

**Título:** Informe Ejecutivo  
**Fecha:** 21/Mar/ 2006

Reto Forense V3.0  
UNAM-CERT/ IRIS CERT

**Reto de Análisis Forense V3.0**  
**UNAM – CERT / IRIS –CERT**

**Informe Ejecutivo**

Ing.-Juan Ángel Hurtado  
Monterrey N.L México

<b>1 INTRODUCCIÓN .....</b>	<b>3</b>
1.1 PRESENTACIÓN .....	3
<b>2 ACERCA DEL ATAQUE .....</b>	<b>3</b>
2.1 TIPO DE ATAQUE .....	3
2.2 COMO Y DESDE DONDE SE LLEVO A CABO EL ATAQUE.....	3
2.3 QUE HIZO EL ATACANTE UNA VEZ DENTRO DEL SISTEMA.....	4
2.4 RECOMENDACIONES AL ADMINISTRADOR.....	4
2.5 CONSIDERACIONES.....	5

## **1 Introducción**

### **1.1 Presentación**

El presente documento fue elaborado en atención a la convocatoria lanzada por UNAM-CERT/Red Iris para el tercer concurso hispano de Análisis Forense "Reto Forense Episodio III". El mismo describe desde un punto de vista no técnico las conclusiones a las que se llegaron a partir del análisis forense realizado sobre la imagen proporcionada por los organizadores para este fin.

La audiencia pretendida por este documento es en general personas como poco o nulo conocimientos técnicos. Se pretende además que este documento sirva como referencia para aquellas personas interesadas en el tema. La metodología usada, descrita de una forma muy breve, consistió en la preparación del laboratorio, identificación del sistema a examinar, extracción y documentación de evidencia, relación de hechos aislados, elaboración de hipótesis y conclusiones a partir de la evidencia colectada. Pasemos pues al tema que nos ocupa.

## **2 Acerca del ataque**

### **2.1 Tipo de ataque**

Por medio de un análisis forense aplicado a la imagen proporcionada, se encontró que la maquina había sido atacada de forma exitosa. El atacante se aprovecho de una vulnerabilidad existente en el sistema operativo para penetrar la maquina. Una vez dentro realizo una serie de actividades que modificaron el sistema y la aplicación que en el corría (Creo cuentas en ambos), existen motivos para pensar que también se robo la identidad del director de la empresa, ya que mediante engaños consiguió que el administrador del servidor ejecutara un exploit (Programa que sirve para aprovechar una vulnerabilidad) y tomar posesión del equipo. Detectamos indicios de los siguientes tipos de ataque, escaneos de vulnerabilidades, penetración del equipo, ingeniería social y probable robo de identidad.

### **2.2 Como y desde donde se llevo a cabo el ataque.**

El día 05 de Febrero de 2006 el servidor COUNTERS fue atacado aprovechando una vulnerabilidad existente en la versión de Windows que tenia instalada (Windows 2003) relacionada la forma en que se procesan los archivos WMF (Windows Meta File) y para la cual no tenia el parche de seguridad instalado

(Parche KB912919). El atacante instaló y ejecutó la herramienta Metasploit, (La cual levanta un servidor que escucha en el puerto 8080 y permite explotar la vulnerabilidad antes descrita cuando la víctima visita vía HTTP al servidor desde una máquina vulnerable) en la IP 70.107.249.150 desde la cual efectuó el ataque.

El atacante envió un correo electrónico desde la dirección alopez@eycsa.com.mx a la dirección de Yahoo del administrador [jonathan.tezca@yahoo.com](mailto:jonathan.tezca@yahoo.com) invitándolo con engaños (Ingeniería Social) a visitar la dirección desde la cual escuchaba el Metasploit <http://70.107.249.150:8080/clientes.wmf> . Un usuario se encontraba en ese momento dentro de la máquina, logueado con la cuenta Johnatan la cual tenía privilegios de administrador, este usuario que suponemos es el dueño de la cuenta checaba vía Web su correo de Yahoo desde el servidor, y accede a la dirección que le envió el atacante. Se produce exitosamente el exploit de la vulnerabilidad y el atacante recibe una terminal con privilegios de administrador

### **2.3 Que hizo el atacante una vez dentro del sistema.**

Encontramos que el atacante crea una nueva cuenta en el sistema operativo (La cuenta ver0k) la cual agrega también como Administrador. Ejecuta también el programa reg.exe, el cual le permite ver y modificar el registro de Windows, verifica la versión de Windows usando winver.exe . El servidor tenía el Terminal Services habilitado, a las 12:47 PST inicia conexión de la cuenta ver0k, el atacante inicia sesión muy probablemente a través del Terminal Services para ver0k (Ver anexo 2), a partir de ahí tiene acceso de modo gráfico al servidor con una cuenta con privilegios de administrador. El atacante ejecuta el Internet Explorer, el Outlook Express, intenta acceder al servidor de MySQL ejecutando el MySQLAdministrator, Utiliza el wordpad para ver el contenido del archivo config.php, a las 13:57 PST se conectó vía Web a la aplicación WebERP con la cuenta acontreras desde la misma máquina que ejecutó el ataque y creó el usuario admin.

### **2.4 Recomendaciones al administrador.**

En base a lo observado se recomienda al administrador observar los siguientes puntos:

- Mantener al día las actualizaciones del servidor. Aun que el menciona que este estaba actualizado, el parche de seguridad que corregía la vulnerabilidad de la que se aprovechó el atacante ya existía al momento de que sucedió el ataque, y este no estaba instalado.
- Dar de baja las cuentas que no son indispensables.
- Corregir o cambiar la versión de WebERP. En la versión más reciente descargada de la Web todavía se envía el password en texto claro. Quizás sea conveniente evaluar otro sistema de ERP.
- No utilizar el servidor para cosas que no sean estrictamente de trabajo.
- Cambiar los passwords de todos los usuarios del WebERP.

- Disminuir el número de administradores del WebERP.
- El manual del Apache debe ser removido, el dejar el manual instalado permite a los atacantes identificar de forma sencilla el Web Server. También el contenido de la carpeta cgi-bin.
- Mantener una estricta confidencialidad de la información crítica de la empresa.

## **2.5 Consideraciones.**

El ataque fue un ataque dirigido, el atacante conocía al administrador del servidor y tomó como blanco específicamente este servidor. Aunque el correo que envió el atacante venía a nombre del director de la empresa propietaria del servicio, resultaría un poco ilógico que sea el quien atacó un servidor que finalmente le pertenecía. Puede ser también que el atacante haya robado la identidad del Director de la empresa para enviar el correo. Puede suponerse que el ataque se efectuó bajo alguno de los siguientes escenarios:

- Abuso de confianza por uno o más empleados.
- Revancha de usuarios que hayan sido separados de la empresa.
- Espionaje industrial.
- Falta a la confidencialidad de información crítica por parte del administrador.

Entre otros, descubrir bajo que escenario se llevó a cabo, requeriría entrevistar a los presuntos implicados lo cual queda fuera del alcance de este análisis.