

Respuesta al

Reto de Análisis Forense



Resumen ejecutivo

Marzo de 2006

Germán Martín Boizas

Introducción

Este documento es el resumen ejecutivo en respuesta al reto de análisis forense lanzado por UNAM-CERT y RedIRIS en colaboración con otras empresas en Febrero de 2006 a través de su página web

<http://www.seguridad.unam.mx/eventos/reto/>

El objetivo del mismo es el análisis de un sistema Windows 2003 previamente atacado y comprometido. Para ello, como única información, se proporciona una imagen (o copia) de dicho sistema.

Análisis

Para la realización del análisis se procedió a la instalación de un entorno de trabajo en el que, de forma segura y garantizando el no modificar la evidencia, proceder a la ejecución de las herramientas de análisis forense seleccionadas, la mayoría de carácter público y accesibles en la red.

El detalle del trabajo técnico realizado se describe en el informe técnico, si bien es interesante resaltar la cantidad de tiempo empleado en el mismo (un mínimo de 5 jornadas/hombre de trabajo). Esto demuestra que, aunque muchas veces los hackers justifican sus acciones diciendo que en realidad no hacen daño al sistema, las horas de trabajo perdidas únicamente en analizar que esto es verdad producen un daño económico importante.

Sumario del incidente

Tras el análisis de la evidencia aportada, podemos resumir este incidente de seguridad en los siguientes puntos:

- El sistema atacado es un Windows 2003 Server SP1, con licencia de evaluación de 14 días, de nombre COUNTERS.
- Dicho sistema fue instalado y conectado a la red el 25 de enero de 2006.
- El 26 de enero se instalaron en el sistema algunas aplicaciones, destacando entre ellas el sistema ERP de código abierto 'webERP' (www.weberp.org) que a su vez emplea el servidor web Apache y la base de datos MySQL.
- Desde dicha fecha hasta el 5 de febrero, el sistema mantuvo una actividad que puede considerarse como normal, incluyendo algunos intentos de ataque al servidor web sin mayores consecuencias, la instalación de alguna nueva aplicación como PostGreSQL, y la copia de múltiples ficheros de Microsoft Word, Powerpoint, Excel, documentos PDF e imágenes pornográficas en formato JPEG por parte de algún usuario.
- El 5 de febrero, un atacante logró acceso con privilegios de administración al sistema. Para ello, empleó métodos de ingeniería social, enviando un correo a un usuario del sistema con privilegios de administrador (Johnatan) a su cuenta en yahoo.com, incitándole a acceder con su navegador a una URL en la que el atacante tenía preparada un exploit.
- Dicho exploit consistía en aprovechar una vulnerabilidad recientemente descubierta en la librería GDI (Graphics Device Interface) existente en varias

versiones de Windows, y entre ellas 2003 server (ver boletín de Microsoft en <http://www.microsoft.com/technet/security/bulletin/ms06-001.msp>) ; esta librería se emplea para la generación y presentación de gráficos en el sistema, y el exploit se ejecutó al acceder a un fichero gráfico Windows Metafile (WMF) que no era tal sino que en realidad cargó un código que abrió una línea de comando al atacante sin que el usuario víctima del engaño se diera cuenta.

