetMeeting	Perteneciente a Windows 2003
OutlookExpress	Perteneciente a Windows 2003
PCHealth	Perteneciente a Windows 2003
PHP 4.4.2	C:\apache\Apache\php
SchedulingAgent	Perteneciente a Windows 2003

Las entradas en el registro pertenecen al sistema operativo, a excepción de las marcadas de color rojo que son los *fixes de seguridad*, el programa *Mozilla Firefox 1.5.01* y *PHP 4.4.2*.

Programas Instalados de los usuarios

Revisé el archivo *NTUSER.DAT* de cada usuario para encontrar la entrada de registro *Software*, solo los usuarios *Administrator* y *ver0k* tienen instalados programas adicionales:

Archivo de registro:	\Documents and Settings\Administrator\NTUSER.DAT
Llave de registro:	HKEY_CURRENT_USER\Software

Programas que no son pertenecientes por default a Windows 2003:

```
BitTorrent      (Es para el intercambio de archivos P2P)
IM Providers -> MSN Messenger
Macromedia -> FlashPlayer
Microsoft -> Elementos del SO
Mozilla -> Mozilla Firefox
Sysinternals -> TCPView (Escucha puertos TCP/UDP de Sysinternals)
```

Archivo de registro:	\Documents and Settings\ver0k\NTUSER.DAT
Llave de registro:	HKEY_CURRENT_USER\Software

Programas que no son pertenecientes por default a Windows 2003:

```
IM Providers -> MSN Messenger
```

Programas Usados

También revisé la llave *AppPaths* por si había algún registro de un software no conocido:

Archivo de registro:	\windows\system32\config\software
Llave de registro:	Microsoft\Windows\CurrentVersion\AppPaths

CluAdmin.exe	Perteneciente a Windows 2003
Cmmgr32.exe	Perteneciente a Windows 2003
CONF.EXE	Perteneciente a Windows 2003
Dialer.exe	Perteneciente a Windows 2003
Firefox.exe	C:\Program Files\Mozilla Firefox\firefox.exe
HELPCTR.EXE	Perteneciente a Windows 2003
ICWCONN1.EXE	Perteneciente a Windows 2003
ICWCONN2.EXE	Perteneciente a Windows 2003

IEXPLORE.EXE	Perteneciente a Windows 2003
INETWIZ.EXE	Perteneciente a Windows 2003
Install.exe	Perteneciente a Windows 2003
ISIGNUP.EXE	Perteneciente a Windows 2003
Mplayer2.exe	Perteneciente a Windows 2003
MSCONFIG.EXE	Perteneciente a Windows 2003
Msimn.exe	Perteneciente a Windows 2003
Msinfo32.exe	Perteneciente a Windows 2003
MSNMSGR.EXE	Mensajería Instantánea
Pbrush.exe	Perteneciente a Windows 2003
Setup.exe	Perteneciente a Windows 2003
Table30.exe	Perteneciente a Windows 2003
Wab.exe	Perteneciente a Windows 2003
Wabmig.exe	Perteneciente a Windows 2003
Winn32.exe	Perteneciente a Windows 2003
Wmplayer.exe	Perteneciente a Windows 2003
WORDPAD.EXE	Perteneciente a Windows 2003
WRITE.EXE	Perteneciente a Windows 2003

Solo se encontraron *FireFox* y *MSN Messenger*, también busqué en la llave:

Archivo de registro:	\windows\system32\config\software
Llave de registro:	HKEY_LOCAL_MACHINE\Software

Programas que no son pertenecientes por default a Windows 2003:

```
Apache Group
PostgreSQL
PgAdmin III
MySQL AB
Mozilla
```

Comparando el resultado, eliminé las entradas que pertenecen a Windows 2003, y quedan las 5 aplicaciones conocidas mostradas en el recuadro anterior, que corresponde a las aplicaciones que están instaladas (*Apache*, *MySQL*, *PostgreSQL*, *Firefox*).

Adicionalmente busqué por archivos con extensión *.com*, *.exe*, *.bat*, *.pif* y *.cmd* en los perfiles de los usuarios encontrando solo archivos *.exe* en los perfiles de **Administrator** y **maick**, los cuales el comando *file* confirma que son ejecutables *PE executable for MS Windows (GUI) Intel 80386 32-bit* que corresponde a los ejecutables de los parches de seguridad, los programas anteriormente descubiertos (*BitTorrent* y *Firefox*), utilerías y animaciones de los famosos *huevo-cartoons*. Solo cabe destacar el directorio: *Sof7w4r3*, que contiene los archivos de instalación y comprimido de *postgresql-8.1.0-2*, las utilerías *Tcpview.exe* de Sysinternals, *cports* de Nirsoft y *languardnss6.exe* de GFI, las cuales son herramientas que pudieron ayudar en el manejo de la red al Administrador.

Tareas programadas

Busqué archivos con extensión *.job* que corresponde al *Programador de Tareas* (*schtasks.exe*), no había ningún archivo normal o con atributo escondido (*h*):

```
$ ls -la /z/windows/tasks/*.job
ls: /z/windows/tasks/*.job: No such file or directory
```

Arranque de programas al inicio

Existen programas como *AutoStart* de DiamondCS o *Autoruns* de SysInternals dedicados a recolectar los datos necesarios para saber que programas corren al inicio del sistema, sin embargo deben ser usados en un sistema funcionando (*en-caliente*). Para ver que programas se cargan desde el inicio, comprobé manualmente cada directorio y entrada del registro:

Lugar	Descripción																
\Documents and Settings \%User%\Start Menu \Programs \Startup	Folder Inicio (Startup) del usuario, de: <table border="1"> <thead> <tr> <th>Usuario</th> <th>Programas</th> </tr> </thead> <tbody> <tr> <td>Administrator</td> <td>Ninguno</td> </tr> <tr> <td>Johnatan</td> <td>Ninguno</td> </tr> <tr> <td>maick</td> <td>Ninguno</td> </tr> <tr> <td>maru</td> <td>Ninguno</td> </tr> <tr> <td>Postgres</td> <td>Ninguno</td> </tr> <tr> <td>reno</td> <td>Ninguno</td> </tr> <tr> <td>ver0k</td> <td>Ninguno</td> </tr> </tbody> </table>	Usuario	Programas	Administrator	Ninguno	Johnatan	Ninguno	maick	Ninguno	maru	Ninguno	Postgres	Ninguno	reno	Ninguno	ver0k	Ninguno
Usuario	Programas																
Administrator	Ninguno																
Johnatan	Ninguno																
maick	Ninguno																
maru	Ninguno																
Postgres	Ninguno																
reno	Ninguno																
ver0k	Ninguno																
\Documents and Settings \ All Users \Start Menu \Programs \Startup	Folder Inicio de todos los usuarios. Ningún programa encontrado.																
HKEY_CURRENT_USER \Software \Microsoft WindowsNT \CurrentVersion \Windows \load	Lugar poco utilizado pero factible. No se encontró la llave <i>load</i> .																
HKEY_LOCAL_MACHINE \Software \Microsoft WindowsNT \CurrentVersion \Winlogon \Userinit	Lugar que puede iniciar programas cuando el sistema inicia. No se encontró programa.																
HKEY_CURRENT_USER \Software \Microsoft Windows \CurrentVersion \Policies \Explorer \Run HKEY_LOCAL_MACHINE \Software \Microsoft Windows \CurrentVersion \Policies \Explorer \Run	Explorer \ Run, existe en las 2 llaves raíz. No se encontró la llave.																
HKEY_CURRENT_USER \Software \Microsoft Windows \CurrentVersion \RunOnce \Setup HKEY_LOCAL_MACHINE \SOFTWARE \Microsoft Windows \CurrentVersion \RunOnce \Setup	Aquí se especifican los programas a correr después de que el usuario se loguea. No se encontró la llave.																
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce	<i>MACHINE</i> : Corre el programa después que el usuario se loguea. <i>USER</i> : Corre después de que el SO corre el contenido del folder Inicio (Startup).																
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnceEx HKEY_CURRENT_USER \Software \Microsoft Windows \CurrentVersion \Run	USER: No se encontró programa. MACHINE: No se encontró llave.																
HKEY_LOCAL_MACHINE \SOFTWARE \Microsoft Windows \CurrentVersion \Run	Preceden al folder de inicio. No se encontró programa.																

Detección de código malicioso

Revisé la unidad completa con *TheCleaner* actualizado al 31 de Enero 2006.

No se encontraron caballos de Troya en ninguno de los 19,456 archivos analizados.

Revisé la unidad completa con *Norton Antivirus* actualizado al 12 de febrero 2006.

No se encontraron virus, pero se identificaron los siguientes archivos peligrosos en el perfil de la cuenta *Administrator*:

Nombre Archivo	Nombre Amenaza	Acción
a.exe	Adware.MediaTicket	Publicidad no deseada
dr-1.exe	Adware.DollarRevenue	Publicidad no deseada

Ambos archivos comprimidos en:

Z:\Documents and Settings\Administrator\My Documents\explorer.exe

Detección de Alternate Data Streams (ds)

Un sistema NTFS es un sistema NO-Monolitico que separa la información de un archivo y sus recursos, por ejemplo localización, fonts, iconos, datos del autor y más información. Mantiene un mapeo por medio del Master File Table (MFT) que es administrada por el API de Windows y accedida por las aplicaciones, pero existe una inconsistencia de DataStreams documentada en el artículo [Q101353](#) de Microsoft, que permite “ocultar” datos. Por medio de la herramienta *sfind* realicé una búsqueda de este tipo de archivos ocultos:

```
j:\reto>sfind z:\
Searching...
Z:\Documents and Settings\Johnatan\My Documents\imagenes
  Thumbs.db:encryptable Size: 0
Finished
```

No se encontró más que una cadena escondida en el archivos *Thumbs.db* del usuario *Johnatan*, sin embargo esto no es extraño para este tipo de archivos (base de datos para imágenes).

Recuperar archivos borrados

Realicé una búsqueda normal de archivos borrados con *PC Inspector File Recovery*, y encontré lo siguiente:

PID de Apache

Archivo borrado	Descripción
\apache\apache\logs\httpd.pid	Contiene el identificador de un proceso corriendo.
Contenido relevante	Causa de borrado
1156	Es normal que la aplicación borre este tipo de archivos una vez que el servicio fue dado de baja.

PID de MySQL

Archivo borrado	Descripción
\apache\apache\mysql\data\counters.pid	Contiene el identificador de un proceso corriendo.
Contenido relevante	Causa de borrado
3972	Es normal que la aplicación borre este tipo de archivos una vez que el servicio fue dado de baja.

Documents and Settings

Usuario	Archivos
Administrator	Dentro de su perfil de usuario, borró un archivo XML del historial de Internet Explorer llamado allservices[1].xml
Ruta Completa:	\Documents and Settings\Administrator\LocalSettings\Temporary Internet Files\Content.IE5\0VAMEMD9

Contenido relevante	Causa de borrado
Ninguno	Toda la actividad de Internet es guardada en sus archivos temporales, es posible que el usuario ni siquiera sepa el nombre del archivo que borró, simplemente pudo haber borrado su historial desde el IExplorer.

Usuario	Archivos
Johnatan	Dentro de su perfil de usuario, borró directorios y archivos del historial de Internet Explorer.

Ruta Completa: \Documents and Settings\Johnatan\LocalSettings\Temporary Internet Files\Content.IE5*

Contenido relevante	Causa de borrado
Incluye formas del programa webERP	Toda la actividad de Internet es guardada en sus archivos temporales, es posible que el usuario ni siquiera sepa el nombre de los archivos y carpetas que borró, simplemente pudo haber borrado su historial desde el IExplorer.

Nota: Las formas en formato *.htm* muestra actividad con privilegios para el programa webERP con la posibilidad de editar y borrar cuentas de usuario, debido a que se muestra el nombre del usuario Alberto Contreras Zacarías (acontreras) en lugar de Johnatan Tezca (según su correo registrado en sus archivos temporales de internet jonathan.tezca@yahoo.com) se anexa evidencia para que el responsable del sistema determine si es correcto que este usuario posea estos privilegios.

Usuario	Archivos
ver0k	Dentro de su perfil de usuario, los archivos borrados corresponden a la aplicación Messenger.
	Dentro de sus archivos temporales se incluían archivos de imagen
	Se encontró un acceso directo <i>Windows Media Player.lnk</i> dentro de la carpeta Entertainment.

Ruta Completa: \Documents and Settings\ver0k\LocalSettings\Temporary Internet Files\Content.IE5*

\Documents and Settings\ver0k\LocalSettings\Temp\1*.tmp

\Documents and Settings\ver0k\Start Menu\Programs\Accesorios\Entertainment

Contenido relevante	Causa de borrado
Ninguno	Toda la actividad de Internet es guardada en sus archivos temporales, es posible que el usuario ni siquiera sepa el nombre del archivo que está borrado.

Archivos de PostgreSQL

Archivo borrado	Descripción
\Program Files\PostgreSQL\8.1\data\postmaster.pid	Contiene el identificador de un proceso corriendo.

Contenido relevante	Causa de borrado
2664	Es normal que la aplicación borre este tipo de archivos una vez que el servicio fue dado de baja.

Archivo borrado	Descripción
\Program Files\PostgreSQL\8.1\data\global\pgstat.stat	Contiene el monitor que lleva las estadísticas de <i>pg</i> .

Contenido relevante	Causa de borrado
Ninguno	Probablemente borrado por la aplicación.

Temporales Borrados

Archivo borrado	Descripción
\Windows\Temp\ib5	Contiene la salida de INNODB MONITOR perteneciente a la aplicación MySQL.

Contenido relevante	Causa de borrado
Ninguna para este análisis	Es normal que la aplicación borre sus archivos temporales.

Nota: También se encontraron los archivos *ib6* e *ib7* que pertenecen a la misma aplicación pero con ningún contenido (tamaño 0).

System Volume Information

Se encontraron archivos en la carpeta *catalog.wci*; estas carpetas son parte del sistema de restauración que permite poner puntos de tiempo en el sistema para poder realizar un *rollback*. Existe registro de estas carpetas en los eventos registrados:

```
Tipo de suceso:      Información
Origen del suceso:   Ci
Categoría del suceso: Servicio CI
Id. suceso:          4137
Fecha:               26/01/2006
Hora:                04:13:10 p.m.
Usuario:             No disponible
Equipo:              COUNTERS
Descripción:
Se ha iniciado el índice de contenido para el catálogo c:\system volume
information\catalog.wci.
```

Revisión Memoria de Intercambio

Con el comando *strings* de *cygwin* se analizó el archivo *c:\pagefile.sys* arrojando las cadenas de caracteres legibles en el archivo, se encontraron llaves y datos del registro de *Windows* las cuales revisé con *Windows Registry File Viewer* sin embargo no encontré datos relevantes que me pudieran aportar una pista.

