

## RECUPERAR DATOS:VIRUS FIZZER

"Fizzer captura todo lo tecleado por su víctima, y lo guarda en un archivo que luego puede ser descargado por un intruso, obteniendo así datos que comprometen la seguridad y privacidad del usuario infectado."

### ¿QUÉ ES?

Fizzer es un gusano peligroso, puesto que está preparado para capturar las pulsaciones de teclado que realiza el usuario del ordenador afectado y guardarlas en un fichero de texto.

De este modo, cualquier hacker que acceda a este fichero podría conseguir información confidencial de este usuario, como son contraseñas de acceso a ciertos servicios (programas de chat, correo electrónico, claves de acceso a cuentas bancarias, etc).

Además, Fizzer está preparado para finalizar ciertos procesos relacionados fundamentalmente con programas antivirus.

Fizzer se propaga principalmente a través de los programas de chat IRC y del correo electrónico. Manda una copia de sí mismo a todos los contactos que encuentra en la Libreta de direcciones de Windows.

### ¿QUÉ CLASES HAY?

**Alias:**W32/Fizzer@MM (McAfee), W32/Fizzer-A (Sophos), W32/Fizzer (Panda Software), WORM\_FIZZER.A (Trend Micro), W32.HLLW.Fizzer@mm (Symantec), Win32.Fizzer.A@mm (Bit Defender), W32/Fizzer (Hacksoft), Fizzer (F-Secure), I-Worm.Fizzer (Kaspersky (viruslist.com)), Win32.Fizzer (Computer Associates), Win32/Fizzer.A@mm (RAV)

### ¿CÓMO ACTÚA?

Los distintos componentes del gusano se encargan de las siguientes tareas:

1. Capturador de direcciones de Libreta de direcciones de Outlook
2. Capturador de direcciones de Libreta de direcciones de Windows (WAB)
3. Capturador de direcciones encontradas en el sistema local
4. Generador aleatorio de direcciones
5. Lanzador IRC bot (Internet Relay Chat)
6. Lanzador AIM bot (AOL Instant Messenger)
7. Keylogger
8. Gusano para KaZaa
9. Servidor HTTP
10. Terminador de software Anti-virus.
11. El gusano contiene su propio motor SMTP aunque podrá usar el establecido en la configuración del registro del sistema.
12. Llegará en un fichero adjunto a alguno de los varios tipos de mensajes que utiliza para propagarse. El contenido del campo From(de) no tiene por qué ser el del emisor original. El cuerpo del mensaje y el asunto pueden tener diferentes contenidos. Las extensiones de los ficheros adjuntos podrán ser (.com, .exe, .pif, .scr).

Los **mensajes** serán similares a los siguientes:

Subject: why?

Body: The peace

Attachment: desktop.scr

Subject: Re: You might not appreciate this...

Body: lautlach

Attachment: service.scr

Subject: Re: how are you?

Body: I sent this program (Sparky) from anonymous places on the net

Attachment: Jesse20.exe

Subject: Fwd: Mariss995

Body: There is only one good, knowledge, and one evil, ignorance.

Attachment: Mariss995.exe

Subject: Re: The way I feel - Remy Shand

Body: Nein

Attachment: Jordan6.pif

Al ser ejecutado el adjunto, realizará las siguientes **tareas**:

1. Extraerá varios ficheros sobre el directorio (%WinDir%).
  - a. initbak.dat (220,160 bytes) - Copia del gusano
  - b. iservc.exe (220,160 bytes) - Copia del gusano
  - c. ProgOp.exe (15,360 bytes) - Manejador de procesos
  - d. iservc.dll (7,680 bytes) - Controlador temporal.
2. Creará la siguiente entrada en el registro para iniciarse junto a Windows:  
HKEY\_LOCAL\_MACHINE\Software\Microsoft\Windows\CurrentVersion\  
Run "SystemInit" = C:\WINDOWS\ISERVC.EXE
3. Modificará el registro para provocar la ejecución del gusano cada vez que sea abierto un fichero del tipo TXT:  
HKEY\_CLASSES\_ROOT\txtfile\shell\open\command  
(Predeterminado) =  
c:\windows\PROGOP.EXE 0 7 ' c:\windows\notepad.exe %1'  
'c:\windows\INITBAK.DAT' 'c:\windows\ISERVC.EXE'
4. Hará lo anterior para el siguiente registro:  
HKCR\Applications\ProgOp.exe\shell\Open\Command  
(Predeterminado) =  
c:\windows\PROGOP.EXE 0 7 ' c:\windows\notepad.exe %1'  
'c:\windows\INITBAK.DAT' 'c:\windows\ISERVC.EXE'
5. En sistemas WinNT/2K/XP creará un proceso denominado S1TRACE.

