



➤ 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:

```

004014F4  68 9C164000  PUSH UnPackMe.0040169C
004014F9  E8 F0FFFFFF  CALL <JMP.&MSUBUM60.#100>
004014FE  . 0000       ADD BYTE PTR DS:[EAX],AL
00401500  . 0000       ADD BYTE PTR DS:[EAX],AL
    
```

press RUN (F9) and see what happen:



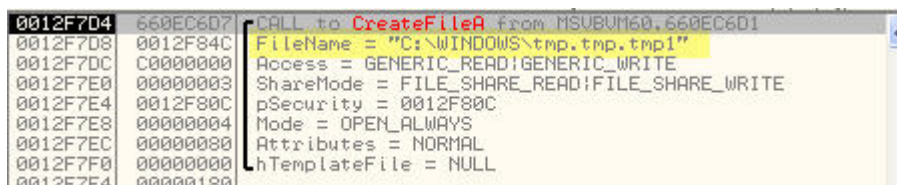
Close ollydbg and app is still running, it seems like 2 processes are running or something like this, just open PUPE and check running processes:

Procesos en ejecución	ID Proceso	ID Módulo	Nº Threads	Privilegio
pupe.exe	00000680	00000000	00000001	Normal
drwtsn32.exe	000008E8	00000000	00000001	Normal
tmp.tmp.tmp1	00000DF0	00000000	00000001	Normal
snagpriv.exe	0000037C	00000000	00000002	Normal
tschelp.exe	00000E9C	00000000	00000001	Normal
snagit32.exe	00000CB8	00000000	00000005	Normal
winword.exe	00000C38	00000000	00000005	Normal

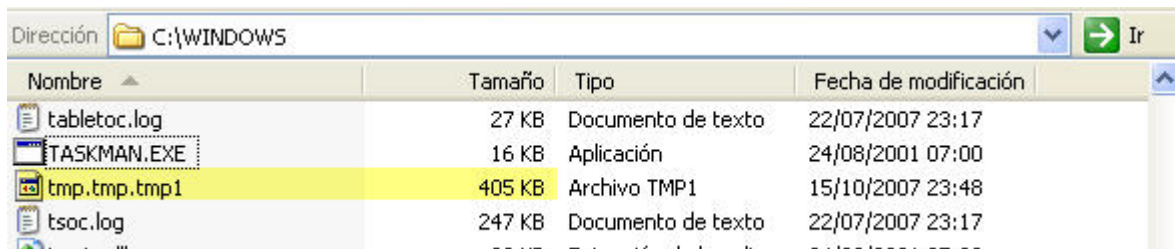
let's check this, open target again in Olly, and set a BP on CreateFileA, first stop land here:



continue with RUN, until you see the tmp file:



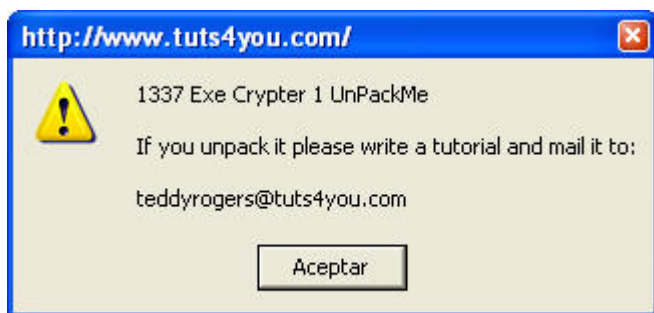
ok, this is all we need to know, so, close olly now, go to path c:\windows and find the tmp.tmp.tmp1 file:



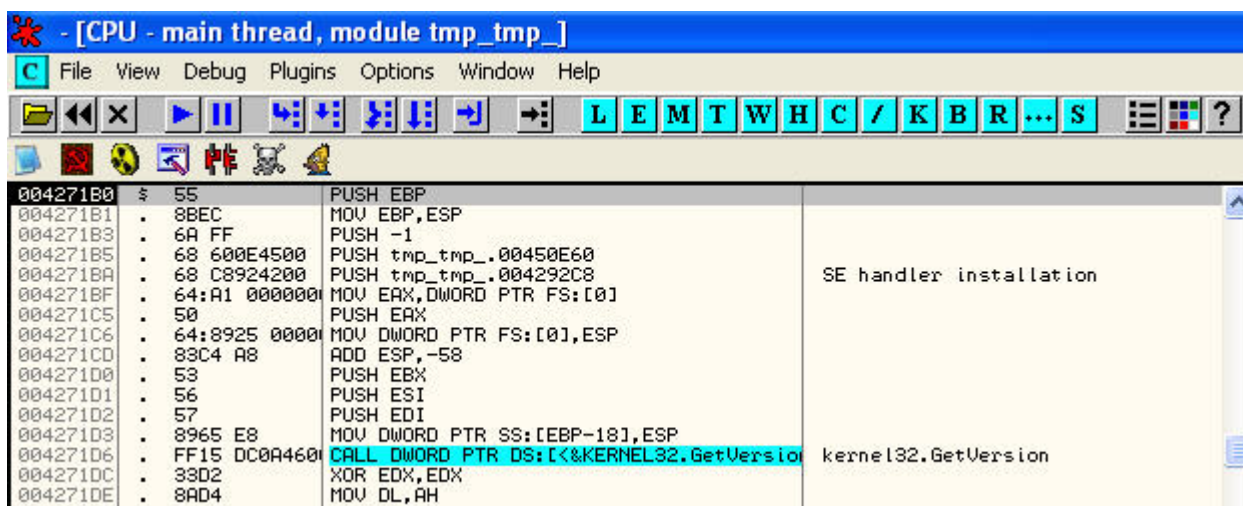
too big !!, change the name to .exe:



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](mailto:solidreverser@gmail.com)

