



VIRUS TASIN

INTRODUCCIÓN

Reconocido por primera vez el día 19 de Noviembre de 2004 por Panda, el virus TASIN está en camino de convertirse en uno de los virus más peligrosos ya que es capaz de borrar archivos de nuestros ordenadores. Se trata de un virus creado en España, con mensajes escritos en castellano y que está generando una gran alarma general en los países de habla hispana.

Su nomenclatura más usual es "**Tasin**", aunque las diferentes compañías de antivirus le están comenzando a asignar diferentes nombres, claro síntoma de que cada vez es más necesario un acuerdo consensuado entre éstas para homogeneizar los nombres, con el fin de no confundir aún más al usuario.

¿QUÉ ES?

Tasin es un gusano que se propaga a través del correo electrónico con mensajes en español, utilizando su propio motor SMTP y que infecta a plataformas Windows XP XP/2000/NT/ME/98/95

Otros nombres con que se denomina este virus según las diferentes firmas son:

Panda 19.11.2004 18:51:04 :: W32/Tasin.A.worm
Kaspersky 21.11.2004 04:18:37 :: I-Worm.VB.w
TrendMicro 22.11.2004 23:20:59 :: WORM_ANZAE.A
eTrust-Iris 23.11.2004 00:54:50 :: Win32/Inzae.A.Dropper

Adicionalmente Kaspersky actualizó su firma el día 22 para modificar el nombre con que detectaba al gusano:

Kaspersky 22.11.2004 04:05:02 :: I-Worm.Pawur.a

Cuando se ejecuta, es notoria la caída del rendimiento del sistema infectado. Contiene código que intenta borrar todos los archivos con alguna de las siguientes extensiones:

ASM, ASP, BDSPROJ, BMP, CPP, CS, CSPROJ, CSS, DOC, DPR, FRM, GIF, HTM, HTML, JPEG, JPG, MDB, MP3, NFM, NRG, PAS, PCX, PDF, PHP, PPT, RC, RC2, REG, RESX, RPT, SLN, TXT, VB, VBP, VBPROJ, WAV y XLS.

Adicionalmente, el gusano intenta conectar con el sitio web del ayuntamiento de Écija, en la provincia de Sevilla, España; o intenta descargar una DLL (Librería de Enlace Dinámico) desde Internet.

¿QUÉ CLASES HAY?

Desde su aparición el día 19 hasta el día 22 han aparecido tres variantes del gusano: Tasin.A, Tasin.B y Tasin.C.

- Las tres variantes tienen las siguientes **características comunes**:

- Es un gusano que se propaga a través del correo electrónico, en un mensaje de características variables escrito en castellano.

- Contiene código que intenta borrar todos los archivos con alguna de las siguientes extensiones: ASM, ASP, BDSPROJ, BMP, CPP, CS, CSPROJ, CSS, DOC, DPR, FRM, GIF, HTM, HTML, JPEG, JPG, MDB, MP3, NFM, NRG, PAS, PCX, PDF, PHP, PPT, RC, RC2, REG, RESX, RPT, SLN, TXT, VB, VBP, VBPROJ, WAV y XLS.



- Contienen mensajes en el asunto similares a los siguientes ejemplos:

re:Amor verdadero
re:Como el aire...
re:Crees que puede ser verdad?
re:Déjate de rollos y vivé!!!
re:Eso con queso rima con...xD
re:La Luna
re:Neptuno y Mercurio
re:Psicología
re:Voodoo un tanto ps...
re:xD no me lo puedo creer!!

- Contienen alguno de los siguientes textos del mensaje, o similares:

Crees en el amor de verdad?,miralo y ya hablamos,ciaooo
Esa moribunda y solitaria Luna, Impresionante!chao.
Mira lo que te mando y ya verás que los detalles mas pequeños son los que importan,ciaoo
No comment,xDD,Nos vemos!!
No veas que cosas xD,luego me cuentas,chao.
Qué relación tienen estos planetas?,miralo y luego me cuentas,chao.
Renvíalo a todo que es que se meannn xD,nos vemos!
Será cierta la magia negra?,sal de dudas y ya me cuentas,chao.
Test para ver si andas bien de las neuronassss! xD,luego hablamos, chao
Ver es creer!!!!chao.