**NOTA:** En todos los casos, "C:\Windows" puede variar de acuerdo al sistema operativo instalado (con ese nombre por defecto en Windows 9x/ME y XP, y como "C:\WinNT" en Windows NT/2000).

#### **Rutina de envío masivo**

Utilizará su propio motor SMTP para enviarse a todas las direcciones de la libreta de contactos de Outlook, y a direcciones generadas aleatoriamente como las siguientes:

- Nombres aleatorios recogidos de una lista interna del gusano
- Números aleatorios
- Nombres de domino aleatorios (@dominio) recogidos de la siguiente lista interna:
  - o aol.com
  - o earthlink.com
  - o gte.net
  - o hotmail.com
  - o junos.com
  - o msn.com
  - o netzero.com
  - o yahoo.com

El **asunto, mensaje y nombre** del archivo adjunto los crea utilizando de forma aleatoria diferentes cadenas de texto, como:

"So how are you?"  
"Check it out"  
"There is only one good, knowledge, and on evil, ignorance"  
"I sent this program (sparky) from anonymous places on the net"  
"you must not show this to anyone"  
"Today is a good day to die"  
"thought I'd let you know"  
"The way to gain a good reputation is to endeavor to be what you desire ..."  
"Filth is a death"  
"wie geht es Ihnen?"  
"Philosophy imputes, reinterprets faith"  
"If you don't like it, just delete it"  
"delete this as soon as you look at it"  
"Did you ever stop to think that viruses are good for the economy? ..."  
"the incredibly bright faith"  
"you don't have to if you don't want to"  
"I wonder what can be so bad ..."  
"Watchin' the game, having a bud."  
"the attachment is only for you to look at"  
"Let me know what you think of this..."

## **IRC Bot:**

También envía copias a los usuarios conectados a los canales de chat que visite la víctima. Además, envía PINGS a diferentes servidores de IRC (generalmente por el puerto TCP/6667). PING (Packet INternet Groper) es un comando usado para comprobar las conexiones a uno o más hosts remotos enviando un paquete de bytes que normalmente es devuelto como un eco.

Cuando recibe una respuesta, se conecta a un canal usando diferentes nombres de una lista interna, y espera las instrucciones de un atacante, actuando como un BOT (copia de un usuario en un canal de IRC, preparado para responder ciertos comandos que se les envía en forma remota, de modo de lograr múltiples acciones coordinadas en forma simultánea).

La siguiente, es la lista de **servidores IRC**:

1. irc2p2pchat.net
2. irc.idigital-web.com
3. irc.cyberchat.org
4. irc.othernet.org
5. irc.beyondirc.net
6. irc.chatx.net
7. irc.cyberarmy.com
8. irc.gameslink.net

## **Propagación a través de KaZaA:**

Para propagarse a través de este programa de intercambio de ficheros punto a punto, sigue el siguiente proceso:

- Crea dentro del directorio compartido varias copias de sí mismo. Estas copias tendrán nombres aleatorios.
- Otros usuarios de KaZaA podrán acceder a este directorio compartido. Así, se descargarán voluntariamente en su ordenador alguno de los ficheros nombrados anteriormente, pensando que se trata de alguna aplicación interesante. En realidad, se estarán descargando en sus ordenadores una copia del gusano.
- Cuando esos usuarios ejecutan el fichero que se han descargado, quedarán infectados.

## **Keylogger: Capturador de pulsaciones del teclado.**

Captura las pulsaciones de teclado que realiza el usuario. Fizzer guarda estas pulsaciones en un fichero de texto que él mismo ha creado en el directorio de Windows, llamado ISERVC.KLG. Después lo encripta. Si un hacker consigue este fichero, tendrá acceso a datos confidenciales del usuario del ordenador afectado, como pueden ser claves de acceso a servicios de Internet, cuentas bancarias, etc.

