Como hacer un troyano indetectable: sacado de elhacker(punto)net

-Tecnica, cambiando los offset con el procdump

-Herramientas: Procdump, upx (compresor)

Empezamos: bien en este manual se modifica el bifrost, pero tambien es factible con otros troyanos....

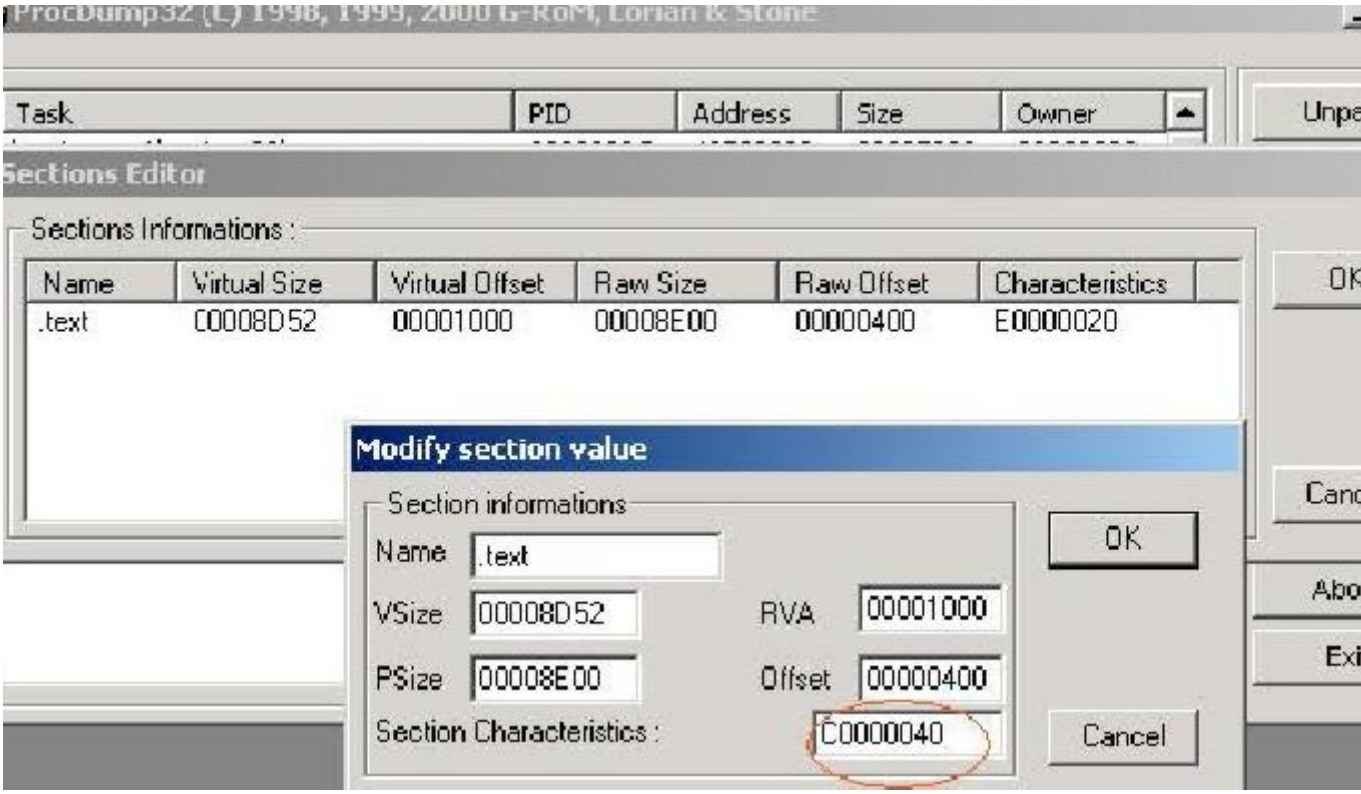
Observaciones: no se debe poner autopack al configurar el server.

Ejecutamos el procdump:

-Hacemos clic en PE Editor, despues seleccionamos el ejecutable Â¦..

(nos tendria Â que salir algo como eso)

-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, entonces, se lo cambiamos a C0000040, eje, que paso ahoraâ€™ Â, pues lo estamos poniendo como si estuviera empaquetado.

