

VIRUS MYDOOM

A pesar de que el virus Mydoom no produce pérdida de datos, hemos creído oportuno realizar este informe sobre su acción dada la gran repercusión social y a la enorme propagación que está generando.

“El gusano Mydoom lleva camino de convertirse en uno de los más nocivos de cuantos se han extendido por Internet en los últimos meses (1 de cada 6 mensajes de correo han sido infectados). Los expertos de las compañías antivirus han advertido que Mydoom se extiende más rápidamente que Sobig F. y Klez, dos de los virus más peligrosos de 2003.”

¿QUÉ ES?

Mydoom es un gusano que se propaga a través del correo electrónico en un mensaje con características variables y a través del programa de ficheros compartidos KaZaA.

Tiene capacidades de puerta trasera, lo cual permite que un usuario remoto pueda acceder al equipo infectado.

Realiza ataques de Denegación de Servicio Distribuida contra las páginas *web* www.sco.com y www.microsoft.com.

¿QUÉ CLASES HAY?

Este gusano proviene del virus Mimail, virus sin efectos dañinos pero con gran capacidad de propagación a través del envío masivo de correos.

Fue identificado por primera vez el 26 de enero de 2004, y se presenta en dos versiones: versión .A y .B, esta última detectada el 28 de enero de 2004.

La nueva variante es aún más peligrosa que la anterior, ya que está diseñada para impedir que muchos programas antivirus puedan actualizarse correctamente.

Otra diferencia de la nueva variante en relación con Mydoom.A. es que, está diseñada para causar ataques de denegación de servicio contra los servidores de la compañía Microsoft, mientras que el primero lanzaba ataques contra la *web* www.sco.com.

NOTA: En las últimas horas se ha detectado la aparición de dos nuevos virus relacionados con Mydoom. Uno de ellos es Doomjuice.A (W32/Doomjuice.A.worm). Se trata de un gusano que se propaga a través de Internet, para ello, utiliza la puerta trasera creada por Mydoom.A y Mydoom.B con el fin de realizar copias de sí mismo en los ordenadores afectados por estos gusanos. Doomjuice.A lanza ataques de Denegación de Servicio Distribuida (DDoS) contra el sitio *web* www.microsoft.com. El otro es Deadhat y desinstala las versiones del virus Mydoom que encuentre y luego trata de neutralizar la protección anti-virus de la computadora. Ambas, a diferencia del Mydoom original, no viajan a través del correo electrónico, sino que buscan direcciones e-mail en máquinas conectadas infectadas.

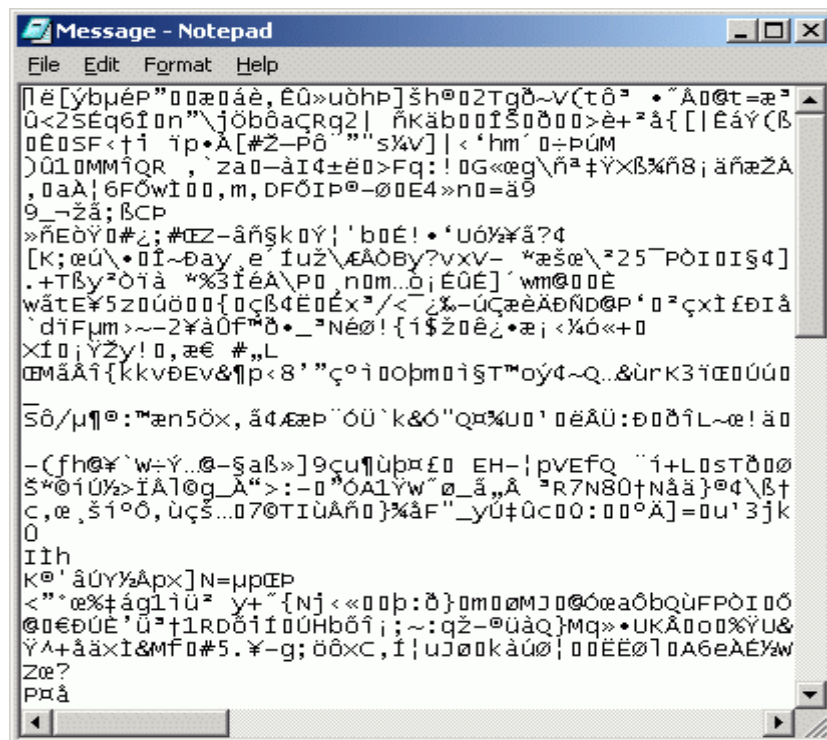
¿CÓMO ACTÚA?

