

BOLETÍN INFORMATIVO

A todos los Jefes de Informática, Encargados de Plazas Comunitarias, Apoyos Técnicos y Promotores: Les recordamos que deben actualizar el Sistema Operativo y antivirus de sus equipos. Para mas información, visitar la pagina web de su fabricante correspondiente.

El día 30 de abril, Microsoft ha recibido información de un gusano identificado como "W32.Sasser.worm" que está circulando actualmente en el Internet. El gusano se aprovecha de una vulnerabilidad en el Local Security Authority Subsystem Service (LSASS). Esta vulnerabilidad fue arreglada en la Actualización de Seguridad de Microsoft MS04-011 el día 13 de abril de 2004. Para conocer la información más reciente por favor visite <http://www.microsoft.com/security>.

Microsoft invita activamente a sus clientes a que se protejan contra este gusano, instalando el Boletín de Seguridad de Microsoft MS04-011

<www.microsoft.com/technet/security/bulletin/ms04-011.msp> inmediatamente.

En esta liga se encuentra una herramienta que detecta si el equipo esta infectado o no.

[Http://www.microsoft.com/security/incident/sasser.asp](http://www.microsoft.com/security/incident/sasser.asp)

Actualización de Seguridad para las diferentes versiones de Microsoft Windows (835732)

[Http://www.microsoft.com/technet/security/bulletin/ms04-011.msp](http://www.microsoft.com/technet/security/bulletin/ms04-011.msp)

De acuerdo con los últimos reportes, el gusano Sasser podría ser comparado con el gusano Blaster o Lovsan que apareció en Agosto del año pasado.

El gusano Sasser al igual que el gusano Blaster es un gusano de red que se propaga de forma automática afectando sistemas Windows 2000, XP y 2003, escaneando direcciones IP aleatoriamente y utilizando un FTP para transferir el archivo del gusano al servidor infectado.

De forma similar, Sasser causa que las computadoras que no estan actualizadas se reinicien, apareciendo una pantalla similar a la que aparecía con el gusano Blaster, pero hace referencia al archivo de sistema `/C:\WINNT\system32\lsass.exe/`.

Fecha de Liberación: 1 de Mayo de 2004

Sistemas Afectados * Windows 2000 * Windows XP

El gusano inicia 128 subprocesos que escanean direcciones escogidas de forma aleatoria. Esto consume demasiada memoria y como resultado disminuye su desempeño considerablemente.

Solución.- *Aplicar una Actualización del Distribuidor

Se recomienda instalar la actualización de seguridad que soluciona la vulnerabilidad que explota este gusano. *Microsoft Security Bulletin MS04-011

Security Update for Microsoft Windows (835732)*

<http://www.microsoft.com/technet/security/bulletin/MS04-011.msp>

<<http://www.microsoft.com/technet/security/bulletin/MS04-011.msp>>

* Ejecutar, administrar y actualizar un software antivirus. Aunque un paquete de software antivirus actualizado no puede brindar protección contra todos los códigos maliciosos, para la mayoría de los usuarios representa la primera línea de defensa contra ataques de código malicioso.

* Eliminación Manual

o Finalizar el proceso malicioso.

1. Presiona Ctrl+Alt+Suprimir una sola vez.

2. Da clic en el Administrador de Tareas.

3. Da clic en la pestaña Procesos.

4. Da doble clic en la columna Nombre de Imagen para ordenar alfabéticamente los procesos.

5. Localiza en la lista los siguientes procesos: + avserve.exe + cualquier proceso con un nombre consistente de 4 o 5 dígitos seguidos por _up.exe.

6. Si se encuentran dichos procesos, da clic en ellos, y después en Terminar Proceso.

7. Da salir del Administrador de Tareas.

o Deshabilitar System Restore (Windows XP).

1. Da clic en Inicio.

2. Da clic con el botón secundario en el icono Mi PC y, a continuación, da clic en Propiedades.

3. Da clic en la pestaña Restaurar sistema.

4. Marca la casilla Desactivar Restaurar sistema o la casilla Desactivar Restaurar sistema en todas las unidades.

5. Da clic en Aplicar y a continuación, en Aceptar

6. Como se vera en el mensaje, esta acción eliminará todos los puntos de restauración existentes. Da clic en Sí para llevar a cabo esta acción.

7. Da clic en Aceptar y reinicia el sistema.

o Eliminar los valores que fueron agregados al registro y reiniciar el equipo.

1. Da clic en Inicio y después en Ejecuta.

2. Escribe regedit y dale Aceptar.

3. Busca la siguiente llave

HKEY_CURRENT_USER\SOFTWARE\Microsoft\Windows\CurrentVersion\Run

4. En el panel de la derecha elimina el siguiente valor:

"avserve.exe"="%Windir%\avserve.exe"

5. Sal del editor del registro.

6. Reinicia el equipo.

Para cualquier duda o aclaración estamos a sus órdenes:

01800 6902726 ctro_apoyo@conevyt.org.mx