Directorios Temporales

Temporales del Sistema

Se encontraron en *c:\windows\TEMP* los archivos *UPD5F.tmp* y *UPD6F.tmp* los cuales son de tipo ejecutable:

```
$ file UPD5F.tmp UPD6F.tmp
UPD5F.tmp: PE executable for MS Windows (console) Intel 80386 32-bit
UPD6F.tmp: PE executable for MS Windows (console) Intel 80386 32-bit
```

Este tipo de archivos los he visto en otros sistemas *Windows*, por lo que muy probablemente puedo comprobar que son pertenecientes a los fixes de seguridad instalados previamente, para esto revisé el contenido de las Bitacoras de instalación de parches:

```
$ cat /z/WINDOWS/KB*.log | grep UPD5F.tmp
2.547: Source:c:\windows\TEMP\UPD5F.tmp (6.2.29.0)
2.562: Source:c:\windows\TEMP\UPD5F.tmp (6.2.29.0)
12.062: Source:c:\windows\TEMP\UPD5F.tmp (6.2.29.0)
12.094: Source:c:\windows\TEMP\UPD5F.tmp (6.2.29.0)
3.687: Source:c:\windows\TEMP\UPD5F.tmp (6.2.29.0)
...
...
```

Lo mismo para el otro archivo:

```
$ cat /z/WINDOWS/KB*.log | grep UPD6F.tmp
2.547: Source:c:\windows\TEMP\UPD6F.tmp (6.2.29.0)
2.562: Source:c:\windows\TEMP\UPD6F.tmp (6.2.29.0)
```

```

12.062: Source:c:\windows\TEMP\UPD6F.tmp (6.2.29.0)
12.094: Source:c:\windows\TEMP\UPD6F.tmp (6.2.29.0)
3.719: Source:c:\windows\TEMP\UPD6F.tmp (6.2.29.0)
...
...

```

La salida la muestro truncada por fines prácticos, sin embargo una sola aparición es suficiente para determinar el origen de estos archivos. También se encontraron en *TEMP* los archivos **ibx** que pertenecen al manejador de base de datos de *MySQL*.

Temporales de los Usuarios

Analizando la clave Environment del registro (\windows\system32\config\system) por medio de *Windows Registry File Viewer* los directorios **TEMP** y **TMP** definidos se encuentran en %USERPROFILE%\LocalSettings\Temp

No se encontró información relevante de los archivos temporales en los perfiles de usuarios:

reno: Su directorio solo contenía residuos de páginas web en formato *.tmp*, de los sitios: Universidad de Valladolid, imágenes de Conapesca y www.vlex.com editorial jurídica.

maick: Su directorio solo contenía los archivos *tmp.xpi*, *tmp-1.xpi*, *tmp-2.xpi* que forman parte de la instalación de *Flash* en forma de *plug-in* para el Explorador de Internet.

administrator: Se encontraron algunos archivos y carpetas:

```

Z:\Documents and Settings\Administrator\Local Settings\Temp>tree
Listado de rutas de carpetas
El número de serie del volumen es 00003F5C A803:85D0
Z: .
+---ff_temp
|   +---xpcom.ns
|   |   +---bin
|   |   |   +---components
+---~nsu.tmp

```

Al hacer un listado recursivo se muestran los siguientes archivos en:

Z:\Documents and Settings\Administrator\Local Settings\Temp				
25/11/2004	04:36	p.m.	1,818	DuplicateConf.awk
01/02/2006	12:50	p.m.	<DIR>	ff_temp
24/11/2004	02:10	p.m.	35,639	httpd.conf-dist-win
26/01/2006	08:38	p.m.	41,415,680	mysql_server.msi
12/10/2005	05:02	a.m.	79,377	qmgr.cab
12/10/2005	05:02	a.m.	2,072	qmgr.inf
25/11/2004	04:36	p.m.	940	RewriteConf.awk
04/02/2006	03:18	p.m.	<DIR>	~nsu.tmp

Directorio de Z:\Documents and Settings\Administrator\Local Settings\Temp\ff_temp\xpcom.ns\bin				
01/02/2006	12:50	p.m.	413,789	js3250.dll
01/02/2006	12:50	p.m.	155,748	nspr4.dll
01/02/2006	12:50	p.m.	28,777	plc4.dll
01/02/2006	12:50	p.m.	24,676	plds4.dll
01/02/2006	12:50	p.m.	68,203	xpcom_compat.dll
01/02/2006	12:50	p.m.	401,510	xpcom_core.dll

Directorio de Z:\Documents and Settings\Administrator\Local Settings\Temp\ff_temp\xpcom.ns\bin\components				
01/02/2006	12:50	p.m.	60,516	jar50.dll

```
01/02/2006 12:50 p.m. 165,990 xpinstal.dll
```

```
Directorio de Z:\Documents and Settings\Administrator\Local Settings\Temp\~nsu.tmp
```

```
01/02/2006 12:51 p.m. 99,487 Au_.exe
```

Buscando referencias confiables en Internet mediante *Google* (sitios oficiales de publicaciones y no páginas personales o similar), se puede determinar que los archivos *qmgr.** pertenecen a *Microsoft MSN*, también se aprecian archivos de instalación de *MySQL* y el directorio *ff_temp* que pertenece a *Mozilla Firefox*. El último directorio *~nsu.tmp* tiene *au_.exe* el cual es el instalador de un programa *antispyware* llamado *spyaxe*.

Investigación de Usuarios

Fecha de última modificación ordenado por fecha:

```
$ ls -calt /z/Documents\ and\ Settings/  
total 0  
drwxrwx---+ 14 Administradores SYSTEM 0 Feb 5 15:49 maick  
drwxrwxr-x+ 10 Administradores SYSTEM 0 Feb 5 15:10 ..  
drwxrwx---+ 14 Administradores SYSTEM 0 Feb 5 14:47 ver0k  
drwxrwxr-x+ 13 Administradores SYSTEM 0 Feb 5 14:47 .  
drwxrwx---+ 14 Administradores SYSTEM 0 Feb 4 16:46 postgres  
drwxrwx---+ 15 Administradores SYSTEM 0 Feb 4 15:26 Administrator  
drwxrwx---+ 14 Administradores SYSTEM 0 Feb 2 20:34 reno  
drwxrwx----+ 14 Administradores SYSTEM 0 Feb 2 19:53 Johnatan  
drwxrwx----+ 14 Administradores SYSTEM 0 Jan 26 16:59 maru  
drwxrwx----+ 5 Administradores SYSTEM 0 Jan 26 00:58 LocalService  
drwxrwx----+ 5 Administradores SYSTEM 0 Jan 26 00:58 NetworkService  
drwxrwxr-x+ 14 Administradores SYSTEM 0 Jan 26 00:42 Default User  
drwxrwxr-x+ 9 Administradores SYSTEM 0 Jan 26 00:40 All Users
```

La fecha de la creación de perfiles de usuarios (*All Users* y *Default User*) es el 26 de enero así como de las cuentas del sistema *LocalService* y *NetworkService*, las cuales permiten iniciar sesión como un servicio, indicativo que utilizaron *RemoteDesktop* o similar después de creados los perfiles. La primera cuenta creada fue **maru** el mismo día 26 de enero, las demás cuentas fueron creadas hasta el mes de febrero siendo las últimas en crearse el día 5.

Nota: La versión XP desde donde se realizan los comandos es en español, por lo que existen cuentas y grupos interconstruidos, por ejemplo "Administradores". No confundir al leer la salida de comandos donde se muestra al propietario y grupo de los archivos.

Fecha de último logueo de usuarios

Para determinar la fecha de la última vez que se loguearon los usuarios busqué la fecha de modificación de los archivos *NTUSER.DAT* en los perfiles de los usuarios:

```
$ find /z/Documents\ and\ Settings/ -name NTUSER.DAT -exec ls -la {} \;  
-rwx-----+ 1 Administradores ????????? 1048576 Feb 5 17:44 /z/Documents  
and Settings/Administrator/NTUSER.DAT  
-rwxrwxr-x+ 1 Administradores SYSTEM 217088 Jan 26 00:42 /z/Documents and  
Settings/Default User/NTUSER.DAT  
-rwx-----+ 1 Administradores ????????? 786432 Feb 5 16:28 /z/Documents  
and Settings/Johnatan/NTUSER.DAT  
-rwxrwx---+ 1 ????????? ????????? 217088 Feb 5 17:44 /z/Documents and  
Settings/LocalService/NTUSER.DAT  
-rwx-----+ 1 ????????? ????????? 524288 Feb 3 21:33 /z/Documents and  
Settings/maick/NTUSER.DAT  
-rwx-----+ 1 Administradores ????????? 524288 Jan 26 19:57 /z/Documents  
and Settings/maru/NTUSER.DAT
```

```

-rwxrwx---+ 1 ?????????? ?????????? 262144 Feb 5 17:44 /z/Documents and
Settings/NetworkService/NTUSER.DAT
-rwx-----+ 1 ?????????? ?????????? 217088 Feb 5 17:44 /z/Documents and
Settings/postgres/NTUSER.DAT
-rwx-----+ 1 ?????????? ?????????? 524288 Feb 2 22:38 /z/Documents and
Settings/reno/NTUSER.DAT
-rwx-----+ 1 Administradores ?????????? 786432 Feb 5 17:44 /z/Documents
and Settings/ver0k/NTUSER.DAT

```

La creación de usuarios en Windows 2003 puede hacerse mediante la consola de administración *mmc* y mediante el comando *dsadd*, sin embargo su fecha de acceso indica que no se utilizó:

```

Z:\WINDOWS\system32\dllcache>DIR DSADD.EXE /TA
El volumen de la unidad Z no tiene etiqueta.
El número de serie del volumen es: A803-85D0

Directorio de Z:\WINDOWS\system32\dllcache

26/01/2006 04:36 p.m.          147,456 dsadd.exe
          1 archivos          147,456 bytes
          0 dirs    2,669,223,936 bytes libres

```

```

Z:\WINDOWS\system32\dllcache>CD ..

Z:\WINDOWS\system32>DIR DSADD.EXE /TA
El volumen de la unidad Z no tiene etiqueta.
El número de serie del volumen es: A803-85D0

Directorio de Z:\WINDOWS\system32

26/01/2006 04:24 p.m.          147,456 dsadd.exe
          1 archivos          147,456 bytes
          0 dirs    2,669,223,936 bytes libres

```

Y el último acceso de *mmc* fue:

```

Z:\WINDOWS\system32>dir mmc.exe /TA
El volumen de la unidad Z no tiene etiqueta.
El número de serie del volumen es: A803-85D0

Directorio de Z:\WINDOWS\system32

05/02/2006 05:11 p.m.          1,353,216 mmc.exe
          1 archivos          1,353,216 bytes
          0 dirs    2,669,223,936 bytes libres

```

Si vemos la fecha de creación de usuarios, *ver0k* fue crado el día 5 de febrero, pero a las **2:47**, *mmc* fue ejecutado posteriormente:

```

Z:\Documents and Settings>dir /TC
El volumen de la unidad Z no tiene etiqueta.
El número de serie del volumen es: A803-85D0

Directorio de Z:\Documents and Settings

25/01/2006 03:03 p.m.    <DIR>      .
25/01/2006 03:03 p.m.    <DIR>      ..
26/01/2006 01:37 p.m.    <DIR>      Administrator
25/01/2006 03:03 p.m.    <DIR>      All Users
02/02/2006 07:53 p.m.    <DIR>      Johnatan
03/02/2006 08:11 p.m.    <DIR>      maick
26/01/2006 04:59 p.m.    <DIR>      maru
04/02/2006 04:46 p.m.    <DIR>      postgres
02/02/2006 08:34 p.m.    <DIR>      reno
05/02/2006 02:47 p.m.    <DIR>      ver0k
          0 archivos          0 bytes
          10 dirs    2,669,223,936 bytes libres

```

Pertenencia de los usuarios

Con el comando *cacls* de windows es posible ver a que grupos pertenecen:

```
Z:\Documents and Settings\>cacls *
Z:\Documents and Settings\Administrator <Dominio de la cuenta no encontrado>F
      NT AUTHORITY\SYSTEM:F
      BUILTIN\Administradores:F
      <Dominio de la cuenta no encontrado>(OI)(CI)(IO)F
      NT AUTHORITY\SYSTEM:(OI)(CI)(IO)F
      BUILTIN\Administradores:(OI)(CI)(IO)F

Z:\Documents and Settings\Johnatan <Dominio de la cuenta no encontrado>F
      NT AUTHORITY\SYSTEM:F
      BUILTIN\Administradores:F
      <Dominio de la cuenta no encontrado>(OI)(CI)(IO)F
      NT AUTHORITY\SYSTEM:(OI)(CI)(IO)F
      BUILTIN\Administradores:(OI)(CI)(IO)F

Z:\Documents and Settings\maick <Dominio de la cuenta no encontrado>F
      NT AUTHORITY\SYSTEM:F
      BUILTIN\Administradores:F
      <Dominio de la cuenta no encontrado>(OI)(CI)(IO)F
      NT AUTHORITY\SYSTEM:(OI)(CI)(IO)F
      BUILTIN\Administradores:(OI)(CI)(IO)F

Z:\Documents and Settings\maru <Dominio de la cuenta no encontrado>F
      NT AUTHORITY\SYSTEM:F
      BUILTIN\Administradores:F
      <Dominio de la cuenta no encontrado>(OI)(CI)(IO)F
      NT AUTHORITY\SYSTEM:(OI)(CI)(IO)F
      BUILTIN\Administradores:(OI)(CI)(IO)F

Z:\Documents and Settings\postgres <Dominio de la cuenta no encontrado>F
      NT AUTHORITY\SYSTEM:F
      BUILTIN\Administradores:F
      <Dominio de la cuenta no encontrado>(OI)(CI)(IO)F
      NT AUTHORITY\SYSTEM:(OI)(CI)(IO)F
      BUILTIN\Administradores:(OI)(CI)(IO)F

Z:\Documents and Settings\reno <Dominio de la cuenta no encontrado>F
      NT AUTHORITY\SYSTEM:F
      BUILTIN\Administradores:F
      <Dominio de la cuenta no encontrado>(OI)(CI)(IO)F
      NT AUTHORITY\SYSTEM:(OI)(CI)(IO)F
      BUILTIN\Administradores:(OI)(CI)(IO)F

Z:\Documents and Settings\ver0k <Dominio de la cuenta no encontrado>F
      NT AUTHORITY\SYSTEM:F
      BUILTIN\Administradores:F
      <Dominio de la cuenta no encontrado>(OI)(CI)(IO)F
      NT AUTHORITY\SYSTEM:(OI)(CI)(IO)F
      BUILTIN\Administradores:(OI)(CI)(IO)F
```

De este recuadro quité las cuentas interconstruidas *All Users*, *Default User*, *Local Service*, *Network Service*, para mostrar solo los usuarios que se utilizaban. Como se puede apreciar todos pertenecen al grupo de maximos privilegios.

Nota: La version XP desde donde se realizan los comandos es en español, por lo que existen cuentas y grupos interconstruidos, por ejemplo "Administradores". No confundir al leer la salida de comandos donde se muestra al propietario y grupo de los archivos.

Documentos y archivos de los usuarios

Cookies

Es posible revisar las *cookies* con un programa de *Foundstone* llamado *galleta*:

Reno: No tenía cookies.