- A continuación, y una vez lograda una ventana como administrador, de forma inmediata el atacante procedió a crear una cuenta de nombre 'verOk', dotándola de privilegios de administración, y a modificar el sistema para permitir el acceso remoto al mismo.
- Accediendo con Terminal remoto y con la cuenta recién creada, el atacante accedió a la base de datos de la aplicación WebERP, mediante el interfaz de administración de MySQL y extrajo directamente de las tablas la información disponible sobre clientes y sobre cuentas de usuario. Esta información fue enviada al exterior mediante MSN Messenger a la cuenta *hackIII-2@hotmail.com*.
- Posteriormente el atacante procedió a buscar y visualizar los diferentes ficheros existentes bajo C:\Documents and Settings, incluyendo imágenes en formato JPEG, algún video, y con especial atención archivos en formato .DOC. No pudo visualizar ficheros Excel, aunque lo intentó, por cuanto esta aplicación no estaba instalada en el sistema. Ficheros en otros formatos (Powerpoint ó PDF) no fueron accedidos.
- Finalmente, procedió a determinar cómo acceder a la aplicación 'WebERP' para desde ella crear una nueva cuenta de usuario de la propia aplicación (de nombre 'admin' y privilegios de administración de la misma) que le permitiera el acceso a la aplicación en el futuro, para después abandonar el sistema.
- Los reponsables del sistema COUNTERS determinaron de forma muy rápida la presencia de algún intruso en el sistema, al detectar una cuenta no autorizada, y procediendo velozmente a intentar realizar una copia del disco, empleando para ello utilidades disponibles en el CD-ROM de F.I.R.E. (Forensics and Incident Response Environment Bootable CD, descargable en <http://fire.dmzs.com/>) o uno similar basado en éste. Después de bastantes intentos de copia con el sistema 'en vivo' al parecer infructuosos, procedieron a la parada final del sistema el 5 de Febrero de 2006 a las 15:44.

Principales Conclusiones del análisis

1. El ataque al sistema se realizó con una cierta planificación y con carácter específico hacia este sistema en particular. Esta conclusión está basada en los siguientes datos:
 - ▶ El correo enviado al usuario Johnatan a su cuenta para conseguir su colaboración indirecta está escrito en castellano, así como simula ser un contacto habitual del mismo (Alberto López, Director General de

- Electrónica y Computación S.A.). Además, es en un segundo correo cuando se produce la intrusión real.
- ▶ Una vez conseguido el acceso, y creado un usuario para su uso posterior, el atacante analiza muchos de los documentos existentes en el servidor.
 - ▶ Parece conocer bien que webERP es la principal aplicación del sistema, y es la que ataca. Otra base de datos instalada, PostGreSQL, no merece la más mínima atención del atacante.
 - ▶ No instala ningún tipo de herramienta de 'rootkit', o de 'hacking' en general como haría un atacante genérico que simplemente buscara nuevas bases de ataque.
 - ▶ Tras conseguir crear un usuario administrador en el aplicativo webERP, finaliza toda su actividad.
2. El ataque fue posible a pesar de que el sistema estaba, en general, bastante bien configurado y a un alto nivel de parcheo. Aunque es cierto que se utilizó una vulnerabilidad de reciente descubrimiento, fue el uso indebido del servidor para navegar de forma genérica por Internet, especialmente grave cuando el usuario empleado para ello tiene privilegios de administración, lo que posibilitó el ataque.
 3. El análisis del sistema ha podido ser muy detallado gracias a que el administrador del mismo se preocupó de configurar en un alto nivel de detalle el sistema de auditoría de Windows, lo que demuestra la importancia de estar preparado por anticipado ante un posible ataque.
 4. En general, da la impresión de que el sistema no era un sistema en producción real, sino un servidor preparado para generar una imagen que fuera posible usar en un reto de análisis forense. Esta conclusión está basada en los siguientes datos:
 - ▶ El sistema está instalado y en marcha con una licencia de evaluación de Windows 2003 Server, únicamente válida para 14 días, y a la que le quedaban únicamente 4 días para la activación final que nunca se produjo.
 - ▶ En el sistema están creados 16 cuentas de usuarios (además del administrador y el que crea el atacante) de las cuales únicamente se han empleado 4.
 - ▶ En el servidor se copiaron una gran cantidad de ficheros de Microsoft Excel, PowerPoint y Adobe PDF; sin embargo, ninguna de estas aplicaciones está instalada. Aunque podría pensarse que los ficheros podrían ser accedidos desde la red, no fue así en realidad tal y como revelan las fechas de creación y acceso.
 - ▶ La primera reacción de los administradores ante la creación final de las cuentas del atacante en webERP y en el sistema, es intentar generar de forma inmediata una imagen del sistema, más que analizar exactamente qué estaba ocurriendo, o detener/desconectar de la red el sistema para minimizar el daño.
 - ▶ Algunas de las cuentas de correo de 'clientes' almacenadas dentro de WebERP corresponden a dominios inexistentes en la realidad.