W32/MyDoom es un gusano de email, con un componente de puerta trasera, que busca direcciones en el disco duro del sistema infectado y las utiliza para enviarse también como remitente, por lo que no se sabe de dónde procede realmente.

El gusano incita al usuario a abrir un archivo de programa adjunto. El icono de dicho fichero representa un archivo de texto, a fin de engañar al usuario.



Cuando se ejecuta por primera vez, el gusano abre el bloc de notas, y muestra caracteres sin sentido, del tipo:



El gusano instala el código dañino en el sistema y se envía a sí mismo a todos los contactos de la libreta de direcciones localizados en archivos con las siguientes extensiones: WAB, TXT, HTM, SHT, PHP, ASP, DBX, TBB, ADB y PL

Usa mensajes con asuntos, textos y nombres de archivos adjuntos variables. El mensaje suele medir de 30 a 35 Kb.

El mensaje puede tener alguno de los siguientes asuntos:

- [caracteres sin sentido o vacío]
- Delivery Error
- Error
- hello
- hi
- Mail Delivery System
- Mail Transaction Failed
- Returned mail
- Server Report
- Status
- Undeliverable: Mail Delivery System

Los archivos adjuntos, pueden tener alguno de los siguientes nombres:

- [caracteres sin sentido]
- body
- data
- doc
- document
- file
- message
- readme
- test
- text

El texto del mensaje puede ser alguno de los siguientes, entre otros generados al azar:

Ejemplo 1:

*sendmail daemon reported:
Error #804 occurred during SMTP session.
Partial message has been received.*

Ejemplo 2:

*Mail transaction failed. Partial message
is available.*

Ejemplo 3:

*The message contains Unicode characters and
has been sent as a binary attachment.*

Ejemplo 4:

*The message contains MIME-encoded graphics
and has been sent as a binary attachment.*

Ejemplo 5:

*The message cannot be represented in 7-bit
ASCII encoding and has been sent as a binary
attachment.*

Difusión mediante KaZaA

Se copia a si mismo a la carpeta compartida de KaZaa, con los siguientes nombres:

- activation_crack.bat
- activation_crack.pif
- activation_crack.scr
- icq2004-final.bat
- icq2004-final.pif
- icq2004-final.scr
- nuke2004.bat
- nuke2004.pif
- nuke2004.scr
- office_crack.bat
- office_crack.pif
- office_crack.scr
- rootkitXP.bat
- rootkitXP.pif
- rootkitXP.scr
- strip-girl-2.0bdcom_patches.bat
- strip-girl-2.0bdcom_patches.pif
- strip-girl-2.0bdcom_patches.scr
- winamp5.bat
- winamp5.pif
- winamp5.scr

De esta forma otros usuarios de KaZaA pueden descargar el virus.

Instalación

Cuando se ejecuta, crea los siguientes archivos en el sistema infectado:

- %TEMP%\Message
- c:\windows\system\shimgapi.dll
- c:\windows\system\taskmon.exe

NOTA : La carpeta TEMP está ubicada en "c:\windows\temp", "c:\winnt\temp", o "c:\documents and settings\[usuario]\local settings\temp", de acuerdo al sistema operativo.