## **Terminación de software Anti-virus**

Para evitar ser detectado, finaliza procesos que contengan en sus nombres las siguientes cadenas:

- ANTIV
- AVP
- F-PROT
- NMAIN
- SCAN
- TASKM
- VIRUS
- VSHW
- VSS

## **¿CÓMO ELIMINARLO?**

### **Antivirus**

1. Actualice sus antivirus con las últimas definiciones
2. Ejecútelos en modo escaneo, revisando todos sus discos
3. Borre los archivos detectados como infectados

## Borrado manual de los archivos creados por el virus

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

```
c:\windows\ISERVC.KLG  
c:\windows\INITBAK.DAT  
c:\windows\ISERVC.EXE  
c:\windows\ISERVC.DLL  
c:\windows\PROGOP.EXE
```

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

Borre también los mensajes electrónicos similares al descrito antes.

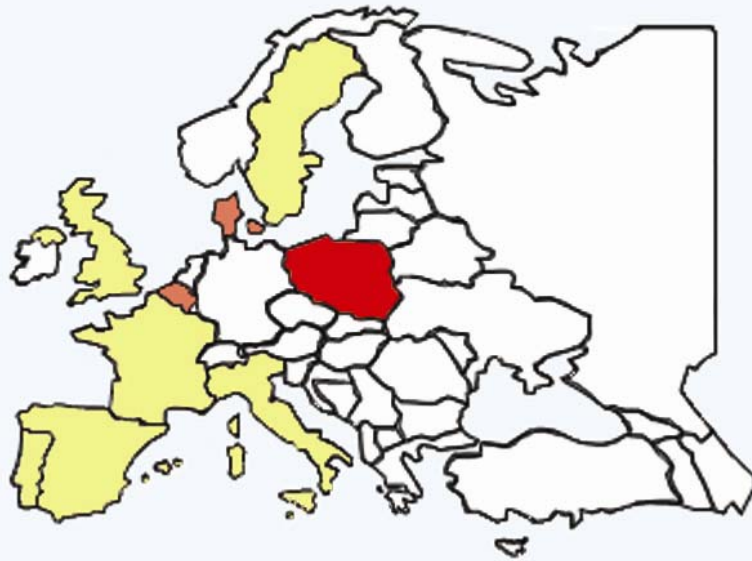
## Editar el registro

1. Ejecute el editor de registro: Inicio, ejecutar, escriba REGEDIT y pulse ENTER
2. En el panel izquierdo del editor, pinche en el signo "+" hasta abrir la siguiente rama:  
HKEY\_LOCAL\_MACHINE  
SOFTWARE  
Microsoft  
Windows  
CurrentVersion  
Run
3. Pinche en la carpeta "Run" y en el panel de la derecha, bajo la columna "Nombre", busque y borre la siguiente entrada:  
SystemInit
4. En el panel izquierdo del editor, pinche en el signo "+" hasta abrir la siguiente rama:  
HKEY\_CLASSES\_ROOT  
txtfile  
shell  
open  
command
5. Pinche en la carpeta "command" y en el panel de la derecha, bajo la columna "Nombre", y cambie el contenido de (Predeterminado) por lo siguiente:  
(Predeterminado) = C:\WINDOWS\notepad.exe %1
6. En el panel izquierdo del editor, pinche en el signo "+" hasta abrir la siguiente rama:  
HKEY\_CLASSES\_ROOT  
Applications  
ProgOp.exe
7. Pinche en la carpeta "ProgOp.exe" y bórrala.
8. Use "Registro", "Salir" para salir del editor y confirmar los cambios.
9. Reinicie su computadora (Inicio, Apagar el sistema, Reiniciar).

**NOTA:** En todos los casos, "C:\Windows" puede variar de acuerdo al sistema operativo instalado (con ese nombre por defecto en Windows 9x/ME y XP, y como "C:\WinNT" en Windows NT/2000).

**VIRUS FIZZER**

Mayo 2003



- +

**RECOVERY LABS®**