

Informe Reto Forense 3 - Informe Técnico -

[\(http://www.seguridad.unam.mx/eventos/reto/\)](http://www.seguridad.unam.mx/eventos/reto/)

Fernando Gozalo Díaz
fernando.gozalo@gmail.com
Madrid (España)

Tabla de contenidos

<i>Antecedentes del incidente</i> _____	3
<i>Recolección de datos</i> _____	3
<i>Descripción de la evidencia</i> _____	3
<i>Entorno del análisis</i> _____	4
Descripción de las Herramientas _____	4
<i>Análisis de la evidencia</i> _____	4
Información del sistema analizado _____	4
<i>Línea del tiempo del sistema</i> _____	6
<i>Alcance de la intrusión</i> _____	19
¿El sistema ha sido comprometido? _____	19
¿Quién (desde dónde) se realizó el ataque? y ¿Cómo se realizó el ataque? _	19
¿Qué hizo el atacante en el sistema comprometido? _____	21

Antecedentes del incidente

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 acceso 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 acceder 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.

Ahora es necesario determinar si existió un ingreso no autorizado, cómo ocurrió y el alcance del daño al sistema y a la información contenida en él.

Recolección de datos

Se dispone de una Imagen de disco con el sistema. Se desconoce la arquitectura de red (firewalls, etc).

Descripción de la evidencia

Imagen analizada: windows2003.dd (5.239.471.104 bytes)
Md5sum: 062cf5d1ccd000e20cf4c006f2f6cce4

Entorno del análisis

Para realizar el análisis se ha utilizado un Pentium 4 2GHZ con Windows XP Professional. Además para corroborar resultados, se ha dispuesto de otra máquina (un Pentium 3 800 Mhz) utilizando Live CD's de recuperación de datos (Helix y miniPE) un disco duro del mismo tamaño que el analizado (6GB) y se ha volcado la imagen para contrastar los resultados obtenidos con la imagen.

Descripción de las Herramientas

Winimage (<http://www.winimage.com/>)
DD for Windows (<http://uranus.it.swin.edu.au/~jn/linux/rawwrite/dd.htm>),
Herramientas contenidas en Helix: (<http://www.e-fense.com/helix/>)
Herramientas contenidas en MiniPE:
(<http://jacksonian.ca/brian/info/miniPE.htm>)
Ultraedit (<http://www.ultraedit.com/>)
Visor de eventos de Windows:
(http://www.microsoft.com/resources/documentation/windows/xp/all/prod/docs/en-us/snap_event_viewer.mspx)
L0Phtcrack (<http://www.securityfocus.com/tools/1005>)
IEHistoryView (<http://www.nirsoft.net/utils/iehv.html>)
Virtual Disk Driver (v3) (<http://chitchat.at.infoseek.co.jp/vmware/vdk.html>)

Análisis de la evidencia

Información del sistema analizado

Sistema operativo	Microsoft Windows 2003 R2 AdvancedServer Service Pack 1 en Inglés.
Nombre del Host	COUNTERS
Parches instalados	KB890046, KB896358, KB896422, KB896424, KB896428, KB896688, KB896727, KB899587, KB899589, KB901017, KB901214, KB902400, KB903235, KB905414, KB908519, Q147222
Memoria física:	480MB

Software (excluyendo el del sistema operativo) instalado en el servidor, por orden cronológico de instalación:



















Fecha y Hora

Software y localización del instalable

27/01/2006,3:00:53	Apache 1.3.34 instalado desde DP(1)0-0+5\ERP\apache_1.3.34-win32-x86-no_src.exe
27/01/2006,3:03:12	PHP 4.4.2 instalado desde DP(1)0-0+5\ERP\php-4.4.2-installer.exe
27/01/2006,3:38:20	MySQL 4.1.16 instalado desde C:\Documents and Settings\Administrator\Desktop\mysql-4.1.16-win32\Setup.exe
01/02/2006,19:50:53	Firefox 1.5 instalado desde C:\Documents and Settings\Administrator\My Documents\Firefox Setup 1.5.exe
01/02/2006,19:51:33	BitTorrent instalado desde C:\Documents and Settings\Administrator\My Documents\BitTorrent-4.4.0.exe
01/02/2006,19:57:14	PostgreSQL 8.1.2-1 instalado desde C:\Documents and Settings\Administrator\Desktop\postgresql-8.1.2-1-binaries-no-installer\pgsql\bin\psql.exe
04/02/2006,23:59:27	TCPView instalado desde DP(1)0-0+6\herramientas\Tcpview.exe

Evidencia: fichero del visor de eventos localizado en
 \WINDOWS\system32\config\SecEvent.Evt

Usuarios detectados en el sistema:

Domain	User Name
	Administrator
	Guest
	SUPPORT_388945a0
	Johnatan
	ernesto
	amado
	maick
	lalo
	moni
	maru
	mirna
	katy
	caracheo
	ovejas
	reno
	pili
	zamorano
	mpenelope
	postgres
	verOk

Información extraída con L0phtcrack 5 del fichero contenedor de la SAM: \WINDOWS\system32\config\SAM

En los ficheros de log del servidor Web, se han detectado varios escaneos de Nessus y Nikto. Las direcciones de los escaneos han sido internas dos de ellas (192.168.100.144, 192.168.5.32, y otra más externa (84-18-17-15.usul.arrakis.es [84.18.17.15]). Las internas han sido escaneos de "Nikto", la externa parece haber ha utilizado "Nessus".

Evidencia en "\apache\Apache\logs" ficheros: access.log y error.log

No se han detectado fallos reportados a Securiteam de Buffer Overflow en los programas instalados que tienen puertos TCP/IP expuestos a Internet (MySQL, Apache)

El sistema aparte de servidor de ficheros y dominio se usa para albergar una aplicación Web llamada Web-erp (<http://www.weberp.org/> puede verse una demo de ella en : <http://web-erp.sourceforge.net/web-erp/index.php>)

El administrador tras la instalación de este producto, modifica el fichero de configuración "config.php" y se olvida que ha dejado un fichero .bak de configuración (**que no parece haber sido accedido vía http (access.log)**) (en cualquier caso no le sería útil a un atacante ya que no contiene la contraseña correcta de la BD).

