

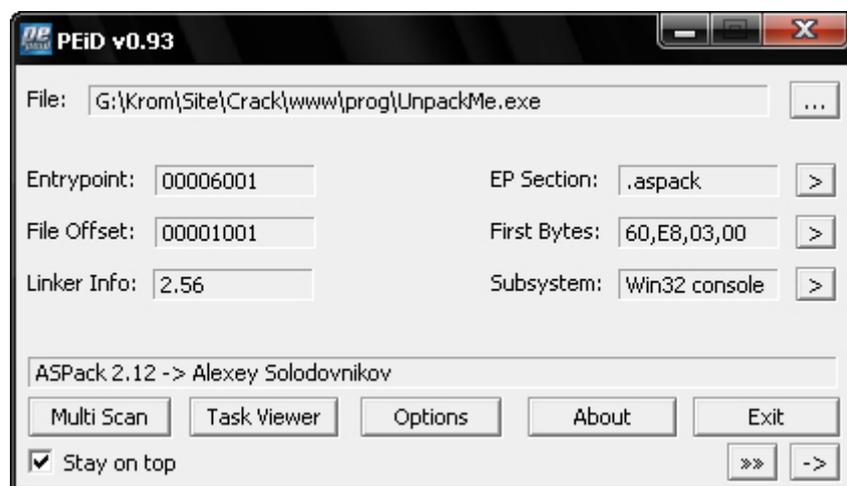
## Cours N° 9

Dans ce cours, nous allons voir la protection ASPack 2.12 sur un UnpackMe, il est téléchargeable [ICI](#)

- <http://www.KromCrack.com/prog/UnpackMe.exe>

Je ne vais pas ici refaire la théorie sur le packer, mais juste vous expliquer comment Unpacker la protection ASPack 2.12

Un des premiers reflexes à avoir est de l'analyser avec PEiD, qui nous dit ceci :



Quand on essaie de l'ouvrir avec OllyDBG, un message d'erreur apparaît nous disant que l'EP est placé en dehors du code.

Nous voyons aussi qu'il ne trouve aucune références dans :

- ->> Search for ->> All Referenced text strings.

Donc la même si vous ne l'aviez pas analysé avec PEiD, aucun doute qu'il est bien packé.

On voit aussi que le code Désassemblé est illisible et qui Commence par un PUSHAD.

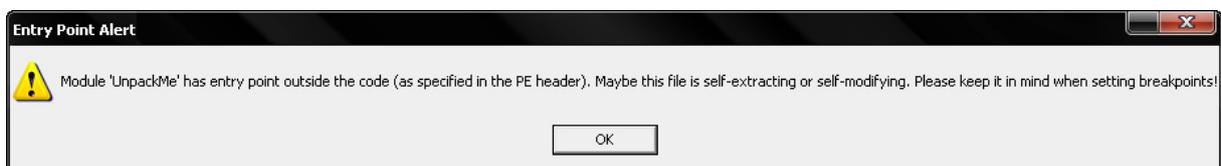
```

00406001 60          PUSHAD
00406002 E8 03000000 CALL UnpackMe.0040600A
00406007 -E9 EB045D45 JMP 459D64F7
0040600C 55          PUSH EBP
0040600D C3          RETN
0040600E E8 01000000 CALL UnpackMe.00406014
00406013 v EB 5D     JMP SHORT UnpackMe.00406072
00406015 BB EDFFFFFF MOV EBX,-13
0040601A 0300      ADD EBX,EBP
0040601C 81EB 00600000 SUB EBX,6000
00406022 83BD 22040000 00 CMP DWORD PTR SS:[EBP+422],0
00406029 899D 22040000 MOV DWORD PTR SS:[EBP+422],EBX
0040602F v 0F85 65030000 JNZ UnpackMe.0040639A
00406035 8D85 2E040000 LEA EAX,DWORD PTR SS:[EBP+42E]
0040603B 50        PUSH EAX
0040603C FF95 4D0F0000 CALL DWORD PTR SS:[EBP+F4D]
00406042 8985 26040000 MOV DWORD PTR SS:[EBP+426],EAX
00406048 8BF8     MOV EDI,EAX
0040604A 8D5D 5E     LEA EBX,DWORD PTR SS:[EBP+5E]
0040604D 53        PUSH EBX
0040604E 50        PUSH EAX
0040604F FF95 490F0000 CALL DWORD PTR SS:[EBP+F49]
00406055 8985 4D050000 MOV DWORD PTR SS:[EBP+54D],EAX
0040605B 8D5D 6B     LEA EBX,DWORD PTR SS:[EBP+6B]
0040605E 53        PUSH EBX
0040605F 57        PUSH EDI
00406060 FF95 490F0000 CALL DWORD PTR SS:[EBP+F49]
00406066 8985 51050000 MOV DWORD PTR SS:[EBP+551],EAX
0040606C 8D45 77     LEA EAX,DWORD PTR SS:[EBP+77]
0040606F FFE0     JMP EAX
00406071 56        PUSH ESI
00406072 6972 74 75616C41 IMUL ESI,DWORD PTR DS:[EDX+74],416C6175
00406079 6C        INS BYTE PTR ES:[EDI],DX
  