- Contienen alguno de los siguientes datos adjuntos:

el_rechazo.zip
gnito.zip
love-me.zip
moon(luna).zip
my life(mi vida).zip
para-brisas.zip
planetario.zip
quico-mix.zip
rimaz.zip
voodoo!.zip

La infección se produce solo si el usuario abre y ejecuta el adjunto con un doble clic.



► **Diferencias entre las variantes:**

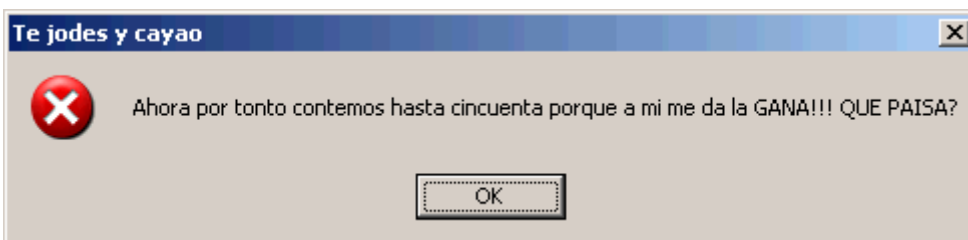
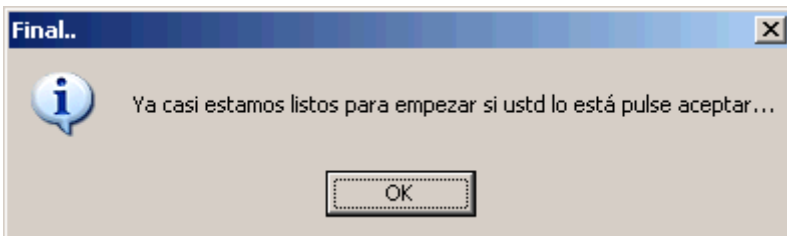
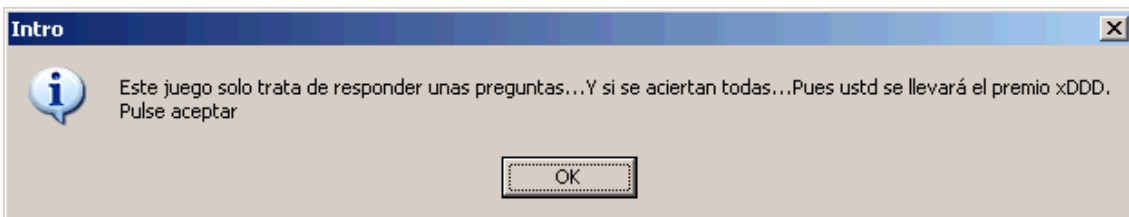
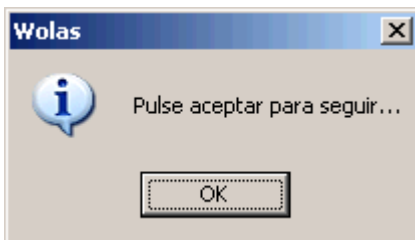
1. TASN.A

Adicionalmente, el gusano intenta conectar con el sitio web del ayuntamiento de Écija, en la provincia de Sevilla, España:

www.ecija.org

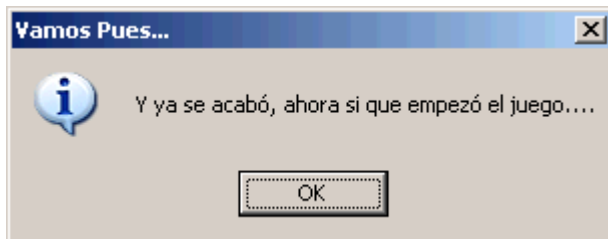
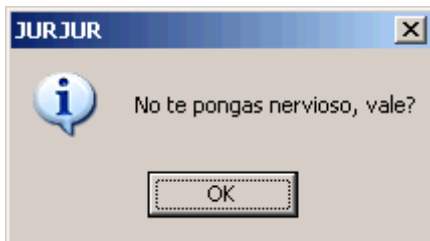
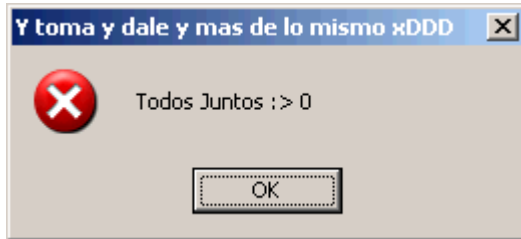
SINTOMAS VISIBLES:

Tasin.A es fácilmente reconocible una vez que ha afectado nuestro ordenador debido a una serie de mensajes que muestra en pantalla una vez que el gusano se ha ejecutado.

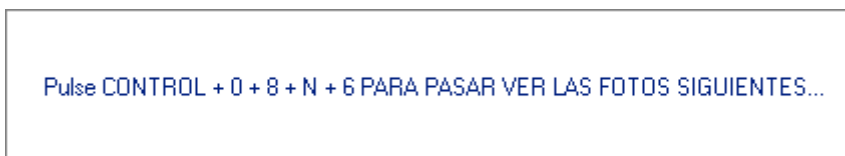




En este momento nos muestra un mensaje por cada número, desde el 0 al 50. Todos estos mensajes intentan distraer la atención del usuario mientras el gusano realiza la propagación a través del correo electrónico.



Finalmente aparece la pantalla en blanco con el siguiente texto.



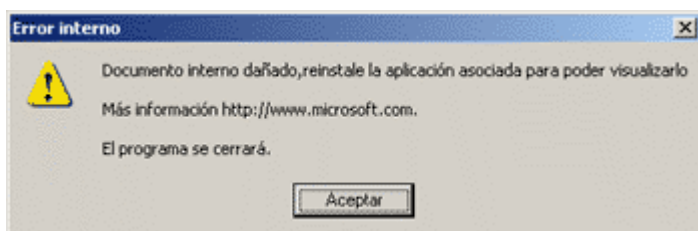


2. TASIN.B

Adicionalmente, *Tasin.B* intenta descargar una DLL (Librería de Enlace Dinámico) desde Internet

SINTOMAS VISIBLES:

Tasin.B es fácilmente reconocible una vez que ha afectado nuestro ordenador debido a un mensaje que muestra en pantalla una vez que el gusano se ha ejecutado.



3. TASIN.C

Adicionalmente, *Tasin.C* intenta descargar una DLL (Librería de Enlace Dinámico) desde Internet

SINTOMAS VISIBLES:

Tasin.C es fácilmente reconocible una vez que ha afectado nuestro ordenador ya que abre Internet Explorer y muestra en pantalla la fotografía de una mujer desnuda.

¿CÓMO ACTÚA?

El sistema deja de responder a cualquier combinación de teclas (menos CTRL+ALT+SUPR).

En este punto, el gusano crea una tarea llamada PEGOTE (muestra el icono de un CD musical), y un proceso cuyo nombre de imagen es INZAX.EXE. En Windows XP, si el usuario pulsa CTRL+ALT+SUPR, puede matar el proceso creado por el gusano.

Los siguientes archivos pueden ser creados en el sistema:

```
c:\windows\system32\svchosl.pif  
c:\windows\system32\m.zip
```

Dichos archivos son copias del propio gusano.

También crea los siguientes archivos:

```
c:\windows\system32\inzax.exe  
c:\windows\system32\sw.exe  
c:\windows\system32\sx.exe  
c:\windows\system32\sz.exe
```

INZAX.EXE es el programa que muestra las ventanas de mensajes descritos antes, y los tres restantes son utilizados por la rutina de propagación vía correo electrónico, tarea para la cuál utiliza su propio motor SMTP.



