

Como hacer un Trojan Horse indetectable

Tecnica :

- Cambiando los Offset con el PROCDUMP

Herramientas:

- PROCDUMP
- UPX
- IMAGINACION J

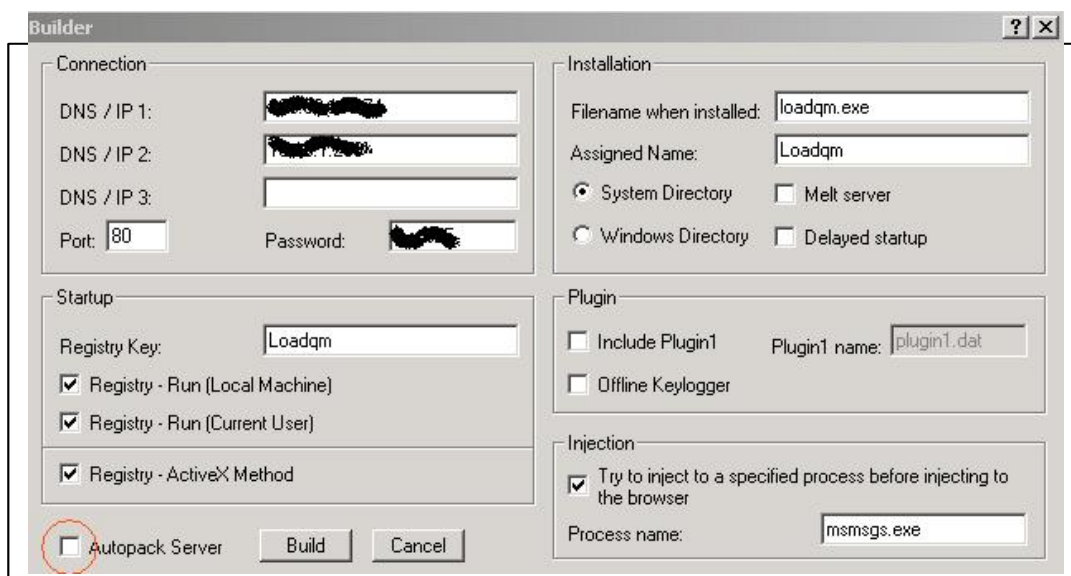
“Aquel que este leyendo este manual, espero que sea de gran ayuda en ampliar un poco tus conocimientos, este manual es solamente informacion no me hago responsable del mal uso que se le pueda dar o de los resultados del programa una vez modificado.”

1.-Creando el server

Bueno, como saben , normalmente cuando sale un trojan horse , tiene un tiempo de vida de + - 5 meses, pasado ese tiempo podemos decir que ya esta quemado(por los antivirus), esto sucede por la cantidad de usuarios que manejan estos programas (mayoria newbite o lammers), que se la pasan jodiendo a sus victimas , con abre cd, cierra cd, y de mas huevadas, haciendo que los usuarios y las compañías de antivirus tomen carta en el asunto, pero bueno ese no es el tema, lo que voy a explicar es una tecnica conocida y MUY EFECTIVA.

Entrando al tema, poniendo como ejemplo al server del Bifrost (puede ser otro, pero a este le tengo mucha fe)

