

# Informe Técnico

## Reto Análisis Forense UNAM CERT /RED IRIS

“¿A quién va usted a creer, a mí o a sus propios ojos?”  
Groucho Marx, Actor estadounidense. 1890-1977

“Si tu intención es describir la verdad, hazlo con sencillez, y la elegancia déjasela al sastre.”  
Albert Einstein, Científico alemán, nacionalizado estadounidense. 1879-1955

# Índice

---

Audiencia.....	3
Introducción.....	3
Montaje del sistema espejo para el análisis.....	4
Análisis del sistema de ficheros.....	7
Recogida de datos de la máquina.....	8
Tipos de Logon en Windows.....	11
Ficheros Log.....	11
Perfiles de usuario en Windows.....	16
La papelera de Reciclaje.....	18
Breve resumen de pistas.....	20
Index.dat e Internet Explorer.....	22
Localizando direcciones IP.....	26
El agujero de Seguridad.....	28
Resumen final.....	31
Recomendaciones.....	34
Conclusión Final.....	36
Referencias.....	36
Curiosidades.....	37

---

## Audiencia

---

Este documento mantendrá un estilo informal pero sin desprestigiar el aspecto técnico del mismo, para facilitar y hacer más amena su lectura, evitando de esta manera el estilo correcto y serio que redactaría si fuese para un cliente. Se pretende así que este documento llegue a mucha más gente interesada en la informática forense, y puedan aprender a la vez que se divierten. Este documento describirá de manera detallada todos los aspectos técnicos, comandos y operaciones que se utilizaron para realizar el informe, por lo que los usuarios con mayor conocimiento podrán pasar por alto dichas explicaciones, y centrarse más en el aspecto práctico. He detallado paso por paso todas las acciones que he realizado en el sistema, porque aunque el sistema operativo Windows es bien conocido por todos, es de código propietario. Eso me ha dificultado a la hora de "visualizar" distintos tipos de datos y archivos, ya que algunos archivos estaban "codificados" para el ojo humano. Por otra parte me ha resultado bastante fácil conseguir información sobre aspectos técnicos del sistema operativo, gracias a la abundante información, manuales y boletines de seguridad encontrados en la amplia base de datos que posee Microsoft. En concreto de [Microsoft Knowledge Base](#). Las explicaciones detalladas servirán para que no nos "perdamos" ningún detalle en el análisis.

## Introducción

---

Este documento pretende dar una visión técnica sobre el análisis realizado sobre la máquina COUNTERS.

El análisis se ha realizado utilizando una máquina instalada desde cero con el sistema operativo Windows 2000 Server.

El fichero .img de la máquina atacada se montó como sistema de archivos.

Las herramientas que he utilizado son las habituales en un sistema operativo Windows, necesitando en algunos campos herramientas de terceros. Las herramientas de terceros que he necesitado las describo a continuación:

- ✚ FileDisk: Herramienta que emula un disco virtual en Windows NT/2000/XP. Emula discos físicos. Licencia GPL. Url: <http://www.acc.umu.se/~bosse/>
- ✚ NTLast 3.0: Herramienta para usar con Windows NT. Nos da información acerca de los logon de una máquina. Licencia: FreeWare para uso personal y no comercial. Fabricante: FoundStone
- ✚ Pasco: Herramienta que nos permitirá ver las URL visitadas en el Internet Explorer. Licencia: FreeWare para uso personal y no comercial. Fabricante: FoundStone
- ✚ Rifiuti: Herramienta de análisis forense que nos ayudará a examinar los archivos que se encuentran en la papelera de reciclaje. Licencia: FreeWare. Fabricante: FoundStone
- ✚ Md5sum.exe: Herramienta compilada a PE (Portable Ejecutable) para que podamos utilizarla en entornos Windows. Nos ayudará a verificar la integridad de las imágenes del reto. Licencia: FreeWare. URL: <http://unxutils.sourceforge.net/>

- ✚ WRR: Windows Registry Recovery es una herramienta que nos ayudará a recomponer el registro de Windows de un sistema afectado. Licencia: FreeWare. Fabricante: MiTec
- ✚ Visual IP Trace Report. Herramienta de localización de IP. Licencia: Versión de prueba 15 días. Fabricante: VisualWare.

El análisis se centrará en los ficheros y fechas de los mismos, descartándose lo relativo a los procesos en ejecución y memoria física de la máquina (volcado).

## Montaje del sistema espejo para el análisis

---

El sistema espejo se componía de un AMD Athlon XP 2600 con 1GB de memoria RAM. Un disco duro de 20 GB en donde se montó un sistema operativo Windows 2000 Server desde cero para el análisis, con todas las actualizaciones de seguridad existentes hasta la fecha. La instalación se realizó incluyendo las herramientas habituales en cualquier sistema Windows. El sistema se montó sin conexiones de red que pudiesen interferir en el análisis. En los análisis forenses se debe procurar tener un sistema limpio, con esto evitaremos posibles contaminaciones en los archivos a examinar.

---

**Nota:** Las fechas que aparecen en este informe datan del estado del reloj interno de la máquina afectada (COUNTERS) en el momento del ataque. Pueden diferir de las fechas reales del ataque si dicho reloj no se encontraba sincronizado o desfasado con respecto a la hora real.

---

Después de descomprimir la imagen Windows2003.img.gz con Winrar se obtiene la imagen correspondiente al sistema atacado. Esta imagen se montó en el sistema espejo a partir de la ruta c:\RetoForense.

Antes de montar la imagen correspondiente, comprobé que la firma MD5 del archivo Windows2003.img correspondía con la firma que me habían facilitado.

La firma que me facilitaron para la imagen descomprimida fue la siguiente:

**062cf5d1ccd000e20cf4c006f2f6cce4**

Para comprobar la firma utilicé la herramienta md5sum.exe de Unxutils.sourceforge.net. No explico el funcionamiento de esta herramienta dada su sencillez de ejecución. El comando que se utilizó para la extracción de la firma MD5 fue el siguiente:

```
C:\>md5sum.exe Windows2003.img
```

```
Salida: 062cf5d1ccd000e20cf4c006f2f6cce4 *windows2003.img
```

Una vez comprobado que disponía de las imágenes correctas e inalteradas procedí al montaje y preparación del análisis.

Para montar las imágenes utilicé la herramienta FileDisk. Es una herramienta que emula discos virtuales en Windows NT/2000/XP y nos va a venir al dedillo para montar las imágenes.

Su instalación es muy sencilla y se hace de la siguiente manera:

Copiaremos el driver "filedisk.sys" al directorio

```
%systemroot%\system32\drivers\
```

Importaremos el archivo de registro filedisk.reg, reiniciaremos la máquina espejo y ya está! Tenemos emulador de discos físicos!

El funcionamiento de esta herramienta es muy sencillo e intuitivo, como veremos a continuación:

La sintaxis del comando filedisk.exe es la siguiente:

```
C:\>filedisk
```

syntax:

```
filedisk /mount <devicenum> <filename> [size[k|M|G] | /ro | /cd]  
<drive:>
```

```
filedisk /umount <drive:>
```

```
filedisk /status <drive:>
```

filename formats:

```
c:\path\filedisk.img
```

```
\Device\Harddisk0\Partition1\path\filedisk.img
```

```
\\server\share\path\filedisk.img
```

example:

```
filedisk /mount 0 c:\temp\filedisk.img 8M f:
```

```
filedisk /mount 1 c:\temp\cdimage.iso /cd i:
```

```
filedisk /umount f:
```

```
filedisk /umount i:
```

Nuestra imagen está ubicada en el directorio c:\RetoForense, y montaremos la imagen en modo de sólo lectura, para que no sea posible su contaminación externa desde el sistema espejo. El comando resultante para realizar esta acción será el siguiente:

```
C:\>filedisk /mount 0 c:\RetoForense\windows2003.img /ro z:
```

Este comando nos montará la imagen comprometida en un disco físico virtual en modo de sólo lectura, y la ubicará en la unidad z.

Para facilitar la tarea de montaje y desmontaje realicé dos scripts en .bat sencillísimos de comprender y utilizar, para no tener que andar montando y desmontando a base de comandos. La ley del más flojo... Los scripts son los siguientes:

---

Monta.bat

@echo off

filedisk /mount 0 c:\RetoForense\windows2003.img /ro z:

exit

---

Desmonta.bat

@echo off

filedisk /umount z:

exit

---

Doble clic para montar, y doble clic para desmontar. Economía de movimientos!

Ya tenemos el sistema listo y operativo para ser analizado. He puesto en el reproductor de música las bandas sonoras de "La jungla de Cristal" y "Los jueces de la noche", de Michael Kamen y Alan Silvestri, bandas sonoras que me encantan y las cuales me ayudarán a "emocionarme" todavía más.

Así que señoras y señores, denle al play y cojan papel y bolígrafo, porque empieza el análisis...

---

## Análisis del sistema de ficheros

---

Como ya comenté en el informe ejecutivo, un análisis forense se puede abordar de muchas maneras, y atendiendo a la volatilidad de la misma, deberemos atender antes los datos que puedan degradarse más rápidamente con el tiempo. Podríamos dividir el análisis en:

1. Recogida de datos de la organización
2. Tipología de la red
3. Gente directa o indirectamente implicada
4. Tipo de escenario y equipo/s implicados
5. Memoria del sistema
6. Procesos en ejecución
7. Conexiones de red
8. Sistemas de ficheros
9. Bloques de disco

La recogida de datos de la organización es muy importante. Recabar información acerca del estado de la empresa y sus funciones pueden dar muchas respuestas. La tipología de red también es importante, porque nos ayudará a visualizar cómo de segura es la red a analizar. El tipo de escenario y los equipos implicados son también muy buena información, ya que con ello podremos averiguar el alcance del ataque. El análisis de un volcado de memoria es muy difícil de interpretar, ya que los datos que en ellos se encuentran son muy difíciles de leer, incluso para Clark Kent. Los procesos en ejecución se deben de obtener de la manera más rápida posible, ejecutando por ejemplo el comando `netstat -ab`, el cual nos mostraría una salida con todas las conexiones y puertos de escucha, mostrando además el ejecutable que crea la conexión o puerto de escucha. Todos los comandos y herramientas que utilicemos serán ajenas al sistema, y nos cercioraremos de que son genuinas y “poco intrusivas” en el sistema. Tenemos que hacerlo así, ya que las herramientas del sistema comprometido pueden estar manipuladas y arrojar falsos positivos, lecturas erróneas, etc.... Intentaremos en la medida de lo posible no alterar el escenario a analizar. La configuración de red también es importante analizarla, ya que podríamos detectar la presencia de un sniffer comprobando si nuestra tarjeta de red se encuentra en modo promiscuo.