```

Quand il est ouvert dans OllyDBG le programme commence au PUSHAD en 00406001. Pourquoi j'ai mis 6001 en rouge ? Parce que c'est l'actuel EP ( Entry Point ) et non l'OEP ( Original Entry Point ).

Alors commençons !

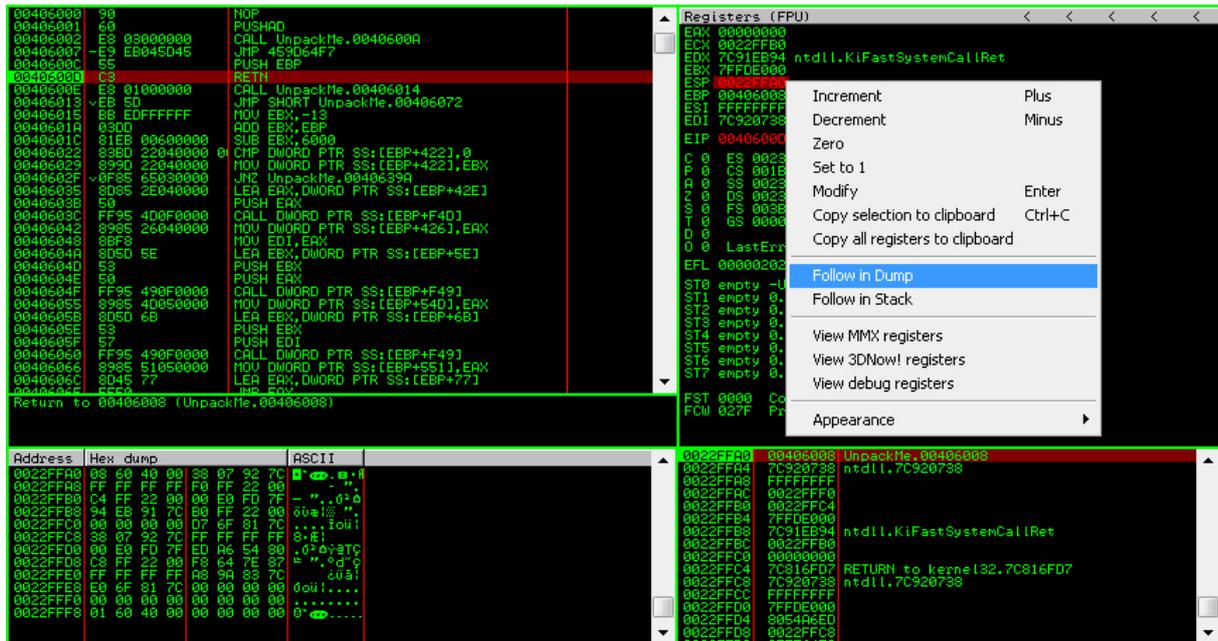
Quand vous l'ouvrez avec OllyDBG, un message d'erreur vient vous dire que l'EP se situe en dehors du Code. Cliquez sur "Ok" et continuons :



Vous commencez au PUSHAD à la ligne 00406001.

Faites une série de F7 ( Et surtout pas F8 ) jusqu'à arriver au RETN en 0040600D ( 5x F7 en tout ).

Arrivé là, faites un Clic droit sur le contenu du registre ESP, puis ->> Follow in Dump.

