

Informe Reto Forense 3 - Resumen Ejecutivo -

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

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

Tabla de contenidos

<i>Motivos de la Intrusión</i>	3
<i>Desarrollo de la Intrusión</i>	3
<i>Resultados del análisis</i>	3
<i>Recomendaciones</i>	3

Motivos de la Intrusión

El motivo principal de la intrusión es el **robo de información**, ya que los primeros movimientos del atacante son para obtener la lista de Clientes y Usuarios del sistema Web-Erp.

Desarrollo de la Intrusión

Johnatan tras recibir un correo de una fuente “conocida” accedió a una dirección Web, la cual, aprovechando un fallo del sistema operativo (del que en ese momento aún no existía solución) consiguió crear un usuario en el sistema. Tras la creación, se accedió de forma remota al sistema desde Internet gracias a los servicios de Terminal que estaban activados en el servidor. Tras esto, el intruso obtuvo información del sistema ERP (lista de Clientes y Usuarios) y curioseó por los ficheros del servidor.

Resultados del análisis

El sistema ha sido comprometido el día: **05/02/2006,21:47:21** por una persona desde la dirección IP: **70.107.249.155 el proveedor de Internet está en Marina del Rey (California)**

El atacante ha aprovechado un fallo de seguridad del sistema operativo (Windows) aún sin parchear por Microsoft en la fecha del ataque.

Recomendaciones

- Reducir la superficie de exposición al riesgo configurando el firewall para que sólo pueda accederse desde el exterior a los puertos estrictamente necesarios. En este caso al puerto TCP-80 (Web) únicamente. Desconocemos si además del firewall que trae Windows la empresa dispone de un firewall para hacer esta tarea, posiblemente no. Una empresa que tenga servicios en Internet es altamente recomendable que disponga de uno. No es necesario realizar un gran gasto, hay distribuciones de Linux (extremadamente ligeras) que permiten hacerlo con un ordenador antiguo con pocos recursos y los proveedores de ADSL proveen de routers que pueden realizar también esta funcionalidad. Si por algún motivo no es posible poner un firewall, el servidor que está en Internet deberá tener desactivados todos los servicios posibles, esto incluye, NETBIOS (UDP 138, TCP 139 y TCP 445) y Escritorio remoto (3389).
- Restringir los privilegios administrativos de los usuarios al mínimo (y si es posible eliminarlos por completo). Uno de los motivos por los que la intrusión ha tenido éxito es porque un usuario del sistema tenía derechos administrativos sobre el dominio.

- Procurar sólo realizar tareas de administración en los servidores. Y en ningún caso permitir que usuarios accedan localmente al sistema para realizar su trabajo diario.
- Suscripción a boletines de seguridad de fabricantes (y expertos en seguridad) para estar al tanto de los fallos que van apareciendo y poder así llevar una Política de actualización de parches de seguridad. Cada fabricante marca una política de actualizaciones de seguridad (Microsoft por ejemplo, el segundo martes de cada mes es el día que elige para sacar las actualizaciones de seguridad a no ser que sean críticas, que pueden salir en cualquier momento)
- Revisar el sistema (sobre todo la parte Web pública) en busca de ficheros temporales (.bak, .old, etc) y eliminarlos ya que pueden dar mucha información a un atacante.
- Revisión de contraseñas de los usuarios. Dado que en el sistema han accedido, es obligatorio el cambiar todas las contraseñas, tanto del web-erp (imprescindible) como de los usuarios del Dominio. Y por supuesto eliminar el usuario "ver0k".
- Disponer de Antivirus y tenerlo actualizado. Se ha detectado en el sistema un posible virus, el servidor no dispone de antivirus (desconocemos si en los puestos de trabajo existe o no). En cualquier caso se recomienda en ambas partes tanto en el servidor como en los puestos de trabajo.
- Activación de logs en el sistema. En este caso el administrador con muy buen criterio los ha activado (al menos unos cuantos eventos), permitiéndonos así conocer algunos detalles del alcance del ataque. Dado que es casi imposible proteger el sistema totalmente es muy conveniente disponer sistemas de detección de intrusiones y logs de eventos de seguridad en los sistemas. A ser posible, además estos logs deberían registrarse en máquinas diferentes (y sin acceso administrativo para evitar el borrado) ya que el atacante podría haberlos borrado