En este caso partiré a partir del punto 8 y a partir de ahí empezaré el análisis.






---

## Recogida de datos de la máquina

---

En este apartado trataremos de recabar información acerca de la máquina atacada, tales como servipacks instalados, aplicaciones, parches relativos a la seguridad, configuración IP, servicios funcionando, etc..

Toda esta información se encuentra recogida en los archivos del sistema del registro de Windows, los cuales se localizan en %systemroot%\system32\config, y atienden a los nombres siguientes:

-  SECURITY
-  SOFTWARE
-  SYSTEM
-  SAM
-  DEFAULT

Windows define al registro como una base de datos jerárquica central utilizada en todas las versiones de Windows, con el fin de almacenar información necesaria para configurar el sistema para uno o varios usuarios, aplicaciones y dispositivos hardware.

El registro contiene información que Windows utiliza como referencia constantemente, como por ejemplo los perfiles de usuario, las aplicaciones instaladas, los parches o hotfixes instalados, etc..

Los archivos del registro de Windows se almacenan en archivos binarios, es decir, que si abrimos estos ficheros con un editor de texto, como puede ser notepad, no podremos leerlo.

Para leer estos ficheros utilizaremos la herramienta Windows Registry Recovery de MiTec y abriremos los archivos anteriores.

De los archivos de registro obtenemos la siguiente información:

### Nivel de Hardware (Archivo SYSTEM)

Procesador:	Intel Pentium III
Unidades de Disco duro:	Barracuda Ultra ATA/100 80GB 7200 rpm SanDisk Cruzer Mini USB Device Kingston DataTraveler 2.0 USB Device
Adaptador de Vídeo:	Trident MicroSystems Accelerator Blade 3D/ProMedia
Monitor:	Samsung SyncMaster 550v
Adaptadores de Red:	3Com 3C900B-TPO Ethernet Adapter Realtek RTL8139
Tarjeta Sonido:	VIA AC'97 Audio Controller

### Datos Generales (Archivo SOFTWARE)

Nombre de producto: Microsoft Windows Server 2003 R2  
Product ID: 69763-024-0099217-43782  
Product Key: CCK3G-XQV9G-4JF22-3WF7P-DQC6Y  
Fecha Instalación: 26/01/2006 6:56:44  
Servipack: Servipack 1  
System Root: C:\Windows

### Aplicaciones Instaladas (Archivo SOFTWARE)

MySQL Server	versión 4.1.16
Apache http Server	versión 1.3.34
Mozilla Firefox	versión 1.5.0.1
MSN Messenger	versión 7.5.0311.0
MySQL Administrador	versión 1.1.7
PHP	versión 4.4.2
PostgreSQL	versión 8.1

### Hotfixes y parches instalados (Archivo SOFTWARE)

KB908519  
KB905414  
KB903235  
KB902400  
KB901214  
KB901017  
KB899589  
KB899587  
KB896727  
KB896688  
KB896428  
KB896424  
KB896422  
KB896358  
KB890046

### Configuración IP del adaptador de red (Archivo SYSTEM)

Dirección IP:	192.168.5.5
Puerta de Enlace:	192.168.5.254
DNS Primario:	83.217.93.246
DNS Secundario:	67.102.133.222

[Servicios Instalados en modo automático \(Archivo SYSTEM\)](#)

Alerter  
Apache  
Application Experience Lookup Service  
Automatic Updates  
Background Intelligent Transfer Service  
COM+ Event System  
Computer Browser  
Cryptographic Services  
DCOM Server Process Launcher  
DHCP Client  
Distributed File System  
Distributed Link Tracking Client  
Distributed Transaction Coordinator  
DNS Client  
DNS Server  
Error Reporting Service  
Event Log  
Help and Support  
HTTP SSL  
Indexing Service  
IPSEC Service  
Kerberos Key Distribution Center  
Logical Disk Manager  
MYSQL  
Performance Logs and Alerts  
Plug and Play  
Postgre SQL DataBase Server 8.1  
Print Spooler  
Protected Storage  
Remote Desktop Help Session Manager  
Remote Procedure Call (RPC)  
Remote Registry  
Secondary Logon  
Security Accounts Manager  
Server  
Shell Hardware Detection  
System Event Notification  
Task Scheduler  
TCP/IP NetBios Helper  
Telephony  
Windows Audio  
Windows Firewall ICS  
Windows Management Instrumentation  
Windows Time  
Wireless Configuration  
WorkStation

## Tipos de Logon en Windows

---

La categoría de inicio de sesión en Windows registrará la entrada con un evento ID 528, el cual contendrá una serie de datos importantes, como son el tipo de entrada y el ID de inicio de sesión.

Dependiendo del inicio de sesión que hagamos en la máquina, ya sea a través de recursos compartidos, de forma remota o de forma física, Windows registrará ese inicio de sesión con una numeración u otra.

Algunos tipos de inicio de sesión son los siguientes:

Tipo 2. Interactivo. Entrada a un sistema desde la consola (teclado)

Tipo 3. Red. Entrada al sistema a través de la red. Por ejemplo con el comando net use, recursos compartidos, impresoras, etc...

Tipo 4. Batch. Entrada a la red desde un proceso por lotes o script programado.

Tipo 5. Servicio. Cuando un servicio arranca con su cuenta de usuario.




Tipo 7. Unlock. Entrada al sistema a través de un bloqueo de sesión.

Tipo 10. Remote Interactive. Cuando accedemos a través de Terminal Services, Escritorio Remoto o Asistencia Remota.

## Ficheros Log

---

Los ficheros Log de una máquina, sea la que sea, son una fuente de información importantísima en un análisis forense. Empezaremos con estos ficheros. Los sistemas Windows basados en NT tienen su principal fuente de Log en los archivos de sistema siguientes:

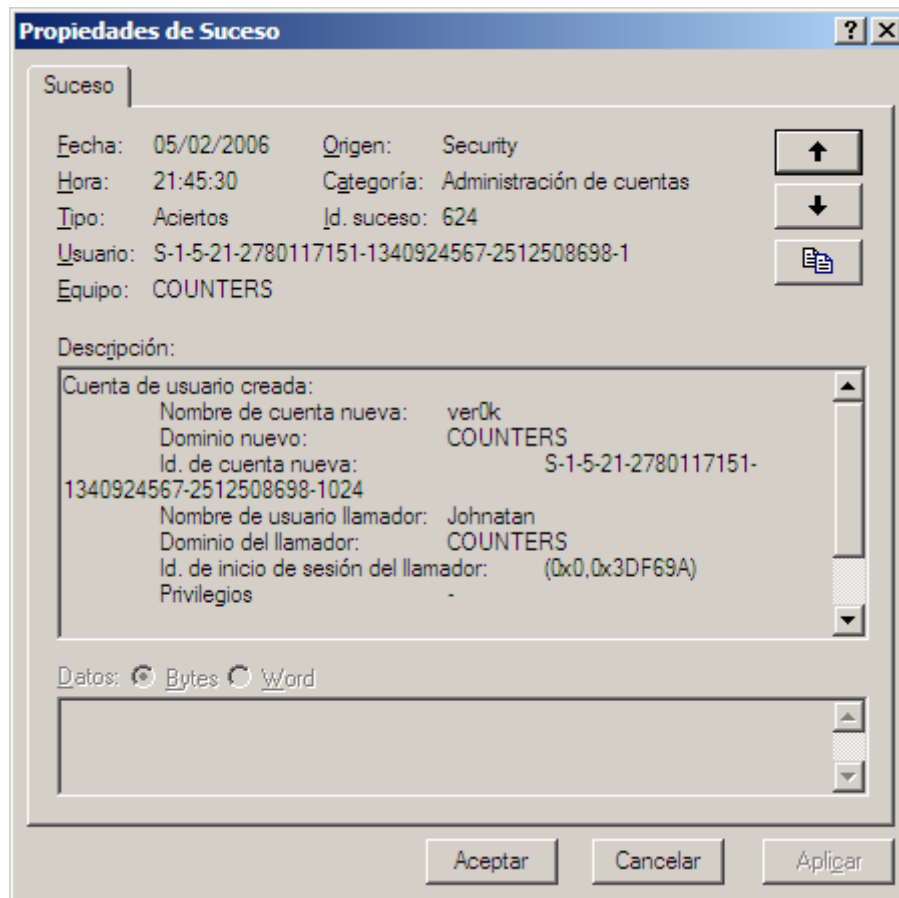
-  SysEvent.Evt. Registra los sucesos relativos al sistema
-  SecEvent.Evt. Registra los sucesos relativos a la seguridad
-  AppEvent.Evt. Registra los sucesos relativos a aplicaciones

Estos ficheros se encuentran en el directorio %systemroot%\system32\config. Nos centraremos con especial atención en el archivo Log SecEvent.Evt.

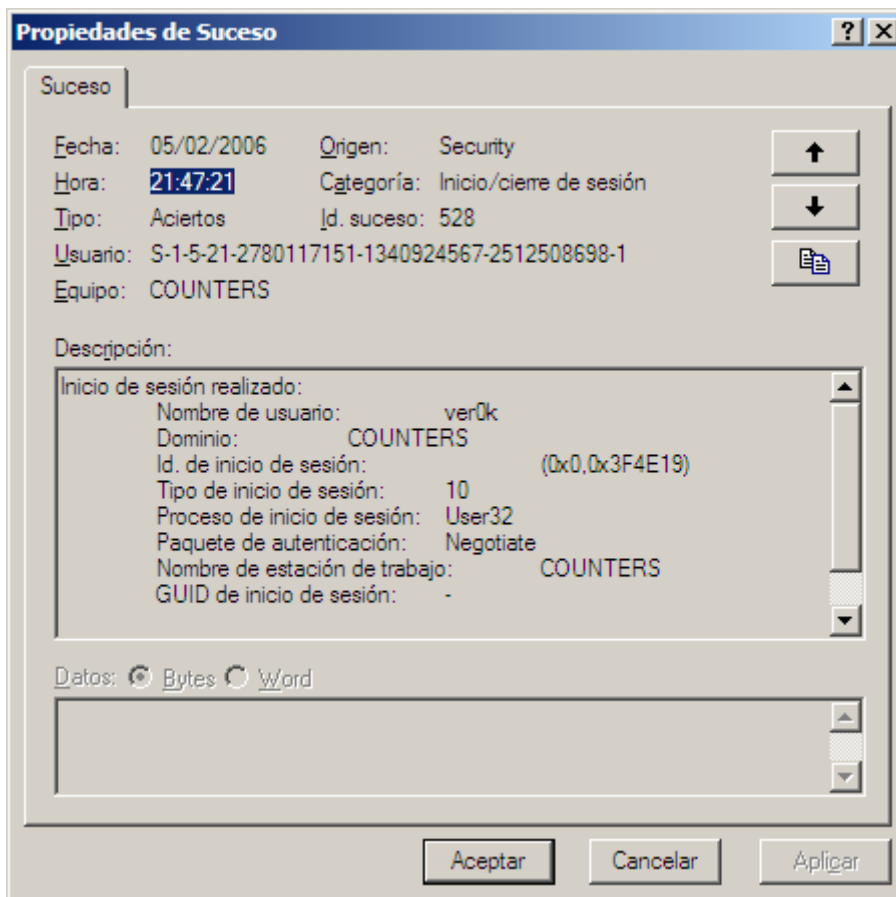
Para visualizar este fichero utilizaremos la herramienta de Windows eventvwr.msc, comúnmente llamada "Visor de Sucesos". Abriremos con esta herramienta el archivo SecEvent.Evt, que es el encargado de almacenar los sucesos relativos a la seguridad, tales como ingresos en la máquina, cambio de directivas, etc... Buscaremos sobre todo accesos físicos a la máquina, cambio de directivas y creación de cuentas de usuario.