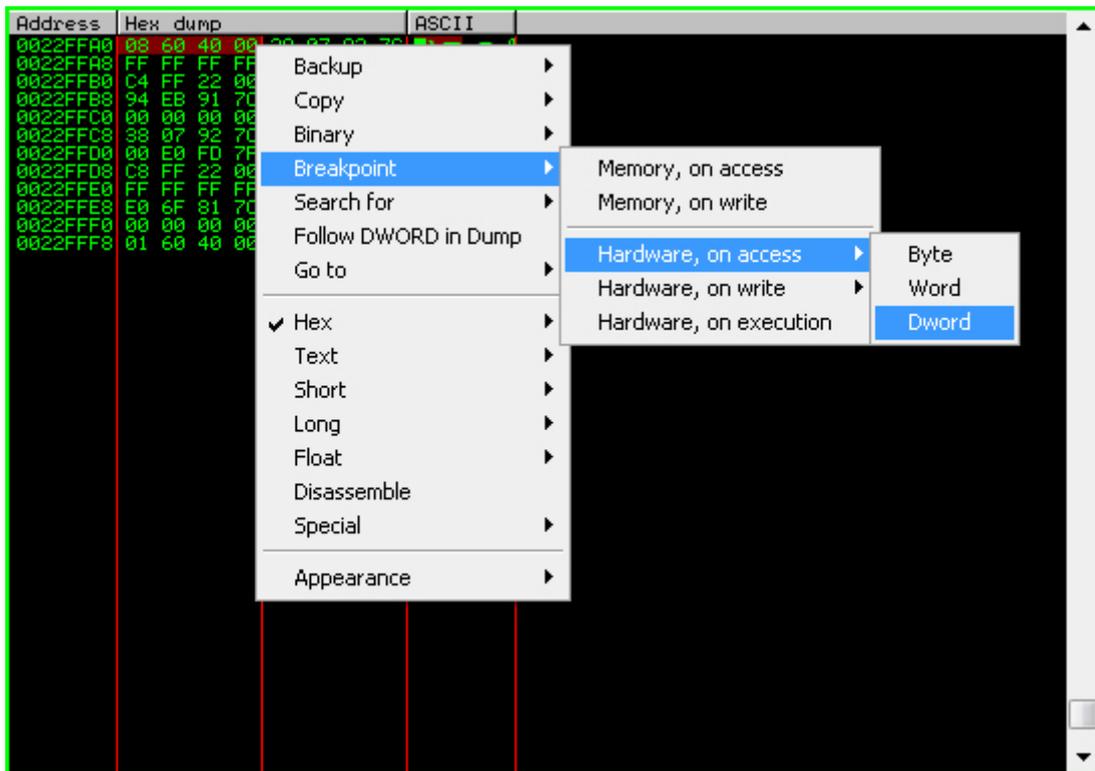


Arrivé dans le Dump à l'adresse 0022FFA0 ( Contenu du registre ESP ), sélectionnez les 4 premiers nombres Hexadécimaux, puis Clic droit ->> Breakpoint ->> Hardware, on Access ->> Dword.

Il faut sélectionner les 4 premiers car l'on veut savoir à quel moment le registre ESP va être consulté et comme c'est un registre de 32 Bits, il faut mettre un Breakpoint sur l'ensemble du registre.

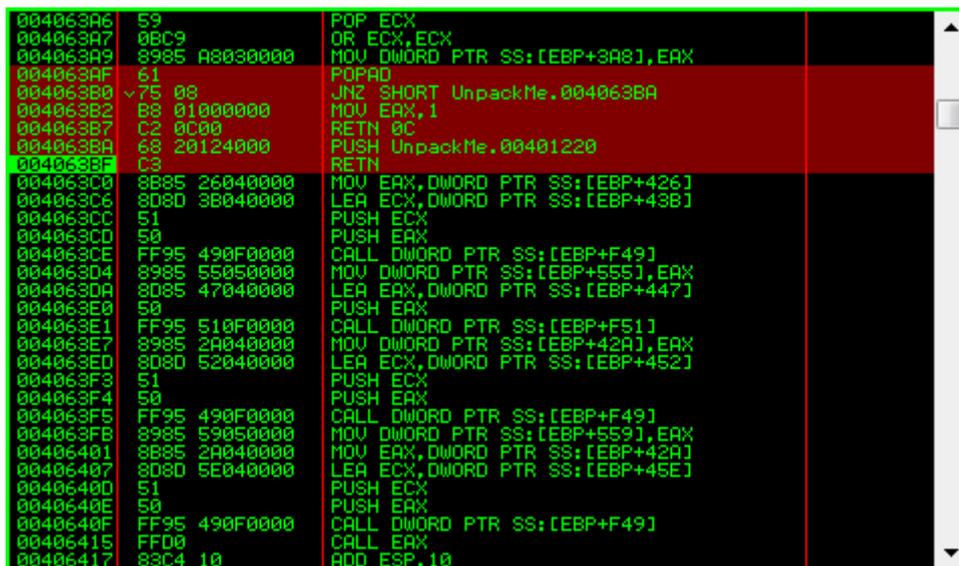
Petite parenthèse :