Maick:

```
C:\>galleta "Z:\Documents and Settings\maick\Cookies\maick@google.com[1].txt"
Cookie File: Z:\Documents and Settings\maick\Cookies\maick@google.com[1].txt
```

SITE	VARIABLE	VALUE	CREATION TIME	EXPIRE TIME	FLAGS
google.com.mx/	PREF	ID=d441ba94af965db7:TM=1139019103:LM=1139019103:S=xWE5ArWrVlmlonO7	02/03/2006 20:11:44	01/17/2038 13:14:07	1536

```
C:\>galleta "Z:\Documents and Settings\maick\Cookies\maick@google[1].txt"
Cookie File: Z:\Documents and Settings\maick\Cookies\maick@google[1].txt
```

SITE	VARIABLE	VALUE	CREATION TIME	EXPIRE TIME	FLAGS
google.com/	PREF	ID=3c59499d38401c27:TM=1139019103:LM=1139019103:S=IDADze h2szTe2GvI	02/03/2006 20:11:43	01/17/2038 13:14:07	1536

Administrador:

```
C:\>galleta "Z:\Documents and Settings\Administrador\Cookies\administrator@google.com[1].txt"
Cookie File: Z:\Documents and Settings\Administrador\Cookies\administrator@google.com[1].txt
```

SITE	VARIABLE	VALUE	CREATION TIME	EXPIRE TIME	FLAGS
google.com.mx/	PREF	ID=083f47e0627b41e6:TM=1138489399:LM=1138489399:S=5bx0fD rpk9AqORBG	01/28/2006 19:49:44	01/17/2038 13:14:07	1536

```
C:\>galleta "Z:\Documents and Settings\Administrador\Cookies\administrator@google[1].txt"
Cookie File: Z:\Documents and Settings\Administrador\Cookies\administrator@google[1].txt
```

SITE	VARIABLE	VALUE	CREATION TIME	EXPIRE TIME	FLAGS
google.com/	PREF	ID=3f163b18bc131962:TM=1138489398:LM=1138489398:S=1mp81J fNpIkuE9n7	01/28/2006 19:49:43	01/17/2038 13:14:07	1536

```
C:\>galleta "Z:\Documents and Settings\Administrador\Cookies\administrator@img.wmp10.elsitiadc[1].txt"
Cookie File: Z:\Documents and Settings\Administrador\Cookies\administrator@img.wmp10.elsitiadc[1].txt
```

SITE	VARIABLE	VALUE	CREATION TIME	EXPIRE TIME	FLAGS
img.wmp10.elsitiadc.com/		CLAXSON 192.168.100.145.10405113908804486602/04/2006 15:20:46	02/02/2014 15:20:44	1536	

```
C:\>galleta "Z:\Documents and Settings\Administrador\Cookies\administrator@msn[1].txt"
Cookie File: Z:\Documents and Settings\Administrador\Cookies\administrator@msn[1].txt
```

SITE	VARIABLE	VALUE	CREATION TIME	EXPIRE TIME	FLAGS
msn.com/	MC1	V=3&GUID=57c20cc76bed48389f24853781827bc2	10/04/2021 14:00:00	1024	02/03/2006 20:02:58

```
C:\>galleta "Z:\Documents and Settings\Administrador\Cookies\administrator@serviceswitching[1].txt"
Cookie File: Z:\Documents and Settings\Administrador\Cookies\administrator@serviceswitching[1].txt
```

SITE	VARIABLE	VALUE	CREATION TIME	EXPIRE TIME	FLAGS
serviceswitching.metaservices.microsoft.com/	msid	6c871036 -bac0-4388-b9a8-fcba7413f6f6	02/04/2006 15:20:44	02/02/2016 15:20:431536	

VerOk:

```
C:\>galleta "Z:\Documents and Settings\verOk\Cookies\verOk@atdmt[1].txt"
Cookie File: Z:\Documents and Settings\verOk\Cookies\verOk@atdmt[1].txt
```

SITE	VARIABLE	VALUE	CREATION TIME	EXPIRE TIME	FLAGS
atdmt.com/	AA002	001139173460-251665895/1140383060	02/05/2006 15:04:22	02/03/2011 18:00:00	1024

```
C:\>galleta "Z:\Documents and Settings\verOk\Cookies\verOk@img.wmp10.elsitiadc[1].txt"
Cookie File: Z:\Documents and Settings\verOk\Cookies\verOk@img.wmp10.elsitiadc[1].txt
```

SITE	VARIABLE	VALUE	CREATION TIME	EXPIRE TIME	FLAGS
img.wmp10.elsitiadc.com/		CLAXSON 192.168.100.145.29773113917409552702/05/2006 15:14:57	02/03/2014 15:14:55	1536	

```
C:\>galleta "Z:\Documents and Settings\verOk\Cookies\verOk@msn[1].txt"
Cookie File: Z:\Documents and Settings\verOk\Cookies\verOk@msn[1].txt
```

SITE	VARIABLE	VALUE	CREATION TIME	EXPIRE TIME	FLAGS
msn.com/	ANON	A=28E4C4351600C5FFFE5853DF7FFFFFFFFF&E=3b2&W=1	02/05/2006 15:04:04	08/23/2006 19:00:00	9216

```

msn.com/          NAP          V=1.2&E=358&C=3wY065EwdWYYqaakJ6hZJQM2MrzinOztPSkNI_tFxyzuwSr0DajloA&W=1
02/05/2006 15:04:04    05/15/2006 19:00:00    9216
msn.com/          MSNADS  UM=          02/05/2006 15:04:25    04/26/2022 07:00:009216

C:\>galleta "Z:\Documents and Settings\ver0k\Cookies\ver0k@serviceswitching[1].txt"
Cookie File: Z:\Documents and Settings\ver0k\Cookies\ver0k@serviceswitching[1].txt

SITE      VARIABLE      VALUE      CREATION TIME      EXPIRE TIME      FLAGS
serviceswitching.metaservices.microsoft.com/serviceswitching/  msid      245d4278-6c2e-4a64-821c-
aee27a54276d  02/05/2006 15:14:56    02/03/2016 15:14:541536

```

Historial de Navegación

Administrador: En el directorio `\Documents and Settings\Administrator\Local Settings\History\History.IE5` se encontraron los siguientes directorios:

```

MSHist012006012320060130
MSHist012006013020060131
MSHist012006020120060202
MSHist012006020220060203
MSHist012006020320060204
MSHist012006020420060205
MSHist012006020520060206

```

Que contienen el archivo `index.dat`, el cual es el cache del Internet Explorer. Ubicados en el directorio `History.IE5` teclee el comando `file`:

```

$ file */*
MSHist012006012320060130/index.dat: Microsoft Internet Explorer Cache File Version Ver 5.2
MSHist012006013020060131/index.dat: Microsoft Internet Explorer Cache File Version Ver 5.2
MSHist012006020120060202/index.dat: Microsoft Internet Explorer Cache File Version Ver 5.2
MSHist012006020220060203/index.dat: Microsoft Internet Explorer Cache File Version Ver 5.2
MSHist012006020320060204/index.dat: Microsoft Internet Explorer Cache File Version Ver 5.2
MSHist012006020420060205/index.dat: Microsoft Internet Explorer Cache File Version Ver 5.2
MSHist012006020520060206/index.dat: Microsoft Internet Explorer Cache File Version Ver 5.2

```

Al analizarse todos los `index.dat` con el comando `strings` desde el mismo directorio `History.IE5`, nos muestra los últimos URLs visitados:

```

$ strings */*
Client UrlCache MMF Ver 5.2
HASH
URL
:2006012320060130: Administrator@http://localhost
URL
:2006012320060130: Administrator@file:///C:/apache/Apache/php/install.txt
URL
:2006012320060130: Administrator@file:///C:/apache/Apache/logs/error.log
URL
:2006012320060130: Administrator@file:///C:/apache/Apache/htdocs/web-erp/sql/mysql/weberp-demo.sql
URL
:2006012320060130: Administrator@http://localhost/manual/howto/cgi.html
URL
:2006012320060130: Administrator@file:///E:/apache-php-mysql-win/apache-php-mysql.htm
URL
:2006012320060130: Administrator@http://www.google.com.mx
URL
:2006012320060130: Administrator@http://localhost/manual/mod/directive-dict.html
URL
:2006012320060130: Administrator@file:///C:/WINDOWS/php.ini
URL
:2006012320060130: Administrator@http://localhost/info.php
URL
:2006012320060130: Administrator@--mmc:pagebreak.1
URL
:2006012320060130: Administrator@file:///C:/apache/Apache/README-WIN.TXT
URL
:2006012320060130: Administrator@http://localhost/manual/mod/mod_so.html
URL
:2006012320060130: Administrator@http://localhost/manual/configuring.html
URL
:2006012320060130: Administrator@http://localhost/manual/index.html
URL
:2006012320060130: Administrator@http://localhost/manual/mod/mod_mime.html
URL
:2006012320060130: Administrator@file:///C:/WINDOWS/system32/oobe/actshell.htm
URL

```

```
:2006012320060130: Administrator@Host: localhost
URL
/*+$
:2006012320060130: Administrator@file:///C:/apache/Apache/conf/httpd.conf
URL
:2006012320060130: Administrator@http://www.britishcouncil.org.mx
URL
:2006012320060130: Administrator@Host: www.britishcouncil.org.mx
URL
:2006012320060130: Administrator@Host: www.google.com.mx
URL
/*+$
:2006012320060130: Administrator@Host: My Computer
Client UrlCache MMF Ver 5.2
HASH
URL
:2006013020060131: Administrator@--mmc:pagebreak.1
URL
:2006013020060131: Administrator@Host: My Computer
Client UrlCache MMF Ver 5.2
HASH
URL
:2006020120060202: Administrator@file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/fondo.jpg
URL
:2006020120060202: Administrator@Host: My Computer
URL
:2006020120060202: Administrator@file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/m001.jpg
URL
:2006020120060202: Administrator@file:///E:/Reto/bittorrent.txt
URL
:2006020120060202: Administrator@http://www.google.com.mx
URL
:2006020120060202: Administrator@file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/index.html
URL
:2006020120060202: Administrator@Host: www.google.com.mx
URL
:2006020120060202: Administrator@http://www.google.com.mx/search?hl=es&q=mozilla+firefox+meta=
URL
:2006020120060202: Administrator@http://www.mozilla-europe.org/es/products/firefox
URL
:2006020120060202: Administrator@Host: www.mozilla-europe.org
URL
:2006020120060202: Administrator@http://search.bittorrent.com
URL
/Y`
:2006020120060202: Administrator@Host: mozilla-chi.osuosl.org
URL
:2006020120060202: Administrator@http://mozilla-chi.osuosl.org/pub/mozilla.org/firefox/releases/1.5/win32/es-
ES/Firefox%20Setup%201.5.exe
URL
:2006020120060202: Administrator@Host: search.bittorrent.com
URL
:2006020120060202: Administrator@file:///C:/apache/Apache/logs/error.log
URL
:2006020120060202: Administrator@file:///C:/apache/Apache/logs/access.log
URL
:2006020120060202: Administrator@file:///C:/apache/Apache/conf/httpd.conf
Client UrlCache MMF Ver 5.2
HASH
URL
:2006020220060203: Administrator@file:///C:/apache/Apache/logs/access.log
URL
:2006020220060203: Administrator@Host: My Computer
Client UrlCache MMF Ver 5.2
HASH
URL
:2006020320060204: Administrator@file:///D:/index.html
URL
:2006020320060204: Administrator@Host: My Computer
URL
OTKi
nw<)
:2006020320060204: Administrator@file:///C:/apache/Apache/logs/error.log
URL
:2006020320060204: Administrator@Host: messenger.msn.com
URL
d!./)
:2006020320060204: Administrator@http://messenger.msn.com/xp/downloadx.aspx
URL
@D{f
:2006020320060204: Administrator@file:///C:/apache/Apache/logs/access.log
URL
:2006020320060204: Administrator@file:///C:/apache/Apache/mysql/my.ini
URL
:2006020320060204: Administrator@file:///C:/apache/Apache/mysql/my-huge.ini
URL
:2006020320060204: Administrator@file:///C:/apache/Apache/mysql/my-template.ini
Client UrlCache MMF Ver 5.2
HASH
URL
:2006020420060205: Administrator@file:///C:/Documents%20and%20Settings/reno/My%20Documents/imagenes/overlay_8.jpg
URL
:2006020420060205: Administrator@Host: My Computer
URL
:2006020420060205: Administrator@file:///C:/Documents%20and%20Settings/reno/My%20Documents/imagenes/overlay_int2.jpg
```

```

URL
:2006020420060205: Administrator@file:///E:/Audita_Tools/scanline/readme.txt
Client UrlCache MMF Ver 5.2
HASH
URL
qrJ*
:2006020520060206:
Administrator@file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/My%20Videos/modelos/nm06032003.jpeg
URL
qrJ*
:2006020520060206: Administrator@:Host: My Computer
URL
ItJ*
:2006020520060206:
Administrator@file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/My%20Videos/modelos/nm06042003.jpeg
URL
:2006020520060206:
Administrator@file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/My%20Videos/modelos/nm06052003.jpeg
URL
pIGwJ*
:2006020520060206:
Administrator@file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/My%20Videos/modelos/nm06082003.jpeg
URL
:2006020520060206:
Administrator@file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_3_2006020107031.jpg
URL
:2006020520060206: Administrator@http://fire.dmzs.com/news.html
URL
:2006020520060206: Administrator@file:///D:/index.html
URL
:2006020520060206: Administrator@:Host: fire.dmzs.com

```

Renó: En `\Documents and Settings\reno\Local Settings\History\History.IE5` se encontró el directorio:

MSHist012006020220060203

El cual al visualizar los *strings* sobre *index.dat* muestra:

```

Client UrlCache MMF Ver 5.2
HASH
@xN
@y>T
@b#M
URL
:2006020220060203:
reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/Doc4_Rev1_Proyecto_Declaracion_Mar_del_Plata_ESP.DOC
URL
:2006020220060203: reno@:Host: My Computer
URL
G-<k(
:2006020220060203:
reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/GEN%2013%20Segundo%20Informe%20del%20Comit%20de%20Progra
ma.doc
URL
Y|((
|kk(
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/Windows_XP.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/WASC_TC-1.0.spa.doc
URL
@^((
dlk(
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/vlex.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/violencia%20de%20genero.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/version0.doc
URL
5mk(
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/usos-y-abusos.doc
URL
W_((
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/Users99.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/uru_cas_unive.doc
URL
!nk(
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/Trabajo%203.doc
URL
H`((
knk(
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/TERMINOS%20ALIMENTOS-2.doc
URL
-a((
Pok(
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/temas.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/ssl.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/semin_uade_fin.doc
URL
-qk(

```

```

:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/S03-WSIS-DOC-0004!MSW-S.doc
URL
rgk(
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/Respuestas-139882180805013859.doc
URL
m)c((
Lqk(
:2006020220060203:
reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/Res%5Bl%5D%5Bl%5D.Convocatoria%202004.doc
URL
Oc((
rgk(
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/Reglamento_aprobado_por_el_CP.doc
URL
%rk(
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/Reglamento%20EPS.doc
URL
:kd((
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/reg_tes_nuevo.doc
URL
od((
:2006020220060203:
reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/Referencias_INAB-
PAFG%20Capacidad%20uso%20tierra-completo.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/rbecaspost.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/proy2002.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/practica_dssoo_2005_2006.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/pract2.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/plantilla.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/Peru_PR.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/Perez_Inocencia_PEC1.doc
URL
$sk(
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/neuron.doc
URL
)sk(
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/mistica-es.doc
URL
">.sk(
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/mirc_scripting_tornamen.doc
URL
2sk(
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/Memoria2004_Nodo05_CIC.doc
URL
7sk(
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/manualCDS.doc
URL
<sk(
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/manual_bibdig3_bibliotecas.doc
URL
)e((
8Msk(
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/lib_handbooks_s04pre.doc
URL
.e((
Qsk(
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/key_res_ix_06_s.doc
URL
3e((
Vsk(
:2006020220060203:
reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/Juego%20de%20las%20parejas%20para%20pulsador.doc
URL
O8e((
[sk(
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/jabber.doc
URL
=e((
j`sk(
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/IVconvenio%20colectivo.doc
URL
Ae((
esk(
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/Introduccion_linux.doc
URL
Fe((
isk(
:2006020220060203:
reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/Infraestructura_de_red_SMB_Battlecard.doc
URL
bke((
nsk(
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/INFORME%20FINAL%20REV.1-ESP.doc
URL
Pe((
]ssk(
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/Informe%20Ecuador.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/2004-bAUDITORIA%203.doc