En una primera instancia vemos que la máquina en cuestión se llamaba MACHINENAME. Le cambiaron el nombre a COUNTERS. Como sabemos por el supuesto que la máquina la estaban migrando a otro servidor, puede deberse ahí el cambio de nombre. Sabemos también por el supuesto que el Administrador de sistemas era el que tenía potestad para crear cuentas de usuario. Ningún otro usuario tenía autoridad para crear cuentas. Pero dado que había usuarios que estaban en el grupo Administradores, podían no tener autoridad, pero sí el "poder" para crearlas. Con esta información nos detenemos en la fecha 05 de Febrero del 2006 a las 21:44:12 horas.

Un usuario llamado Johnatan utiliza el comando net para crear una cuenta de usuario llamada ver0k y le asigna privilegios administrativos. La cuenta se crea a las 21:45:30 horas. Tenemos nuestra primera prueba y nuestro primer sospechoso, llamado Johnatan. La prueba "a" señores.



Estupefacto me quedo cuando apenas 3 minutos después de la creación de la cuenta de usuario ver0k, veo que el sospechoso número 2 (ver0k) se conecta a la máquina en cuestión con tipo de sesión 10, es decir, se conecta a través de terminal service o escritorio remoto. Prueba "b" señores.



En las sucesivas entradas del registro de sucesos podemos comprobar que el usuario ver0k se ha detenido un tiempo a visualizar archivos sin "importancia general" como los que se muestran en esta lista:

- ✚ C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\fiesta en el antro.exe
- ✚ C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\el df.exe
- ✚ C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\amigas de huevos.exe
- ✚ C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\mi vecina.exe
- ✚ C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\mordida.exe
- ✚ C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\Muchos Huevos.exe
- ✚ C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\no existieras.exe
- ✚ C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\no muerdo.exe
- ✚ C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\Perdonam.exe
- ✚ C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\Poetas Huevos 2a Edicion.exe

- ✚ C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\saludosamama.exe
- ✚ C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\sarten.exe
- ✚ C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\Te quiero como a mi huevo.exe
- ✚ C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\temoc.exe
- ✚ C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\tequieromasqueamis.exe
- ✚ C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\TestdeRavenH.exe
- ✚ C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\tortuga1.exe
- ✚ C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\tortuga2.exe
- ✚ C:\Documents and Settings\Administrator\My Documents\My Videos\cartoons\unbaileparati.exe

Aunque desgraciadamente sí que tuvo acceso a aplicaciones que si bien no son un riesgo para la seguridad nacional, nos arrojan a nuevas preguntas. La lista de aplicaciones a las que tuvo acceso el usuario ver0k son:

- ✚ C:\Program Files\Windows NT\Accessories\wordpad.exe
- ✚ C:\WINDOWS\system32\notepad.exe
- ✚ C:\Program Files\MySQL\MySQL Administrator 1.1\MySQLAdministrator.exe
- ✚ C:\Program Files\MSN Messenger\msnmsgr.exe

Wordpad y Notepad son dos aplicaciones para visualizar archivos. Dado que el servidor no tenía Microsoft Office ni OpenOffice instalados, tuvo que acceder a diversos archivos a través de estas aplicaciones.

MySQL Administrator es una aplicación que permite realizar tareas administrativas sobre servidores de MySQL, incluyendo entre otras cosas la administración de usuarios y la visualización del catálogo de datos.

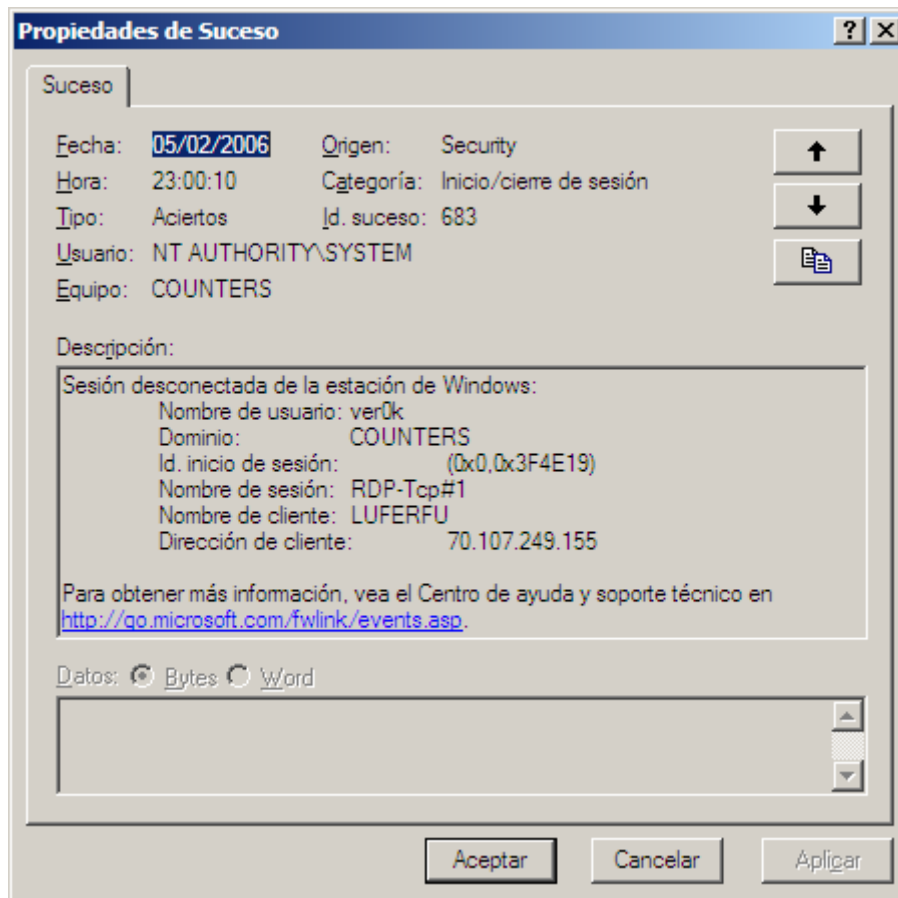
El día 05 de Febrero de 2006 a las 22:04:14 el Firewall de Windows detectó una aplicación que empezó a escuchar tráfico de Internet. La aplicación en sí fue msnmsgr.exe, más comúnmente llamado Messenger.

Esta aplicación es un cliente de mensajería instantánea propiedad de Microsoft Corporation que sirve para chatear en línea con personas que estén agregadas en tu lista de contactos, mandar y recibir archivos, compartir escritorio de forma remota y muchas funcionalidades más. Esto es maravilloso, pero yo, que no tengo una mentalidad malvada☺, pienso y se me ocurren cosas malísimas para realizar, desde conectarme con otro equipo, hasta descargarme virus y troyanos vía Messenger...

Ver0k tuvo tiempo de hacer todas estas cosas y me figuro que alguna que otra más, lo que sucede es que todavía no las conocemos, pero como diría un amigo mío, "tiempo al tiempo".

Mirando las sucesivas entradas en el visor de sucesos (eventvwr.msc) me encuentro con la prueba "c" señoras y señores. El sospechoso ver0k se

desconectó del equipo a las 23:00:10. Bien porque notó que el Administrador le pisaba los talones, o bien porque consiguió lo que quería.



Prueba C

Buenas noticias por fin! El registro de sucesos ha registrado datos importantísimos como el nombre de cliente y su dirección, las cuales son las siguientes:

- Nombre de Cliente: LUFERFU
- Dirección de Cliente: 70.107.249.155

Por su dirección IP podremos tener una idea del lugar (País) desde donde se conectó al servidor.

En otras palabras, si este usuario (ver0k) no es un usuario creado por el Administrador y se ha colado en el sistema, ha tenido oportunidad para hacer cosas muy malas en el servidor.

Es hora de ver lo que tocó ver0k...

## Perfiles de usuario en Windows

---






El perfil de usuario contiene las preferencias y las opciones de configuración de cada usuario. En la tabla siguiente se puede ver un ejemplo de la configuración que contienen los perfiles de usuario.

Fuente	Parámetros guardados
Explorador de Windows	Todos los valores definibles por el usuario en el Explorador de Windows.
Mis documentos	Documentos almacenados por el usuario.
Mis imágenes	Imágenes almacenadas por el usuario.
Favoritos	Accesos directos a las ubicaciones favoritas de Internet.
Unidad de red asignada	Asignaciones de unidades de red creadas por el usuario.
Mis sitios de red	Vínculos a otros equipos de la red.
Contenido del escritorio	Elementos almacenados en el Escritorio y en los accesos directos.
Colores y fuentes de pantalla	Toda la configuración de colores y textos presentables en pantalla y definibles por el usuario.
Datos de aplicación y sección del Registro	Datos de aplicación y configuraciones definidas por el usuario.
Configuración de impresoras	Conexiones de impresoras de red.
Panel de control	Todas las configuraciones definidas por el usuario en el Panel de control.
Accesorios	Todas las configuraciones de aplicación definidas por el usuario que afectan al entorno de usuario de Windows, incluidos Calculadora, Reloj, Bloc de notas y Paint.
Programas de instalación de la familia Windows Server 2003	Cualquier programa escrito específicamente para la familia Windows Server 2003 se puede diseñar para que haga un seguimiento de las configuraciones propias de cada usuario. Si dicha información existe, se guarda en el perfil de usuario.
Marcadores de formación en pantalla para el usuario	Los marcadores del sistema de Ayuda de la familia Windows Server 2003.