Evidencia en \apache\Apache\htdocs\web-erp\ ficheros: config.php.bak y config.php

Configuración de .bak:

```
$dbType = 'mysql';
$DatabaseName='weberp';
// sql user & password
$dbuser = 'weberp_db_user';
$dbpassword = 'weberp_db_pwd';
```

Configuración Actual:

```
$dbType = 'mysql';
$DatabaseName='weberp';

// sql user & password
$dbuser = 'weberp_us';
$dbpassword = '';
```

Línea del tiempo del sistema

Gracias a que como vemos a continuación **el Administrador habilita la auditoría** en fecha y hora: **26/1/2006 23:12:52**

Evidencia: fichero del visor de eventos
\WINDOWS\system32\config\SecEvent.Evt

```
26/01/2006,23:12:52,Security,Aciertos,Cambio de plan ,612,S-1-5-21-2780117151-1340924567-2512508698-500,COUNTERS,"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: (0x0,0xEFAA)"

26/01/2006,23:12:49,Security,Aciertos,Cambio de plan ,612,S-1-5-21-2780117151-1340924567-2512508698-500,COUNTERS,"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: (0x0,0xEFAA)"

26/01/2006,23:12:42,Security,Aciertos,Cambio de plan ,612,S-1-5-21-2780117151-1340924567-2512508698-500,COUNTERS,"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: (0x0,0xEFAA)"

26/01/2006,23:12:34,Security,Aciertos,Cambio de plan ,612,S-1-5-21-2780117151-1340924567-2512508698-500,COUNTERS,"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: (0x0,0xEFAA)"

```

26/01/2006,23:12:27,Security,Aciertos,Cambio de plan ,612,S-1-5-21-
2780117151-1340924567-2512508698-500,COUNTERS,"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

```

Podemos saber que el usuario: “Johnatan” crea un usuario llamado “ver0k” en fecha y hora: “05/02/2006 – 21:45:30”

```

Evidencia fichero del visor de eventos
\WINDOWS\system32\config\SecEvent.Evt:
05/02/2006,21:45:30,Security,Aciertos,Administración de cuentas
,642,S-1-5-21-2780117151-1340924567-2512508698-1006,COUNTERS,"Cambiada
cuenta de usuario:
-
Nombre de cuenta destino:      ver0k
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:                  -
"
05/02/2006,21:45:30,Security,Aciertos,Administración de cuentas
,626,S-1-5-21-2780117151-1340924567-2512508698-1006,COUNTERS,"Cuenta
de usuario habilitada:
Nombre de cuenta destino:      ver0k
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)
"
05/02/2006,21:45:30,Security,Aciertos,Administración de cuentas
,624,S-1-5-21-2780117151-1340924567-2512508698-1006,COUNTERS,"Cuenta
de usuario creada:
Nombre de cuenta nueva: ver0k
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                    -

```

Ahora necesitamos saber si el usuario “ver0k” es creado por Johnatan voluntariamente por iniciativa propia o no, todo parece indicar que se ha aprovechado la vulnerabilidad “Windows XP/2003/Vista Metafile Escape() SetAbortProc Code Execution”. Para demostrarlo, hemos buscado entre los ficheros y eventos inmediatamente anteriores a la creación del usuario. Y en

los ficheros eliminados y se ha encontrado la evidencia de esta afirmación, en la caché de Navegador del usuario "Johnatan".

Momentos antes (apenas 2 minutos) de la creación del usuario, Johnatan accede a su cuenta de correo de Yahoo, y ve varios correos. A continuación mostramos uno de ellos:

```
\Documents and Settings\Johnatan\Local Settings\Temporary Internet
Files\Content.IE5\0B8EC9X6

\0B8EC9X6\CAU1CDC1.htm
\0B8EC9X6\CAMA58OV.htm

<pre><tt>Johnny:

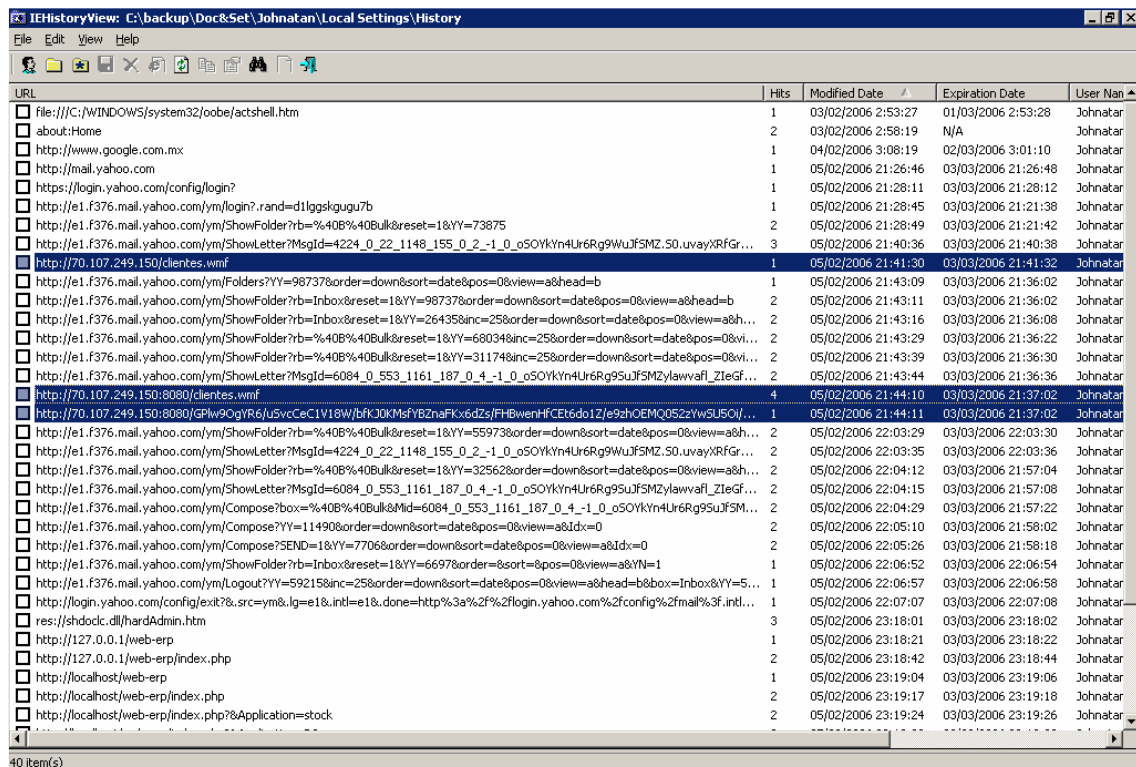
Esta es la liga correcta,

Por favor baja el catalogo que esta en

<a href="http://70.107.249.150:8080/clientes.wmf" target=_blank
onclick="return ShowLinkWarning()"
>http://70.107.249.150:8080/clientes.wmf</a>

Alberto Lopez
Director General
Electronica y Computacion S.A. de C.V.
```

También vemos otro correo que básicamente es igual, salvo por el enlace en el que se le indica a Johnatan que acceda a <http://70.107.249.150/clientes.wmf>



En la imagen se confirma viendo el "Historial" del usuario que Johnatan accede a ambos enlaces, con unos minutos de diferencia, pero es el segundo de ellos (el del puerto 8080) el que produce la descarga en el sistema un fichero llamado "LQ9ClubsIAJKIa2jdYtSFExez4sRyL[2].tiff". Este fichero,

desgraciadamente no está completo, parece que contiene trozos de un fichero creado posteriormente (posiblemente uno de los dos ficheros que más adelante generará el atacante con los datos sustraídos del sistema de datos de web-erp).