En todos los casos, "c:\windows" y "c:\windows\system" pueden variar de acuerdo al sistema operativo instalado ("c:\winnt", "c:\winnt\system32", "c:\windows\system32", etc.).

Y modifica o crea las siguientes entradas en el registro:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Run
TaskMon = c:\windows\system\taskmon.exe
```

```
HKLM\Software\Microsoft\Windows\CurrentVersion\Run
TaskMon = c:\windows\system\taskmon.exe
```

```
HKLM\Software\Microsoft\Windows\CurrentVersion
\Explorer\ComDlg32\Version
```

```
HKCU\Software\Microsoft\Windows\CurrentVersion
\Explorer\ComDlg32\Version
```

Para crear la puerta trasera agrega el archivo SHIMGAPI.DLL en el directorio SYSTEM de WINDOWS, y lo ejecuta como un proceso hijo (child process) de EXPLORER.EXE.

La clave de registro modificada para esta tarea es la siguiente:

```
HKEY_CLASSES_ROOT\CLSID\{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32
"(Default)" = %SysDir%\shimgapi.dll
```

El gusano Mydoom B. puede además enviarse a equipos ya infectados por la versión A. Para ello, su componente backdoor escanea la red por direcciones IP generadas al azar, e intenta conectarse a puertos TCP/3127, utilizado por Mydoom. Si la máquina escaneada está infectada, entonces Mydoom se transfiere a ella y es ejecutado de inmediato. De ese modo las computadoras infectadas son actualizadas a la nueva versión sin necesidad de recibir un nuevo correo con el gusano.

Efectos

1. El gusano busca direcciones de correo electrónico en todos los ficheros con las siguientes extensiones (: WAB, TXT, HTM, SHT, PHP, ASP, DBX, TBB, ADB y PL), reenviándose automáticamente.
2. Abre un troyano de acceso por puerta trasera en las máquinas infectadas permitiendo que un posible intruso controle el equipo infectado de forma remota.
3. El gusano realiza ataques de denegación de servicio, a las siguientes direcciones:

www.sco.com (desde el 1/2/04) www.microsoft.com (desde el 3/2/04)

Estos ataques consisten en el envío de ráfagas de solicitudes GET HTTP. Ambos ataques se realizan en forma simultánea.

El 1 de marzo de 2004, el Mydoom está previsto que deje de propagarse, pero su rutina backdoor seguirá funcionando

¿CÓMO ELIMINARLO?

1. Se aconseja extremar las precauciones con los mensajes de correo electrónico recibidos, así como actualizar lo antes posible las soluciones antivirus y contar con un buen firewall.

Nota: A Menudo los antivirus informan de que 'no puede reparar un fichero' en el caso de gusanos o troyanos debido a que no hay nada que reparar, simplemente hay que borrar el fichero.

2. En el caso de que no se pueda eliminar el fichero del virus, debe terminar manualmente el proceso en ejecución del virus. Abra el Administrador de tareas (presione Control+Mayúsculas+Esc). En Windows 98/Me seleccione el nombre del proceso "SHIMGAPI.DLL" y deténgalo. En Windows 2000/XP, en la pestaña 'Procesos' haga clic derecho en el proceso "SHIMGAPI.DLL" y seleccione 'Terminar Proceso'. A continuación vuelva a intentar el borrado o reparación del fichero.