- Byte == 8 Bits
- Word == 16 Bits
- Dword == 32 Bits



Une fois le Breakpoint en place, lancez-le avec F9. Vous allez Breaker en 004063B0, une ligne après le POPAD.

Continuez F8 jusqu'à arriver au RETN à l'adresse 004063BF. Là on se trouve à la dernière ligne du Packer, faites un F8 de plus et vous arriverez en 00401220.

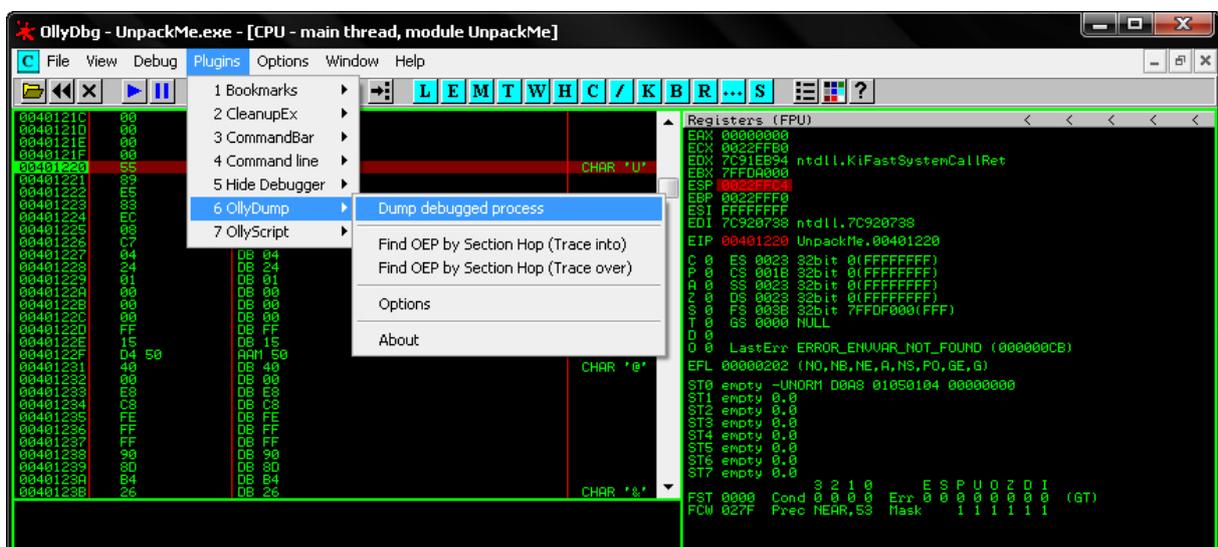


L'OEP se situe donc en 00401220. Maintenant cela change un peu par rapport au [Cours N° 8](#). Pour faire le Dump on ne va se servir de ProcDump, Mais d'un Plugin d'OllyDBG appelé "OllyDump" téléchargeable [ICI](#) ou dans la rubrique "[Download](#)" :