```

URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/2004-bAUDITORIA%204.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/20060126masercisaproyecto609.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/106200509t.doc
URL
:2006020220060203:
reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/11013834211TIC_y_reduccion_pobreza_de_la_pobreza_en_ALC.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/AGRES_00_S.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/AGRICULTURA%20Y%20PESCA.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/ALIMENTOS.doc
URL
:2006020220060203:
reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/BASES%20CAPTURA%20MODIF.%20CON%20RANGO.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/BASES%20elevadores.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/bases_software.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/batasuna.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/Boletin11.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/Cap02c.DOC
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/Capsicum.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/CO-0863r1_e.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/CON_001_ADENDO_1.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/conceptos.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/concha.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/conConicyt.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/congreso8.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/COP7DOC16_3.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/cop9_doc03_s.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/cp09393s11.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/CP11591S08.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/CuartoPeriodo-INFORME%20DEL%20RELATOR.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/CurriculoSistemaOperativo.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/cursos%20junio2005varios.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/cursounix.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/dde5614s.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/difusion_convenio_ico-idae_2002.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/Diptico_Premios.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/directorio.doc
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/imagenes/overlay_5_2005112211035.jpg
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/imagenes/1_2005121110036.jpg
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/imagenes/9.jpg
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/imagenes/overlay_2_2006020110004.jpg
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/imagenes/overlay_8_2006020110005.jpg
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/imagenes/overlay_9_2006020110006.jpg
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/imagenes/overlay_int2.jpg
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/imagenes/overlay_6_2005112211035.jpg
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/imagenes/overlay_3_2006020107031.jpg
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/imagenes/overlay_4_2005112211035.jpg
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/imagenes/overlay_6_2006020110004.jpg
URL
:2006020220060203:
reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/imagenes/overlay_por_2006020107034_20060201190204.jpg
URL
:2006020220060203:
reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/imagenes/overlay_por_2006020110007_20060201224249.jpg
URL

```
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/imagenes/overlay_7_2006020110005.jpg
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/imagenes/overlay_4_2006020110004.jpg
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/imagenes/overlay_1_2006020110003.jpg
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/imagenes/2_2005121110036.jpg
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/imagenes/3_2005121110036.jpg
URL
:2006020220060203: reno@file:///C:/Documents%20and%20Settings/reno/My%20Documents/imagenes/overlay_2_2005112211034.jpg
```

Maick: En `Documents and Settings\maick\Local Settings\History\History.IE5` se encontró el directorio:

```
MSHist012006020320060204
```

El cual al visualizar los strings sobre `index.dat` muestra:

```
Client UrlCache MMF Ver 5.2
HASH
URL
96Z0)
:2006020320060204: maick@http://www.google.com.mx
URL
96Z0)
:2006020320060204: maick@:Host: www.google.com.mx
```

VerOk: En `Documents and Settings\verOk\Local Settings\History\History.IE5` se encontró el directorio:

```
MSHist012006020520060206
```

El cual al visualizar los strings sobre `index.dat` muestra:

```
Client UrlCache MMF Ver 5.2
HASH
URL
:2006020520060206: verOk@file:///C:/apache/Apache/htdocs/web-erp/AccountGroups.php
URL
:2006020520060206: verOk@:Host: My Computer
URL
:2006020520060206: verOk@file:///C:/apache/Apache/htdocs/web-erp/config.php
URL
:2006020520060206: verOk@file:///C:/users.txt
URL
:2006020520060206: verOk@:Host: rad.msn.com
URL
:2006020520060206: verOk@http://imagine-msn.com/messenger/runonce/v75/mosaic.aspx?locale=es-MX
URL
:2006020520060206: verOk@:Host: imagine-msn.com
URL
:2006020520060206: verOk@file:///C:/clientes.txt
URL
:2006020520060206: verOk@file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/1_2005121110036.jpg
URL
:2006020520060206: verOk@file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/2_2005121110036.jpg
URL
:2006020520060206: verOk@file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/3_2005121110036.jpg
URL
:2006020520060206: verOk@file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/9.jpg
URL
:2006020520060206:
verOk@file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_1_2005112211034.jpg
URL
:2006020520060206:
verOk@file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_1_2006020107030.jpg
URL
:2006020520060206:
verOk@file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_1_2006020110003.jpg
URL
:2006020520060206:
verOk@file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_2_2005112211034.jpg
URL
:2006020520060206:
verOk@file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_2_2006020110004.jpg
URL
:2006020520060206:
verOk@file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_3_2005112211034.jpg
URL
:2006020520060206:
verOk@file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_3_2006020107031.jpg
URL
:2006020520060206:
verOk@file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_4_2005112211035.jpg
```

```

URL
:2006020520060206:
ver0k@file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_4_2006020110004.jpg
URL
:2006020520060206: ver0k@file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_5.jpg
URL
@ "_V*
:2006020520060206:
ver0k@file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_5_2005112211035.jpg
URL
:2006020520060206:
ver0k@file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_5_2006020110004.jpg
URL
:2006020520060206:
ver0k@file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_6_2005112211035.jpg
URL
ujv*
:2006020520060206:
ver0k@file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_6_2006020110004.jpg
URL
XmV*
:2006020520060206:
ver0k@file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_7_2006020110005.jpg
URL
:2006020520060206: ver0k@file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_8.jpg
URL
:2006020520060206:
ver0k@file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_8_2006020110005.jpg
URL
`tKyV*
:2006020520060206:
ver0k@file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_9_2006020110006.jpg
URL
:2006020520060206:
ver0k@file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_por_2006020107034_20060201190204.jpg
URL
:2006020520060206:
ver0k@file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_por_2006020110007_20060201224249.jpg
URL
:2006020520060206: ver0k@file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/a017.jpg
URL
:2006020520060206:
ver0k@file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/My%20Videos/modelos/nm06032003.jpeg
URL
:2006020520060206:
ver0k@file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/My%20Videos/modelos/nm06042003.jpeg
URL
:2006020520060206:
ver0k@file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/My%20Videos/modelos/nm06052003.jpeg
URL
:2006020520060206:
ver0k@file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/My%20Videos/modelos/nm06082003.jpeg
URL
:2006020520060206: ver0k@file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/formulario.doc
URL
:2006020520060206: ver0k@file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/Notas.doc
URL
]eW*
:2006020520060206: ver0k@file:///C:/Documents%20and%20Settings/reno/My%20Documents/Boletin1.doc
URL
:2006020520060206: ver0k@file:///C:/Documents%20and%20Settings/reno/My%20Documents/concha.doc
URL
:2006020520060206: ver0k@http://www.huevocartoon.com/home_contry.asp
URL
:2006020520060206: ver0k@Host: www.huevocartoon.com
URL
:2006020520060206: ver0k@file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/30SEP_bolecart-book.doc
URL
:2006020520060206: ver0k@file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/%CDNDICE%20DOCTORADO.doc
URL
:2006020520060206: ver0k@file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/Indice%20Pormenorizado.doc
URL
:2006020520060206: ver0k@file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/RRGEPNotas.doc
URL
:2006020520060206: ver0k@file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/RRGEPPortadas.doc
URL
:2006020520060206: ver0k@file:///C:/Documents%20and%20Settings/maick/Sti_Trace.log
URL
:2006020520060206: ver0k@file:///C:/apache/Apache/ABOUT_APACHE.TXT
URL
:2006020520060206: ver0k@file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/examen.gif
URL
:2006020520060206: ver0k@http://rad.msn.com/ADSAdClient31.dll?GetAd?PG=IMSMXS?SC=HF?ID=0006000094d02e8a

```

Estos datos pueden comprobarse viendo la carpeta *Recent Documents* dentro de *Local Settings*. Sería interesante conocer la razón que tuvo el usuario para ver archivos de otros perfiles (por ejemplo *Administrator*) así como el archivo *clientes.txt*, del cual no se encontró rastro.

Favoritos de IExplorer

Nadie tiene links propios en favoritos.

Recuperación de bitácoras

Cuando escribí sobre el registro de Windows, mencioné que las bitácoras también se encontraban en el directorio `\windows\system32\config`, después de revisarlas con *Event Viewer* y no encontrar inconsistencias como borrado de eventos o fechas no consecutivas, puedo resumir:

Sistema:

El primer registro inicia el **25 de enero**; a las 3:03pm se inicia el registro de sucesos. El nombre de la máquina es *MACHINENAME*. Posteriormente el **día 26** a las 12:26am el nombre NetBIOS y el nombre de host DNS cambia a *COUNTERS*. A las 12:57am hubo un reinicio del servidor, por la razón: `Operating System: Upgrade (Planned)`. Los fixes de seguridad se instalaron entre las 3:53pm y las 4:02pm. Reiniciaron a las 4:04pm.

Por medio del *Service Control Manager* es posible ver los servicios que se levantaron, entre ellos el que considero riesgoso en una máquina con conexión al exterior es:

```
Tipo de suceso: Información
Origen del suceso: Service Control Manager
Categoría del suceso: Ninguno
Id. suceso: 7036
Fecha: 26/01/2006
Hora: 04:07:13 p.m.
Usuario: No disponible
Equipo: COUNTERS
Descripción: El servicio Terminal Services entró en estado running.
```

Este servicio permite la conexión remota de equipos al escritorio de *Windows* mediante el protocolo *RDP* con el programa *RemoteDesktop* de *Windows* o similar. Este mismo *SCM* nos da una idea de que servicios se cargaban por *default*, por ejemplo:

```
Tipo de suceso: Información
Origen del suceso: Service Control Manager
Categoría del suceso: Ninguno
Id. suceso: 7035
Fecha: 26/01/2006
Hora: 08:00:45 p.m.
Usuario: S-1-5-21-2780117151-1340924567-2512508698-500
Equipo: COUNTERS
Descripción: Se ha enviado satisfactoriamente un control start al servicio Apache.
```

En este caso es el servidor de páginas web *Apache* en el entorno *Administrator*, como lo indica el campo *Usuario*: `S-1-5-21-2780117151-1340924567-2512508698-500` donde se puede apreciar el SID que termina en 500, doy por entendido que es el usuario administrador.

Después se estuvo mandando la señal de *stop* y *start* al servicio *Apache*, posiblemente por cambios de configuración hasta las 8:55pm del mismo día, por el mismo usuario *Administrator*. El servicio *MySQL* se levanta por primera vez a las 8:42pm.

El día 27 de enero, solo tomo en cuenta la advertencia de que la hora no se pudo sincronizar:

```
Tipo de suceso: Advertencia
Origen del suceso: W32Time
Categoría del suceso: Ninguno
Id. suceso: 36
Fecha: 27/01/2006
Hora: 04:05:32 p.m.
Usuario: No disponible
Equipo: COUNTERS
Descripción: El servicio de hora no ha podido sincronizar la hora del sistema en 86400 segundos porque ninguno de los proveedores de hora ha podido proporcionar un sello de hora que se pueda usar. El reloj del sistema no está sincronizado.
```

El día 28 de enero, se reinició de forma inesperada a las 11:43am. Se inician nuevamente los eventos a las 6:47pm:

```
Tipo de suceso:      Error
Origen del suceso:   EventLog
Categoría del suceso: Ninguno
Id. suceso:          6008
Fecha:               28/01/2006
Hora:                06:47:56 p.m.
Usuario:             No disponible
Equipo:              COUNTERS
Descripción:         El cierre anterior del sistema a las 11:43:26 AM del 1/28/2006
resultó inesperado.
```

Y a las 6:56pm el administrador registra la razón del apagado:

```
Tipo de suceso:      Advertencia
Origen del suceso:   USER32
Categoría del suceso: Ninguno
Id. suceso:          1076
Fecha:               28/01/2006
Hora:                06:56:03 p.m.
Usuario:             S-1-5-21-2780117151-1340924567-2512508698-500
Equipo:              COUNTERS
Descripción:         La razón que ha suministrado el usuario para el último reinicio
inesperado de este equipo es: Power Failure: Environment
```

Los días 29, 30 y 31 de enero y 1, 2 de febrero siguió registrando actividad a diferentes horas. El día 3 de febrero se registró un reinicio del escritorio de *Administrator*, el usuario administrador estuvo haciendo pruebas con MySQL y mandando señales de *stop / start* hasta las 9:57pm. El día 4 de febrero, el usuario inició el servicio de DNS, el sistema inició el servicio PostgreSQL.

El día 5 de febrero, el sistema inició a las **5:11pm** el servicio *Removable Storage*, el cual se utiliza cuando se conectan dispositivos como discos duros externos, memorias USB, etc. Sin embargo se registró el siguiente error:

```
Tipo de suceso:      Error
Origen del suceso:   Removable Storage Service
Categoría del suceso: Ninguno
Id. suceso:          111
Fecha:               05/02/2006
Hora:                05:11:29 p.m.
Usuario:             No disponible
Equipo:              COUNTERS
Descripción:         No se encuentra la descripción del Id. de suceso ( 111 ) en el origen
( Removable Storage Service ). Es posible que el equipo local no tenga la información de
Registro o archivos DLL de mensajes necesarios para mostrar mensajes desde un equipo
remoto. Es posible que pueda usar el indicador /AUXSOURCE= para recuperar esta descripción;
consulte Ayuda y soporte técnico para obtener más detalles. La siguiente información es
parte del suceso: Drive 0, Kingston DataTraveler 2.0 USB Device.
```

Según <http://www.eventid.net> el suceso **111** del origen *Removable Storage Service* se refiere a que no pudo encontrar el medio en el drive, sin embargo por experiencia propia este error lo he encontrado cuando se intenta acceder a dispositivos USB pero específicamente de la marca *Kingston* mediante una sesión de RemoteDesktop.