También crea los siguientes archivos:

X:\codm
X:\extasis8.pif
X:\inzae.pif
X:\ph003.pif
X:\rd2_roberto.pif
X:\simbolic3.pif
X:\sin_mas_menos.pif

Donde "X" es una de las siguientes unidades de disco (o aquellas que existan):

c:\
d:\
e:\
f:\

Para ejecutarse en próximos reinicios, el gusano crea la siguiente entrada en el registro:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Svchost = c:\windows\system32\svchosl.pif

NOTA: "c:\windows\system32" puede variar de acuerdo al sistema operativo instalado (con ese nombre por defecto en Windows XP y Windows Server 2003, como "c:\winnt\system32" en Windows NT y 2000 y "c:\windows\system" en Windows 9x y ME).

El gusano intenta establecer una conexión HTTP , desde donde intenta descargar otros archivos o intenta descargar una DLL (Librería de Enlace Dinámico) desde Internet.

El código del gusano contiene el siguiente texto:

-Worm by cUk- : -name Paula- : -version a- : -Date 01/11/04- : -Made in Spanish-

El gusano puede borrar archivos con las siguientes extensiones:

.asm
.asp
.bdsproj
.bmp
.cpp
.cs
.csproj
.css
.doc
.dpr
.frm
.gif
.htm
.html
.jpeg
.jpg
.mdb
.mp3
.nfm
.nrg



.pas
.pcx
.pdf
.php
.ppt
.rc
.rc2
.reg
.resx
.rpt
.sln
.txt
.vb
.vbp
.vbproj
.wav
.xls

¿CÓMO ELIMINARLO?

A. Borrar manualmente archivos agregados por el virus

Notas adicionales:

1. *Si su ordenador tiene Windows Millenium, debe seguir los siguientes pasos:*

Haga clic en *Inicio*.
Seleccione *Configuración*.
Pulse en *Panel de control*.
Haga doble clic en *Sistema*.
Seleccione la ficha *Rendimiento*.
Pulse en *Sistema de archivos*.
Haga clic en la ficha *Solución de problemas*.
Active la casilla *Deshabilitar Restaurar sistema*.
Pulse en *Aplicar*.
Desactive la casilla *Deshabilitar Restaurar sistema*.
Haga clic en *Aplicar*.
Guarde los cambios pulsando en el botón *Aceptar*.
El equipo le preguntará si desea reiniciarlo. Hágalo y al arrancar de nuevo su equipo los virus y otras amenazas habrán sido eliminados.
Para confirmar que el equipo está correctamente desinfectado realice un análisis de todo su sistema con el programa antivirus.

2. *Si su ordenador tiene Windows XP, debe seguir los siguientes pasos:*

Inicie sesión en el equipo con el usuario *Administrador* o con un usuario que tenga permisos de *Administrador*.
Haga clic con el botón derecho del ratón sobre *MI PC*.
Seleccione la opción *Propiedades*.
Pulse en *Restaurar sistema*.
Active la casilla *Desactivar restaurar sistema* o *Desactivar restaurar sistema en todas las unidades*.
Pulse *Aplicar* y luego *Aceptar*.

Pasos para activar de nuevo la opción Restaurar sistema

Haga clic con el botón derecho del ratón sobre *MI PC*.
Seleccione la opción *Propiedades*.
Pulse en *Restaurar sistema*.
Desactive la casilla *Desactivar restaurar sistema* o *Desactivar restaurar sistema en todas las unidades*.
Pulse *Aplicar* y luego *Aceptar*.



Una vez realizados estos pasos para confirmar que el equipo está correctamente desinfectado realice un análisis de todo su sistema con el programa antivirus.

► **Desde el Explorador de Windows, localice y borre los siguientes archivos:**

c:\windows\system32\inzax.exe
c:\windows\system32\m.zip
c:\windows\system32\svchosl.pif
c:\windows\system32\sw.exe
c:\windows\system32\sx.exe
c:\windows\system32\sz.exe

X:\codm

X:\extasis8.pif

X:\inzae.pif

X:\ph003.pif

X:\rd2_roberto.pif

X:\simbolic3.pif

X:\sin_mas_menos.pif

Donde "X" es una de las siguientes unidades de disco (o aquellas que existan):

c:\

d:\

e:\

f:\

IMPORTANTE: No borre C:\WINDOWS\SYSTEM32\SVCHOST.EXE, ya que es un archivo legítimo de Windows.