```
\Documents and Settings\Johnatan\My Documents\Local Settings\Temporary Internet Files\Content.IE5\0B8EC9X6\LQ9ClubsIAJKIa2jdYtSFExez4sRyL[2].tiff

Language|s:5:"en_GB";AttemptsCounter|i:0;AccessLevel|s:1:"8";CustomerID|s:0:"";UserBranch|s:0:"";Module|s:6:"system";PageSize|s:0:"";UserStockLocation|s:2:"DF";DatabaseName|s:6:"weberp";DefaultPageSize|s:6:"letter";ModulesEnabled|a:9:{i:0;s:1:"1";i:1;s:1:"1";i:2;s:1:"1";i:3;s:1:"1";i:4;s:1:"1";i:5;s:1:"1";i:6;s:1:"1";i:7;s:1:"1";i:8;s:0:"";}UsersRealName|s:26:"Alberto Contreras..."
```

Dado que desde la lectura del correo y creación del TIFF (21h44m11s) hasta la creación del usuario (21h45m30s) transcurre mas de un minuto, podemos descartar que el payload contenido en el TIFF creó el usuario, sino que el TIFF contenía un ataque de tipo shell o reverse shell, que le ha proporcionado al atacante un “cmd” en la máquina local con las credenciales de “Johnatan”. Y posiblemente con unos cuantos simples comandos ha creado el usuario

```
Suposición de los comandos ejecutados en el sistema:

Para crear el usuario en el sistema:
Net user ver0k p@ssw0rd /add (la password es una suposición ya que no se ha intentado su crackeo)

Para obtener los nombres de los grupos del sistema:
net group
(el atacante obtendría el nombre del grupo administrativo del dominio)

Net group "nombre_del_grupo_de_administradores" ver0k /add
```

Por otro lado, el administrador del sistema tiene en su carpeta de “Mis Documentos” las típicas cosas que se envían por correo: fotos, powerpoints (el administrador del sistema casi con seguridad es un hombre), ejecutables y bromas “graciosas” varias, etc.

```
Evidencia: \Documents and Settings\Administrator\My Documents
```

Incluso tiene un troyano en el fichero “explorer.exe” (QLowZones-2.gen) en esa misma carpeta (aunque no hay evidencias de que nadie ejecute el troyano) más información del troyano en: http://vil.nai.com/vil/content/v_128525.htm

Tras la creación del usuario “ver0k” (21:45:30), este se loga por primera vez al sistema en fecha y hora **05/02/2006,21:47:21**

Evidencia: Inicio de sesión en el visor de eventos:

05/02/2006, 21:47:21, Security, Aciertos, Inicio de sesión de la cuenta ,680,S-1-5-21-2780117151-1340924567-2512508698-1024,COUNTERS, Inicio de sesión intentado por: MICROSOFT_AUTHENTICATION_PACKAGE_V1_0
Cuenta de inicio de sesión: ver0k
Estación de trabajo de origen: COUNTERS
Código de error: 0x0

El usuario al logarse al sistema ejecuta diferentes programas (consulta ficheros de texto, lanza el Messenger, el Explorer incluso lanza alguna conexión a la base de datos y se dedica a curiosear por los ficheros de bromas del administrador y por ficheros de otros usuarios del sistema.

Podemos ver algunos ficheros de los que ha consultado

Evidencia: Usando el explorador de archivos, viendo los ficheros creados / modificados desde el 05/02/2006 21:47:21)

```
Evidencia completa en \Documents and Settings\ver0k\Recent
05/02/2006 21:49 817 AccountGroups.php.lnk
05/02/2006 21:50 780 config.php.lnk
05/02/2006 21:50 613 web-erp.lnk
05/02/2006 22:05 415 clientes.txt.lnk
05/02/2006 22:06 396 users.txt.lnk
05/02/2006 22:06 293 Local Disk (C).lnk
05/02/2006 22:16 1.026 overlay_5_2006020110004.jpg.lnk
05/02/2006 22:16 1.026 overlay_6_2005112211035.jpg.lnk
05/02/2006 22:16 1.026 overlay_6_2006020110004.jpg.lnk
05/02/2006 22:16 1.026 overlay_7_2006020110005.jpg.lnk
05/02/2006 22:16 956 overlay_8.jpg.lnk
05/02/2006 22:17 1.026 overlay_8_2006020110005.jpg.lnk
05/02/2006 22:17 1.026 overlay_9_2006020110006.jpg.lnk
05/02/2006 22:17 1.111
overlay_por_2006020107034_20060201190204.jpg
.lnk
05/02/2006 22:17 1.111
overlay_por_2006020110007_20060201224249.jpg
.lnk
05/02/2006 22:17 722 imagenes.lnk
05/02/2006 22:18 863 a017.jpg.lnk
05/02/2006 22:18 1.156 nm06032003.jpeg.lnk
05/02/2006 22:18 1.156 nm06042003.jpeg.lnk
05/02/2006 22:18 1.156 nm06052003.jpeg.lnk
05/02/2006 22:19 1.156 nm06082003.jpeg.lnk
05/02/2006 22:19 884 modelos.lnk
05/02/2006 22:23 1.116 Boletin11.doc.lnk
05/02/2006 22:26 790 concha.doc.lnk
05/02/2006 22:26 599 Israel Robledo Gonzáles's
Documents.lnk
05/02/2006 22:40 942 30SEP_bolecart-book.doc.lnk
05/02/2006 22:40 897 formulario.doc.lnk
05/02/2006 22:41 927 ÍNDICE DOCTORADO.doc.lnk
05/02/2006 22:41 947 Índice Pormenorizado.doc.lnk
05/02/2006 22:41 868 Notas.doc.lnk
05/02/2006 22:47 897 RRGEPNotas.doc.lnk
05/02/2006 22:47 912 RRGEPPortadas.doc.lnk
05/02/2006 22:49 657 Sti_Trace.log.lnk
05/02/2006 22:49 473 maick.lnk
05/02/2006 22:53 619 ABOUT_APACHE.TXT.lnk
05/02/2006 22:53 450 Apache.lnk
05/02/2006 22:58 875 examen.gif.lnk
05/02/2006 22:58 666 Administrator's Documents.lnk
```

Hay evidencia de que por lo menos el usuario "ver0k" lee los siguientes ficheros:

\\apache\Apache\htdocs\web-erp\AccountGroups.php (21:49)

\\apache\Apache\htdocs\web-erp\config.php (21:50)

Tras la consulta de "Config.php" vemos en el visor de eventos:

```
05/02/2006, 21:51:16, Security, Aciertos, Seguimiento detallado , 592, S-1-5-21-2780117151-1340924567-2512508698-1024, COUNTERS, "Se ha creado un proceso:
  Id. de proceso:          392
  Nombre de proceso 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)
```

Y efectivamente se crean los ficheros horas de configuración de MySQL a las **21:51 horas:**

\\Documents and Settings\ver0k\Application Data\MySQL

mysqlx_common_options.xml

mysqlx_user_connections.xml

El segundo fichero contiene la información de conexión:

```
<?xml version="1.0" ?>
- <user_connections>
  <last_connection>0</last_connection>
  <password_storage_type>1</password_storage_type>
- <user_connection>
  <connection_name />
  <username>weberp_us</username>
  <hostname>127.0.0.1</hostname>
  <port>3306</port>
  <schema />
- <advanced_options>
  <advanced_option>COMPRESS=Yes</advanced_option>
  <advanced_option>ANSI_QUOTES=Yes</advanced_option>
</advanced_options>
  <storage_path />
  <notes />
  <connection_type>0</connection_type>
  <storage_type>2</storage_type>
  <password />
</user_connection>
</user_connections>
```

Aprovechando esta conexión de base de datos a las **22:05** genera 2 ficheros en C:\ llamados:

Clientes.txt

Users.txt

La creación de estos ficheros hace que accidentalmente se destruya el fichero TIFF antes mencionado. Como podemos ver a continuación al tratar de recuperarlo no contiene la información esperada:

```
Language|s:5:"en_GB";AttemptsCounter|i:0;AccessLevel|s:1:"8";CustomerID|s:0:"";UserBranch|s:0:"";Module|s:6:"system";PageSize|s:0:"";UserStorageLocation|s:2:"DF";DatabaseName|s:6:"weberp";DefaultPageSize|s:6:"letter";ModulesEnabled|a:9:{i:0;s:1:"1";i:1;s:1:"1";i:2;s:1:"1";i:3;s:1:"1";i:4;s:1:"1";i:5;s:1:"1";i:6;s:1:"1";i:7;s:1:"1";i:8;s:0:"";}UsersRe
```