A las **5:43pm** el sistema recibe la señal de *shutdown* por el administrador:

```
Tipo de suceso:      Información
Origen del suceso:   USER32
Categoría del suceso: Ninguno
Id. suceso:          1074
Fecha:               05/02/2006
Hora:                05:43:54 p.m.
```

```

Usuario: S-1-5-21-2780117151-1340924567-2512508698-500
Equipo: COUNTERS
Descripción: El proceso Explorer.EXE ha comenzado el reinicio COUNTERS por la
siguiente razón: Security issue
Razón menor: 0x84050013
Tipo de apagado: shutdown

```

Seguridad:

El primer registro inicia el **25 de enero** a las 3:05pm, se aprecian cambios en la directiva de auditoria en diversas ocasiones. Se registran las instalaciones de *Apache*, *PHP* y *MySQL* durante el día **26 de enero**, y la modificación de reglas del *Firewall* de Windows para permitir determinado tráfico. Durante el **27 y 28 de enero** se registran aciertos y errores en servicios como *RAS*, *IPSec* y *CHAP* y la respectiva modificación de reglas del Firewall, el cual se puede apreciar como sigue:

```

Tipo de suceso: Aciertos
Origen del suceso: Security
Categoría del suceso: Cambio de plan
Id. suceso: 848
Fecha: 28/01/2006
Hora: 06:48:08 p.m.
Usuario: NT AUTHORITY\SYSTEM
Equipo: COUNTERS
Descripción:
La siguiente directiva estaba activa cuando se inició el Firewall de Windows.

Directiva de grupo aplicada: No
Perfil usado: Standard
Interfaz: All interfaces
Modo operativo: On
Servicios:
  Archivos e impresoras compartidos: Enabled
  Escritorio remoto: Enabled
  Entorno UPnP : Enabled
Permitir administración remota: Disabled
Permitir respuestas de monodifusión al tráfico de multidifusión o difusión: Disabled
Registro de seguridad:
  Registrar paquetes perdidos: Disabled
  Registrar conexiones correctas Disabled
ICMP:
  Permitir solicitud de eco entrante: Enabled
  Permitir solicitud de marca de tiempo entrante: Disabled
  Permitir solicitud de máscara entrante: Disabled
  Permitir solicitud de enrutador entrante: Disabled
  Permitir destino inalcanzable saliente: Disabled
  Permitir paquete de control de flujo (source quench) saliente: Disabled
  Permitir problema de parámetro saliente: Disabled
  Permitir tiempo excedido saliente: Disabled
  Permitir redirección: Disabled
  Permitir paquete de salida demasiado grande: Disabled

```

Y el último cambio de directivas de auditoria se registró como sigue:

```

Tipo de suceso: Aciertos
Origen del suceso: Security
Categoría del suceso: Cambio de plan
Id. suceso: 612
Fecha: 01/02/2006
Hora: 12:31:47 p.m.
Usuario: S-1-5-21-2780117151-1340924567-2512508698-500
Equipo: COUNTERS
Descripción:
Cambio de directiva de auditoría:
Nueva directiva:
  Éxito  Error
  +      +   Inicio de sesión/Fin de sesión
  +      +   Acceso a objeto
  +      +   Uso privilegiado
  +      +   Administración de cuentas
  +      +   Cambio de directiva
  +      +   Sistema
  +      +   Seguimiento detallado
  +      +   Acceso del servicio de directorio
  +      +   Cuenta de inicio de sesión
Cambiado por:
Nombre de usuario: Administrator
Nombre de dominio: COUNTERS
Id. de inicio de sesión: (0x0,0x174CF3)

```

No se tenía antecedente del usuario *verOk*, hasta las **2:45** del día domingo 5 de febrero, donde el usuario *Johnatan* asigna nombre, contraseñas, permiso y activación de la cuenta:

```
Tipo de suceso:      Aciertos
Origen del suceso:  Security
Categoría del suceso: Administración de cuentas
Id. suceso:         628
Fecha:              05/02/2006
Hora:               02:45:30 p.m.
Usuario:            S-1-5-21-2780117151-1340924567-2512508698-1006
Equipo:             COUNTERS
Descripción:
Conjunto de contraseñas de cuentas de usuario:
Nombre de cuenta destino:      verOk
Dominio destino:               COUNTERS
Id. de cuenta destino:         S-1-5-21-2780117151-1340924567-2512508698-1024
Nombre de usuario llamador:    Johnatan
Dominio del llamador:          COUNTERS
Id. de inicio de sesión del llamador: (0x0,0x3DF69A)
```

```
Tipo de suceso:      Aciertos
Origen del suceso:  Security
Categoría del suceso: Administración de cuentas
Id. suceso:         642
Fecha:              05/02/2006
Hora:               02:45:30 p.m.
Usuario:            S-1-5-21-2780117151-1340924567-2512508698-1006
Equipo:             COUNTERS
Descripción:
Cambiada cuenta de usuario:
Nombre de cuenta destino:      verOk
Dominio destino:               COUNTERS
Id. de cuenta destino:         S-1-5-21-2780117151-1340924567-2512508698-1024
Nombre de usuario llamador:    Johnatan
Dominio del llamador:          COUNTERS
Id. de inicio de sesión del llamador: (0x0,0x3DF69A)
Privilegios:                  -
```

```
Tipo de suceso:      Aciertos
Origen del suceso:  Security
Categoría del suceso: Administración de cuentas
Id. suceso:         626
Fecha:              05/02/2006
Hora:               02:45:30 p.m.
Usuario:            S-1-5-21-2780117151-1340924567-2512508698-1006
Equipo:             COUNTERS
Descripción:
Cuenta de usuario habilitada:
Nombre de cuenta destino:      verOk
Dominio destino:               COUNTERS
Id. de cuenta destino:         S-1-5-21-2780117151-1340924567-2512508698-1024
Nombre de usuario llamador:    Johnatan
Dominio del llamador:          COUNTERS
Id. de inicio de sesión del llamador: (0x0,0x3DF69A)
```

```
Tipo de suceso:      Aciertos
Origen del suceso:  Security
Categoría del suceso: Administración de cuentas
Id. suceso:         624
Fecha:              05/02/2006
Hora:               02:45:30 p.m.
Usuario:            S-1-5-21-2780117151-1340924567-2512508698-1006
Equipo:             COUNTERS
Descripción:
Cuenta de usuario creada:
Nombre de cuenta nueva:        verOk
Dominio nuevo:                 COUNTERS
Id. de cuenta nueva:           S-1-5-21-2780117151-1340924567-2512508698-1024
Nombre de usuario llamador:    Johnatan
Dominio del llamador:          COUNTERS
Id. de inicio de sesión del llamador: (0x0,0x3DF69A)
Privilegios:                  -
```

```
Tipo de suceso:      Aciertos
Origen del suceso:  Security
Categoría del suceso: Administración de cuentas
Id. suceso:         632
Fecha:              05/02/2006
Hora:               02:45:30 p.m.
Usuario:            S-1-5-21-2780117151-1340924567-2512508698-1006
Equipo:             COUNTERS
Descripción:
Miembro de grupo global habilitado de seguridad agregado:
Nombre del miembro:           -
Id. del miembro:               S-1-5-21-2780117151-1340924567-2512508698-1024
Nombre de cuenta destino:      None
Dominio de destino:            COUNTERS
Id. de cuenta destino:         %S-1-5-21-2780117151-1340924567-2512508698-513}
Nombre de usuario llamador:    Johnatan
Dominio del llamador:          COUNTERS
Id. de inicio de sesión del llamador: (0x0,0x3DF69A)
Privilegios:                  -
```

Posteriormente a las **2:45pm** ejecuta comandos de administración:

```
Tipo de suceso:      Aciertos
Origen del suceso:  Security
Categoría del suceso: Seguimiento detallado
Id. suceso:         592
Fecha:              05/02/2006
Hora:               02:45:30 p.m.
Usuario:            S-1-5-21-2780117151-1340924567-2512508698-1006
Equipo:             COUNTERS
Descripción:
Se ha creado un proceso:
  Id. de proceso:      3700
  Nombre de archivo de imagen: C:\WINDOWS\system32\net1.exe
  Id. de proceso creador: 2988
  Nombre de usuario:   Johnatan
  Dominio:             COUNTERS
  Id. de inicio de sesión: (0x0,0x3DF69A)
```

```
Tipo de suceso:      Aciertos
Origen del suceso:  Security
Categoría del suceso: Seguimiento detallado
Id. suceso:         592
Fecha:              05/02/2006
Hora:               02:45:30 p.m.
Usuario:            S-1-5-21-2780117151-1340924567-2512508698-1006
Equipo:             COUNTERS
Descripción:
Se ha creado un proceso:
  Id. de proceso:      2988
  Nombre de archivo de imagen: C:\WINDOWS\system32\net.exe
  Id. de proceso creador: 3376
  Nombre de usuario:   Johnatan
  Dominio:             COUNTERS
  Id. de inicio de sesión: (0x0,0x3DF69A)
```

Los servicios *net* son usados para la administración de usuarios, impresión, recursos compartidos, revisión de conexiones, etc. Unos segundos después se registra que el usuario *ver0k* ya forma parte del grupo de administradores:

```
Tipo de suceso:      Aciertos
Origen del suceso:  Security
Categoría del suceso: Administración de cuentas
Id. suceso:         636
Fecha:              05/02/2006
Hora:               02:45:53 p.m.
Usuario:            S-1-5-21-2780117151-1340924567-2512508698-1006
Equipo:             COUNTERS
Descripción:
Miembro de grupo local habilitado de seguridad agregado:
  Nombre del miembro: -
  Id. del miembro:      S-1-5-21-2780117151-1340924567-2512508698-1024 ← SID de ver0k
  Nombre de cuenta destino: Administrators
  Dominio de destino: Builtin
  Id. de cuenta destino: BUILTIN\Administradores
  Nombre de usuario llamador: Johnatan
  Dominio del llamador: COUNTERS
  Id. de inicio de sesión del llamador: (0x0,0x3DF69A)
  Privilegios: -
```

Nota: La versión XP desde donde se realizan los comandos es en español, por lo que existen cuentas y grupos interconstruidos, por ejemplo "Administradores". No confundir al leer la salida de comandos donde se muestra al propietario y grupo de los archivos.

Siguió utilizando *net* hasta que ejecutó el comando *reg*:

```
Tipo de suceso:      Aciertos
Origen del suceso:  Security
Categoría del suceso: Seguimiento detallado
Id. suceso:         593
Fecha:              05/02/2006
Hora:               02:46:23 p.m.
Usuario:            S-1-5-21-2780117151-1340924567-2512508698-1006 ← SID de johnatan
Equipo:             COUNTERS
Descripción:
Ha terminado un proceso:
  Id. de proceso:      3984
  Nombre de archivo de imagen: C:\WINDOWS\system32\reg.exe
  Nombre de usuario:   Johnatan
  Dominio:             COUNTERS
  Id. de inicio de sesión: (0x0,0x3DF69A)
```

Este comando permite agregar, modificar o visualizar subclaves del registro así como sus valores. Posteriormente el usuario *ver0k* inicia sesión:

```
Tipo de suceso:      Aciertos
Origen del suceso:   Security
Categoría del suceso: Inicio/cierre de sesión
Id. suceso:         528
Fecha:              05/02/2006
Hora:               02:47:21 p.m.
Usuario:            S-1-5-21-2780117151-1340924567-2512508698-1024 ← SID de ver0k
Equipo: COUNTERS
Descripción:
Inicio de sesión realizado:
Nombre de usuario:   ver0k
Dominio:             COUNTERS
Id. de inicio de sesión: (0x0,0x3F4E19)
Tipo de inicio de sesión: 10
Proceso de inicio de sesión: User32
Paquete de autenticación: Negotiate
Nombre de estación de trabajo: COUNTERS
GUID de inicio de sesión: -
```

Nota: Fijarse que el tipo de inicio es 10, es decir *RemoteInteractive* (osea mediante los servicios Terminal Services o Remote Desktop).

```
Tipo de suceso:      Aciertos
Origen del suceso:   Security
Categoría del suceso: Uso de privilegios
Id. suceso:         576
Fecha:              05/02/2006
Hora:               02:47:21 p.m.
Usuario:            S-1-5-21-2780117151-1340924567-2512508698-1024 ← SID de ver0k
Equipo: COUNTERS
Descripción:
Privilegios especiales asignados al nuevo inicio de sesión:
Usuario:
Dominio:
Id. de inicio de sesión: (0x0,0x3F4E19)
Privilegios: SeSecurityPrivilege
              SeBackupPrivilege
              SeRestorePrivilege
              SeTakeOwnershipPrivilege
              SeDebugPrivilege
              SeSystemEnvironmentPrivilege
              SeLoadDriverPrivilege
              SeImpersonatePrivilege
```

```
Tipo de suceso:      Aciertos
Origen del suceso:   Security
Categoría del suceso: Inicio/cierre de sesión
Id. suceso:         528
Fecha:              05/02/2006
Hora:               02:47:21 p.m.
Usuario:            S-1-5-21-2780117151-1340924567-2512508698-1024
Equipo: COUNTERS
Descripción:
Inicio de sesión realizado:
Nombre de usuario:   ver0k
Dominio:             COUNTERS
Id. de inicio de sesión: (0x0,0x3F4E19)
Tipo de inicio de sesión: 10
Proceso de inicio de sesión: User32
Paquete de autenticación: Negotiate
Nombre de estación de trabajo: COUNTERS
GUID de inicio de sesión: -
```

El primer programa registrado que utilizó *ver0k* es el Explorador de Windows:

```
Tipo de suceso:      Aciertos
Origen del suceso:   Security
Categoría del suceso: Seguimiento detallado
Id. suceso:          592
Fecha:               05/02/2006
Hora:                02:47:34 p.m.
Usuario:             S-1-5-21-2780117151-1340924567-2512508698-1024
Equipo: COUNTERS
Descripción:
Se ha creado un proceso:
  Id. de proceso:      720
  Nombre de archivo de imagen: C:\WINDOWS\explorer.exe
  Id. de proceso creador: 3960
  Nombre de usuario:   ver0k
  Dominio:             COUNTERS
  Id. de inicio de sesión: (0x0,0x3F4E19)
```

Y ejecutó la biblioteca de instalación de Outlook que viene por default en Windows:

```
Tipo de suceso:      Aciertos
Origen del suceso:   Security
Categoría del suceso: Seguimiento detallado
Id. suceso:          592
Fecha:               05/02/2006
Hora:                02:47:42 p.m.
Usuario:             S-1-5-21-2780117151-1340924567-2512508698-1024
Equipo: COUNTERS
Descripción:
Se ha creado un proceso:
  Id. de proceso:      3980
  Nombre de archivo de imagen: C:\Program Files\Outlook Express\setup50.exe
  Id. de proceso creador: 720
  Nombre de usuario:   ver0k
  Dominio:             COUNTERS
  Id. de inicio de sesión: (0x0,0x3F4E19)
```

Posteriormente ejecutó el programa *regsvr32.exe* el cual es un comando de Windows que permite registrar archivos de biblioteca *.dll* en el registro del sistema operativo:

```
Tipo de suceso:      Aciertos
Origen del suceso:   Security
Categoría del suceso: Seguimiento detallado
Id. suceso:          593
Fecha:               05/02/2006
Hora:                02:47:42 p.m.
Usuario:             S-1-5-21-2780117151-1340924567-2512508698-1024
Equipo: COUNTERS
Descripción:
Ha terminado un proceso:
  Id. de proceso:      700
  Nombre de archivo de imagen: C:\WINDOWS\system32\regsvr32.exe
  Nombre de usuario:   ver0k
  Dominio:             COUNTERS
  Id. de inicio de sesión: (0x0,0x3F4E19)
```

Ejecuta el comando *unregmp2.exe*, el cual al revisar en <http://es.filename.info> se puede apreciar que es parte de la desinstalación de *Windows Media Player*.

```
Tipo de suceso:      Aciertos
Origen del suceso:   Security
Categoría del suceso: Seguimiento detallado
Id. suceso:          592
Fecha:               05/02/2006
Hora:                02:47:43 p.m.
```

```

Usuario: S-1-5-21-2780117151-1340924567-2512508698-1024
Equipo: COUNTERS
Descripción:
Se ha creado un proceso:
  Id. de proceso: 2148
  Nombre de archivo de imagen: C:\WINDOWS\inf\unregmp2.exe
  Id. de proceso creador: 3060
  Nombre de usuario: ver0k
  Dominio: COUNTERS
  Id. de inicio de sesión: (0x0,0x3F4E19)

```

Existe un exploit de nombre similar al archivo anterior, sin embargo modifica la llave de registro HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce añadiendo un valor WMC_ReebotCheck, en este caso no existe como se vió al revisar los programas que se ejecutan al inicio del sistema operativo.