Haga clic con el botón derecho sobre el icono de la "Papelera de reciclaje" en el escritorio, y seleccione "Vaciar la papelera de reciclaje".

► **Editar el registro**

*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.***

Nota: algunas de las ramas en el registro aquí mencionadas, pueden no estar presentes ya que ello depende de que versión de Windows se tenga instalada.

1. Ejecute el editor de registro: Inicio, ejecutar, escriba REGEDIT y pulse ENTER

2. En el panel izquierdo del editor, haga clic en el signo "+" hasta abrir la siguiente rama:

```
HKEY_LOCAL_MACHINE
\SOFTWARE
\Microsoft
\Windows
\CurrentVersion
\Run
```

3. Haga clic en la carpeta "Run" y en el panel de la derecha, bajo la columna "Nombre", busque y borre la siguiente entrada:

```
Svchost = c:\windows\system32\svchosl.pif
```



4. Use "Registro", "Salir" para salir del editor y confirmar los cambios.
5. Reinicie su computadora (Inicio, Apagar el sistema, Reiniciar).

B. Herramienta de limpieza automática

Las diferentes firmas de antivirus van creando diferentes herramientas para eliminar los virus según van apareciendo, hasta las actualizaciones pertinentes de sus antivirus.

Algunas de estas herramientas puedes encontrarlas en las páginas Web de las diferentes firmas antivirus.

MINIMICE LOS DAÑOS DE UN VIRUS:

1. Si posee ordenadores conectados en red, aíse el ordenador o Pc infectado para que la infección no se propague.
2. Suspanda 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.

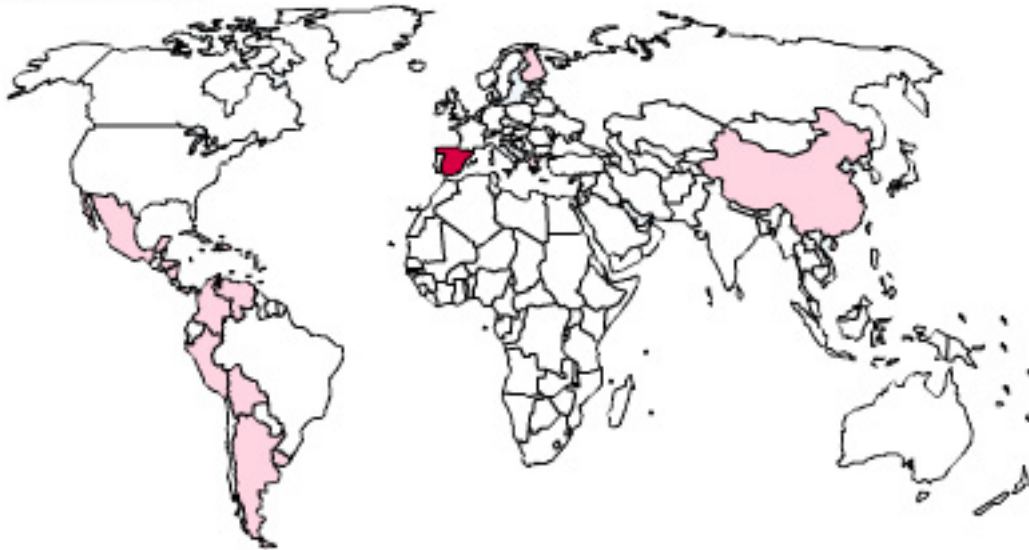
MÁS INFORMACIÓN SOBRE VIRUS:

- Alerta Antivirus (<http://alerta-antivirus.red.es/>)
- Panda Software (<http://www.pandasoftware.es/>)
- Trend Micro (<http://es.trendmicro-europe.com/>)
- Enciclopedia Virus (Ontinent) (<http://www.enciclopediavirus.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 TASIN

Noviembre 2004



RECOVERY LABS®

Fuente: Panda Software