```

alName|s:26:"Alberto
Contreras
Zacarías";Theme|s:5:"fresh";UserID|s:10:"acontreras";DisplayRecordsMax
|s:2:"50";AllowedPageSecurityTokens|a:15:{i:0;s:1:"1";i:1;s:1:"2";i:2;
s:1:"3";i:3;s:1:"4";i:4;s:1:"5";i:5;s:1:"6";i:6;s:1:"7";i:7;s:1:"8";i:
8;s:1:"9";i:9;s:2:"10";i:10;s:2:"11";i:11;s:2:"12";i:12;s:2:"13";i:13;
s:2:"14";i:14;s:2:"15";}AllowSalesOfZeroCostItems|d:0;AutoDebtorNo|d:0
;CheckCreditLimits|d:0;Check_Price_Charged_vs_Order_Price|d:1;Check_Qt
y_Charged_vs_Del_Qty|d:1;CountryOfOperation|s:3:"MXP";CreditingControl
ledItems_MustExist|d:0;DB_Maintenance|d:1;DB_Maintenance_LastRun|s:10:
"2006-02-
05";DefaultBlindPackNote|d:1;DefaultCreditLimit|d:1000;DefaultDateForm
at|s:5:"d/m/Y";DefaultDisplayRecordsMax|d:50;DefaultPriceList|s:2:"DE"
;DefaultTaxCategory|d:1;DefaultTheme|s:5:"fresh";Default_Shipper|d:1;D
ispatchCutOffTime|d:14;DoFreightCalc|d:0;EDIHeaderMsgId|s:15:"D:01B:UN
:EAN010";EDIReference|s:6:"WEBERP";EDI_Incoming_Orders|s:36:"companies
/weberp/EDI_Incoming_Orders";EDI_MsgPending|s:31:"companies/weberp/EDI
_MsgPending";EDI_MsgSent|s:25:"companies/weberp/EDI_Sent";FreightCharg
eAppliesIfLessThan|d:1000;FreightTaxCategory|d:1;HTTPS_Only|d:0;MaxIma
geSize|d:300;NumberOfPeriodsOfStockUsage|d:12;OverChargeProportion|d:3
0;OverReceiveProportion|d:20;PackNoteFormat|d:1;PageLength|d:48;part_p
ics_dir|s:26:"companies/weberp/part_pics";PastDueDays1|d:30;PastDueDay
s2|d:60;PO_AllowSameItemMultipleTimes|d:1;QuickEntries|d:10;RadioBeaco
nFileCounter|s:29:"/home/RadioBeacon/FileCounter";RadioBeaconFTP_user_
name|s:32:"RadioBeacon ftp server user
name";RadioBeaconHomeDir|s:17:"/home/RadioBeacon";RadioBeaconStockLoca
tion|s:2:"BL";RadioBraconFTP_server|s:11:"192.168.2.2";RadioBraconFil
ePrefix|s:5:"ORDXX";RadionBeaconFTP_user_pass|s:39:"Radio Beacon
remote ftp server
password";reports_dir|s:24:"companies/weberp/reports";RomalpaClause|s:
80:"Ownership will not pass to the buyer until the goods have been
paid for in
full.";Show_Settled_LastMonth|d:1;SO_AllowSameItemMultipleTimes|d:1;Ta
xAuthorityReferenceName|s:20:"Referencias
impuesto";YearEnd|d:11;CompanyDefaultsLoaded|b:1;CompanyRecord|a:48:{i
:0;s:38:"Electrónica y Computación S.A. de
C.V.";s:7:"coyname";s:38:"Electrónica y Computación S.A. de
C.V.";i:1;s:15:"not entered yet";s:5:"gstno";s:15:"not entered
yet";i:2;s:15:"Eje central 234";s:10:"regoffice1";s:15:"Eje central
234";i:3;s:11:"Col. Centro";s:10:"regoffice2";s:11:"Col.
Centro";i:4;s:9:"México DF";s:10:"regoffice3";s:9:"México
DF";i:5;s:6:"México";s:10:"regoffice4";s:6:"México";i:6;s:0:"";s:10:"r
egoffice5";s:0:"";i:7;s:0:"";s:10:"regoffice6";s:0:"";i:8;s:0:"";s:9:"
telephone";s:0:"";i:9;s:0:"";s:3:"fax";s:0:"";i:10;s:15:"admin@eycsa.c
om";s:5:"email";s:15:"admin@eycsa.com";i:11;s:3:"MXP";s:15:"currencyde
fault";s:3:"MXP";i:12;s:4:"1100";s:10:"debtorsact";s:4:"1100";i:13;s:4
:"4900";s:14:"pytdiscontact";s:4:"4900";i:14;s:4:"2100";s:12:"credito
rsact";s:4:"2100";i:15;s:4:"2400";s:10:"payrollact";s:4:"2400";i:16;s:
4:"2150";s:6:"grnact";s:4:"2150";i:17;s:4:"4200";s:15:"exchangediffact
";s:4:"4200";i:18;s:4:"5200";s:24:"purchasesexchangediffact";s:4:"5200
";i:19;s:4:"3500";s:16:"retainedearnings";s:4:"3500";i:20;s:4:"5600";s
:10:"freightact";s:4:"5600";i:21;s:1:"1";s:14:"gllink_debtors";s:1:"1"
;i:22;s:1:"1";s:16:"gllink_creditors";s:1:"1";i:23;s:1:"1";s:12:"gllin
k_stock";s:1:"1";}...
9 0 obj
<< /Length 10 0 R
/Filter /FlateDecode
...

```

Lo dicho se confirma además mirando el Historial del usuario “ver0k”:

URL	Hits	Modified Date	Expiration Date	User Name
about:Home	2	05/02/2006 21:47:41	N/A	ver0k
file:///C:/apache/Apache/htdocs/web-erp/AccountGroups.php	1	05/02/2006 21:49:51	03/03/2006 21:42:44	ver0k
file:///C:/apache/Apache/htdocs/web-erp/config.php	1	05/02/2006 21:50:02	03/03/2006 21:42:54	ver0k
http://messenger.msn.com/redirs/FIRST_TIME_EX.asp?GeoID=000000a6&Pclid=0c0a8&CLCID=080a8&Country=MX&BrandID=msmsgs8...	1	05/02/2006 22:04:20	03/03/2006 21:57:12	ver0k
http://g.msn.com/5mees_mx/1162	1	05/02/2006 22:04:20	03/03/2006 21:57:12	ver0k
http://g.msn.com/5meen_us/153?GeoID=000000a6&Pclid=0c0a8&CLCID=080a8&Country=MX&BrandID=msmsgs8&Build=7.5.0311&OS...	1	05/02/2006 22:04:21	03/03/2006 21:57:14	ver0k
http://image.msn.com/messenger/rononce/v75/mosaic.aspx?locale=es-MX	2	05/02/2006 22:04:38	03/03/2006 21:57:30	ver0k
file:///C:/clientes.txt	2	05/02/2006 22:05:56	03/03/2006 21:58:48	ver0k
file:///C:/users.txt	1	05/02/2006 22:06:37	03/03/2006 22:06:38	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/1_2005121110036.jpg	1	05/02/2006 22:12:36	03/03/2006 22:05:28	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/2_2005121110036.jpg	1	05/02/2006 22:12:52	03/03/2006 22:05:44	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/3_2005121110036.jpg	1	05/02/2006 22:13:01	03/03/2006 22:05:52	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/9.jpg	1	05/02/2006 22:13:07	03/03/2006 22:06:00	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_1_2005112211034.jpg	1	05/02/2006 22:13:15	03/03/2006 22:06:06	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_1_2006020107030.jpg	1	05/02/2006 22:13:20	03/03/2006 22:06:12	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_1_2006020110003.jpg	1	05/02/2006 22:13:25	03/03/2006 22:13:26	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_2_2005112211034.jpg	1	05/02/2006 22:13:29	03/03/2006 22:13:30	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_2_2006020110004.jpg	1	05/02/2006 22:13:36	03/03/2006 22:13:38	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_3_2005112211034.jpg	1	05/02/2006 22:13:42	03/03/2006 22:13:44	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_3_2006020107031.jpg	1	05/02/2006 22:13:48	03/03/2006 22:13:50	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_4_2005112211035.jpg	1	05/02/2006 22:13:54	03/03/2006 22:13:56	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_4_2006020110004.jpg	1	05/02/2006 22:14:02	03/03/2006 22:14:04	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_5.jpg	1	05/02/2006 22:14:08	03/03/2006 22:14:10	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_5_2005112211035.jpg	1	05/02/2006 22:16:27	03/03/2006 22:16:28	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_5_2006020110004.jpg	1	05/02/2006 22:16:32	03/03/2006 22:16:34	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_6_2005112211035.jpg	1	05/02/2006 22:16:40	03/03/2006 22:16:42	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_6_2006020110004.jpg	1	05/02/2006 22:16:46	03/03/2006 22:16:48	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_7_2006020110005.jpg	1	05/02/2006 22:16:51	03/03/2006 22:16:52	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_8.jpg	1	05/02/2006 22:16:55	03/03/2006 22:16:56	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_8_2006020110005.jpg	1	05/02/2006 22:17:06	03/03/2006 22:17:08	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_9_2006020110006.jpg	1	05/02/2006 22:17:11	03/03/2006 22:17:12	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_por_2006020107034_20060201190204.jpg	1	05/02/2006 22:17:22	03/03/2006 22:17:24	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_por_2006020110007_20060201224249.jpg	1	05/02/2006 22:17:31	03/03/2006 22:17:32	ver0k

Como vemos en la anterior imagen, a las 22:05:56 abre el fichero de clientes y a las 22:06:37 el de usuarios, y posiblemente selecciona todo el texto y lo copia (de esta forma se lo lleva a su máquina local)

Luego los borra (ya que no han sido encontrados en el disco)

Tras esto, como acabamos de ver en el historial y como confirmamos viendo los documentos recientes del usuario "ver0k". Este curioso se por los ficheros del administrador (fotos y videos)

Evidencia:	Fecha	Hora	Tamaño	Nombre
\Documents and Settings\ver0k\Recent				
05/02/2006	22:16	1.026	overlay_5_2006020110004.jpg.lnk	
05/02/2006	22:16	1.026	overlay_6_2005112211035.jpg.lnk	
05/02/2006	22:16	1.026	overlay_6_2006020110004.jpg.lnk	
05/02/2006	22:16	1.026	overlay_7_2006020110005.jpg.lnk	
05/02/2006	22:16	956	overlay_8.jpg.lnk	
05/02/2006	22:17	1.026	overlay_8_2006020110005.jpg.lnk	
05/02/2006	22:17	1.026	overlay_9_2006020110006.jpg.lnk	
05/02/2006	22:17		1.111	
overlay_por_2006020107034_20060201190204.jpg				
.lnk				
05/02/2006	22:17		1.111	
overlay_por_2006020110007_20060201224249.jpg				
.lnk				
05/02/2006	22:17	722	imagenes.lnk	
05/02/2006	22:18	863	a017.jpg.lnk	
05/02/2006	22:18	1.156	nm06032003.jpeg.lnk	
05/02/2006	22:18	1.156	nm06042003.jpeg.lnk	
05/02/2006	22:18	1.156	nm06052003.jpeg.lnk	
05/02/2006	22:19	1.156	nm06082003.jpeg.lnk	
05/02/2006	22:19	884	modelos.lnk	

Después de las fotos, también ejecuta algunos programas de "Bromas" Macromediaflash

Evidencia de ejecución de programas:

```

05/02/2006,22:14:26,Security,Aciertos,Seguimiento detallado ,592,S-1-5-21-2780117151-1340924567-2512508698-1024,COUNTERS,"Se ha creado un proceso:
  Id. de proceso:                3744
  Nombre de archivo de imagen:   C:\Program Files\Windows Media Player\wmplayer.exe
  Id. de proceso creador:        720
  Nombre de usuario:              ver0k
  Dominio:                        COUNTERS
  Id. de inicio de sesión:       (0x0,0x3F4E19)
"
"
05/02/2006,22:28:37,Security,Aciertos,Seguimiento detallado ,592,S-1-5-21-2780117151-1340924567-2512508698-1024,COUNTERS,"Se ha creado un proceso:
  Id. de proceso:                2796
  Nombre de archivo de imagen:   C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\fiesta en el antro.exe
  Id. de proceso creador:        720
  Nombre de usuario:              ver0k
  Dominio:                        COUNTERS
  Id. de inicio de sesión:       (0x0,0x3F4E19)
"
"
05/02/2006,22:30:19,Security,Aciertos,Seguimiento detallado ,593,S-1-5-21-2780117151-1340924567-2512508698-1024,COUNTERS,"Ha terminado un proceso:
  Id. de proceso:                3160
  Nombre de archivo de imagen:   C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\mordida.exe
  Nombre de usuario:              ver0k
  Dominio:                        COUNTERS
  Id. de inicio de sesión:       (0x0,0x3F4E19)

```

Luego abre el Explorer (posiblemente abierto de forma automática al finalizar la ejecución de algún programa de los de Macromedia Flash):

```

05/02/2006,22:30:45,Security,Aciertos,Seguimiento detallado ,592,S-1-5-21-2780117151-1340924567-2512508698-1024,COUNTERS,"Se ha creado un proceso:
  Id. de proceso:                3672
  Nombre de archivo de imagen:   C:\Program Files\Internet Explorer\IEXPLORE.EXE
  Id. de proceso creador:        3688
  Nombre de usuario:              ver0k
  Dominio:                        COUNTERS
  Id. de inicio de sesión:       (0x0,0x3F4E19)

```

Y continúa viendo los ficheros del administrador:

```

05/02/2006,22:32:03,Security,Aciertos,Seguimiento detallado ,593,S-1-5-21-2780117151-1340924567-2512508698-1024,COUNTERS,"Ha terminado un proceso:
  Id. de proceso:                3736
  Nombre de archivo de imagen:   C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\no existieras.exe
  Nombre de usuario:              ver0k
  Dominio:                        COUNTERS
  Id. de inicio de sesión:       (0x0,0x3F4E19)

```

Tras ver muchos de los ejecutables que no creemos sean interesantes para el análisis ya que el único interesante sería el con el troyano "Explorer.exe" y este no es abierto. El usuario curioseaba también archivos:

"C:\Documents and Settings\reno\My Documents\Boletin11.doc"
 "C:\Documents and Settings\reno\My Documents\concha.doc"
 Y en general los archivos personales de Israel Robledo Gonzáles:
 "C:\Documents and Settings\reno\My Documents"

Evidencia:	\Documents and Settings\ver0k\Recent
05/02/2006 22:23	1.116 Boletin11.doc.lnk
05/02/2006 22:26	790 concha.doc.lnk
05/02/2006 22:26	599 Israel Robledo Gonzáles's Documents.lnk
05/02/2006 22:40	942 30SEP_bolecart-book.doc.lnk
05/02/2006 22:40	897 formulario.doc.lnk
05/02/2006 22:41	927 ÍNDICE DOCTORADO.doc.lnk
05/02/2006 22:41	947 Indice Pormenorizado.doc.lnk
05/02/2006 22:41	868 Notas.doc.lnk
05/02/2006 22:47	897 RRGEPPortadas.doc.lnk
05/02/2006 22:47	912 RRGEPPortadas.doc.lnk
05/02/2006 22:49	657 Sti_Trace.log.lnk
05/02/2006 22:49	473 maick.lnk
05/02/2006 22:53	619 ABOUT_APACHE.TXT.lnk
05/02/2006 22:53	450 Apache.lnk
05/02/2006 22:58	875 examen.gif.lnk
05/02/2006 22:58	666 Administrator's Documents.lnk

Se confirma mirando los últimos accesos en el historial del usuario "ver0k":

URL	Hits	Modified Date	Expiration Date	User Name
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_4_2005112211035.jpg	1	05/02/2006 22:13:54	03/03/2006 22:13:56	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_4_2006020110004.jpg	1	05/02/2006 22:14:02	03/03/2006 22:14:04	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_5.jpg	1	05/02/2006 22:14:08	03/03/2006 22:14:10	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_5_2005112211035.jpg	1	05/02/2006 22:16:27	03/03/2006 22:16:28	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_5_2006020110004.jpg	1	05/02/2006 22:16:32	03/03/2006 22:16:34	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_6_2005112211035.jpg	1	05/02/2006 22:16:40	03/03/2006 22:16:42	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_6_2006020110004.jpg	1	05/02/2006 22:16:46	03/03/2006 22:16:48	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_7_2006020110005.jpg	1	05/02/2006 22:16:51	03/03/2006 22:16:52	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_8.jpg	1	05/02/2006 22:16:55	03/03/2006 22:16:56	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_8_2006020110005.jpg	1	05/02/2006 22:17:06	03/03/2006 22:17:08	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_9_2006020110006.jpg	1	05/02/2006 22:17:11	03/03/2006 22:17:12	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_por_2006020107034_20060201190204.jpg	1	05/02/2006 22:17:22	03/03/2006 22:17:24	ver0k
file:///C:/Documents%20and%20Settings/Johnatan/My%20Documents/imagenes/overlay_por_2006020110007_20060201224249.jpg	1	05/02/2006 22:17:31	03/03/2006 22:17:32	ver0k
file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/a017.jpg	1	05/02/2006 22:18:05	03/03/2006 22:18:06	ver0k
file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/My%20Videos/modelos/nm06032003.jpeg	1	05/02/2006 22:18:27	03/03/2006 22:11:18	ver0k
file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/My%20Videos/modelos/nm06042003.jpeg	1	05/02/2006 22:18:43	03/03/2006 22:11:34	ver0k
file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/My%20Videos/modelos/nm06052003.jpeg	1	05/02/2006 22:18:55	03/03/2006 22:11:46	ver0k
file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/My%20Videos/modelos/nm06082003.jpeg	1	05/02/2006 22:19:05	03/03/2006 22:11:58	ver0k
file:///C:/Documents%20and%20Settings/reno/My%20Documents/Boletin11.doc	1	05/02/2006 22:23:47	03/03/2006 22:23:48	ver0k
file:///C:/Documents%20and%20Settings/reno/My%20Documents/concha.doc	1	05/02/2006 22:26:39	03/03/2006 22:19:32	ver0k
http://www.huevocartoon.com/animaciones/index.asp	1	05/02/2006 22:30:50	03/03/2006 22:30:52	ver0k
http://www.huevocartoon.com/home_contry.asp	2	05/02/2006 22:30:53	03/03/2006 22:30:54	ver0k
file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/30SEP_bolecart-book.doc	2	05/02/2006 22:40:16	03/03/2006 22:33:08	ver0k
file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/formulario.doc	1	05/02/2006 22:40:45	03/03/2006 22:33:38	ver0k
file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/Indice%20DOCTORADO.doc	1	05/02/2006 22:41:06	03/03/2006 22:33:58	ver0k
file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/Indice%20Pormenorizado.doc	2	05/02/2006 22:41:16	03/03/2006 22:34:08	ver0k
file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/Notas.doc	1	05/02/2006 22:41:23	03/03/2006 22:34:16	ver0k
file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/RRGEPNotas.doc	1	05/02/2006 22:47:24	03/03/2006 22:40:16	ver0k
file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/RRGEPPortadas.doc	1	05/02/2006 22:47:42	03/03/2006 22:40:34	ver0k
file:///C:/Documents%20and%20Settings/maick/Sti_Trace.log	1	05/02/2006 22:49:52	03/03/2006 22:49:54	ver0k
file:///C:/apache/Apache/ABOUT_APACHE.TXT	1	05/02/2006 22:53:46	03/03/2006 22:53:48	ver0k
file:///C:/Documents%20and%20Settings/Administrator/My%20Documents/examen.gif	1	05/02/2006 22:58:56	03/03/2006 22:58:58	ver0k
http://rad.msn.com/ADSAdClient31.dll?GetAd?PG=IMSMYS75C=HF?ID=000600094d02e8a	4	05/02/2006 22:59:32	03/03/2006 22:59:34	ver0k

Finalmente, se desconecta (bruscamente) la sesión remota desde "LUFERFU" en 70.107.249.155:

05/02/2006,23:00:10,Security,Aciertos,Inicio/cierre de sesión ,683,NT AUTHORITY\SYSTEM,COUNTERS,"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"

En el visor de eventos puede verse finalmente como a partir de las 23:21:01 Jonathan usando un CD con herramientas salva la imagen del disco y comprueba la integridad del sistema (D:\Kit_de_respuesta\...)

Además en la caché también de Johnatan se ha localizado el fichero:
 \Johnatan\Local Settings\Temporary Internet
 Files\Content.IE5\0B8EC9X6\0B8EC9X6\WWW_Users[1].htm
 Con fecha: lunes, 06 de febrero de 2006, 23:19:38
 Vemos la lista de usuarios del sistema ERP
 (Johnatan consulta la lista de usuarios para ver si se ha creado algún usuario en el sistema web-erp)

Electrónica y Computación S.A. de C.V.:									1. Main Menu 2. Select Customer 3. Select Item 4. Select Supplier 8. Manual 0 Logout	
User Maintenance										
User Login	Full Name	Telephone	Email	Custo mer Code	Bran ch Cod e	Last Visit	Security Group	Report Size		
acontreras	Alberto Contreras Zacarías	67434898	acontreras@gmail.com			05/02/2006	System Administrator	letter	Edit	Delete
admin	Admin.					//	System Administrator	A4	Edit	Delete
amed	Antonio Medina Ocaña	61423075	anmeo@msn.com			03/02/2006	Inventario	letter	Edit	Delete
amirac	Astrid Miranda Acuña	63300459	asmaq@latinmail.com			//	Secretaria	letter	Edit	Delete
andre	Andrea Escalera Nava	56850085	andre@terra.com.mx			//	Gerente de Recursos Humanos	letter	Edit	Delete
carsel	Carmen Serrano Luna	75963175	carmser@yahoo.com.mx			//	Compras	letter	Edit	Delete
chtorret	Chema Torret	55669843	chtorret@hotmail.com			03/02/2006	Compras	letter	Edit	Delete
dizav	Diego Zárate Vite	67963301	diegz@yahoo.com			//	Ventas	letter	Edit	Delete
eduajt	Eduardo Jiménez Tapia	96542357	eduardj@terra.com.mx			03/02/2006	Ventas	letter	Edit	Delete
egavilan	Ernesto	889876432	egavila@			//	System	letter	Edit	Delete

	Gavilán	4	yahoo.com.mx				Administrador		it	te
gabsa	Gabriela Sandoval Portillo	52983477	gabsa@at.net.mx			//	Inventario	letter	Edit	Delete
gruvalcaba	Gumaro Ruvalcaba	87593456	gumru@hotmail.com			03/02/2006	Inventario	letter	Edit	Delete
Jehern	Jesús Hernandez Cuevas	52487974	jesush@hotmail.com			//	Inventario	letter	Edit	Delete
juma	Juan Morales Fierro	56189455	jmorales@msn.com			//	Bancos	legal	Edit	Delete
ladelga	Luis Ignacio Aguiñaga Delgado	63459785	luia@gmail.com			03/02/2006	Ventas	letter_landscap	Edit	Delete
majogar	María José García Rubio	54869302	may@gmail.com			03/02/2006	Inventario	legal	Edit	Delete
mamuria	Miguel Angel Muria Torres	74663221	mamt@prodigy.net.mx			03/02/2006	Inventario	letter	Edit	Delete
maubar	Mauricio Barrios Santiago	54789632	maubao@msn.com			03/02/2006	Inventario	letter	Edit	Delete
mavep	Mayra Velázquez Prieto	58759689	mavp@prodigy.net.mx			03/02/2006	Inventario	letter	Edit	Delete
ncanes	Napoleón Canes	55779834	ncanes@yahoo.com			05/02/2006	Gerente de Compras y Abatecimiento	letter	Edit	Delete
rodid	Rodrigo Ibarra Díaz	53380498	ribarrad@latinmail.com			03/02/2006	System Administrator	letter	Edit	Delete
roxar	Roxana Aguilar de la Riva	45987166	roxar@msn.com			02/02/2006	System Administrator	letter	Edit	Delete
sarnua	Sara Núñez Aldana	54789112	sarnu@gmail.com			//	Compras	legal	Edit	Delete

Finalmente al cerrar el sistema se cierra por completo su sesión y sus programas abiertos