- <http://www.KromCrack.com/prog/OllyDump.dll>

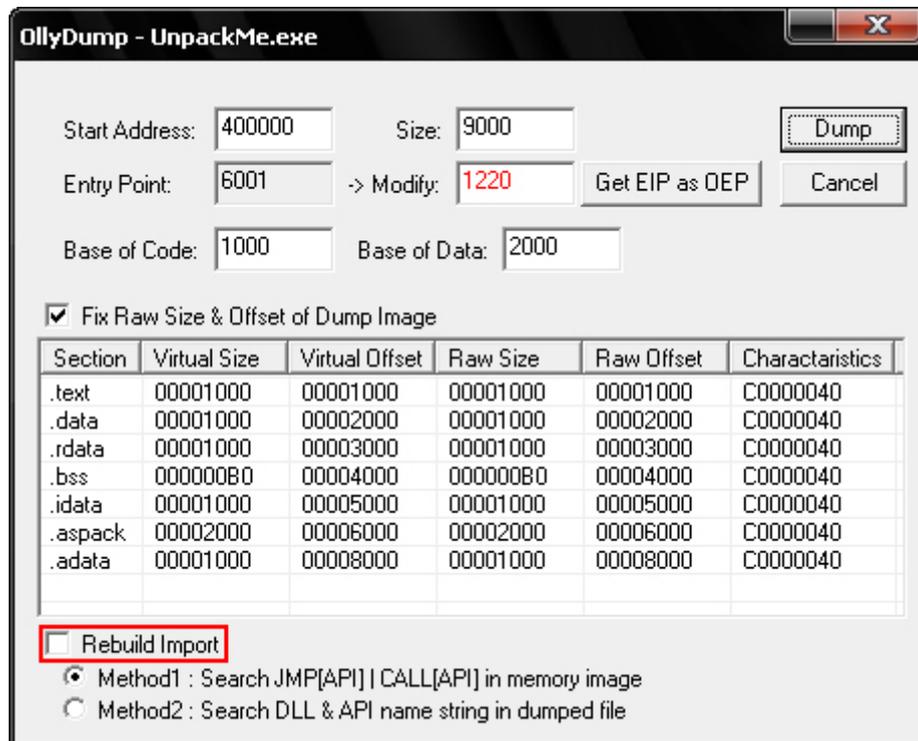
Pour l'installer, vous devez la placer dans le même répertoire qu'OllyDBG. une fois arrivé à la ligne 00401220 ( qui est l'OEP ) faites :

- Plugins ->> OllyDump ->> Dump debugged process.

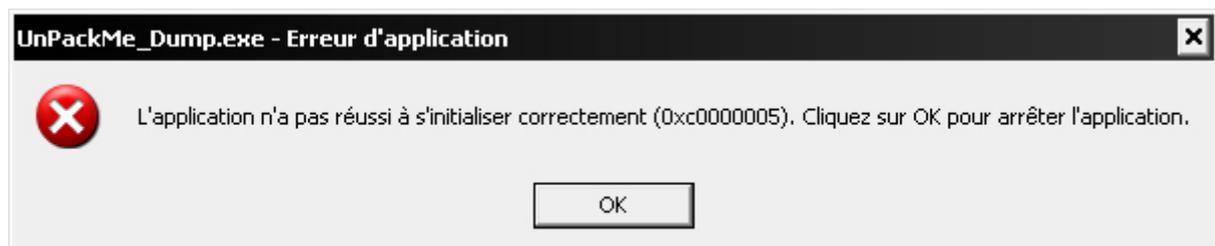


Une nouvelle fenêtre s'ouvre et nous voyons l'EP : 6001 et l'OEP : 1220

Décochez la case "Rebuild Import", puis Cliquez sur "Dump", et sauvez-le sous "UnpackMe\_Dump.exe"

