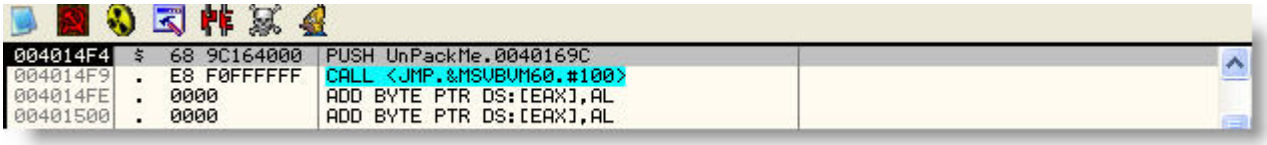
Programa	UnPackMe_1337 Exe Crypter 1
Versión	
Herramientas	
Compilador	OLLYDGB - PUPE
Objetivos	VISUAL C++
Cracker	UNPACK

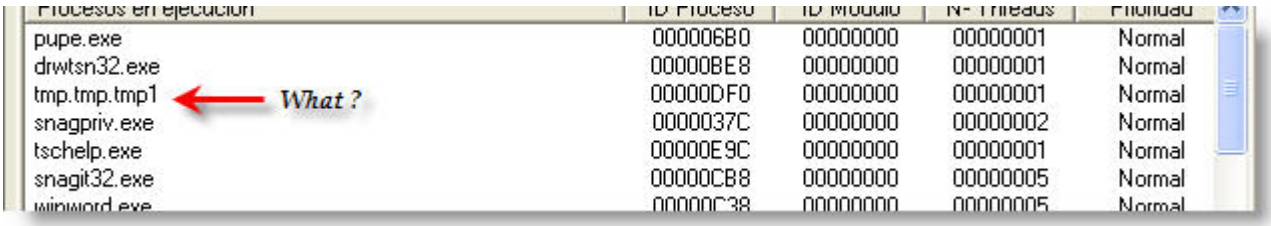
Solid

Open your target in Olly, it seems to be a standard VB app:



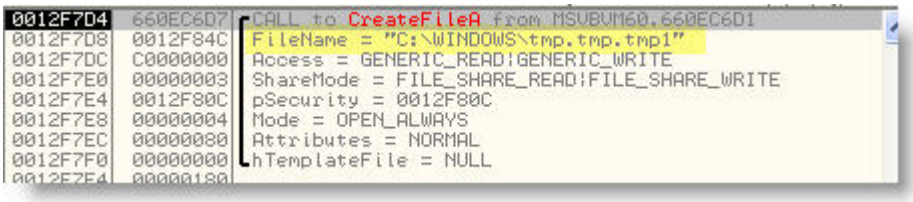
press RUN (F9) and see what happen:

Close ollydbg and app is still running, it seems like 2 processes are running or something like this, just open PUPE and check running processes:

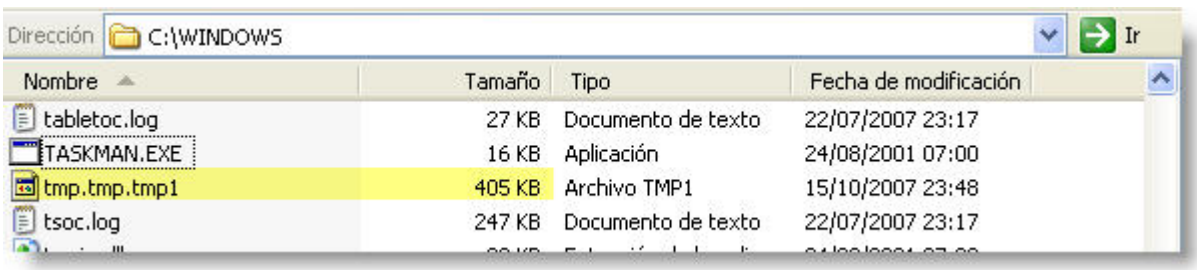


let's check this, open target again in Olly, and set a BP on CreateFileA, first stop land here:

continue with RUN, untill you see the tmp file:



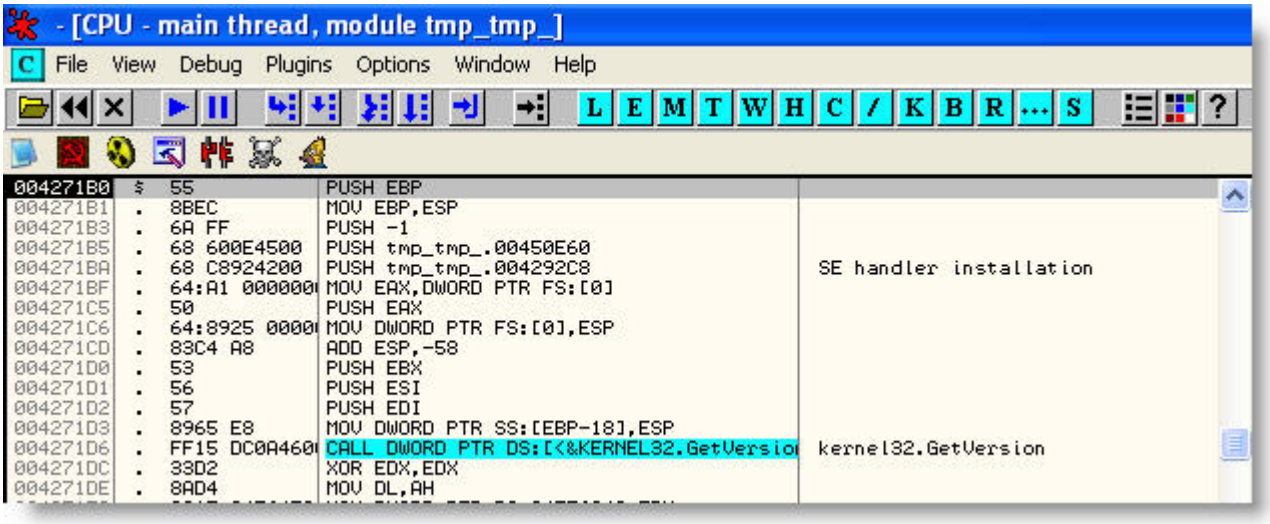
ok, this is all whe need to know, so, close olly now, go to path c:\windows and find the tmp.tmp.tmp1 file:



too big !!, change the name to .exe:

you can see the icon now !!!!, just double click on it:

amazing !!! - open it with olly and you can see, we have the right file:



ok. There's nothing to unpack.

Thanks to all CrAcKsLatiNoS members, tuts4you members, and thank you for reading this tut.

solidreverser@gmail.com


Solid