

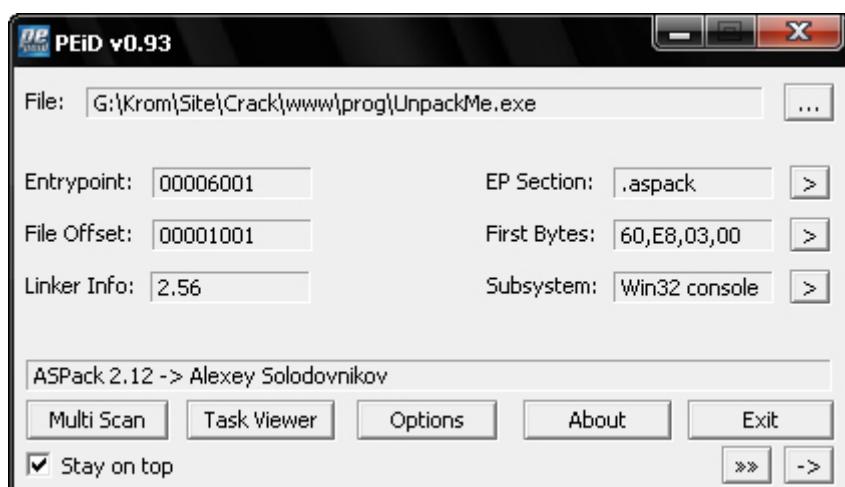
Cours N° 9

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.

```

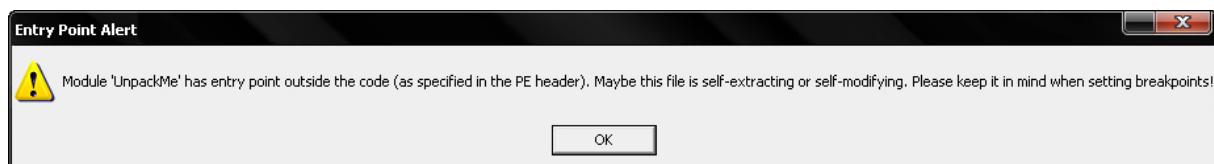
00406001 60          PUSHAD
00406002 E8 03000000  CALL UnpackMe.0040600A
00406007 -E9 EB045D45  JMP 459064F7
0040600C 55          PUSH EBP
00406000 C9          RETN
0040600E E8 01000000  CALL UnpackMe.00406014
00406013 ✓EB SD        JMP SHORT UnpackMe.00406072
00406015 BB EDFFFFFF  MOU EBX,-13
0040601A 03D0          ADD EBX,EBP
0040601C 81EB 00600000  SUB EBX,6000
00406022 83BD 22040000 00  CMP DWORD PTR SS:[EBP+422],0
00406029 8990 22040000  MOU DWORD PTR SS:[EBP+422],EBX
0040602F ✓0F85 65B30000  JNZ UnpackMe.0040639A
00406035 8D85 2E040000  LEA EAX,DWORD PTR SS:[EBP+42E]
0040603B 50          PUSH EAX
0040603C FF95 400F0000  CALL DWORD PTR SS:[EBP+F40]
00406042 8985 26040000  MOU DWORD PTR SS:[EBP+426],EAX
00406048 8BF8          MOU EDI,EAX
0040604A 8D50 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 40050000  MOU DWORD PTR SS:[EBP+540],EAX
00406058 8D50 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 51B50000  MOU 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
0040607A 48          ENDS
I/O command

```

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'ouvrir 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.

The screenshot shows the Immunity Debugger interface with several panes:

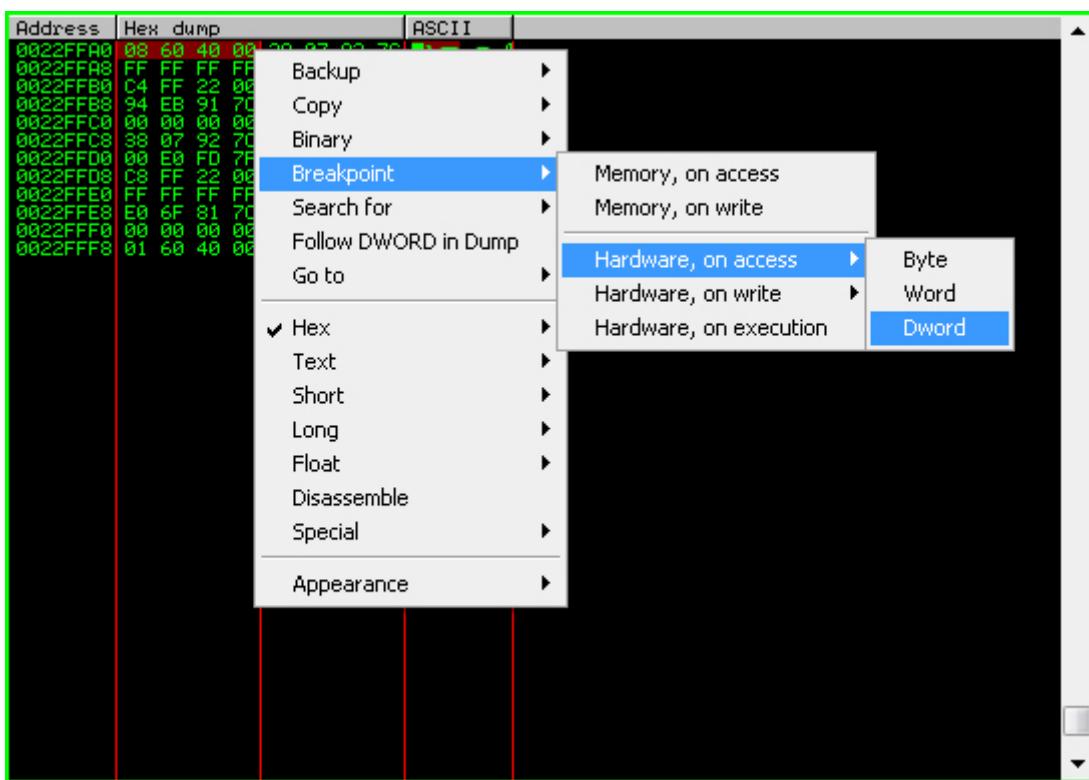
- Registers (FPU) pane:** Shows CPU registers (ERX, ECX, EDX, EBX, ECSP, ECBP, ECIP, EFL) and floating-point registers (ST0-ST7). A context menu is open over the ECIP register.
- Stack pane:** Shows the current stack state with various memory addresses and their values.
- Memory dump pane:** Shows the memory dump starting at address 00222FF00.
- Registers pane:** Shows CPU registers (ERX, ECX, EDX, EBX, ECSP, ECBP, ECIP, EFL).
- Call stack pane:** Shows the call stack with function names and addresses.