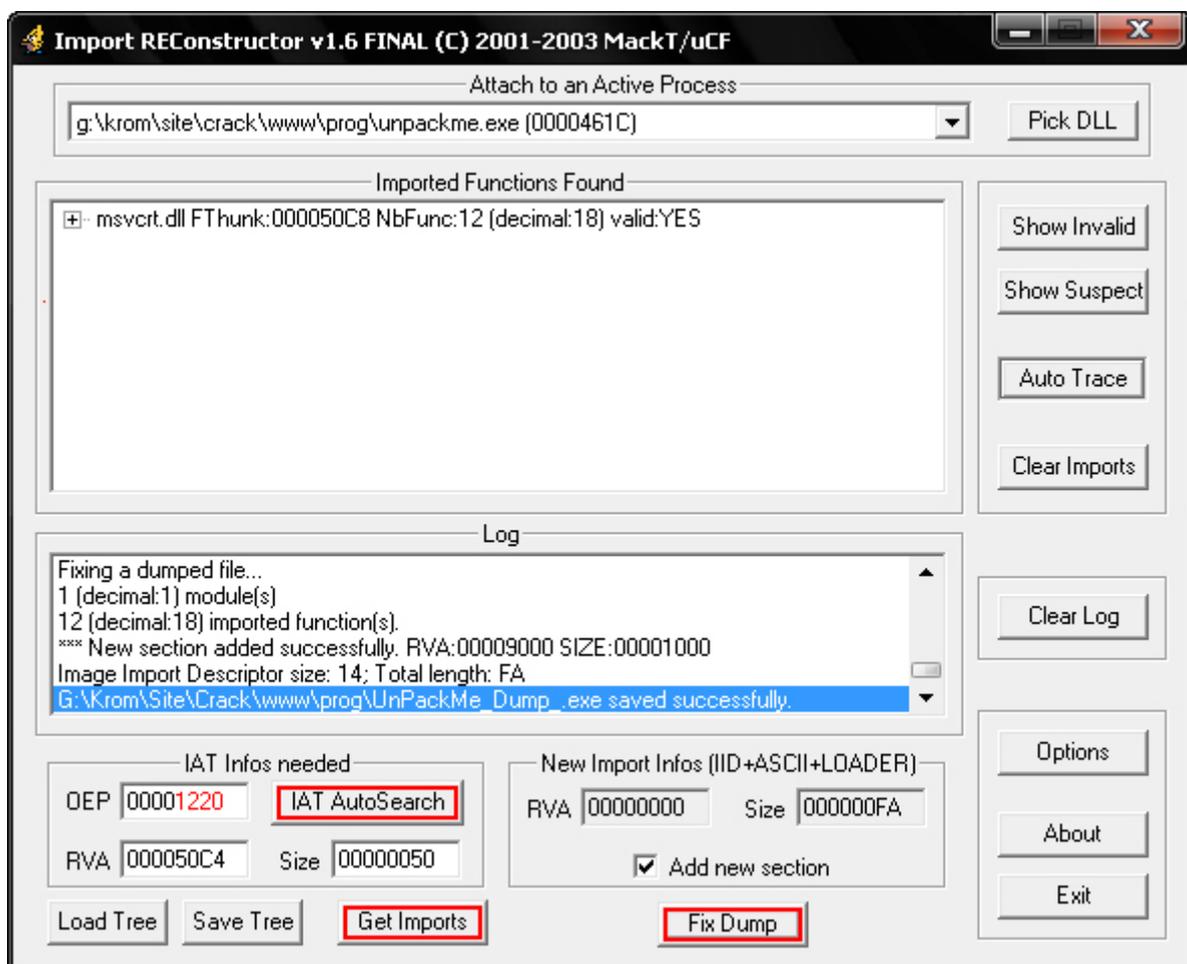


Si vous essayez de l'ouvrir, Windows va vous renvoyer une erreur 0xc0000005 car vous n'avez pas encore reconstituer l'IAT



On va donc la reconstituer avec [ImportRec 1.6](#).

- Il faut lancer le programme Packé - UnpackMe.exe
- Ensuite sélectionnez-le dans "Attach to an Active Process"
- Modifiez l'OEP en y mettant **1220**.
- Cliquez sur "IAT AutoSearch"
- Cliquez ensuite sur "GetImports"
- Puis "Fix Dump" et sélectionnez notre fichier Dumper "UnpackMe\_Dump.exe"
- Le fichier Unpacker est enregistré sous "UnpackMe\_Dump\_.exe"