Al mismo tiempo el usuario *Johnatan* ejecutaba el comando *ping* para comprobar conectividad con algún otro host:

```

Tipo de suceso: Aciertos
Origen del suceso: Security
Categoría del suceso: Seguimiento detallado
Id. suceso: 593
Fecha: 05/02/2006
Hora: 02:47:50 p.m.
Usuario: S-1-5-21-2780117151-1340924567-2512508698-1006
Equipo: COUNTERS
Descripción:
Ha terminado un proceso:
  Id. de proceso: 200
  Nombre de archivo de imagen: C:\WINDOWS\system32\ping.exe
  Nombre de usuario: Johnatan
  Dominio: COUNTERS
  Id. de inicio de sesión: (0x0,0x3DF69A)

```

A las **2:49** inicia *ver0k* a ejecutar *wordpad* varias ocasiones, posiblemente en este momento veía los archivos del usuario Administrator:

```

Tipo de suceso: Aciertos
Origen del suceso: Security
Categoría del suceso: Seguimiento detallado
Id. suceso: 592
Fecha: 05/02/2006
Hora: 02:49:50 p.m.
Usuario: S-1-5-21-2780117151-1340924567-2512508698-1024
Equipo: COUNTERS
Descripción:
Se ha creado un proceso:
  Id. de proceso: 520
  Nombre de archivo de imagen: C:\Program Files\Windows NT\Accessories\wordpad.exe
  Id. de proceso creador: 3100
  Nombre de usuario: ver0k
  Dominio: COUNTERS
  Id. de inicio de sesión: (0x0,0x3F4E19)

```

Y por alguna razón también la aplicación MySQL:

```

Tipo de suceso: Aciertos
Origen del suceso: Security
Categoría del suceso: Seguimiento detallado
Id. suceso: 592
Fecha: 05/02/2006
Hora: 02:51:16 p.m.
Usuario: S-1-5-21-2780117151-1340924567-2512508698-1024
Equipo: COUNTERS
Descripción:
Se ha creado un proceso:

```

Id. de proceso:	392
Nombre de archivo de imagen:	C:\apache\Apache\mysql\bin\mysql.exe
Id. de proceso creador:	2320
Nombre de usuario:	ver0k
Dominio:	COUNTERS
Id. de inicio de sesión:	(0x0,0x3F4E19)

A las **3:04pm** se registra que *MSN* que se estaba ejecutando en el entorno de *ver0k* empezó a escuchar una conexión entrante:

Tipo de suceso:	Aciertos
Origen del suceso:	Security
Categoría del suceso:	Seguimiento detallado
Id. suceso:	861
Fecha:	05/02/2006
Hora:	03:04:14 p.m.
Usuario:	S-1-5-21-2780117151-1340924567-2512508698-1024
Equipo:	COUNTERS
Descripción:	El Firewall de Windows detectó una aplicación al escuchar el tráfico entrante.
Nombre:	MSN Messenger 7.5
Ruta de acceso:	C:\Program Files\MSN Messenger\msnmsgr.exe
Identificador del proceso:	2448
Cuenta de usuario:	ver0k
Dominio de usuario:	COUNTERS
Servicio:	No
Servidor RPC:	No
Versión IP:	IPv4
Versión IP:	UDP
Número de puerto:	9
Permitido:	Yes
Usuario notificado:	No

Posteriormente ejecutó *Windows Media Player*, posiblemente en este momento veía los archivos del usuario Administrator:

Tipo de suceso:	Aciertos
Origen del suceso:	Security
Categoría del suceso:	Seguimiento detallado
Id. suceso:	593
Fecha:	05/02/2006
Hora:	03:14:27 p.m.
Usuario:	S-1-5-21-2780117151-1340924567-2512508698-1024
Equipo:	COUNTERS
Descripción:	Ha terminado un proceso:
Id. de proceso:	3744
Nombre de archivo de imagen:	C:\Program Files\Windows Media Player\wmplayer.exe
Nombre de usuario:	ver0k
Dominio:	COUNTERS
Id. de inicio de sesión:	(0x0,0x3F4E19)

Posteriormente continua viendo archivos con *wordpad*, *wmplayer* y ejecutando los binarios que pertenecen al usuario *administrator*, como *los huevo-cartoons* en el directorio *My Videos*:

Tipo de suceso:	Aciertos
Origen del suceso:	Security
Categoría del suceso:	Seguimiento detallado
Id. suceso:	592
Fecha:	05/02/2006
Hora:	03:33:50 p.m.
Usuario:	S-1-5-21-2780117151-1340924567-2512508698-1024
Equipo:	COUNTERS
Descripción:	Se ha creado un proceso:
Id. de proceso:	2492

```
Nombre de archivo de imagen: C:\Documents and Settings\Administrator\My Documents\My
Videos\cartoons\Te quiero como a mi huevo.exe
Id. de proceso creador: 720
Nombre de usuario: ver0k
Dominio: COUNTERS
Id. de inicio de sesión: (0x0,0x3F4E19)
```

También terminó la aplicación MySQLAdministrator:

```
Tipo de suceso: Aciertos
Origen del suceso: Security
Categoría del suceso: Seguimiento detallado
Id. suceso: 593
Fecha: 05/02/2006
Hora: 03:59:16 p.m.
Usuario: S-1-5-21-2780117151-1340924567-2512508698-1024
Equipo: COUNTERS
Descripción:
Ha terminado un proceso:
  Id. de proceso: 2320
  Nombre de archivo de imagen: C:\Program Files\MySQL\MySQL Administrator
  1.1\MySQLAdministrator.exe
  Nombre de usuario: ver0k
  Dominio: COUNTERS
  Id. de inicio de sesión: (0x0,0x3F4E19)
```

Posteriormente a las **4:00pm** se registra una desconexión del usuario *ver0k* via **RDP (Remote Desktop Protocol)** que utiliza el servicio *Terminal Services* para la conexión remota desde la dirección IP externa **70.107.249.155**:

```
Tipo de suceso: Aciertos
Origen del suceso: Security
Categoría del suceso: Inicio/cierre de sesión
Id. suceso: 683
Fecha: 05/02/2006
Hora: 04:00:10 p.m.
Usuario: NT AUTHORITY\SYSTEM
Equipo: COUNTERS
Descripción:
Sesión desconectada de la estación de Windows:
  Nombre de usuario: ver0k
  Dominio: COUNTERS
  Id. inicio de sesión: (0x0,0x3F4E19)
  Nombre de sesión: RDP-Tcp#1
  Nombre de cliente: LUFERFU
  Dirección de cliente: 70.107.249.155
```

21 minutos después, a las **4:21pm** del mismo día domingo **2 de febrero** se crea un proceso de la herramienta **PTStart.exe** (perteneciente a trisnap spywaredata) en el entorno de Johnatan desde el cd-rom:

```
Tipo de suceso: Aciertos
Origen del suceso: Security
Categoría del suceso: Seguimiento detallado
Id. suceso: 592
Fecha: 05/02/2006
Hora: 04:21:01 p.m.
Usuario: S-1-5-21-2780117151-1340924567-2512508698-1006
Equipo: COUNTERS
Descripción:
Se ha creado un proceso:
  Id. de proceso: 3844
  Nombre de archivo de imagen: D:\PTStart.exe
  Id. de proceso creador: 904
  Nombre de usuario: Johnatan
  Dominio: COUNTERS
  Id. de inicio de sesión: (0x0,0x3DF69A)
```

Posteriormente corre el Explorador de Windows y el programa *winver.exe* que permite ver la descripción precisa del sistema operativo corriendo. Corre algunas herramientas desde el CD-ROM como *CMD* y *dd*:

```
Tipo de suceso:          Aciertos
Origen del suceso:      Security
Categoría del suceso:   Seguimiento detallado
Id. suceso:             592
Fecha:                  05/02/2006
Hora:                   04:25:37 p.m.
Usuario:                S-1-5-21-2780117151-1340924567-2512508698-1006
Equipo: COUNTERS
Descripción:
Se ha creado un proceso:
  Id. de proceso:          3644
  Nombre de archivo de imagen: D:\kit_de_respuesta\win2k_xp\dd.exe
  Id. de proceso creador:  3656
  Nombre de usuario:      Johnatan
  Dominio:                COUNTERS
  Id. de inicio de sesión: (0x0,0x3DF69A)
```

Inicia el usuario Administrator desde la misma consola:

```
Tipo de suceso:          Aciertos
Origen del suceso:      Security
Categoría del suceso:   Inicio/cierre de sesión
Id. suceso:             528
Fecha:                  05/02/2006
Hora:                   04:26:57 p.m.
Usuario:                S-1-5-21-2780117151-1340924567-2512508698-500
Equipo: COUNTERS
Descripción:
Inicio de sesión realizado:
  Nombre de usuario:      Administrator
  Dominio:                COUNTERS
  Id. de inicio de sesión: (0x0,0x50D2D6)
  Tipo de inicio de sesión: 2
  Proceso de inicio de sesión: seclogon
  Paquete de autenticación: Negotiate
  Nombre de estación de trabajo: COUNTERS
  GUID de inicio de sesión: -
```

```
Tipo de suceso:          Aciertos
Origen del suceso:      Security
Categoría del suceso:   Inicio/cierre de sesión
Id. suceso:             552
Fecha:                  05/02/2006
Hora:                   04:26:57 p.m.
Usuario:                S-1-5-21-2780117151-1340924567-2512508698-1006
Equipo: COUNTERS
Descripción:
Intento de inicio de sesión usando las credenciales explícitas:
  Usuario que ha iniciado sesión:
    Nombre usuario:      Johnatan
    Dominio:             COUNTERS
    Id. de inicio de sesión: (0x0,0x3DF69A)
    GUID de inicio de sesión: -
  Usuario cuyas credenciales se usaron:
    Nombre usuario:      Administrator
    Dominio:             COUNTERS
```

Y ejecuta las mismas herramientas *CMD* y *dd* que el usuario Johnatan:

```
Tipo de suceso:          Aciertos
Origen del suceso:      Security
Categoría del suceso:   Seguimiento detallado
```

```

Id. suceso:          592
Fecha:              05/02/2006
Hora:               04:26:58 p.m.
Usuario:            NT AUTHORITY\SYSTEM
Equipo: COUNTERS
Descripción:
Se ha creado un proceso:
  Id. de proceso:          176
  Nombre de archivo de imagen: D:\kit_de_respuesta\win2k_xp\CMD.EXE
  Id. de proceso creador:   836
  Nombre de usuario:        COUNTERS$
  Dominio:                  WORKGROUP
  Id. de inicio de sesión:  (0x0,0x3E7)

```

Nota: Analizando el valor `\DosDevicesID:` en la llave de registro `MountedDevices` es como se que la unidad `D` es un CD-ROM, en este caso registrado como un IDE marca LG:

```

\ ? ? \ I D E # C d R o m L G _ C D - R O M _ C R D - 8 5 2 2 B _ _ _ _ _
_ _ _ _ _ 2 . 0 0 _ _ _ # 5 & 3 3 3 2 1 8 c c & 0 & 0 . 0 . 0 # { 5 3 f 5 6 3 0 d - b
6 b f - 1 1 d 0 - 9 4 f 2 - 0 0 a 0 c 9 1 e f b 8 b }

```

Para obtener una vista de los datos de la llave, utilicé el mismo programa `Windows Registry File Viewer` con su función `Data View`.

Posteriormente los usuarios `Administrator` y `Johnatan` cierran sus sesiones:

```

Tipo de suceso:      Aciertos
Origen del suceso:   Security
Categoría del suceso: Inicio/cierre de sesión
Id. suceso:          538
Fecha:               05/02/2006
Hora:                04:28:28 p.m.
Usuario:              S-1-5-21-2780117151-1340924567-2512508698-500
Equipo: COUNTERS
Descripción:
Cierre de sesión de usuario:
  Nombre de usuario:      Administrator
  Dominio:                 COUNTERS
  Id. de inicio de sesión: (0x0,0x50D2D6)
  Tipo de inicio de sesión: 2

```

```

Tipo de suceso:      Aciertos
Origen del suceso:   Security
Categoría del suceso: Inicio/cierre de sesión
Id. suceso:          551
Fecha:               05/02/2006
Hora:                04:28:34 p.m.
Usuario:              S-1-5-21-2780117151-1340924567-2512508698-1006
Equipo: COUNTERS
Descripción:
Cierre de sesión iniciada por el usuario:
  Nombre usuario:         Johnatan
  Dominio:                 COUNTERS
  Id. de inicio de sesión: (0x0,0x3df69a)

```

Posteriormente se vuelve a loguear el **administrador**, sin embargo al estar nervioso teclea mal su nombre de usuario y se registra este evento:

```

Tipo de suceso:      Errores
Origen del suceso:   Security
Categoría del suceso: Inicio/cierre de sesión
Id. suceso:          529
Fecha:               05/02/2006
Hora:                04:29:01 p.m.
Usuario:              NT AUTHORITY\SYSTEM
Equipo: COUNTERS
Descripción:

```

```

Error al iniciar sesión:
  Razón:                               Nombre de usuario desconocido o contraseña incorrecta
  Nombre de usuario:                     adminstrator
  Dominio:                               COUNTERS
  Tipo de inicio de sesión:              2
  Proceso de inicio de sesión:           User32
  Paquete de autenticación:              Negotiate
  Nombre de estación de trabajo:         COUNTERS

```

Una vez logueado vuelve a correr las mismas herramientas:

```

Tipo de suceso:      Aciertos
Origen del suceso:   Security
Categoría del suceso: Seguimiento detallado
Id. suceso:          592
Fecha:               05/02/2006
Hora:                04:29:47 p.m.
Usuario:             S-1-5-21-2780117151-1340924567-2512508698-500
Equipo: COUNTERS
Descripción:
Se ha creado un proceso:
  Id. de proceso:      3640
  Nombre de archivo de imagen: D:\kit_de_respuesta\win2k_xp\CMD.EXE
  Id. de proceso creador: 3120
  Nombre de usuario:   Administrator
  Dominio:             COUNTERS
  Id. de inicio de sesión: (0x0,0x50ED34)

```

```

Tipo de suceso:      Aciertos
Origen del suceso:   Security
Categoría del suceso: Seguimiento detallado
Id. suceso:          592
Fecha:               05/02/2006
Hora:                04:30:27 p.m.
Usuario:             S-1-5-21-2780117151-1340924567-2512508698-500
Equipo: COUNTERS
Descripción:
Se ha creado un proceso:
  Id. de proceso:      860
  Nombre de archivo de imagen: D:\kit_de_respuesta\win2k_xp\dd.exe
  Id. de proceso creador: 3640
  Nombre de usuario:   Administrator
  Dominio:             COUNTERS
  Id. de inicio de sesión: (0x0,0x50ED34)

```

Ejecutó el comando *dd* 7 veces y por alguna razón ejecutó *mmc* que es la consola de administración de Microsoft:

```

Tipo de suceso:      Aciertos
Origen del suceso:   Security
Categoría del suceso: Seguimiento detallado
Id. suceso:          592
Fecha:               05/02/2006
Hora:                05:11:02 p.m.
Usuario:             S-1-5-21-2780117151-1340924567-2512508698-500
Equipo: COUNTERS
Descripción:
Se ha creado un proceso:
  Id. de proceso:      1724
  Nombre de archivo de imagen: C:\WINDOWS\system32\mmc.exe
  Id. de proceso creador: 3120
  Nombre de usuario:   Administrator
  Dominio:             COUNTERS
  Id. de inicio de sesión: (0x0,0x50ED34)

```

También se registró en el entorno de *Administrator* el uso de las herramientas:

Hora	Comando
05:32:21pm	D:\win32\fire.exe
05:32:44pm	D:\win32\CMD.EXE
05:32:53pm	D:\statbins\win32\LS.EXE
05:32:54pm	D:\statbins\win32\LS.EXE
05:33:47pm	D:\win32\wdd.exe
05:36:14pm	D:\win32\dumpel.exe
05:39:03pm	D:\statbins\win32\LS.EXE
05:42:11pm	D:\win32\sysinternals\pslist.exe

También, el usuario *Administrator* cerró la sesión de *ver0k*, ya que terminó la conexión *RDP* pero no cerró sesión el usuario. Esta información coincide con *NTUSER.DAT* de *ver0k*:

```
Tipo de suceso:      Aciertos
Origen del suceso:  Security
Categoría del suceso:  Uso de privilegios
Id. suceso:         578
Fecha:              05/02/2006
Hora:                05:43:56 p.m.
Usuario:             S-1-5-21-2780117151-1340924567-2512508698-500
Equipo: COUNTERS
Descripción:
Operación de objetos con privilegios:
  Servidor de objetos:      Security
  Identificador de objeto:  0
  Id. de proceso:          356
  Nombre de usuario principal:  COUNTERS$
  Dominio principal:       WORKGROUP
  Id. de inicio de sesión principal: (0x0,0x3E7)
  Nombre de usuario cliente: Administrator
  Dominio de cliente:      COUNTERS
  Id. de inicio de sesión de cliente: (0x0,0x50ED34)
  Privilegios:             SeShutdownPrivilege
```

Y procedió con el apagado del sistema:

```
Tipo de suceso:      Aciertos
Origen del suceso:  SECURITY
Categoría del suceso:  Suceso del sistema
Id. suceso:         513
Fecha:              05/02/2006
Hora:                05:44:17 p.m.
Usuario:             No disponible
Equipo: COUNTERS
Descripción:
Windows está apagándose. Todas las sesiones iniciadas finalizarán con este apagado.
```

Hasta este momento la actividad me parece muy extraña por lo que no quisiera hacer especulaciones, ya que todas son evidencias circunstanciales.