En Windows 2003 Server, los perfiles de cada usuario se almacenan en el directorio Documents and Settings de la raíz. Como sabemos por el registro que el equipo estaba montado en la unidad C: \, el directorio de los perfiles se encontrará en el directorio siguiente:

C:\Documents and Settings\usuario

Dentro de la carpeta de ver0k (C:\Documents and Settings\ver0k) hay un directorio que se llama "Documentos recientes" y no es más que una carpeta en la que se encuentran los accesos directos a los documentos utilizados recientemente, y las carpetas a las que se ha tenido un acceso reciente. Pues bien, desgraciadamente dentro de esa carpeta me encuentro con que el usuario ver0k ha tenido acceso a estos ficheros y directorios:

-  AccountGroups.php
-  Clientes.txt
-  Config.php
-  Users.txt
-  Web-erp

Aparentemente está todo menos dos ficheros, que visto por el nombre de los ficheros, parecen ser de suma importancia. Los ficheros son los siguientes:

-  Clientes.txt
-  Users.txt

Estos ficheros estaban en la raíz del equipo, es decir, en C:. Y ahora no están. Se los ha llevado? Tal vez el Administrador los borró? No tengo ni idea. Muchas veces me han dicho que por la basura se pueden conocer muchos datos de las personas. Así que señoras y señores, pónganse guantes y mascarillas para la cara, porque nos toca rebuscar en la papelera...

## La papelera de reciclaje

---

Al contrario de lo que se piensa mucha gente, cuando un archivo se borra de una computadora, realmente no se borra. Los archivos se "modifican" por decirlo de alguna manera, para que el sistema operativo no los "vea". Windows utiliza un depósito para los archivos borrados llamado Papelera de Reciclaje. La existencia de este depósito permite que un usuario pueda recuperar la información, si ésta ha sido borrada accidentalmente por ejemplo. Cuando Windows da orden para borrar cierto archivo o directorio, la información debe ser guardada en expedientes, por si el usuario se arrepiente y quiere recuperar sus datos. El archivo que contiene esta información se llama INFO2 y reside en el directorio de la Papelera de Reciclaje, es decir, está dentro de la Papelera.

Es necesario explicar cómo funciona la Papelera de Reciclaje antes de que discutamos las estructuras del archivo INFO2. Cuando un usuario "suprime" un archivo a través del explorador de Windows, una copia del archivo se mueve al directorio del compartimiento de la Papelera de Reciclaje. La localización de este directorio es distinta, dependiendo de la versión de Windows que tengamos. En la que nos ocupa (Windows 2003), el archivo INFO2 se encuentra en el directorio:

**C:\Recycler\\INFO2**

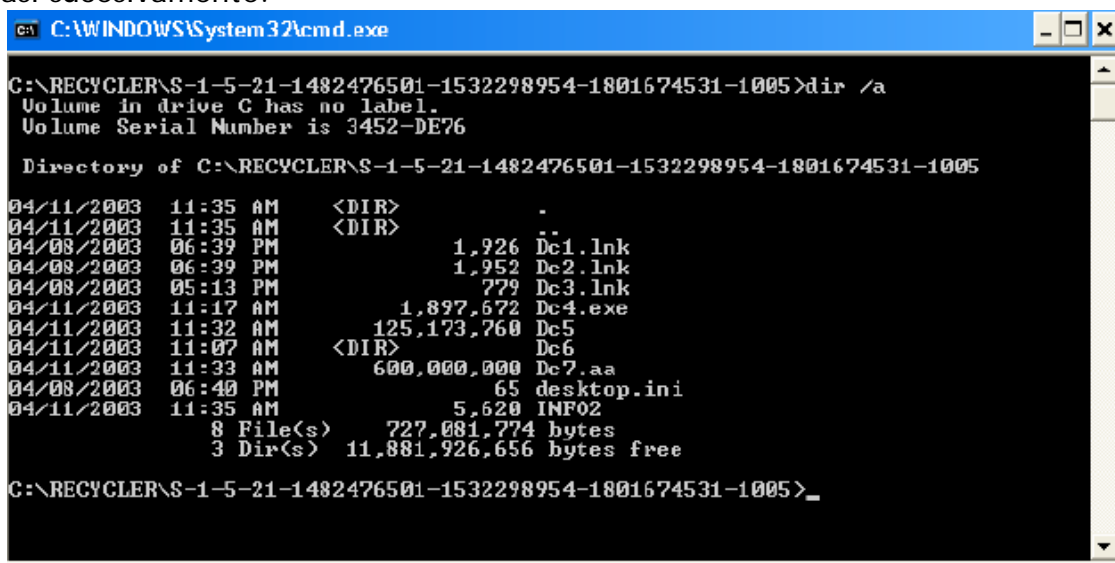
Cuando borramos un fichero, Windows lo renombra siguiendo este parámetro:

D<Unidad raíz del sistema><número> .Extensión del archivo

Es decir, que si nosotros borrásemos el archivo Reto.txt y lo mandásemos a la Papelera de Reciclaje, Windows lo renombraría de la siguiente manera:

DC1.Txt

Si borrásemos otro archivo, a éste nuevo archivo se le pondría el número 2, y así sucesivamente.



```
C:\WINDOWS\System32\cmd.exe
C:\RECYCLER\S-1-5-21-1482476501-1532298954-1801674531-1005>dir /a
Volume in drive C has no label.
Volume Serial Number is 3452-DE76

Directory of C:\RECYCLER\S-1-5-21-1482476501-1532298954-1801674531-1005

04/11/2003  11:35 AM    <DIR>          -
04/11/2003  11:35 AM    <DIR>          -
04/08/2003  06:39 PM             1,926  Dc1.lnk
04/08/2003  06:39 PM             1,952  Dc2.lnk
04/08/2003  05:13 PM              779  Dc3.lnk
04/11/2003  11:17 AM          1,897,672  Dc4.exe
04/11/2003  11:32 AM        125,173,760  Dc5
04/11/2003  11:07 AM    <DIR>          Dc6
04/11/2003  11:33 AM        600,000,000  Dc7.aa
04/08/2003  06:40 PM              65  desktop.ini
04/11/2003  11:35 AM             5,620  INFO2
            8 File(s)      727,081,774 bytes
            3 Dir(s)   11,881,926,656 bytes free

C:\RECYCLER\S-1-5-21-1482476501-1532298954-1801674531-1005>_
```

*La Papelera de Reciclaje*

Si al menos un archivo se ha movido a la Papelera de Reciclaje, el archivo INFO2 existirá. Cuando se vacía la Papelera de Reciclaje, el contenido del archivo INFO2 se limpiará, y el número se establecerá de nuevo a 1. Es decir, el archivo INFO2 se suprime y se crea un nuevo y vacío INFO2.

Ahora que sabemos un poco sobre la estructura de la Papelera de Reciclaje, creo yo que es hora de que nos pongamos manos a la obra y empecemos a fisgonear.

Para recomponer el archivo INFO2 utilizaremos la herramienta llamada Rifiuti, palabra italiana que se utiliza para llamar a la basura. La estructura de comandos de Rifiuti es tan simple como este comando:

```
Rifiuti.exe INFO2 >INFO2
```

Manos a la obra! Descubramos si ver0k borró algo. En una ventana de MS-DOS teclearemos lo siguiente:

```
Rifiuti.exe c:\recycler\S-1-5-21-2780117151-1340924567-2512508698-1024\INFO2 > C:\INFO2.TXT
```

Hemos redirigido la salida del comando a un archivo .txt para poder visualizarlo con el notepad.

Desgraciadamente la salida no nos muestra nada de nada. El usuario ver0k no borró nada durante su sesión. Repetimos la operación para todos los usuarios, y el único que borró algo fue el Administrador, pero aplicaciones sin importancia. Ni rastro de users.txt ni clientes.txt. La lista de aplicaciones que borró el administrador fueron las siguientes:

- ✚ C:\Documents and Settings\Administrator\Desktop\postgresql-8.1.2-1-binaries-no-installer.zip
- ✚ C:\Documents and Settings\Administrator\Desktop\postgresql-8.1.2-1-binaries-no-installer
- ✚ C:\Documents and Settings\Administrator\Desktop\postgresql-8.1.2-1-ja.zip.sig

Ni Clientes.txt ni Users.txt. Eso indica dos cosas:

- ✚ Que el Administrador se las llevase antes de apagar el equipo
- ✚ Que alguien no autorizado se llevase estos documentos

Ante la duda nos vamos a poner en lo peor...

Nota: El UserId del ver0k viene reflejado en las entradas del visor de sucesos, no necesitando para ello ningún programa adicional.

## Breve resumen de pistas

---

Por el supuesto sabemos lo siguiente:

- ✚ Habían migrado al servidor hacía poco tiempo (posiblemente estuviese en pruebas)
- ✚ El Administrador era el único que tenía potestad para crear cuentas
- ✚ El Servidor se utilizaba para tareas no Administrativas
- ✚ Varios usuarios tenían acceso al servidor y con cuentas Administrativas
- ✚ El Administrador trataba de mantener el sistema actualizado
- ✚ Utilizaban el equipo para tareas personales

Las pistas que hemos encontrado hasta el momento son las siguientes:

- ✓ A las 21:45:30 horas del día 05 de Febrero de 2006 el usuario Johnatan crea una cuenta de usuario llamada ver0k, con permisos Administrativos.
- ✓ A las 21:47:21 horas del mismo día, ver0k se conecta a la máquina en cuestión a través de Escritorio remoto o Terminal Services.
- ✓ Ver0k tuvo acceso a diversas aplicaciones, que si bien no constituyen un riesgo para la seguridad, pudo utilizarlas par fines no éticos
- ✓ El equipo desde el que se conectó ver0k se llamaba LUFERFU
- ✓ La dirección IP desde la que se conectó fue 70.107.249.155
- ✓ Ver0k tuvo acceso a ficheros de configuración y ficheros con nombres importantes, tales como users.txt y clientes.txt
- ✓ Users.txt y clientes.txt no se encuentran en el equipo
- ✓ Ver0k no mandó ningún fichero a la papelera de reciclaje
- ✓ Ver0k se conectó a un cliente de mensajería instantánea (Messenger)
- ✓ Gracias al visor de sucesos hemos podido comprobar que aparte de los ficheros que ha visto, no ha ejecutado ningún ejecutable "peligroso" para el sistema, tales como virus, backdoors o rootkits.