Et une fois l'UnpackMe Unpacké, vous voyez maintenant un code beaucoup plus clair et plus lisible ;) )

```

00401290 | 55          PUSH EBP
00401291 | . 89E5      MOV EBP,ESP
00401293 | . 88EC 18   SUB ESP,18
00401296 | . 88E4 F0   AND ESP,FFFFFF0
00401299 | . B8 00000000 MOV EAX,0
0040129E | . 83C0 0F   ADD EAX,0F
004012A1 | . C1E8 04   SHR EAX,4
004012A7 | . C1E0 04   SHL EAX,4
004012AA | . 8945 F8   MOV DWORD PTR SS:[EBP-8],EAX
004012AD | . 8B45 F8   MOV EAX,DWORD PTR SS:[EBP-8]
004012B0 | . E8 F0040000 CALL UnPackMe.004017B0
004012B5 | . E8 96010000 CALL UnPackMe.00401450
004012BA | . C745 FC 000000 MOV DWORD PTR SS:[EBP-4],0
004012C1 | . C70424 003040 MOV DWORD PTR SS:[ESP],UnPackMe.00403000
004012C8 | . E8 F3050000 CALL <JMP.&msvcr7.prntf>
004012CD | . C70424 043040 MOV DWORD PTR SS:[ESP],UnPackMe.00403000
004012D4 | . E8 E7050000 CALL <JMP.&msvcr7.prntf>
004012D9 | . C70424 583040 MOV DWORD PTR SS:[ESP],UnPackMe.00403000
004012E0 | . E8 00050000 CALL <JMP.&msvcr7.prntf>
004012E5 | . C70424 AC3040 MOV DWORD PTR SS:[ESP],UnPackMe.00403000
004012EC | . E8 CF050000 CALL <JMP.&msvcr7.prntf>
004012F1 | . C70424 583040 MOV DWORD PTR SS:[ESP],UnPackMe.00403000
004012F8 | . E8 C3050000 CALL <JMP.&msvcr7.prntf>
004012FD | . C70424 043040 MOV DWORD PTR SS:[ESP],UnPackMe.00403000
00401304 | . E8 B7050000 CALL <JMP.&msvcr7.prntf>
00401309 | . C70424 FD3040 MOV DWORD PTR SS:[ESP],UnPackMe.00403000
00401310 | . E8 AB050000 CALL <JMP.&msvcr7.prntf>
00401315 | . 8D45 FC   LEA EAX,DWORD PTR SS:[EBP-4]
00401318 | . 894424 04 MOV DWORD PTR SS:[ESP+4],EAX
0040131C | . C70424 183140 MOV DWORD PTR SS:[ESP],UnPackMe.00403110
00401323 | . E8 80050000 CALL <JMP.&msvcr7.scanf>
00401328 | . 317D FC 510CD1 CMP DWORD PTR SS:[EBP-4],8D00C51
0040132F | . 75 0E     JNZ SHORT UnPackMe.0040133F
00401331 | . C70424 1C3140 MOV DWORD PTR SS:[ESP],UnPackMe.00403110
00401338 | . E8 83050000 CALL <JMP.&msvcr7.prntf>
0040133D | . EB 0C     JMP SHORT UnPackMe.0040134B
0040133F | . C70424 3C3140 MOV DWORD PTR SS:[ESP],UnPackMe.00403110
00401346 | . E8 75050000 CALL <JMP.&msvcr7.prntf>
0040134B | . C70424 583140 MOV DWORD PTR SS:[ESP],UnPackMe.00403110
00401352 | . E8 69050000 CALL <JMP.&msvcr7.prntf>
00401357 | . C70424 5E3140 MOV DWORD PTR SS:[ESP],UnPackMe.00403110
0040135E | . E8 30050000 CALL <JMP.&msvcr7.system>
00401363 | . B8 00000000 MOV EAX,0
00401368 | . C9       LEAVE
00401369 | . C3       RETN
0040136A | . 90       NOP
0040136B | . 90       NOP
0040136C | . 90       NOP
0040136D | . 90       NOP
0040136E | . 90       NOP
0040136F | . 90       NOP
00401370 | . 90       NOP
00401371 | . 90       NOP
00401372 | . 90       NOP
00401373 | . 90       NOP
00401374 | . 90       NOP
00401375 | . 90       NOP
00401376 | . 90       NOP
00401377 | . 90       NOP
00401378 | . 90       NOP
00401379 | . 90       NOP
0040137A | . 90       NOP
0040137B | . 90       NOP
0040137C | . 90       NOP
0040137D | . 90       NOP
0040137E | . 90       NOP
0040137F | . 90       NOP
00401380 | . 90       NOP
00401381 | . 90       NOP
00401382 | . 90       NOP
00401383 | . 90       NOP
00401384 | . 90       NOP
00401385 | . 90       NOP
00401386 | . 90       NOP
00401387 | . 90       NOP
00401388 | . 90       NOP
00401389 | . 90       NOP
0040138A | . 90       NOP
0040138B | . 90       NOP