Solución al incidente

Como consecuencia del ataque, el sistema y la información en él contenida han quedado completamente comprometidas. Aunque se ha identificado el origen de la intrusión y el detalle de la actividad realizada, no podemos estar absolutamente seguros de que no haya otros cambios que han pasado desapercibidos a la investigación forense. Por tanto, para recuperarse de la intrusión y conseguir un sistema completamente seguro los pasos recomendables serían, si ello es posible:

- Reinstalar una versión limpia del sistema operativo, siempre sin estar conectado al exterior.
- Deshabilitar los servicios innecesarios.
- Instalar todos los hotfixes de seguridad.
- Consultar periódicamente las alertas de seguridad en este sistema operativo.
- Recuperar con cuidado datos de usuario de los backups y verificar los permisos (propietario, etc) de esos ficheros para que sólo los usuarios que lo necesiten puedan acceder a ellos.
- Cambiar todos los passwords y, sólo entonces, volver a conectarlo a la red externa.

Una guía detallada de cómo recuperar un sistema de una intrusión puede encontrarse bajo:

http://www.cert.org/tech_tips/win-UNIX-system_compromise.html

ó en <http://www.nohack.net/recovery.htm>

Alternativamente, como forma más rápida, si bien carente del 100% de fiabilidad, la recuperación de esta intrusión pasaría por, con el sistema desconectado de Internet:

- Eliminación de las cuentas creadas por el atacante.
- Cambiar todos los passwords tanto del sistema como de la aplicación webERP, y asegurar que dichos passwords cumplen unos estándares mínimos de seguridad.
- Instalación de los hotfixes de seguridad, especialmente los aplicables a la vulnerabilidad empleada en este ataque.
- Poner passwords para el acceso a MySQL Administrator.

Finalmente, el daño producido por la pérdida de confidencialidad en la información (usuarios y clientes de la base de datos) debe mitigarse mediante las acciones de comunicación, modificación y/o legales que los responsables de la empresa consideren oportuno teniendo en cuenta su situación comercial y los requerimientos legales que apliquen.

Recomendaciones finales

De cara a evitar posibles problemas similares a éste en el futuro, se recomiendan las siguientes acciones:

- Instalar de forma inmediata los hotfixes de seguridad de Microsoft, a ser posible de forma automática a través de Windows Update.
- Asegurar que se minimiza el número de cuentas con privilegios de administración existentes, siendo recomendable dejar sólo aquellas estrictamente necesarias.
- Instaurar una política que asegure que no se emplean servidores en producción para actividades personales como navegar por Internet, consultar el correo o jugar.
- Instalar algún sistema antivirus y antispyware, actualmente inexistente.
- Instalar algún programa de detección de intrusión y/o modificación de ficheros clave del sistema operativo.
- Formar a los usuarios en la importancia de la seguridad y la existencia de ataques de 'ingeniería social' ante los que deben estar preparados.
- Asegurar que todos los sistemas de administración (por ejemplo, MySQL) tienen palabras de acceso adecuadas para restringir su acceso.
- Guardar de forma cifrada la información de carácter confidencial, para minimizar la posibilidad de robo de la misma.
- Asegurar que existe en la organización un sistema de gestión operativa de la seguridad, que permita la prevención, detección y eficaz reacción a ataques, en particular debe existir un adecuado mecanismo de alerta.

Por último, comentar que durante la investigación se ha encontrado numerosa información correspondiente a correos de años anteriores (en concreto, la mayoría anteriores a 2004 y pertenecientes a la empresa eycsaa.com.mx, dedicada a la formación a través de internet). Para evitar que este tipo de información se de a conocer, es una buena práctica borrar completamente con una herramienta específica el contenido del disco antes de reinstalar el sistema operativo.