Aplicación:

Existen varias entradas de eventos relacionados con la falta de archivos de librerías DLL:

```
Tipo de suceso:      Información
Origen del suceso:  COM+
Categoría del suceso:  Ninguno
Id. suceso:         781
Fecha:              26/01/2006
Hora:                12:35:39 a.m.
Usuario:             No disponible
Equipo: COUNTERS
Descripción:
```

No se encuentra la descripción del Id. de suceso (781) en el origen (COM+). **Es posible que el equipo local no tenga la información de Registro o archivos DLL de mensajes necesarios para mostrar mensajes desde un equipo remoto.** Es posible que pueda usar el indicador /AUXSOURCE= para recuperar esta descripción; consulte Ayuda y soporte técnico para obtener más detalles. La siguiente información es parte del suceso: 86400, SuppressDuplicateDuration, Software\Microsoft\COM3\Eventlog.

Bitácoras de Servicios

MySQL:

En el archivo /apache/Apache/mysql/data/counters-bin.000001 se aplicó el comando *strings* para obtener las cadenas de texto, después de leerlas línea por línea se apreciaron 2 cosas: las últimas visitas al **web-erp** fueron el día domingo 2 de febrero:

```
$ strings counters-bin.000001 | grep lastvisitdate
UPDATE www_users SET lastvisitdate='2006-02-03 19:59:18'
UPDATE www_users SET lastvisitdate='2006-02-03 19:59:59'
UPDATE www_users SET lastvisitdate='2006-02-05 07:03:46'
UPDATE www_users SET lastvisitdate='2006-02-05 10:38:32'
UPDATE www_users SET lastvisitdate='2006-02-05 10:41:15'
UPDATE www_users SET lastvisitdate='2006-02-05 13:57:51'
UPDATE www_users SET lastvisitdate='2006-02-05 14:18:42'
UPDATE www_users SET lastvisitdate='2006-02-05 14:19:17'
```

Y revisando el archivo completo, determiné que los usuarios en entrar el día domingo fueron *acontreras* y *ncanes*, quienes según *www_users* encontrado en temporales corresponden a los nombres: Alberto Contreras Zacarías registrado como *System Administrator* y Napoleón Canes registrado como *Gerente de Compras y Abastecimiento*.

Un registro de sus actividades se almacena en *counters.log* en el mismo directorio que el archivo anterior, sin embargo se tiene el registro de la creación de una cuenta de usuario llamada *admin* a las 14:00:15pm del día 2 de febrero:

```
060205 14:00:15      1398 Connect      weberp_us@localhost as anonymous on
                   1398 Init DB        weberp
                   1398 Query        SELECT secroleid, secrolename FROM securityroles ORDER BY secroleid
                   1398 Query        INSERT INTO www_users (userid,
                                realname,
                                customerid,
                                branchcode,
                                password,
                                phone,
                                email,
                                pagesize,
                                fullaccess,
                                defaultlocation,
                                modulesallowed,
                                displayrecordsmax,
                                theme,
                                language)
                                VALUES ('admin',
                                'admin',
                                '',
                                '',
                                '5542a545f7178b48162c1725ddf2090e22780e25',
                                '',
                                '',
                                'A4',
                                8,
                                'AGS',
                                '1,1,1,1,1,1,1,1,1,1',
                                50,
                                'fresh',
                                'en_GB')
                   1398 Query        SELECT userid,
                                realname,
                                phone,
                                email,
                                customerid,
                                branchcode,
                                lastvisitdate,
                                fullaccess,
                                pagesize
                   FROM www_users
                   1398 Query        SELECT loccode, locationname FROM locations
                   1398 Quit
060205 14:00:59      1399 Connect      weberp_us@localhost as anonymous on
                   1399 Init DB        weberp
                   1399 Quit
```

Apache:

En el archivo `/apache/Apache/logs/access.log` se encuentran las bitácoras del servidor web *Apache*; se dejaron notar muchos análisis de vulnerabilidades por herramientas como *Nikto*:

```
192.168.100.144 - - [30/Jan/2006:17:28:30 -0900] "HEAD / HTTP/1.1" 200 0
192.168.100.144 - - [30/Jan/2006:17:28:30 -0900] "HEAD / HTTP/1.1" 200 0
192.168.100.144 - - [30/Jan/2006:17:28:30 -0900] "GET /Nikto-1.35-D3nG4mWwXVa0fQQ8.htm HTTP/1.1" 404 303
192.168.100.144 - - [30/Jan/2006:17:28:30 -0900] "GET / HTTP/1.1" 200 1494
192.168.100.144 - - [30/Jan/2006:17:28:30 -0900] "GET /cgi.cgi/ HTTP/1.1" 404 280
192.168.100.144 - - [30/Jan/2006:17:28:30 -0900] "GET /webcgi/ HTTP/1.1" 404 279

192.168.5.32 - - [01/Feb/2006:17:53:03 -0900] "HEAD / HTTP/1.1" 200 0
192.168.5.32 - - [01/Feb/2006:17:53:03 -0900] "GET /Nikto-1.35-HrzubUBFWsfi.htm HTTP/1.1" 404 299
192.168.5.32 - - [01/Feb/2006:17:53:03 -0900] "GET / HTTP/1.1" 200 1494
```

Estas salidas las muestro truncadas por fines prácticos, sin embargo se puede apreciar como algún usuario de nuestra **red interna** realizó análisis automatizados:

```
192.168.100.144 - - [30/Jan/2006:17:28:49 -0900] "GET
/logbook.pl?file=../../../../../../../../bin/cat%20/etc/passwd%00| HTTP/1.0" 404 270
```

En este ejemplo de la bitácora se ve como se quiere realizar un listado del archivo `/etc/passwd` cuando en realidad el sistema no es de Tipo-Unix. También se pueden ver análisis de vulnerabilidades con herramientas automatizadas como *Nessus* pero desde una dirección **IP externa** que corresponde a un host de *araxis.es*:

```
84.18.17.15 - - [04/Feb/2006:14:08:35 -0800] "GET /3/ HTTP/1.1" 404 274
84.18.17.15 - - [04/Feb/2006:14:08:35 -0800] "GET /4/ HTTP/1.1" 404 274
84.18.17.15 - - [04/Feb/2006:14:08:35 -0800] "NESSUS / HTTP/1.0" 501 320
84.18.17.15 - - [04/Feb/2006:14:08:36 -0800] "GET /5/ HTTP/1.1" 404 274
84.18.17.15 - - [04/Feb/2006:14:08:36 -0800] "GET /6/ HTTP/1.1" 404 274
```

La salida la muestro truncada por fines prácticos, pero en este momento ya podemos hacernos una idea de cómo han sucedido las cosas (puntos débiles), pero todavía no podemos afirmarlas pues debemos basarnos en hechos, no en supuestos.

Para determinar quien creo la cuenta de usuario según la bitacora de *MySQL*, hacemos una correlación con la bitacora de *Apache*, donde vemos que el único usuario que realizó una actividad a las 2 de la tarde con 15 segundos del día domingo 5 de febrero del año 2006 fue alguien con la dirección IP **70.107.249.150** que pertenece al mismo segmento de red donde se encuentra *verOk*:

```
70.107.249.150 - - [05/Feb/2006:13:57:37 -0800] "GET /web-erp/ HTTP/1.1" 200 3210
70.107.249.150 - - [05/Feb/2006:13:57:37 -0800] "GET /web-erp/css/professional/login.css HTTP/1.1" 200
1394
70.107.249.150 - - [05/Feb/2006:13:57:37 -0800] "GET /web-erp/css/webERP.gif HTTP/1.1" 200 2506
70.107.249.150 - - [05/Feb/2006:13:57:37 -0800] "GET /web-erp/logo_server.jpg HTTP/1.1" 200 8203
70.107.249.150 - - [05/Feb/2006:13:57:37 -0800] "GET /web-erp/css/bg.gif HTTP/1.1" 200 1275
70.107.249.150 - - [05/Feb/2006:13:57:37 -0800] "GET /web-erp/css/spacer.gif HTTP/1.1" 200 43
70.107.249.150 - - [05/Feb/2006:13:57:37 -0800] "GET /favicon.ico HTTP/1.1" 404 283
70.107.249.150 - - [05/Feb/2006:13:57:52 -0800] "POST /web-erp/index.php HTTP/1.1" 200 76
70.107.249.150 - - [05/Feb/2006:13:57:52 -0800] "GET /web-erp/index.php? HTTP/1.1" 200 6628
70.107.249.150 - - [05/Feb/2006:13:57:52 -0800] "GET /web-erp/css/fresh/default.css HTTP/1.1" 200 6543
70.107.249.150 - - [05/Feb/2006:13:57:52 -0800] "GET /web-erp/favicon.ico HTTP/1.1" 200 1406
70.107.249.150 - - [05/Feb/2006:13:57:52 -0800] "GET /web-erp/css/fresh/images/transactions.gif HTTP/1.1"
200 1548
70.107.249.150 - - [05/Feb/2006:13:57:52 -0800] "GET /web-erp/css/fresh/images/menurcurve.gif HTTP/1.1"
200 976
70.107.249.150 - - [05/Feb/2006:13:57:52 -0800] "GET /web-erp/css/fresh/images/reports.gif HTTP/1.1" 200
434
70.107.249.150 - - [05/Feb/2006:13:57:52 -0800] "GET /web-erp/css/fresh/images/maintenance.gif HTTP/1.1"
200 1383
70.107.249.150 - - [05/Feb/2006:13:57:52 -0800] "GET /web-erp/css/webERPsm.gif HTTP/1.1" 200 357
70.107.249.150 - - [05/Feb/2006:13:57:52 -0800] "GET /web-erp/css/fresh/bullet.gif HTTP/1.1" 200 183
70.107.249.150 - - [05/Feb/2006:13:57:54 -0800] "GET /web-erp/PDFDeliveryDifferences.php? HTTP/1.1" 200
4083
70.107.249.150 - - [05/Feb/2006:13:57:57 -0800] "GET /web-erp/index.php? HTTP/1.1" 200 6628
70.107.249.150 - - [05/Feb/2006:13:58:00 -0800] "GET /web-erp/index.php?&Application=system HTTP/1.1" 200
9083
70.107.249.150 - - [05/Feb/2006:13:58:00 -0800] "GET /web-erp/css/fresh/images/company.gif HTTP/1.1" 200
1741
70.107.249.150 - - [05/Feb/2006:13:58:00 -0800] "GET /web-erp/css/fresh/images/ar.gif HTTP/1.1" 200 1763
```

```

70.107.249.150 - - [05/Feb/2006:13:58:00 -0800] "GET /web-erp/css/fresh/images/inventory.gif HTTP/1.1" 200 1751
70.107.249.150 - - [05/Feb/2006:13:58:02 -0800] "GET /web-erp/SystemParameters.php? HTTP/1.1" 200 16483
70.107.249.150 - - [05/Feb/2006:13:58:06 -0800] "GET /web-erp/index.php? HTTP/1.1" 200 9083
70.107.249.150 - - [05/Feb/2006:13:58:10 -0800] "GET /web-erp/WWW_Users.php? HTTP/1.1" 200 14613
70.107.249.150 - - [05/Feb/2006:13:59:44 -0800] "POST /web-erp/WWW_Users.php? HTTP/1.1" 200 14760
70.107.249.150 - - [05/Feb/2006:14:00:15 -0800] "POST /web-erp/WWW_Users.php? HTTP/1.1" 200 14951
70.107.249.150 - - [05/Feb/2006:14:00:59 -0800] "GET /web-erp/Logout.php? HTTP/1.1" 200 2449
70.107.249.150 - - [05/Feb/2006:14:00:59 -0800] "GET /web-erp/css/fresh/login.css HTTP/1.1" 200 1415
70.107.249.150 - - [05/Feb/2006:14:00:59 -0800] "GET /web-erp/companies/weberp/logo.jpg HTTP/1.1" 200 8203