0040138C | . 90       NOP
0040138D | . 90       NOP
0040138E | . 90       NOP
0040138F | . 90       NOP
00401390 | . 90       NOP
00401391 | . 90       NOP
00401392 | . 90       NOP
00401393 | . 90       NOP
00401394 | . 90       NOP
00401395 | . 90       NOP
00401396 | . 90       NOP
00401397 | . 90       NOP
00401398 | . 90       NOP
00401399 | . 90       NOP
0040139A | . 90       NOP
0040139B | . 90       NOP
0040139C | . 90       NOP
0040139D | . 90       NOP
0040139E | . 90       NOP
0040139F | . 90       NOP
004013A0 | . 90       NOP
004013A1 | . 90       NOP
004013A2 | . 90       NOP
004013A3 | . 90       NOP
004013A4 | . 90       NOP
004013A5 | . 90       NOP
004013A6 | . 90       NOP
004013A7 | . 90       NOP
004013A8 | . 90       NOP
004013A9 | . 90       NOP
004013AA | . 90       NOP
004013AB | . 90       NOP
004013AC | . 90       NOP
004013AD | . 90       NOP
004013AE | . 90       NOP
004013AF | . 90       NOP
004013B0 | . 90       NOP
004013B1 | . 90       NOP
004013B2 | . 90       NOP
004013B3 | . 90       NOP
004013B4 | . 90       NOP
004013B5 | . 90       NOP
004013B6 | . 90       NOP
004013B7 | . 90       NOP
004013B8 | . 90       NOP
004013B9 | . 90       NOP
004013BA | . 90       NOP
004013BB | . 90       NOP
004013BC | . 90       NOP
004013BD | . 90       NOP
004013BE | . 90       NOP
004013BF | . 90       NOP
004013C0 | . 90       NOP
004013C1 | . 90       NOP
004013C2 | . 90       NOP
004013C3 | . 90       NOP
004013C4 | . 90       NOP
004013C5 | . 90       NOP
004013C6 | . 90       NOP
004013C7 | . 90       NOP
004013C8 | . 90       NOP
004013C9 | . 90       NOP
004013CA | . 90       NOP
004013CB | . 90       NOP
004013CC | . 90       NOP
004013CD | . 90       NOP
004013CE | . 90       NOP
004013CF | . 90       NOP
004013D0 | . 90       NOP
004013D1 | . 90       NOP
004013D2 | . 90       NOP
004013D3 | . 90       NOP
004013D4 | . 90       NOP
004013D5 | . 90       NOP
004013D6 | . 90       NOP
004013D7 | . 90       NOP
004013D8 | . 90       NOP
004013D9 | . 90       NOP
004013DA | . 90       NOP
004013DB | . 90       NOP
004013DC | . 90       NOP
004013DD | . 90       NOP
004013DE | . 90       NOP
004013DF | . 90       NOP
004013E0 | . 90       NOP
004013E1 | . 90       NOP
004013E2 | . 90       NOP
004013E3 | . 90       NOP
004013E4 | . 90       NOP
004013E5 | . 90       NOP
004013E6 | . 90       NOP
004013E7 | . 90       NOP
004013E8 | . 90       NOP
004013E9 | . 90       NOP
004013EA | . 90       NOP
004013EB | . 90       NOP
004013EC | . 90       NOP
004013ED | . 90       NOP
004013EE | . 90       NOP
004013EF | . 90       NOP
004013F0 | . 90       NOP
004013F1 | . 90       NOP
004013F2 | . 90       NOP
004013F3 | . 90       NOP
004013F4 | . 90       NOP
004013F5 | . 90       NOP
004013F6 | . 90       NOP
004013F7 | . 90       NOP
004013F8 | . 90       NOP
004013F9 | . 90       NOP
004013FA | . 90       NOP
004013FB | . 90       NOP
004013FC | . 90       NOP
004013FD | . 90       NOP
004013FE | . 90       NOP
004013FF | . 90       NOP

```

J'espère que ce cours a été clair ;) )

Si vous avez rencontré une erreur ou que quelque chose ne marche pas, vous pouvez [m'envoyer un mail](mailto:Admin@KromCrack.com) à **Admin@KromCrack.com** ou en parler sur [le forum](#) :

- <http://www.KromCrack.com/forum/>