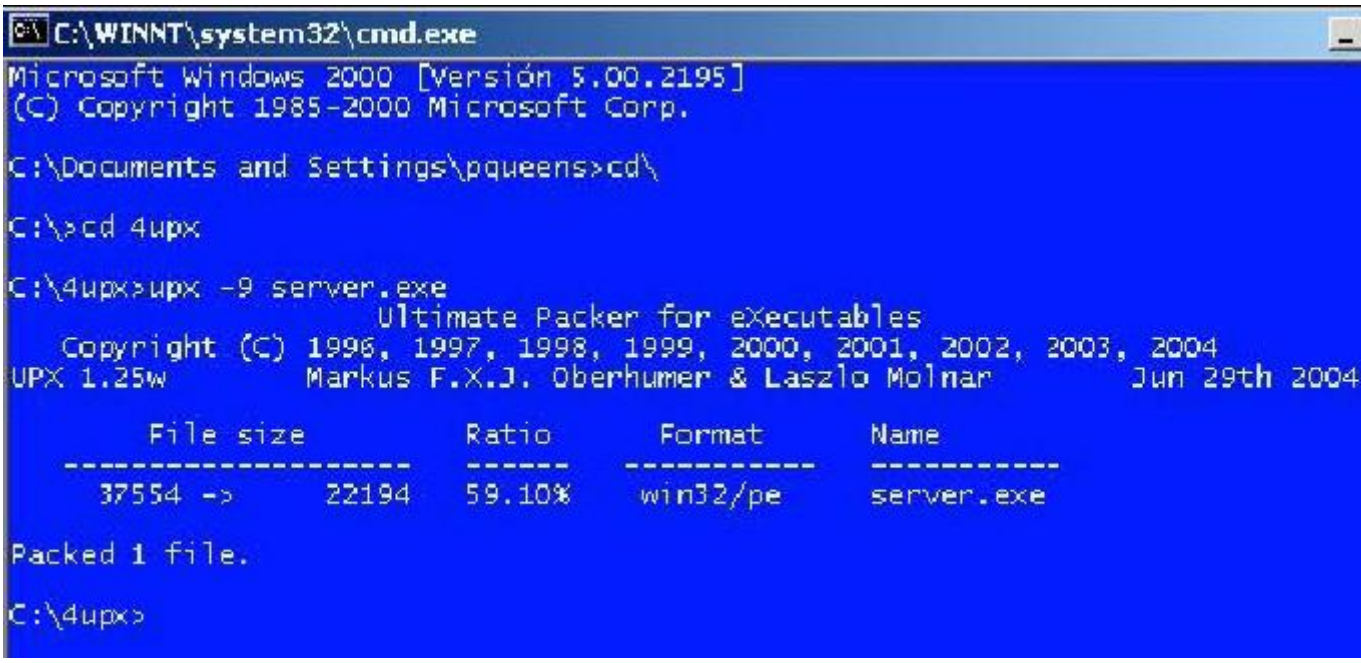


(se cambia el numero original por C0000040)

-una vez cambiado le vamos dando a ok a todo.

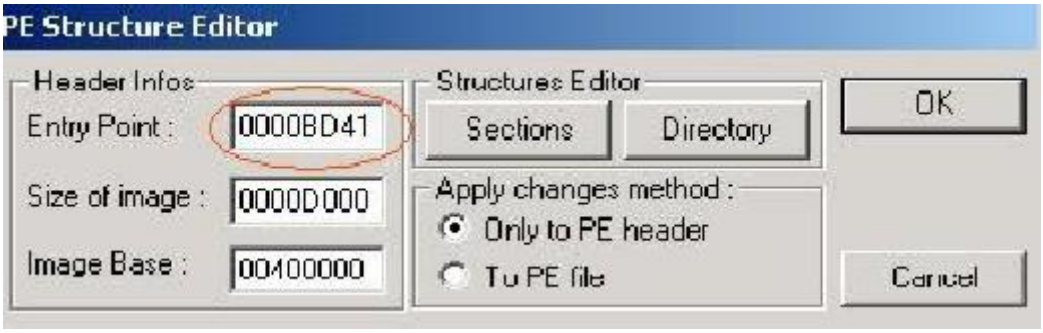
UPX: bueno, ahora vamos al ms-dos, y se pone el siguiente comando para comprimir nuestro server modificado con el upx:

-C:\upx -9 server.exe (en upx poneis la carpeta donde lo tengais) y upx.