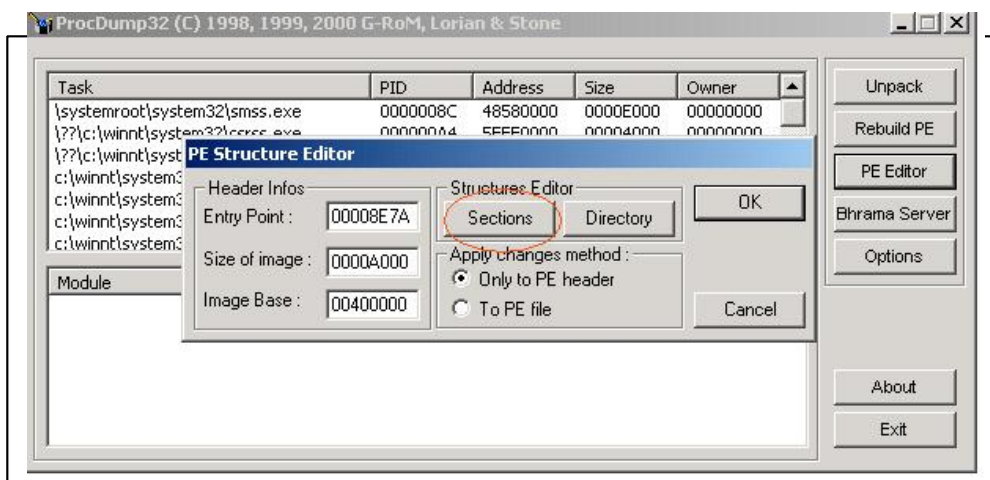
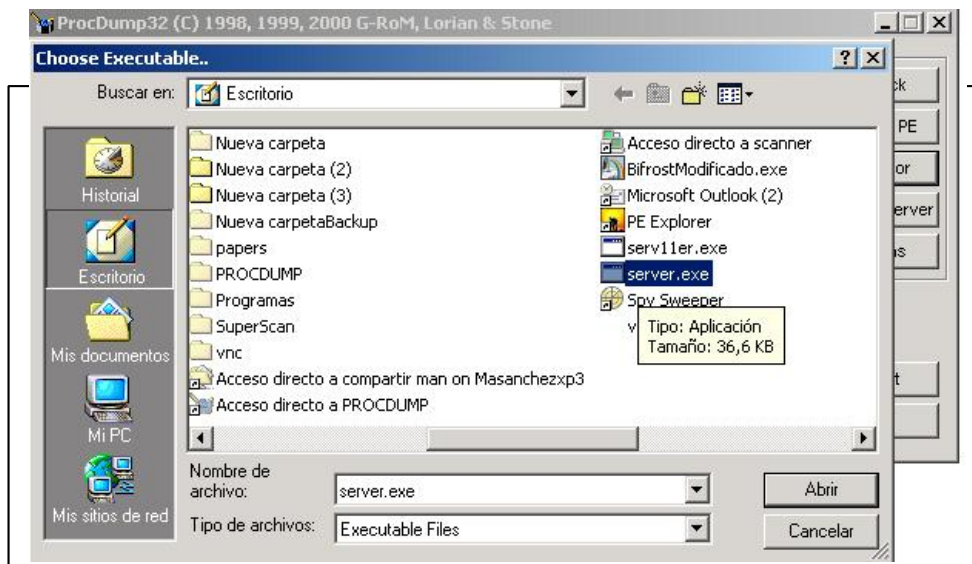
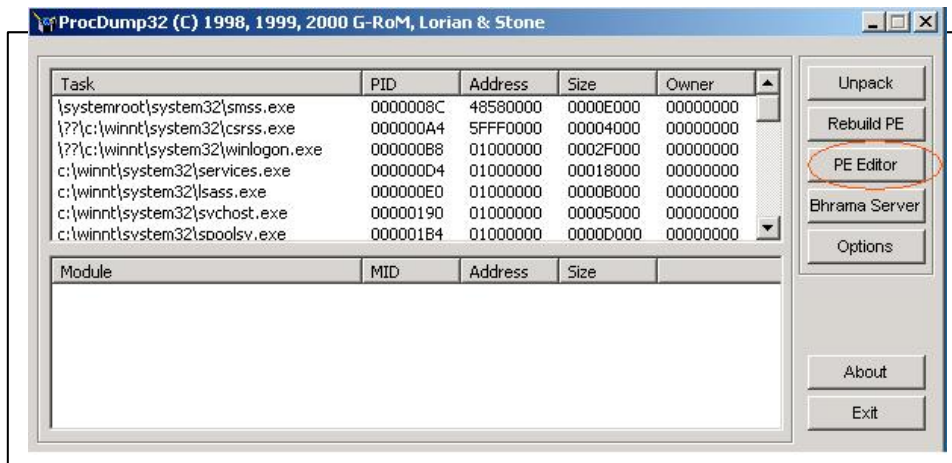
Creando el server:



Man-In-The-Middle: Attacks in tunneled authentication protocols

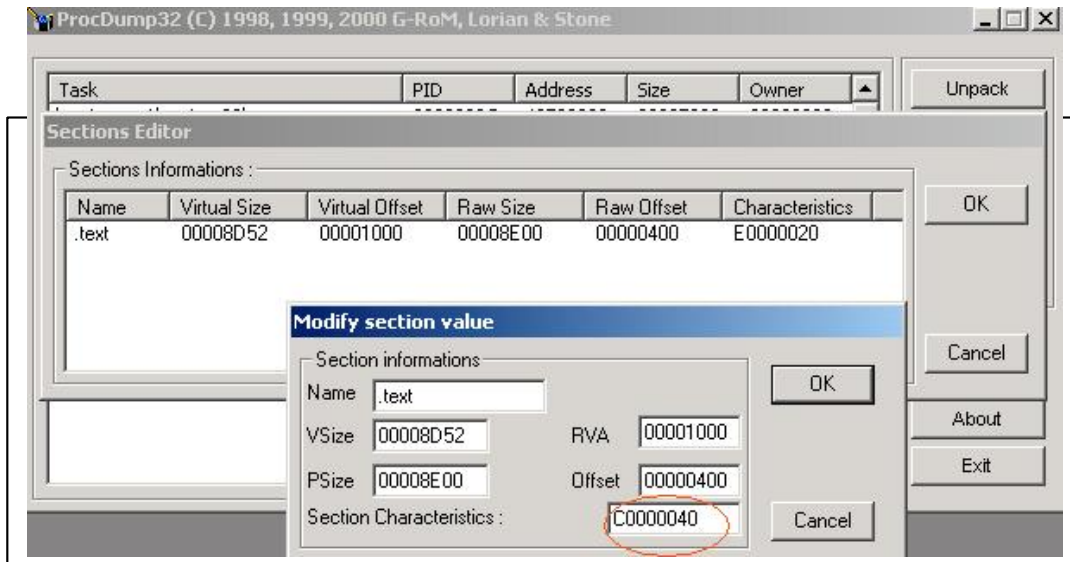
En este caso la compresion no esta activada (Autopack Server), por que despues lo vamos a comprimir con el upx, , mas adelante voy a explicar esa parte.

Ejecutamos el PROCDUMP



Man-In-The-Middle: Attacks in tunneled authentication protocols

Ahora si entramos a la parte bonita , al momento de darle a Sections nos va a arrojar el Section editor, el cual en la cabecera hay un peculiar numero E0000020, eso nos dice que es ejecutable y que no esta comprimido, toncessss, se lo cambiamos a C0000040, eje, que paso ahí, pues lo estamos poniendo como si estuviera empaquetado



Bueno, le damos ok, ok, ok ,ok a todo, pssss , la huevadita esta a media caña, nos vamos a nuestra carpeta del upx y copiamos el server ya modificado y lo comprimimos con la sentencia `c:\upx -9 server.exe` y esto nos bota:

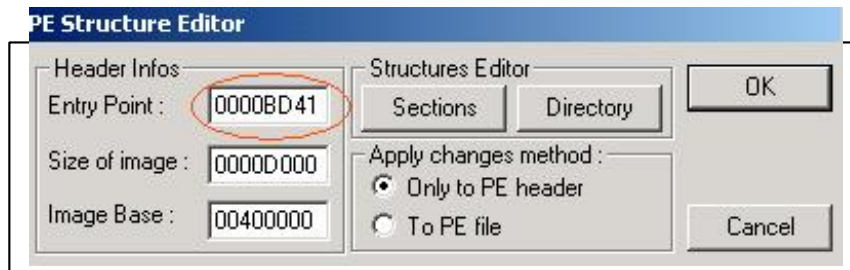
```
C:\WINNT\system32\cmd.exe
Microsoft Windows 2000 [Versión 5.00.2195]
(C) Copyright 1985-2000 Microsoft Corp.

C:\Documents and Settings\pqueens>cd\
C:\>cd 4upx
C:\4upx>upx -9 server.exe
          Ultimate Packer for eXecutables
Copyright (C) 1996, 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004
UPX 1.25w      Markus F.X.J. Oberhumer & Laszlo Molnar      Jun 29th 2004

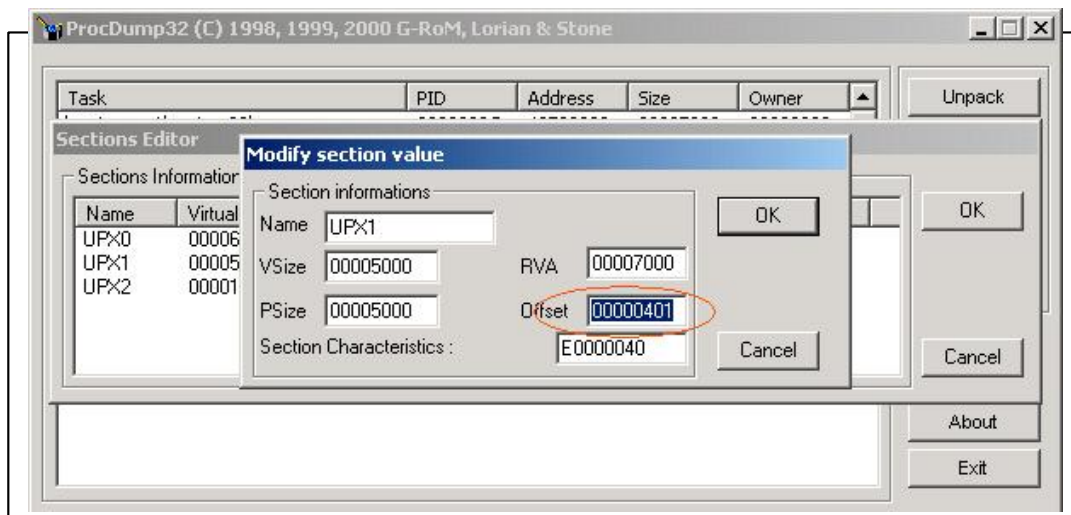
-----
File size      Ratio      Format      Name
-----
37554 ->      22194    59.10%    win32/pe    server.exe

Packed 1 file.
C:\4upx>
```

