

Solución para los virus-gusanos; MSBlast W32/Lovsan.A ,Nachi, Mimail, Sobig.

Solución para los virus-gusanos de agosto;

MSBlast (W32/Lovsan.A ó Blaster / variantes Win32/Nachi), W32/Mimail, W32/Sobig.

El mes de agosto se ha caracterizado por la infección masiva de máquinas que funcionan bajo sistemas de Microsoft el sistema operativo más instalado por los usuarios de Internet, todos estos gusanos se aprovechan de vulnerabilidades de seguridad de Windows. Lo primero y más importante que se tiene que hacer es parchear su sistema operativo con el update de seguridad que proporciona Microsoft.

- Limpiar el MSBlast (W32/Lovsan.A ó Blaster /variantes Win32/Nachi):

Afecta solo a Windows 2000, XP y Windows Server 2003, el gusano se propaga a través del puerto TCP/135, copiándose en otras máquinas que son vulnerables al fallo DCOM/RPC.

Cuando su máquina está infectada muestra el siguiente mensaje en su pantalla;

----- INICIO -----

Apagar el sistema

Se está apagando el sistema. Guarde todo trabajo en curso y cierre la sesión. Se perderá cualquier cambio que no haya sido guardado. El apagado ha sido iniciado por NT AUTHORITY\SYSTEM

Tiempo restante para el apagado: xx:xx:xx

Mensaje

Windows debe reiniciar ahora porque el servicio Llamada a procedimiento remoto (RPC) terminó de forma inesperada

----- FINAL -----

A los sesenta segundos la máquina se apagará sola.

Parche de seguridad de Microsoft (para evitar infectarse de nuevo);

<http://www.microsoft.com/technet/treeview/?url=/technet/security/bulletin/MS03-026.asp>

Seleccione su sistema operativo y el idioma para descargar el parche.

Herramientas para limpiar el gusano;

<ftp://ftp.f-secure.com/anti-virus/tools/f-lovsan.zip>

Copyright (C) F-Secure 2003.

<http://securityresponse.symantec.com/avcenter/FixBlast.exe>

Copyright (C) Symantec 2003.

<http://updates.pandasoftware.com/pq/gen/blaster/pqremove.com>

Copyright (C) Panda Software 2003.

De forma manual (usuarios avanzados);

CTRL+ALT+SUPR pinchar sobre administrador de tareas, localizar el proceso MSBLAST.EXE y pinchar sobre terminar proceso.

Editamos el registro de windows con el Regedit.exe y buscamos la cadena; MSBLAST.EXE cuando la encontremos la borraremos.

Para mas información;

<http://www.microsoft.com/security/incident/blast.asp>

<http://www.microsoft.com/isaserver/techinfo/prevent/blasterworm.asp>

- Limpiar el W32/Sobig:

Afecta a todas las versiones de Windows, su infección se produce por medio del correo electrónico y cuando se infecta intenta propagarse a través de los recursos compartidos que tenga la máquina. Ejemplo del correo que puede recibir;

----- INICIO -----

Asunto: (uno de los siguientes):

'Re: Here is that sample'

'Re: Document'

'Re: Sample'

'Re: Movies'

Como datos adjuntos (NO EJECUTE EL FICHERO);

'Untitled1.pif'

'Document003.pif'

'Movie_0074.mpeg.pif'

----- FINAL -----

Herramientas para limpiar el gusano;

<ftp://ftp.f-secure.com/anti-virus/tools/f-sobig.exe>

Copyright (C) F-Secure 2003.

<http://updates.pandasoftware.com/pq/gen/sobigf/pqremove.com>

Copyright (C) Panda Software 2003.

<http://securityresponse.symantec.com/avcenter/FixSbigF.exe>

Copyright (C) Symantec 2003.

Variantes nuevas del W32/Sobig; Sobig.C / Sobig.D /Sobig.F

Importante este virus solo se infecta de forma manual, lo tiene que ejecutar para que se infecte la máquina.

Cuando la máquina esta infectada el gusano puede descargar y ejecutar nuevos archivos desde Internet, incluida su actualización para que los antivirus no puedan detectarlos por ser un código nuevo, pero el peligro puede ser, si se produce la descarga de un "troyano" para apoderarse del control de la máquina. Las posibles descargas se pueden producir los SABADOS y DOMINGOS, entre las 7 PM y 10 PM Las máquinas infectadas pueden ser usadas como servidores proxy para el envío masivo de correo (spam).

- Limpiar el W32/Mimail:

Afecta a todas las versiones de windows y tienen que estar instaladas algunas de estas versiones del Outlook;

Outlook Express 5.5 Service Pack 2 (con Internet Explorer 5.5 Service Pack 2 en Windows 98 SE, Windows Millenium, Windows NT 4.0 Service Pack 6a, Windows 2000 Service Pack 2 y Windows 2000 Service Pack 3).

Outlook Express 6.0 (con Windows XP Gold)

Outlook Express 6.0 Service Pack 1 (con Internet Explorer 6.0 Service Pack 1 en Windows 98 SE, Windows Millenium, Windows NT 4.0 Service Pack 6a, Windows 2000 Service Pack 2, Windows 2000 Service Pack 3, y Windows XP Service Pack 1)

La infección se produce por medio del correo electrónico al visionar una página o fichero HTML con código maligno que hace que se ejecute un fichero ejecutable, algunas variantes de este gusano cambian la página de inicio y de búsqueda del usuario. Ejemplo del correo que puede recibir;

----- INICIO -----

Asunto: your account

Datos adjuntos: message.zip (19 Kb)

Texto: Hello there,

I would like to inform you about important information regarding your email address. This email address will be expiring. Please read attachment for details.

--- Best regards, Administrator

----- FINAL -----

El archivo adjunto message.zip contiene el fichero message.html y es el causante de la infección en su máquina.

Parche de seguridad de microsoft (para evitar infectarse de nuevo);

<http://www.microsoft.com/windows/ie/downloads/critical/330994/default.asp>

Seleccioné su sistema operativo y el idioma para descargar el parche.

Herramientas para limpiar el gusano;

<http://www.symantec.com/avcenter/FxMimail.exe>

Copyright (C) Symantec 2003.

En todos estos casos es recomendable tener actualizado un antivirus y un cortafuego activo en nuestra máquina, para más información:

[Manual de instalación de cortafuegos](#)

[Manual de instalación de un antivirus](#)

[Escáner de Puertos](#)

[Herramientas para eliminar el gusano Blaster:](#)

[Otra alternativa para la solución del gusano Blaster:](#)

Por desgracia, todo esto parece que brotará de nuevo en septiembre a la finalización de las vacaciones, producido por la vuelta al trabajo, colegios, universidades... las máquinas que no estén parcheadas serán de nuevo víctimas del ciclo, pero recuerden que debido al gusano Blaster y su fallo de programación que resetea a los 60 segundos la máquina, tienen que actualizar forzosamente su sistema, si no se llega a producir este fallo muchas máquinas todavía serían vulnerables al fallo DCOM/RPC y cualquier intruso se podría "colar" y controlar su máquina, paradojas de la vida.

Informe elaborado por José M^a Luque Guerrero.

Para más información o dudas;

seguridad.internautas.org

Fecha artículo: 2003-08-23 10:20:03 - url artículo: <http://www.internautas.org/html/183.html>

Logos y marcas propiedad de sus respectivos autores.

Los comentarios son propiedad y responsabilidad de cada autor.

© 1998-2009 Asociación de Internautas - <http://www.internautas.org>

Inscrita en el Registro Nacional de Asociaciones con el número 164343 - e-mail: asociacion@internautas.org