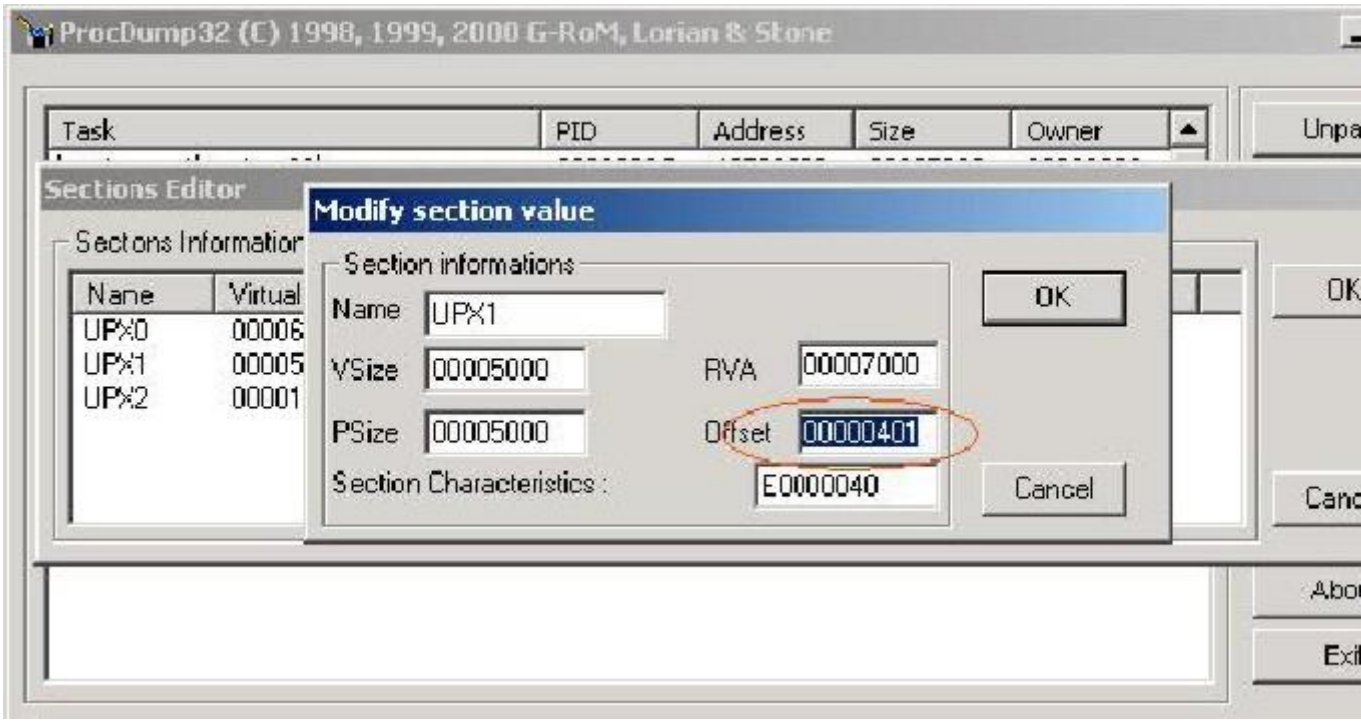


-(Ahora volvemos al procdump) (ahora con ese programa abrimos el server modificado y comprimido)

volvemos hacer los pasos anteriores pero, antes de todo modificamos ahora si
El Entry Point 0000BD40 en mas 1 , es decir 0000BD41.



-entramos Section como la ves anterior y modificamos el UPX1(el server ya comprimido) click derecho , edit section y
modificamos el offset en + 1 , 00000400 en 00000401, le damos ok ok ok ok . etc



-Asi ya tendremos nuestro server indetectableee, testado contra norton y panda, entre otros....l