Se me está ocurriendo una cosa.

El archivo NTuser.dat es la parte del Registro del perfil de usuario. Cuando un usuario cierra la sesión del equipo, el sistema carga la sección del Registro específica de dicho usuario (es decir, HKEY\_CURRENT\_USER) en NTuser.dat y la actualiza. Si ver0k utilizó el Messenger para conectarse en línea, ha podido dejar un rastro en el registro de Windows, es decir, en el archivo NTuser.dat. El archivo NTUser.dat se encuentra dentro del perfil del usuario. Para el caso que nos ocupa se encuentra en la siguiente dirección:

C:\Documents and Settings\ver0k\ntuser.dat

Abriremos este archivo con la aplicación Windows Registry Recovery de MiTec e iremos a la clave siguiente:

HKEY CURRENT USER\Software\Microsoft\Windows\CurrentVersion\UnreadMail

Esta clave almacena las cuentas de correo que utilizamos para el cliente de mensajería instantánea Messenger. Abrimos la carpeta y... BINGO!!!! Estábamos en lo cierto. Ver0k utilizó el Messenger con la siguiente cuenta de correo:

[H4ckIII@hotmail.com](mailto:H4ckIII@hotmail.com)

La cuenta no podía ser más sospechosa eh? Como dirían por ahí: "Es más sospechoso que la relación entre Batman y Robin..." Hasta el momento tenemos dos sospechosos, los cuales son Johnatan y ver0k. Ha llegado la hora de investigar qué visitaron con el navegador.

---

## Index.dat e Internet Explorer

---

Internet Explorer es el navegador por excelencia de Microsoft. A partir de su versión XP, este navegador viene “incrustado” en el sistema operativo, es decir, que no se puede desinstalar.

Internet Explorer guarda una copia de las páginas visitadas en el disco duro. Si vas a una página ya visitada, Internet Explorer busca primero en la caché, y la compara con la página del servidor, mostrándote la página desde tu disco duro, si no ha habido actualizaciones. Con esto conseguimos una carga mucho más rápida de las páginas Web, o como dirían los expertos, “Una mejor experiencia para el usuario final” ☺.

Podemos borrar el caché de disco desde el propio Internet Explorer (herramientas, opciones de Internet, eliminar archivos). El problema es que esta opción borra todo el contenido del historial de Internet (los archivos html, los gráficos, etc.) pero **no borra** el índice de referencia que Internet Explorer usa para buscar dentro de su historial: el archivo **index.dat**. Estos archivos (hay varios index.dat) están definidos como ocultos y de sistema; por eso no podemos acceder a su contenido desde el propio Windows, a no ser que quitemos el atributo de “ocultos” a esos directorios. En ellos se guarda una lista de todos los sitios Web que hemos ido visitando (aunque hayamos borrado el historial, esta lista no está sincronizada, luego no borra esas urls).

Esto supone un problema de privacidad, ya que cualquiera que sepa localizar y leer estos archivos index.dat tendrá un listado completo de los sitios que hayamos visitado (aunque hayamos borrado el historial de tu navegador). Además este archivo está creciendo constantemente, y puede llegar a ocupar varios megas de la forma más innecesaria. Aparte, si por cualquier razón su contenido se corrompe, puede ocasionar que Internet Explorer no pueda visualizar correctamente algunas páginas o no pueda descargar ficheros. La ruta en donde se encuentran estos archivos (index.dat) es la siguiente:

```
Windows 2K/XP  \Documents and Settings\
```

Bien. Sabiendo más o menos como Internet Explorer indexa sus páginas, y sabiendo la ruta en donde se encuentran, vamos a ver el contenido de lo que hay en los archivos Index.dat.

Podemos hacerlo de dos formas diferentes, o por lo menos yo sólo conozco dos formas diferentes de hacerlo (de manera gratuita ☺):

- Desde línea de comandos (MS-DOS) y sin aplicación de terceros.
- Desde línea de comandos con aplicación de terceros (Pasco).

Aquí vamos a explicar las dos. Son dos técnicas muy sencillas y que cualquier persona sin amplios conocimientos sobre informática puede realizar.

### Desde línea de comandos

---

Si quisiésemos visualizar que tenemos en nuestro Index.dat desde línea de comandos y sin aplicación de terceros podríamos utilizar este comando:

```
C:\Documents and Settings\tu_user_name\Configuración  
local\Historial\History.IE5> find /i "http://" index.dat | sort >  
C:\history.txt
```

Explicación: Nos situaremos en el directorio en donde se encuentra el archivo Index.dat de nuestra carpeta Historial, y una vez dentro utilizaremos el comando "find" para buscar cadenas dentro del archivo que empiecen por "<http://>". La opción "/i" indica que no distinga entre mayúsculas y minúsculas y el comando sort lo utilizaremos para ordenar la salida.

### Desde línea de comandos con Pasco

---

La segunda opción que podemos utilizar para visualizar este archivo sería con la aplicación Pasco. Esta aplicación reporta la salida en un fichero con texto delimitado. Nuestra vista lo agradecerá, ya que podremos visualizar este archivo en cualquier hoja de cálculo como Excel, y nos facilitará mucho la tarea a la hora de "husmear". Otra cosa interesante que nos brinda este programa es la opción "undelete". El modo undelete hace caso omiso a la información que hay en la tabla HASH y reconstruye cualquier dato válido de actividad. Gracias a esto podremos recuperar información que con otra aplicación no podríamos.

La línea de comandos que utiliza Pasco es muy sencilla:

```
[kjones: pasco] kjones% ./pasco
```

```
Usage: pasco [options] <filename>  
-d Undelete Activity Records  
-t Field Delimiter (TAB by default)
```

Tan solo tendríamos que poner este sencillo comando:

```
Pasco -d -t index.dat >index.txt
```

Una vez creado index.txt, podremos importar este texto a cualquier hoja de cálculo, como Microsoft Excel por ejemplo.

En el caso que nos ocupa, voy a utilizar esta herramienta.

Ha llegado la hora de ver que actividad recoge Internet Explorer. Todas las pistas indican que fue el navegador más usado. Recordemos que en el servidor estaban instalados Internet Explorer y Mozilla Firefox en su última versión (1.5). El visor de sucesos no indicó ninguna actividad para Firefox y sí para Internet Explorer. Así que analizar!

Los resultados los obtuve de las tres rutas en donde nos encontramos archivos Index.dat, y de todos los usuarios que utilizaron Internet Explorer. Tan sólo me parecieron sospechosos dos usuarios, los cuales muestro a continuación. Los adivináis? Exacto... Johnatan y ver0k.

Johnatan
----------

El día 05 de Febrero de 2006 a las 20:28:11 horas, Johnatan abre la Web de Yahoo para visualizar correo electrónico, tal y como muestra esta línea de su Index.dat

URLindex.datVisited:

[Johnatan@https://login.yahoo.com/config/login?index.datSun Feb 5 20:28:11 2006](https://login.yahoo.com/config/login?index.datSun%20Feb%205%2020:28:11%202006)

Unos minutos después, Johnatan abre la siguiente URL

URLindex.datVisited: [Johnatan@http://70.107.249.150/clientes.wmf](http://70.107.249.150/clientes.wmf)  
index.datSun Feb 5 20:41:30 2006

Sigue mirando su correo y a los pocos minutos después vuelve a abrir la misma URL de antes

URLindex.datVisited: [Johnatan@http://70.107.249.150:8080/clientes.wmf](http://70.107.249.150:8080/clientes.wmf)  
index.datSun Feb 5 20:44:10 2006

Y apenas un segundo después...

URLindex.datVisited:

[Johnatan@http://70.107.249.150:8080/GPlw9OgYR6/uSvcCeC1V18W/bfKJ0KMsfYBZnaFKx6dZs/FHBwenHfCEt6do1Z/e9zhOEMQ052zYwSU50i/AUWWckI2mU/LQ9ClubsIAJKIa2jdYtSFExez4sRyL.tiff](http://70.107.249.150:8080/GPlw9OgYR6/uSvcCeC1V18W/bfKJ0KMsfYBZnaFKx6dZs/FHBwenHfCEt6do1Z/e9zhOEMQ052zYwSU50i/AUWWckI2mU/LQ9ClubsIAJKIa2jdYtSFExez4sRyL.tiff) index.datSun Feb 5 20:44:11 2006

Vamos a detenernos un momentito para pensar con claridad. Qué cosa más rara. Johnatan visita esta URL (<http://70.107.249.150:8080/clientes.wmf>) el día 05 de Febrero del 2006 a las 20:44:10 horas. Y la cuenta ver0k se empieza a crear a las 21:44:11. Exactamente una hora de diferencia. Sabemos por el histórico de sucesos que Johnatan creó la cuenta ver0k desde línea de comandos, es decir, bajo MS-DOS, y con el comando net. Es la misma hora que Johnatan visitó la siguiente URL (<http://70.107.249.150:8080/GPIw9OgYR6/uSvcCeC1V18W/bfKJ0KMsFYBZnaFKx6dZs/FHBwenHfCEt6do1Z/e9zhOEMQ052zYwSU50i/AUWWcki2mU/LQ9ClubsIAJKIa2jdYtSFExez4sRyL.tiff>). Por si no son bastantes casualidades, ahí va otra. Os acordáis de la dirección IP desde la que se conectó ver0k? Os refrescaré la memoria: 70.107.249.155. Apostaría a que la dirección IP es del mismo proveedor de servicios (ISP) que la del Log. Husmeemos lo que tenía ver0k en su Index.dat

Ver0k
-------

Como era de esperar y ya sabíamos, gracias al directorio "Documentos Recientes", ver0k estuvo mirando varios archivos y fotografías, y los siempre intrigantes clientes.txt y users.txt, de los cuales no sabemos nada de nada.

[2006 index.datURL index.datindex.dat](#)  
[URLindex.datVisited: ver0k@file:///C:/users.txt index.datSun Feb 5 21:06:37 2006](#)

[URLindex.datVisited: ver0k@file:///C:/clientes.txt index.datSun Feb 5 21:05:56 2006 index.datSun Feb 5 21:05:56 2006](#)

Habiendo visto los Logs de ver0k y de Johnatan, una pregunta me viene a la mente. ¿Qué no cuadra en estos Logs? Exacto. El desfase horario. En el Log de Johnatan hay exactamente una hora de diferencia entre las URL vistas y la creación de cuenta. Y en el Log de ver0k simplemente no cuadra, porque sabemos por el Visor de Sucesos que ver0k se conectó por primera vez a las 21:47:21 horas del 05 de Febrero del año 2006. Hay datos que me faltan por saber para encajar todas las piezas. Es hora de echar un vistazo a las direcciones IP.