Bueno ya lo tenemos apretado de nuevo, entonces, volvemos con nuestro programita especial PROCDUMP y volvemos hacer los pasos anteriores pero, antes que todo modificamos ahora si El Entry Point 0000BD40 en mas 1, osea 0000BD41

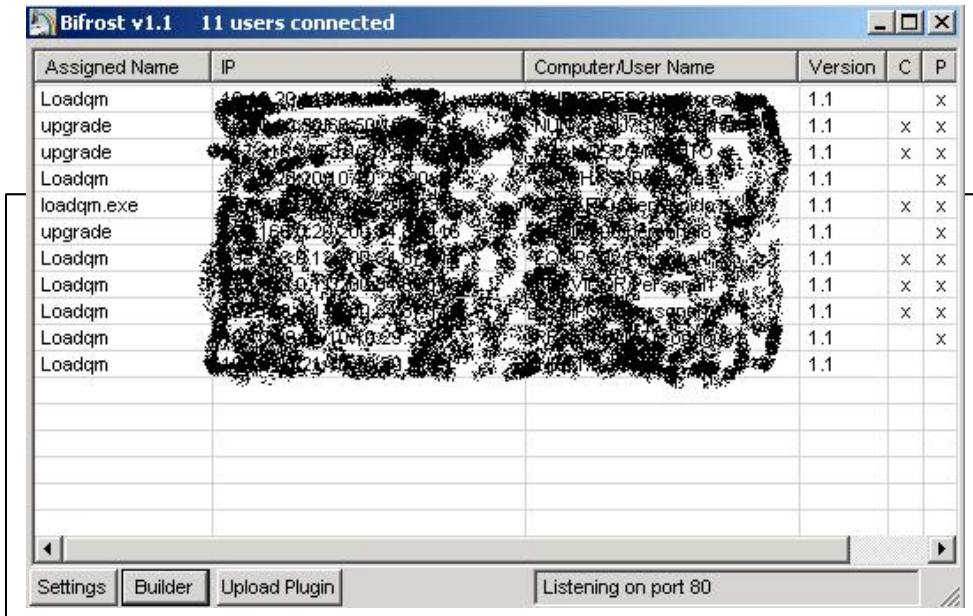


Igual entramos Section como la ves anterior y modificamos el UPX1 click derecho, edit section y modificamos el offset en + 1, 00000400 en 00000401, le damos ok ok ok ok . etc



Y wuaaaalaaa, tenemos un troyano Indetectable, 100% funcional, testeado en win2000, XP, WIN98, con Norton, Trend Micro OfficeScan Client, Panda antivirus, KAV.

Testeo:



Agradecimiento al forum <http://www.elhacker.net/foro/index.php>

A mis amigos: Redrum- Yataco

En el proximo capitulo, como ejecutar dicho trojan horse de forma remota mediante exploit dentro de una lan

Enjoy

Man-In-The-Middle