A continuación hay que editar el registro para deshacer los cambios realizados por el virus. **Sea extremadamente cuidadoso al manipular el registro. Si modifica ciertas claves de manera incorrecta puede dejar el sistema inutilizable. Por lo que recomendamos que si no está completamente seguro de saber utilizarlo correctamente, no modifique el registro.**

Puede acceder al registro a través del menú Inicio, Ejecutar y teclear "regedit", entonces se le abrirá el editor con una estructura en árbol.

Elimine los siguientes valores del registro:

Clave: HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run
Valor: TaskMon = c:\windows\system\taskmon.exe

Clave: HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run
TaskMon: = c:\windows\system\taskmon.exe
Elimine las siguientes claves:

HKEY_LOCAL_MACHINE \Software\Microsoft\Windows\CurrentVersion
\Explorer\ComDlg32\Version

HKEY_CURRENT_USER \Software\Microsoft\Windows\CurrentVersion
\Explorer\ComDlg32\Version
Bajo la siguiente clave:

HKEY_CLASSES_ROOT\CLSID\
{E6FB5E20-DE35-11CF-9C87-00AA005127ED}\InProcServer32

Restaurar los siguientes valores:

-En Windows 2000/XP:

(Predeterminado)=" %SystemRoot%\System32\webcheck.dll"

-En Windows 98/Me:

(Predeterminado)="Windows\System\webcheck.dll"

3. Reinicie su ordenador y explore todo el disco duro con un antivirus para asegurarse de la eliminación del virus. Si desactivó la restauración del sistema, recuerde volver a activarla.

MINIMICE LOS DAÑOS DE UN VIRUS:

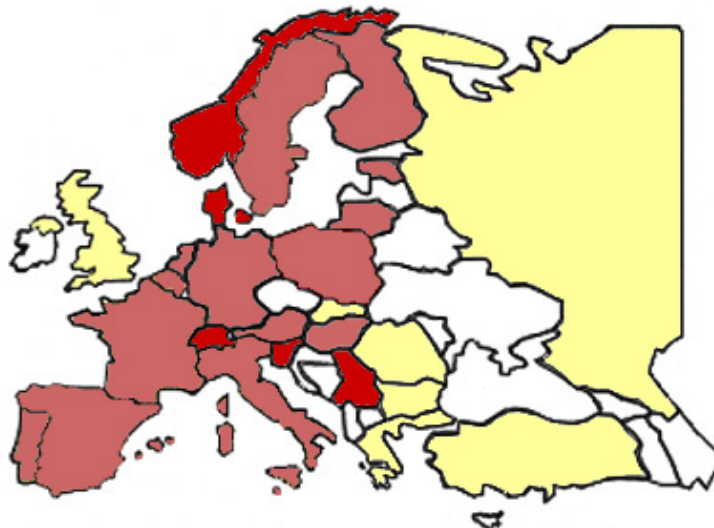
1. Si posee ordenadores conectados en red, aisle el ordenador o Pc infectado para que la infección no se propague.
2. Suspnda el acceso a Internet del ordenador infectado.
3. Si posee software antivirus, contacte con su proveedor y siga las indicaciones para su desinfección.
4. Actualice el antivirus e instale los parches de seguridad de su sistema operativo.
5. Analice el resto de equipos de la red, por si han sido infectados.
6. Si el virus contiene un Troyano que permite el acceso externo de hackers a su equipo, cambie las contraseñas.
7. Si posee copias de seguridad o backups recientes, asegúrese de que están libres de virus antes de recuperarlos.
8. Analice los fallos de su sistema de seguridad y subsane los errores que permitieron la infección.

MÁS INFORMACIÓN SOBRE VIRUS:

- Panda Software (<http://www.pandasoftware.es/>)
- Trend Micro (<http://es.trendmicro-europe.com/>)
- Enciclopedia Virus (Ontinent) (<http://www.encyclopediavirus.com>)
- McAfee (<http://es.mcafee.com>)
- Symantec (<http://www.symantec.com/region/es/>)
- VS Antivirus (<http://www.vsantivirus.com>)
- Kaspersky (viruslist.com) (<http://www.viruslist.com/eng/index.html>)
- Bit Defender (<http://www.bitdefender-es.com/>)
- Sophos (<http://esp.sophos.com>)
- Hacksoft (<http://www.hacksoft.com.pe>)
- PerAntivirus (<http://www.perantivirus.com/>)

VIRUS MYDOOM

Febrero 2004



- □ □ □ □ +

RECOVERY LABS®