## Localizando IP

---

Un poco de historia...

La dirección IP es el identificador de cada equipo (host) dentro de su red de redes. Cada equipo conectado a una red tiene una dirección IP asignada, la cual debe ser distinta a todas las demás direcciones que estén vigentes en ese momento en el conjunto de redes visibles por el equipo. En el caso de Internet, no puede haber dos ordenadores con 2 direcciones IP (públicas) iguales. Pero sí podríamos tener dos ordenadores con la misma dirección IP siempre y cuando pertenezcan a redes independientes entre sí (sin ningún camino posible que las comuniquen).

Las direcciones IP se clasifican en:

- ✚ Direcciones IP públicas. Son visibles en todo Internet. Un ordenador con una IP pública es accesible (visible) desde cualquier otro ordenador conectado a Internet. Para conectarse a Internet es necesario tener una dirección IP pública.
- ✚ Direcciones IP privadas (reservadas). Son visibles únicamente por otros equipos de su propia red o de otras redes privadas interconectadas por routers. Se utilizan en las empresas para los equipos internos. Los ordenadores con direcciones IP privadas pueden salir a Internet por medio de un router o Proxy que tenga una IP pública.

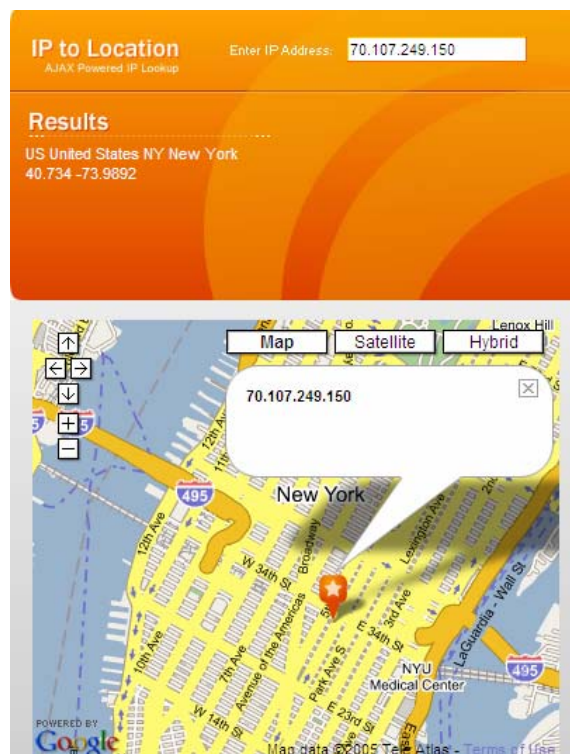
A su vez, las direcciones IP pueden ser:

- ✚ Direcciones IP estáticas (fijas). Un equipo que se conecte a la red con dirección IP estática siempre lo hará con una misma IP. Las direcciones IP públicas estáticas son las que utilizan los servidores de Internet con objeto de que estén siempre localizables por los usuarios de Internet. Estas direcciones hay que contratarlas.
- ✚ Direcciones IP dinámicas. Un equipo que se conecte a la red mediante dirección IP dinámica, cada vez lo hará con una dirección IP distinta. Las direcciones IP públicas dinámicas son las que se utilizan en las conexiones a Internet mediante un módem, cable módem, router, etc. Los proveedores de Internet utilizan direcciones IP dinámicas debido a que suelen tener más clientes que direcciones IP.

Las direcciones IP están formadas por 4 bytes (32 bits). Se suelen representar de la forma a.b.c.d donde cada una de estas letras es un número comprendido entre el 0 y el 255.

Bien, ahora que sabemos más o menos qué es una dirección IP, vamos a localizarlas!

Ambas direcciones IP (70.107.249.155 y 70.107.249.150) corresponden al proveedor de servicios de Internet (ISP) Verizon Internet Services. De los 5 servicios de localización de IP que he probado, 2 de ellos me han localizado las IP en la ciudad de New York, y los otros 3 en la ciudad de Virginia, también en Estados Unidos.



<http://www.seomoz.org/ip2loc/ip2loc.php>



[Visual IP Trace Report](#)

Un localizador de IP no revela la posición geográfica del atacante, sino la de su dirección IP (o donde estaba su IP en ese momento). También cabe señalar que las bases de datos en las que se basan los localizadores de IP sean incorrectas o no estén actualizadas, ya que las direcciones dinámicas cambian cada cierto tiempo de "dueño".

Intuyo por los Log del Administrador en Internet Explorer y Firefox, que la máquina servidora (Windows 2003) posiblemente estuviese ubicada en algún lugar de México, ya que muchas de las páginas, inclusive la de Google, están bajo dominio Mexicano (com.mx). Si adelantamos ese reloj una hora exacta, nos daría la hora de algún lugar del este de Estados Unidos, llámese Nueva York o Virginia.

Esto puede deberse a que el sistema haya registrado la hora de la máquina del sospechoso en vez de la local, o que el sospechoso haya modificado ficheros, lo cual dudo, dado el "poco" tiempo que estuvo conectado a la máquina.

## El agujero de seguridad

---

Llevo un rato pensando en esta entrada del Index.dat de Johnatan:

URLindex.datVisited: [Johnatan@http://70.107.249.150/clientes.wmf](http://70.107.249.150/clientes.wmf)  
index.datSun Feb 5 20:41:30 2006

Así que voy a informarme de qué es un archivo con extensión wmf, porque se me está escapando algo y no sé que es.

Una imagen de metarchivos de Windows (WMF) es un formato de metarchivos de 16 bits que puede contener tanto información vectorial como información del mapa de bits. Está optimizada para el sistema operativo Windows.

Lo primero que hago es informarme de cuáles son las actualizaciones de seguridad de Microsoft para el mes de Febrero, y voilá! Aparece un parche para una vulnerabilidad crítica en el motor de proceso de gráficos (<http://www.microsoft.com/spain/technet/seguridad/boletines/ms06-001-it.mspx>), la cual **no** ha sido parcheada por el Administrador. A día 06 de Enero del año 2006 ya había parche para la vulnerabilidad.

En la tabla siguiente se muestra la gravedad de esta vulnerabilidad, considerada como crítica.

Identificadores de vulnerabilidad	Consecuencia de la vulnerabilidad	Windows 98, Windows 98 SE y Windows ME	Windows 2000	Windows XP Service Pack 1	Windows XP Service Pack 2	Windows Server 2003	Windows Server 2003 Service Pack 1
Vulnerabilidad del motor de proceso de gráficos <a href="#">(CVE-2005-4560)</a> :	Ejecución remota de código	No crítica	Crítica	Crítica	Crítica	Crítica	Crítica

El resumen ejecutivo de esta vulnerabilidad es el siguiente:

“Si un usuario inicia sesión con derechos de usuario administrativos, un intruso que aprovechara esta vulnerabilidad podría lograr el control completo de un sistema afectado. De esta forma, un intruso podría instalar programas; ver, cambiar o eliminar datos; o crear cuentas nuevas con todos los derechos de usuario. Por tanto, los usuarios cuyas cuentas estén configuradas con pocos derechos de usuario en el sistema correrían un riesgo menor que aquellos que cuenten con derechos de usuario administrativos.”

El ataque se produce momentos después de que Johnatan ingresase con el navegador Internet Explorer la URL <http://70.107.249.150/clientes.wmf>, podemos deducir que la intrusión se realizó a través de una vulnerabilidad en el motor de proceso de gráficos de Windows.

Al ingresar en la citada URL, ésta creó una imagen maliciosa, tal y como muestra la siguiente entrada en el Log del Index.dat de Johnatan. La URL:

<http://70.107.249.150:8080/GPlw9OgYR6/uSvcCeC1V18W/bfKJ0KMsfYBZnaFKx6dZs/FHBwenHfCEt6do1Z/e9zhOEMQ052zYwSU50i/AUWWckI2mU/LQ9CIubslAJKla2jdYtSFExez4sRyL.tiff>

El caso que nos ocupa se ve agravado por el hecho de que el navegador Internet Explorer se estaba ejecutando con permisos de Administrador, por lo que se podría haber realizado cualquier acción sobre la máquina. También se ve agravado por el hecho de que el equipo no tenía ningún cliente antivirus instalado en el momento de la ejecución del exploit. Esto unido al alto nivel de privilegios (cuenta bajo grupo de Administradores) que tenía Johnatan en el momento del ataque, hizo que ver0k no tuviese ningún impedimento o problema en entrar en el equipo. Tan sólo les faltó invitar a ver0k a un cafecito y un puro☺.

Una buena medida de seguridad (aparte del antivirus☺) hubiese sido que cualquier servicio y/o aplicación que se ejecutase en la máquina, lo hiciese bajo una cuenta con privilegios mínimos. En el caso de que no fuese posible, se “blindaría” lo máximo el servicio y/o aplicación.

Todos los detalles de esta vulnerabilidad se encuentran en las siguientes URL:

<http://www.microsoft.com/spain/technet/seguridad/boletines/ms06-001-it.msp>

<http://www.vsantivirus.com/faq-wmf-exploit.htm>

<http://www.kb.cert.org/vuls/id/181038>

Cualquier aplicación que muestre una imagen con formato WMF causará que la máquina del usuario se infecte, esto incluye al Windows Explorer (viendo una imagen infectada que esté en el HD), Internet Explorer (automáticamente visitando una Web que contenga una imagen de este tipo), Firefox (en versiones antiguas es vulnerable porque abre los archivos WMF por defecto con el "Windows Picture and Fax Viewer". La versión 1.5 abre estos archivos por defecto con el Windows Media Player, que no es vulnerable, aunque no muestra la imagen), Opera (8.51 y posiblemente inferiores, es vulnerable porque abre los WMF con el "Windows Picture and Fax Viewer"), aunque tanto el Firefox como Opera preguntan al usuario antes de mostrar la imagen. En el enlace siguiente hay una prueba de concepto (vídeo) que explica la vulnerabilidad.

<http://www.websensesecuritylabs.com/images/alerts/wmf-movie.wmv>

Hay varios exploits que explotan esta vulnerabilidad, así que no se sabe a ciencia cierta qué exploit pudo utilizar ver0k, pero por el formato de la imagen tiff malformada, puedo sospechar que se trata de este [exploit](#), publicado por [FIRST](#), bastante más avanzado que los anteriores, ya que este exploit crea el código de la imagen distinto cada vez, lo que hace que sea mucho más difícil de detectar por los antivirus.