```
06/02/2006,0:44:12,Security,Aciertos,Inicio/cierre de sesión ,538,S-1-5-21-2780117151-1340924567-2512508698-1024,COUNTERS,"Cierre de sesión de usuario:
Nombre de usuario:      ver0k
Dominio:                COUNTERS
Id. de inicio de sesión:      (0x0,0x3F4E19)
Tipo de inicio de sesión:    10
"

06/02/2006,0:44:17,SECURITY,Aciertos,Suceso del sistema ,513,No disponible,COUNTERS,Windows está apagándose. Todas las sesiones iniciadas finalizarán con este apagado.
```

Alcance de la intrusión

¿El sistema ha sido comprometido?

Si, se ha accedido al sistema de forma remota con un usuario llamado "ver0k" creado sin el consentimiento del administrador.

¿Quién (desde dónde) se realizó el ataque? y ¿Cómo se realizó el ataque?

Las pruebas de la identidad del individuo que ha realizado el ataque apuntan inicialmente a;

Alberto Lopez
Director General
Electronica y Computacion S.A. de C.V.

O lo que también es posible, alguien haciéndose pasar por él desde la dirección de correo: alopez@eycsa.com.mx mandó un mensaje de correo electrónico a Jonathan a la dirección de correo de Yahoo: jonathan.tezca@yahoo.com

El mensaje de correo enviado con fecha Sun, 5 Feb 2006 14:42:47 -0600 (CST) contenía:

Johnny:

Esta es la liga correcta,

Por favor baja el catalogo que esta en

<http://70.107.249.150:8080/clientes.wmf>

Alberto Lopez
Director General
Electronica y Computacion S.A. de C.V.

Para realizar el ataque se utilizó un servidor Web en la dirección:

70.107.249.150 (en el puerto 8080) para alojar el fichero WMF
(static-70-107-249-150.ny325.east.verizon.net)

Y desde

70.107.249.155 se accedió al sistema el día
05/02/2006 a las 21:47:21 hasta las 23:00:10
(static-70-107-249-155.ny325.east.verizon.net)

Podemos intentar hacer una primera aproximación de dónde se encuentra la IP
Utilizando: (<http://www.sidebit.com/ProjectLocateIP.php>):

VERSION: 1.0
TARGET: 70.107.249.155
NAME: RESERVED-7
NUMBER: 70.0.0.0 - 79.255.255.255
CITY: MARINA DEL REY
STATE: CALIFORNIA
COUNTRY: US
LAT: 33.98
LONG: -118.45
LAT_LONG_GRAN: City
LAST_UPDATED: 07-Aug-2002
NIC: ARIN
LOOKUP_TYPE: Block Allocation
RATING:
DOMAIN_GUESS: iana.org
STATUS: OK

Pero para comprobar a ciencia cierta el culpable sería necesario solicitarle al ISP quien tenía la ip 70.107.249.155 el día y hora: Desde 05/02/2006, 21:47:21 a 23:00:10 del mismo día.

A continuación mostramos la información del dominio para ponerse en contacto con los Administradores del ISP:

Registrant:

Verizon Trademark Services LLC (DOM-382081)
1320 North Court House Road
Arlington VA 22201
US

Domain Name: verizon.net

Registrar Name: Markmonitor.com
Registrar Whois: whois.markmonitor.com
Registrar Homepage: <http://www.markmonitor.com>

Administrative Contact:

Christian R. Andersen (NIC-14209143) Verizon
600 Hidden Ridge Drive HQE03H14
Irving TX 75038
US
christian.andersen@verizon.com
+1.9727187621
Fax- -

Technical Contact, Zone Contact:

Verizon GNI - IP System Operations (NIC-14209152) Verizon GNI
- IP System Operations
1880 CAMPUS COMMONS DR
RESTON VA 20191-1512
US
dns@GNILINK.NET
+1.7032954206

Fax- -

Created on.....: 1999-Jul-06.
Expires on.....: 2006-Jul-06.
Record last updated on..: 2005-Jun-04 04:33:13.

Domain servers in listed order:

NS1.BELLATLANTIC.NET
NS2.BELLATLANTIC.NET
NS2.VERIZON.NET
NS4.VERIZON.NET

Información extraída de : <http://www.whois.net/whois.cgi2?d=verizon.net>

Es muy probable que el atacante haya utilizado Metasploit (<http://www.metasploit.org/>) un framework que automatiza diferentes ataques para que usuarios con pocos conocimientos técnicos sean capaces de realizar ataques de gran nivel (Buffers Overflow para conseguir Reverse Shell, DLL inyecting, creación de usuarios en el sistema remoto, etc..). Lo que es seguro es que ha aprovechado la vulnerabilidad "Metafire Escape() SetAbortProc Code Execution".

Más información del bug en: <http://www.securityfocus.com/bid/16074>

Puede verse una demo de cómo explotarlo en:
<http://www.irongeek.com/i.php?page=videos/metasploitwmf>

A pesar de que el administrador tuviera una política de realización de las actualizaciones de Microsoft el parche fue liberado posteriormente al ataque (<http://www.microsoft.com/downloads/details.aspx?familyid=1584AAE0-51CE-47D6-9A03-DB5B9077F1F2&displaylang=en>)

¿Qué hizo el atacante en el sistema comprometido?

En primer lugar miró la configuración de web-erp como hemos visto anteriormente, tras esto, obtuvo el usuario y contraseña de conexión a la base de datos.

Se conectó a la base de datos y obtuvo la lista de clientes y usuarios, se la copió y la borró.

Tras esto estuvo curioseando por los ficheros del administrador (videos, fotos y algún ejecutable de tipo Macromedia flash con bromas típicas que se envían por correo) luego, para finalizar estuvo mirando los documentos de algunos de los usuarios del sistema (como hemos visto con detalle anteriormente en el punto "Línea del Tiempo del sistema").