```

En esta actividad se aprecia el acceso al script de manejo de usuarios (PHP). En esta misma bitacora se aprecia la actividad de *acontreras* desde el equipo de manera local (127.0.0.1):

```

127.0.0.1 - - [05/Feb/2006:14:18:19 -0800] "GET /web-erp/ HTTP/1.1" 200 3210
127.0.0.1 - - [05/Feb/2006:14:18:19 -0800] "GET /web-erp/css/professional/login.css HTTP/1.1" 200 1394
127.0.0.1 - - [05/Feb/2006:14:18:19 -0800] "GET /web-erp/css/spacer.gif HTTP/1.1" 200 43
127.0.0.1 - - [05/Feb/2006:14:18:19 -0800] "GET /web-erp/css/webERP.gif HTTP/1.1" 200 2506
127.0.0.1 - - [05/Feb/2006:14:18:19 -0800] "GET /web-erp/css/bg.gif HTTP/1.1" 200 1275
127.0.0.1 - - [05/Feb/2006:14:18:19 -0800] "GET /web-erp/logo_server.jpg HTTP/1.1" 200 8203
127.0.0.1 - - [05/Feb/2006:14:18:42 -0800] "POST /web-erp/index.php HTTP/1.1" 200 76
127.0.0.1 - - [05/Feb/2006:14:19:04 -0800] "GET /web-erp HTTP/1.1" 301 307
127.0.0.1 - - [05/Feb/2006:14:19:04 -0800] "GET /web-erp/ HTTP/1.1" 200 3210
127.0.0.1 - - [05/Feb/2006:14:19:04 -0800] "GET /web-erp/css/professional/login.css HTTP/1.1" 200 1394
127.0.0.1 - - [05/Feb/2006:14:19:04 -0800] "GET /web-erp/css/spacer.gif HTTP/1.1" 200 43
127.0.0.1 - - [05/Feb/2006:14:19:04 -0800] "GET /web-erp/logo_server.jpg HTTP/1.1" 200 8203
127.0.0.1 - - [05/Feb/2006:14:19:04 -0800] "GET /web-erp/css/bg.gif HTTP/1.1" 200 1275
127.0.0.1 - - [05/Feb/2006:14:19:04 -0800] "GET /web-erp/css/webERP.gif HTTP/1.1" 200 2506
127.0.0.1 - - [05/Feb/2006:14:19:17 -0800] "POST /web-erp/index.php HTTP/1.1" 200 76
127.0.0.1 - - [05/Feb/2006:14:19:17 -0800] "GET /web-erp/index.php? HTTP/1.1" 200 6628
127.0.0.1 - - [05/Feb/2006:14:19:17 -0800] "GET /web-erp/css/fresh/images/menucurve.gif HTTP/1.1" 200 976
127.0.0.1 - - [05/Feb/2006:14:19:17 -0800] "GET /web-erp/css/fresh/default.css HTTP/1.1" 200 6543
127.0.0.1 - - [05/Feb/2006:14:19:17 -0800] "GET /web-erp/css/fresh/images/transactions.gif HTTP/1.1" 200 1548
127.0.0.1 - - [05/Feb/2006:14:19:17 -0800] "GET /web-erp/css/fresh/images/reports.gif HTTP/1.1" 200 434
127.0.0.1 - - [05/Feb/2006:14:19:18 -0800] "GET /web-erp/css/fresh/images/maintenance.gif HTTP/1.1" 200 1383
127.0.0.1 - - [05/Feb/2006:14:19:18 -0800] "GET /web-erp/css/webERPsm.gif HTTP/1.1" 200 357
127.0.0.1 - - [05/Feb/2006:14:19:18 -0800] "GET /web-erp/css/fresh/bullet.gif HTTP/1.1" 200 183
127.0.0.1 - - [05/Feb/2006:14:19:24 -0800] "GET /web-erp/index.php?&Application=stock HTTP/1.1" 200 8914
127.0.0.1 - - [05/Feb/2006:14:19:29 -0800] "GET /web-erp/index.php?&Application=PO HTTP/1.1" 200 5858
127.0.0.1 - - [05/Feb/2006:14:19:30 -0800] "GET /web-erp/index.php? HTTP/1.1" 200 5858
127.0.0.1 - - [05/Feb/2006:14:19:32 -0800] "GET /web-erp/index.php? HTTP/1.1" 200 5858
127.0.0.1 - - [05/Feb/2006:14:19:33 -0800] "GET /web-erp/index.php?&Application=orders HTTP/1.1" 200 6628
127.0.0.1 - - [05/Feb/2006:14:19:35 -0800] "GET /web-erp/index.php?&Application=system HTTP/1.1" 200 9083
127.0.0.1 - - [05/Feb/2006:14:19:35 -0800] "GET /web-erp/css/fresh/images/ar.gif HTTP/1.1" 200 1763
127.0.0.1 - - [05/Feb/2006:14:19:35 -0800] "GET /web-erp/css/fresh/images/company.gif HTTP/1.1" 200 1741
127.0.0.1 - - [05/Feb/2006:14:19:35 -0800] "GET /web-erp/css/fresh/images/inventory.gif HTTP/1.1" 200 1751
127.0.0.1 - - [05/Feb/2006:14:19:37 -0800] "GET /web-erp/WWW_Users.php? HTTP/1.1" 200 14950
127.0.0.1 - - [05/Feb/2006:14:20:06 -0800] "GET /web-erp/Logout.php? HTTP/1.1" 200 2449
127.0.0.1 - - [05/Feb/2006:14:20:06 -0800] "GET /web-erp/css/fresh/login.css HTTP/1.1" 200 1415
127.0.0.1 - - [05/Feb/2006:14:20:06 -0800] "GET /web-erp/companies/weberp/logo.jpg HTTP/1.1" 200 8203

```

Se aprecia que *acontreras* a las **2:19:37pm** vio las cuentas de usuarios al hacer el listado en el sistema *web-erp*.

Análisis de la información

Se tiene un servidor *Windows 2003* con un solo procesador *Intel*; su hostname es *COUNTERS* y su dirección IP interna es 192.168.5.5 y su gateway es 192.168.5.254 muy probablemente con una tarjeta de red 3com 3C900B y una Realtek RTL8139. Esta información se pudo obtener según las llaves del registro:

```

MACHINE\System\CurrentControlSet\Services\TCPIP\Parameters\Interfaces
ControlSet001\Control\Network\{4D36E972-E325-11CE-BFC1-08002BE10318}\Descriptions

```

Y la comprobé en el *pagefile.sys* y en el registro de eventos del *DNS*. No fue posible extraer la IP externa. Las variables del ambiente son similares a las de cualquier sistema *Windows 2003* por default:

```
SERPROFILE=C:\Documents and Settings\All Users
APPDATA=C:\Documents and Settings\Administrator\Application Data
ClusterLog=C:\WINDOWS\Cluster\cluster.log
CommonProgramFiles=C:\Program Files\Common Files
COMPUTER_NAME=COUNTERS
ComSpec=C:\WINDOWS\system32\cmd.exe
FP_NO_HOST_CHECK=NO
LOGONSERVER=\\COUNTERS
NUMBER_OF_PROCESSORS=1
OS=Windows_NT
Path=C:\WINDOWS\system32;C:\WINDOWS;C:\WINDOWS\System32\Wbem
PATHEXT=.COM;.EXE;.BAT;.CMD;.VBS;.VBE;.JS;.JSE;.WSF;.WSH
PROCESSOR_ARCHITECTURE=x86
PROCESSOR_IDENTIFIER=x86 Family 6 Model 8 Stepping 3, GenuineIntel
PROCESSOR_LEVEL=6
PROCESSOR_REVISION=0803
ProgramFiles=C:\Program Files
SystemDrive=C:
SystemRoot=C:\WINDOWS
TEMP=C:\WINDOWS\TEMP
TMP=C:\WINDOWS\TEMP
USERPROFILE=C:\Documents and Settings\Administrator
windir=C:\WINDOWS
```

Este servidor corría con los servicios de *MySQL*, *Apache*, *PostgreSQL*, así como herramientas de uso diario, pues también se utilizaba como estación de trabajo. El sistema operativo si contaba con los parches/fixes de seguridad instalados. El programa *web-erp* que es el principal motivo de su existencia corría una versión actualizada. *Apache* corría una versión vieja (1.3.34) por lo que es susceptible a la vulnerabilidad *cross-site scripting* en el módulo *mod_imap* según *CVE-2005-3352*.

Se detectaron escaneos y análisis de vulnerabilidades automatizados desde las siguientes direcciones IP:

```
192.168.100.144
192.168.5.32
84.18.17.15
```

Y extrañamente un acceso registrado por *Apache* desde la dirección externa *70.107.249.150* cuyas actividades se registraron por *MySQL*. Esta dirección IP corresponde a la misma red donde se logueo el usuario *ver0k* creado por el usuario *johnatan* el día **2 de febrero**. El historial del Internet Explorer del usuario *ver0k* nos muestra lo siguiente

```
:2006020520060206: ver0k@file:///C:/apache/Apache/htdocs/web-erp/AccountGroups.php
URL
:2006020520060206: ver0k@Host: My Computer
URL
:2006020520060206: ver0k@file:///C:/apache/Apache/htdocs/web-erp/config.php
```

El archivo *AccountGroups.php* es un módulo del programa *web-erp* para el manejo de cuentas de grupos. El programa *config.php* contiene parámetros de configuración del programa, en el cual sobresale lo siguiente:

Su fecha de creación es la misma que la de la creación del sistema:

```
Z:\apache\Apache\htdocs\web-erp>dir config.php /TC
El volumen de la unidad Z no tiene etiqueta.
El número de serie del volumen es: A803-85D0

Directorio de Z:\apache\Apache\htdocs\web-erp

26/01/2006  08:47 p.m.          3,569 config.php
             1 archivos          3,569 bytes
             0 dirs  2,669,223,936 bytes libres
```

Su fecha de modificación es el mismo día, 26 de enero:

```
Z:\apache\Apache\htdocs\web-erp>dir config.php /TW
El volumen de la unidad Z no tiene etiqueta.
```

```
El número de serie del volumen es: A803-85D0
Directorio de Z:\apache\Apache\htdocs\web-erp
26/01/2006 09:01 p.m.          3,569 config.php
1 archivos                    3,569 bytes
0 dirs  2,669,223,936 bytes libres
```

Su último acceso fue el día 5 de febrero a las 3:57pm

```
Z:\apache\Apache\htdocs\web-erp>dir config.php /TA
El volumen de la unidad Z no tiene etiqueta.
El número de serie del volumen es: A803-85D0

Directorio de Z:\apache\Apache\htdocs\web-erp
05/02/2006 03:57 p.m.          3,569 config.php
1 archivos                    3,569 bytes
0 dirs  2,669,223,936 bytes libres
```

También existe el archivo *config.php.bak* con la misma fecha de creación:

```
Z:\apache\Apache\htdocs\web-erp>dir config.php.bak /TC
El volumen de la unidad Z no tiene etiqueta.
El número de serie del volumen es: A803-85D0

Directorio de Z:\apache\Apache\htdocs\web-erp
26/01/2006 08:47 p.m.          3,486 config.php.bak
1 archivos                    3,486 bytes
0 dirs  2,669,223,936 bytes libres
```

Pero con una fecha extraña de modificación, ya que es 13 días antes a su fecha de creación:

```
Z:\apache\Apache\htdocs\web-erp>dir config.php.bak /TW
El volumen de la unidad Z no tiene etiqueta.
El número de serie del volumen es: A803-85D0

Directorio de Z:\apache\Apache\htdocs\web-erp
13/01/2006 08:36 p.m.          3,486 config.php.bak
1 archivos                    3,486 bytes
0 dirs  2,669,223,936 bytes libres
```

Desconozco la razón de este comportamiento. La diferencia entre estos archivos es la directiva:

```
$allow_demo_mode = True;
```

Que fue modificada a:

```
$allow_demo_mode = False;
```

Con la intención de que el programa *web-erp* no muestre un demo login al inicio. Y las directivas default:

```
$dbuser = 'weberp_db_user';
$dbpassword = 'weberp_db_pwd';
```

Fueron cambiadas por:

```
$dbuser = 'weberp_us';
$dbpassword = '';
```

El usuario que manipula la base de datos que se nota en las bitácoras efectivamente es *weberp_us*, pero el password fue eliminado por el mismo administrador, el día de la instalación del servidor. Solo hasta este punto me atrevo a realizar una hipótesis sobre el sistema comprometido.

El administrador de sistemas de quien se desconoce su nombre real, se encontraba en la oficina el día domingo 5 de febrero trabajando presencialmente en el servidor con la cuenta **Johnatan** que pertenece a un usuario de nombre Johnatan Tezca. También se encontraba logueado al sistema *web-erp* mediante la cuenta **acontreras** que pertenece a un usuario de nombre Alberto Contreras

Zacarías. Sin embargo hubo un logueo a *web-erp* desde la IP externa 70.107.249.150 a la **1:57pm** registrada la solicitud de login en *Apache*:

```
70.107.249.150 - - [05/Feb/2006:13:57:37 -0800] "GET /web-erp/css/professional/login.css HTTP/1.1" 200 1394
```

Y a la misma hora/minuto *MySQL* registra un logueo con la cuenta **acontreras**:

```
060205 13:57:51      1389 Connect      weberp_us@localhost as anonymous on
                  1389 Init DB      weberp
                  1389 Query      SELECT www_users.fullaccess,
www_users.customerid,
www_users.lastvisitdate,
www_users.pagesize,
www_users.defaultlocation,
www_users.branchcode,
www_users.modulesallowed,
www_users.blocked,
www_users.realname,
www_users.theme,
www_users.displayrecordsmax,
www_users.userid,
www_users.language
FROM www_users
WHERE www_users.userid='acontreras'
AND (www_users.password='067f1396a8434994b5c1c69edfd29c17571993ee'
OR www_users.password='c0ntr3t0')
```

A las **2:00:15pm** se creó la cuenta **admin** registrado por *MySQL*:

```
060205 14:00:15      1398 Connect      weberp_us@localhost as anonymous on
                  1398 Init DB      weberp
                  1398 Query      SELECT secroleid, secrolename FROM securityroles ORDER BY secroleid
                  1398 Query      INSERT INTO www_users (userid,
```

Coincidentemente en *Apache* se tiene registrada la dirección **70.107.249.150** a la misma hora **2:00:15pm** el acceso a *WWW_Users.php* que es por medio del cual se pueden manejar las cuentas de usuario via *web-erp*:

```
70.107.249.150 - - [05/Feb/2006:14:00:15 -0800] "POST /web-erp/WWW_Users.php? HTTP/1.1" 200 14951
```

El **administrador de sistemas** consulta a las **2:19:37pm** mediante *WWW_Users* los usuarios de *web-erp* y se fija en una cuenta de usuario que el no había hecho:

```
127.0.0.1 - - [05/Feb/2006:14:19:37 -0800] "GET /web-erp/WWW_Users.php? HTTP/1.1" 200 14950
```

Minutos después, a las **2:45pm** crea una cuenta de usuario nueva con iguales privilegios que los demás, de nombre **ver0k**. Posteriormente comprueba conectividad con un host remoto y ejecuta algunos comandos del sistema operativo. A las **2:47pm** un usuario se logea a *Windows 2003* mediante *Remote Desktop* con la cuenta **ver0k** desde la dirección **70.107.249.155** Entre otras cosas, visualiza los archivos *PHP* descritos anteriormente, a las **2:51pm** ejecuta *MySQL* y a las **3:59pm** ejecuta *MySQLAdministrator*, posiblemente un usuario avanzado, amigo del administrador a quien le pidió ayuda. Quien no perdió la oportunidad de ver las fotos de las modelos desnudas de la cuenta *Administrator*. A las **4pm** se desconecta sin cerrar sesión dejando ver su IP y su hostname *static-70-107-249-155.ny325.east.verizon.net*

Igualmente se registra el nombre de cliente *LUFERFU*, que buscando referencia a este como un alias o nick, la única persona asociada a este nombre pertenece a Luis Fernando Fuentes Serrano con correos: *luferru @ hotmail.com lfuentes @ correo.seguridad.unam.mx luis @ cancan.fi-a.unam.mx*

A las **4:21pm** el administrador de sistemas, aún logueado con la cuenta **Johnatan** ejecuta herramientas para revisión de *spyware* y de respuesta a incidentes mediante un *secondary logon* (mediante la opción *Ejecutar como...*), sin embargo decide cerrar sesión y loguearse como *Administrator*. Nervioso se equivoca y logra entrar hasta el segundo intento. Vuelve a correr las mismas herramientas y procedió con el apagado del sistema a las **5:44pm**.

Conclusión del análisis

Partiendo de que solo se contaba con la imagen del sistema afectado, por razones ajenas a mi no se entregó la información volátil que obtuvo el administrador antes de apagar el sistema a pesar de ser solicitada. Se pueden obtener más datos de la imagen del disco, sin embargo es suficiente la información obtenida pues se alcanzó el objetivo principal y ya se pueden responder las preguntas realizadas por el Reto-Forense:

¿El sistema ha sido comprometido?

Si ha sido comprometido, sin embargo no ha sido hackeado. Un usuario logró el ingreso mediante una cuenta de usuario válida con autorización y privilegios.

¿Quién (desde dónde) se realizó el ataque?

Un usuario ubicado en New York (Estados Unidos), con Verizon Internet Services Inc como Proveedor de Internet. Mismo proveedor que el usuario *verOk*, por lo que es posible, forman parte de una red que mantiene conectividad con el sistema *web-erp* por motivos de negocio. Sin embargo, no se descarta la posibilidad que ante las condiciones de oportunidad encontradas, se trate de una broma de un usuario (LUFERFU).



¿Cómo se realizó el ataque?

Comprometiendo la cuenta de usuario, debido a que un atacante busca el camino más fácil los puntos a atacar no siempre son los sistemas o computadoras, también los usuarios. Hay que mencionar que la autenticación con passwords fijos, como en este caso utilizaron *c0ntr3t0* para la cuenta *acontreras*, no siempre es lo más adecuado.

¿Qué hizo el atacante en el sistema comprometido?

Añadió la cuenta *admin* en el sistema *web-erp* dentro del grupo administradores, para mantener su posterior ingreso de manera sencilla. No tengo registro de más actividad relacionada con esta IP. En el resumen ejecutivo, escribiré algunas recomendaciones a tomar así como mis observaciones.