---

## Resumen Final. Datos varios y ejemplo de reporte de ataque

---

Como conclusión resumiré brevemente todo lo que hemos visto en el presente documento:



### Intrusión

La intrusión se llevó a cabo gracias a un bug en el motor de proceso de gráficos de Windows. La intrusión se aprovechó de un defecto de una función que ya es obsoleta, y se conserva sólo por compatibilidad con las versiones de 16 bit de Windows. En concreto, es la secuencia de escape GDI llamada SETABORTPROC, la que el exploit utiliza para ejecutar código de forma arbitraria cuando un archivo WMF es visualizado. Otras funciones similares también podrían ser explotadas.

### Resultados

El resultado del análisis indica que ver0k pudo haber sustraído los ficheros users.txt y clientes.txt, ficheros que actualmente no se encuentran en la imagen analizada (windows2003.img). Estos datos habría que contrastarlos con el Administrador del sistema, a fin de que desvelase estos últimos datos.

### Datos del atacante

 70.107.249.150	Dirección desde la que se inició el ataque
 70.107.249.155	Conexión por Escritorio Remoto o Terminal Service

### Direcciones de Correo

 [h4cklll@hotmail.com](mailto:h4cklll@hotmail.com)

### Cuenta de usuario creada

Ver0k

---

## Datos del ISP

OrgName: Verizon Internet Services Inc.  
OrgID: VRIS  
Address: 1880 Campus Commons Dr  
City: Reston  
StateProv: VA  
PostalCode: 20191  
Country: US

NetRange: 70.104.0.0 - 70.111.255.255  
CIDR: 70.104.0.0/13  
NetName: VIS-70-104  
NetHandle: NET-70-104-0-0-1  
Parent: NET-70-0-0-0-0  
NetType: Direct Allocation  
NameServer: NS1.BELLATLANTIC.NET  
NameServer: NS2.BELLATLANTIC.NET  
NameServer: NS2.VERIZON.NET  
NameServer: NS4.VERIZON.NET  
Comment: Please send all abuse reports to [abuse@verizon.net](mailto:abuse@verizon.net).  
Comment: DO NOT send e-mail to DIA.ADMIN@verizon.com as it will not be answered.  
RegDate: 2004-09-21  
Updated: 2005-04-21

OrgAbuseHandle: VISAB-ARIN  
OrgAbuseName: VIS Abuse  
OrgAbusePhone: +1-214-513-6711  
OrgAbuseEmail: [abuse@verizon.net](mailto:abuse@verizon.net)

OrgTechHandle: ZV20-ARIN  
OrgTechName: Verizon Internet Services  
OrgTechPhone: +1-703-295-4583  
OrgTechEmail: [IPNMC@gnilink.net](mailto:IPNMC@gnilink.net)

---

## Ejemplo de E-mail al ISP reportando el ataque

To: [abuse.verizon.net](mailto:abuse.verizon.net)

A quien corresponda:

El día 05 de Febrero del año 2006 se registró en el visor de sucesos de un servidor Windows 2003 R2 de nuestra propiedad una intrusión en nuestros sistemas. Un análisis cuidadoso de los sistemas implicados revela que el ataque e intrusión a nuestros sistemas procedían de direcciones IP pertenecientes a su compañía.

Las direcciones IP y las fechas mencionados en nuestro informe son las siguientes:

Hora	Dirección IP
21:44:10	70.107.249.150
21:47:21	70.107.249.155

Hora local de la máquina:

Esto es necesario para ayudar al ISP a identificar y ubicar al usuario de la dirección IP a la hora del ataque.

Le pedimos por favor tomen las medidas administrativas y/o legales adecuadas y apropiadas para evitar, en el futuro, y en la medida de lo posible, futuros ataques. Si necesitan cualquier aclaración o información adicionales, no duden en contactar con nosotros a través de los contactos que abajo se mencionan.

Teléfono de la compañía:

E-mail de la compañía:

Agradeciendo su atención y cooperación, se despide atentamente, bla, bla, bla...

---

## Recomendaciones

---

Una máquina no es, ni nunca será, 100% invulnerable. Las máquinas, aplicaciones y hardware están fabricadas por personas, y como todos sabemos, el único ser que conocemos a día de hoy que tropieza dos veces con la misma piedra es el ser humano. A día de hoy el virus más mortífero que conocemos todavía no tiene solución, y los estudios indican que nunca podremos parchear esta vulnerabilidad. El virus en cuestión es el usuario final, es decir, la persona que utilice el ordenador. Aún sabiendo este dato☺, las recomendaciones son las siguientes:

1. El equipo mantendrá una política de actualización constante del sistema en materia de seguridad, atendiendo primero a los parches críticos del sistema, y comprobar con rigurosa exhaustividad si las vulnerabilidades afectan a nuestras máquinas. Para lograr este objetivo disponemos en Internet de listas de correo y páginas Web que nos facilitan muy mucho la labor.
2. Ejecutar los servicios y aplicaciones con privilegios mínimos. En el caso que nos ocupa, la vulnerabilidad aprovechó que el usuario (Johnatan) ejecutó el navegador Internet Explorer con permisos administrativos, lo que facilitó en gran parte al atacante para que pudiese cometer la intrusión.
3. No ejecutar aplicaciones ni servicios que no sean estrictamente necesarios. Como ejemplo destaco que el servidor COUNTERS tenía entre otros el servicio Remote Registry (Registro Remoto) activado y en modo automático, lo que permitiría a usuarios remotos modificar el registro de la máquina.
4. Utilizar el servidor para trabajos exclusivamente de servidor. El correo vía Web se puede visualizar a través de otro equipo que no sea un servidor.
5. Disponer de al menos un Firewall que controle los accesos a la máquina y un antivirus actualizado. Estas herramientas nos ayudarán a tener un control más explícito sobre la máquina y evadiremos un gran porcentaje de ataques.
6. Disponer de huellas digitales para los archivos más importantes del sistema. Nos permitirán conocer si los archivos se han modificado.
7. Revisar periódicamente los ficheros Log de nuestro sistema, e investigaremos y perseguiremos cualquier acto sospechoso en el sistema. Estos ficheros se podrían centralizar en otra máquina "espejo", la cual permitiría analizarlos, en el caso de que se hubiesen borrado de la máquina atacada.

8. Todas las comunicaciones y aplicaciones que requieran contraseñas, se deben cifrar en la medida de lo posible, utilizando herramientas (programas) destinados a ello.
9. Seguridad proactiva: escanear periódicamente nuestra máquina con un escaner de vulnerabilidades ( [www.nessus.org](http://www.nessus.org)) o (MBSA) e instalar un IDS ([www.snort.org](http://www.snort.org)), para poder interpretar algún posible ataque.

La recomendación final es el formateo e instalación del servidor desde cero. Cambiar la política de seguridad y la política de contraseñas. En la máquina servidora, debe de haber sólo un usuario con permisos Administrativos. Los demás usuarios permanecerán en grupos inferiores, tales como Usuarios o Usuarios Avanzados. Por ejemplo se podría renombrar la cuenta Administrador a una cuenta sin privilegios. Con esto conseguiríamos despistar a más de un atacante que quisiese asaltar esta cuenta tan golosa.

Se denegará el acceso al servidor y a sus recursos a cualquier usuario anónimo. La implementación en Windows 2003 es bastante fácil. Basta con crear un valor REG\_DWORD en esta clave de registro:

HKLM\SYSTEM\CurrentControlSet\Control\Lsa

Crearemos un valor llamado RestrictAnonymous, al cual le pondremos como valor "2", sin las comillas.

Los usuarios que tengan acceso físico al servidor y debidamente autenticados, sólo tendrán acceso a ficheros y directorios que dependan exclusivamente de su trabajo, excluyendo ficheros, directorios y aplicaciones que **no** tengan que ver con su labor.

También se procederá a instalar un Firewall que monitorice los controles de acceso y un buen antivirus actualizado. El servidor que nos ocupa tenía activado el Firewall de Windows, pero carecía de antivirus.

Podríamos también "ocultar" el servidor del explorador de Windows con una sencilla entrada en el registro de Windows:

HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\LanManServer\Parameters

Crearemos un valor DWORD llamado "HIDDEN", sin las comillas, y le asignaremos el valor 1. Reiniciaremos el equipo y listo. La máquina no se verá en el explorador de Windows ni en "Mis sitios de Red", pero podremos conectarnos a ella sin problemas. Con esto conseguiremos "despistar" a más de uno que quisiese atacarnos.

Utilizar un comprobador de integridad de archivos y directorios como Tripwire. Es una herramienta que ofrece gran ayuda a administradores de sistemas monitoreando posibles modificaciones en algún set de archivos. Si se usa regularmente en los archivos de sistema (por ej. diariamente), Tripwire puede notificar a los administradores del sistema, si algún archivo fue modificado o reemplazado, y así tomar medidas de control de daños a tiempo. Todas estas implementaciones y muchas más se encuentran detalladas en los manuales de referencia citados en el apartado Referencias.

## Conclusión Final

---

Aunque, en principio, parezca que todo está perdido, no hay que desesperarse, porque como decía el Principio de Locard: "Cada contacto deja un rastro".

El análisis que se ha expuesto en este informe relata una serie de actividades con un orden secuencial. La realidad es que no es la línea que seguí desde un principio. Durante el curso de la investigación se dieron con nuevos hallazgos que me permitieron llegar a donde estoy ahora. En principio pensé que el ataque se pudo deber a un bug en Apache, o en el sistema ERP que habían utilizado (<http://www.weberp.org/>). Se analizaron los Logs de Apache, los cuales llevaron a un callejón sin salida. Había indicios de ataques provenientes de la dirección IP 84.18.17.15, a través del scanner de vulnerabilidades NESSUS, tal y como indican varios campos del fichero access.log de Apache. Una muestra de ejemplo es esta (84.18.17.15 - - [04/Feb/2006:14:22:29 -0800] "GET /cgi-bin/quickstore.cgi?nessus&template=../../../../../../../../../../../../etc/passwd%00html HTTP/1.1" 404 294), o esta otra (84.18.17.15 - - [04/Feb/2006:14:22:29 -0800] "GET /scripts/quickstore.cgi?nessus&template=../../../../../../../../../../../../etc/passwd%00html HTTP/1.1" 404 294). También se registró varios intentos de DOS (Denial of Service) proveniente de la misma dirección IP. Después las pistas me llevaban a que posiblemente hubiese sido un ataque desde el interior, pues en principio parecía tener toda la pinta. Se hicieron anotaciones, se borraron anotaciones, se corrigieron anotaciones, se miraron archivos y se buscaron pistas, y se llegó a una conclusión. Como dije antes y repito ahora, estos datos se deberían cotejar con los datos del Administrador del Sistema, a fin de verificar o corregir este informe. Este documento pretende dar una "visión" de lo que ocurrió en la máquina. Decir tiene que cualquier parecido con la realidad es pura ficción, y que no se "maltrató" a ningún Windows para llegar a estas conclusiones. Tan sólo lo "volvimos loco" un poquito☺. La única que murió fue una quemadora de CD que se "inmoló" mientras miraba unos registros...

Agradezco a todas aquellas personas que ponen a disposición del público sus hallazgos, manuales y explicaciones, todo lo que he aprendido.

Espero que lo disfrutéis leyéndolo, porque como se diría en mi tierra, yo lo he flipado en colores☺.

## Referencias

---

[The Services and Service Accounts Security Planning Guide](#) (Microsoft)

[The Security Risk Management Guide](#) (Microsoft)

[The Security Monitoring and Attack Detection Planning Guide](#) (Microsoft)

[Apuntes Varios](#) (Servidor☺)

[Microsoft Knowledge Base](#) (Base de Datos Microsoft)

---

## Curiosidades

---

En este apartado relataré ciertos aspectos que cuanto menos, son bastante curiosos desde mi punto de vista.

Una de las primeras cosas que miré fue si el equipo COUNTERS disponía de algún tipo de solución de antivirus. Cual fue mi sorpresa al averiguar que no disponía de tal solución. Así que lo siguiente que hice fue scanear el equipo en busca de virus, rootkits, restos de exploits, spyware, malware, etc...

Lo cierto es que no encontré gran cosa en el equipo. No había ningún tipo de "bicho activo" en el equipo. Lo que si que encontré fueron restos de cookies catalogadas como Spyware, ya que podían contener datos relativos al usuario o máquina, un resto de un instalador de Spyaxe (un conocido troyano catalogado como Spyware) en los archivos temporales de la cuenta Administrador(carpeta `~nsu.tmp`), y un troyano embebido en un archivo rar, también en la cuenta de Administrador(explorer.exe).

Los datos de inicio de sesión que me arrojó la aplicación NTLAST son los siguientes:

### Últimos inicios de sesión correctos en la máquina

```
C:\>ntlast -s -null -file SecEvent.Evt
```

Administrator	COUNTERS	COUNTERS	Sun Feb 05 11:29:16pm 2006
Administrator	COUNTERS	COUNTERS	Sun Feb 05 11:26:57pm 2006
verOk	COUNTERS	COUNTERS	Sun Feb 05 09:47:21pm 2006
Johnatan	COUNTERS	COUNTERS	Sun Feb 05 09:23:09pm 2006
Administrator	COUNTERS	COUNTERS	Sun Feb 05 09:04:49pm 2006
Administrator	COUNTERS	COUNTERS	Sun Feb 05 08:49:22pm 2006
Administrator	COUNTERS	COUNTERS	Sun Feb 05 12:11:54am 2006
Administrator	COUNTERS	COUNTERS	Sun Feb 05 12:10:09am 2006
postgres	COUNTERS	COUNTERS	Sat Feb 04 11:46:49pm 2006
postgres	COUNTERS	COUNTERS	Sat Feb 04 11:46:30pm 2006

### Últimos inicios de sesión fallidos en la máquina

```
C:\>ntlast -f -null -file SecEvent.Evt
```

adminstrator	COUNTERS	COUNTERS	Sun Feb 05 11:29:01pm 2006
mpenelope	COUNTERS	COUNTERS	Sun Feb 05 12:10:54am 2006
mpenelope	COUNTERS	COUNTERS	Sun Feb 05 12:10:52am 2006
mpenelope	COUNTERS	COUNTERS	Sun Feb 05 12:10:49am 2006
mpenelope	COUNTERS	COUNTERS	Sun Feb 05 12:10:48am 2006
mpenelope	COUNTERS	COUNTERS	Sun Feb 05 12:10:45am 2006
mpenelope	COUNTERS	COUNTERS	Sun Feb 05 12:10:43am 2006
mpenelope	COUNTERS	COUNTERS	Sun Feb 05 12:10:42am 2006
mpenelope	COUNTERS	COUNTERS	Sun Feb 05 12:10:40am 2006
mpenelope	COUNTERS	COUNTERS	Sun Feb 05 12:10:37am 2006

### Últimos inicios de sesión interactivos en la máquina

C:\>ntlast -i -null -file SecEvent.Evt

Administrator	COUNTERS	COUNTERS	Sun Feb 05 11:29:16pm 2006
Administrator	COUNTERS	COUNTERS	Sun Feb 05 11:26:57pm 2006
Johnatan	COUNTERS	COUNTERS	Sun Feb 05 09:23:09pm 2006
postgres	COUNTERS	COUNTERS	Sat Feb 04 11:46:30pm 2006
Administrator	COUNTERS	COUNTERS	Sat Feb 04 10:17:13pm 2006
Administrator	COUNTERS	COUNTERS	Sat Feb 04 04:34:09am 2006
Administrator	COUNTERS	COUNTERS	Sat Feb 04 03:26:06am 2006
maick	COUNTERS	COUNTERS	Sat Feb 04 03:11:04am 2006
Johnatan	COUNTERS	COUNTERS	Sat Feb 04 03:07:40am 2006
Administrador	COUNTERS	COUNTERS	Sat Feb 04 02:41:30am 2006

### Últimos inicios interactivos de sesión fallidos en la máquina

C:\>ntlast -f -i -file SecEvent.Evt

adminstrator	COUNTERS	COUNTERS	Sun Feb 05 11:29:01pm 2006
administrador	COUNTERS	COUNTERS	Fri Feb 03 03:27:15am 2006
administrador	COUNTERS	COUNTERS	Wed Feb 01 07:32:21pm 2006
administrador	COUNTERS	COUNTERS	Wed Feb 01 07:32:19pm 2006
administrador	COUNTERS	COUNTERS	Wed Feb 01 07:32:17pm 2006

Otra curiosidad que cabe destacar bajo mi punto de vista, es la “supuesta” identidad del atacante en cuestión.

La verdad es que un golpe de suerte, un golpe de lógica, o una casualidad del destino me llevó a estos datos.

En el archivo Index.dat de Internet Explorer de ver0k, aparecen unas URL que ver0k estuvo “bicheando” mientras estuvo dentro del sistema. Estas URL fueron las siguientes:

- ✚ <http://www.atdmt.com> (Agencia de Marketing y publicidad)
- ✚ <http://msn.com> (Esta no la conozco...☺)
- ✚ <http://img.wmp10.elsitiodc.com> (Distribuidora de contenidos de entretenimiento)
- ✚ <http://www.huevocartoon.com/animaciones/index.asp> (Ni idea☺)
- ✚ [http://g.msn.com/5mees\\_mx/162](http://g.msn.com/5mees_mx/162) (No la conozco! ☺)

Bien. Lo primero que hice fue entrar en las dos únicas URL que no me sonaban de nada, las cuales son atdmt.com y elsitiodc.com. La primera es una agencia de Marketing y publicidad, y no pude sacar nada de información al respecto. Con la segunda la cosa cambia radicalmente.

Al ingresar en la dirección elsitiodc.com me encuentro con que es una página que provee y distribuye contenidos de entretenimiento. Estuve hojeándola un buen rato, preguntándome por qué visitó esa página. En el portfolio de la página aparecen las páginas Web sobre las que ellos trabajan directamente, y ni corto ni perezoso, pincho en una cualquiera. Más concretamente en esta dirección: [http://www.elsitio.com/mx/home/home\\_mx.html](http://www.elsitio.com/mx/home/home_mx.html). Muestra una página que nos ofrece bastantes servicios, entre los que se encuentran una sala de Chat, búsqueda del amor eterno, servicios de astrología, etc.... Pero lo que más me llama la atención es el apartado que pone [Regístrate Gratis Ya](#). Al tocar con mi ratón ese vínculo, me aparece una inocente ventana de registro de usuarios. Así que intenté registrarme con el nombre de usuario “verok”. Pero claro, una vez rellenos los datos, la Web me dijo que el usuario ya existía. Así que intenté otra cosita. Intentar modificar los datos del usuario “verok”. El nombre de usuario lo sé, es “verok”, pero, y la contraseña? A ver, no creo que sea tan fácil como poner de password el nombre de usuario, pero bueno, por probar que no quede... Usuario: verok, Clave: verok, y voilà!

The screenshot shows a Microsoft Internet Explorer browser window displaying a registration form for 'El Sitio'. The browser's address bar shows the URL 'http://www.elsitio.com/scripts/tupase/form\_update.php3'. The page title is 'Registro - Microsoft Internet Explorer'. The form is titled 'Tu Pase Modificar mis datos' and includes a 'Contrato de confidencialidad' section with a note that asterisks (\*) denote mandatory fields. The form fields are filled with the following information:

Field	Value
*Nombre	Veronica
*Apellido	Santana
*Fecha de Nacimiento	12 Febrero 1970
*Sexo	<input checked="" type="radio"/> Fem. <input type="radio"/> Masc.
*País de residencia	Mexico
*Provincia/Estado	Aguascalientes
*Ciudad/Localidad	Jardin Balbuena
Dirección	unidad 1 No. 234
Cod. Postal	15900
Teléfono	55714615
Profesión	[Seleccionar]
*Cuenta de mail actual	vsantana@correoweb.c

Below the form, there is a note: '(Si no tienes dirección de correo, coloca el nombre que ingresaste en el campo Usuario, seguido de @elsitio.com, Ej: nombreusuario@elsitio.com)'. A section titled 'Contesta estas preguntas y conviértete en usuario registrado de El Sitio' contains the following questions and answers:

Question	Answer
*Desde donde se conecta?	Trabajo
*Comparto la PC	<input checked="" type="radio"/> Si <input type="radio"/> No
*Si quiero recibir novedades de El Sitio.	<input checked="" type="checkbox"/>
Si quiero recibir novedades de los anunciantes y ofertas comerciales.	<input type="checkbox"/>

Los datos de una tal Verónica Santana aparecen en pantalla. Será nuestro malhechor (malhechora en este caso...)? Lo sabremos en el próximo capítulo....

Me despido con una frase que decía el genial Hannibal Smith fumando su puro habano, en esa entrañable serie, El equipo A.

“Me encanta que los planes salgan bien...”

Muchas Gracias