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.

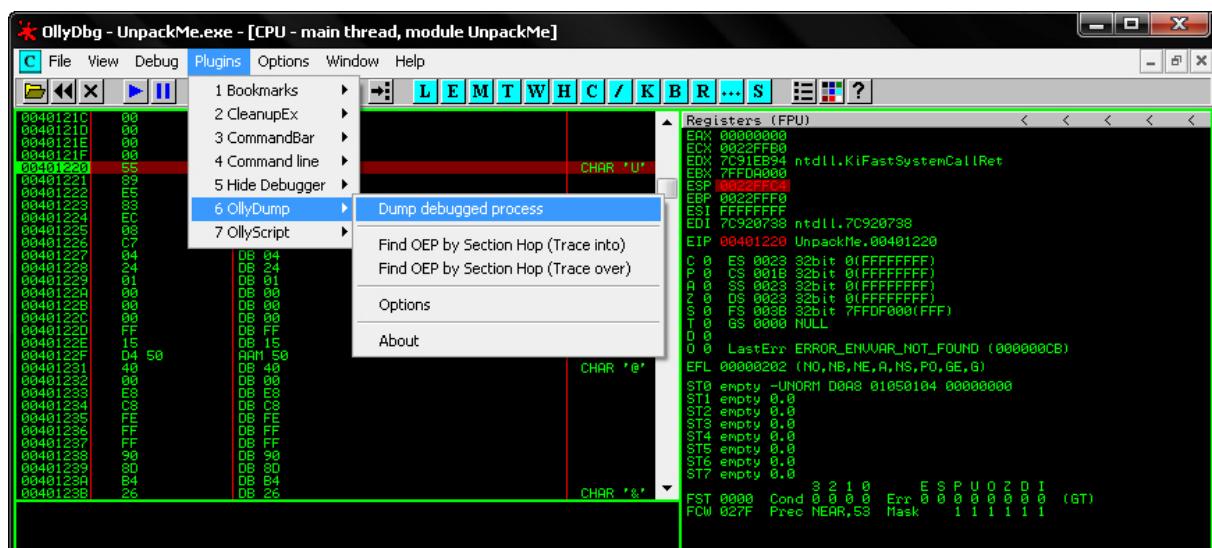
004063A6	59	POP ECX
004063A7	0BC9	OR ECX,ECX
004063A9	8985 A8030000	MOU DWORD PTR SS:[EBP+3A81],EAX
004063A9F	61	POPAD
004063B00	v75 08	JNZ SHORT UnpackMe.004063BA
004063B2	B8 01000000	MOU EAX,1
004063B7	C2 0C00	RETN 0C
004063B9	68 20124000	PUSH UnpackMe.00401220
004063BF	C3	RETN
004063C0	8B85 26040000	MOU EAX,DWORD PTR SS:[EBP+426]
004063C6	8D8D 3B040000	LEA ECX,DWORD PTR SS:[EBP+43B]
004063CC	51	PUSH ECX
004063CD	50	PUSH EAX
004063CE	FF95 490F0000	CALL DWORD PTR SS:[EBP+F49]
004063D4	8985 55050000	MOU DWORD PTR SS:[EBP+555],EAX
004063DA	8D85 47040000	LEA EAX,DWORD PTR SS:[EBP+447]
004063E0	50	PUSH EAX
004063E1	FF95 510F0000	CALL DWORD PTR SS:[EBP+F51]
004063E7	8985 2A040000	MOU DWORD PTR SS:[EBP+42A],EAX
004063ED	8D8D 52040000	LEA ECX,DWORD PTR SS:[EBP+452]
004063F3	51	PUSH ECX
004063F4	50	PUSH EAX
004063F5	FF95 490F0000	CALL DWORD PTR SS:[EBP+F49]
004063FB	8985 59050000	MOU DWORD PTR SS:[EBP+559],EAX
00406401	8B85 2A040000	MOU EAX,DWORD PTR SS:[EBP+42A]
00406407	8D8D 5E040000	LEA ECX,DWORD PTR SS:[EBP+45E]
0040640D	51	PUSH ECX
0040640E	50	PUSH EAX
0040640F	FF95 490F0000	CALL DWORD PTR SS:[EBP+F49]
00406415	FFD0	CALL EAX
00406417	83C4 10	ADD ESP,10

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>

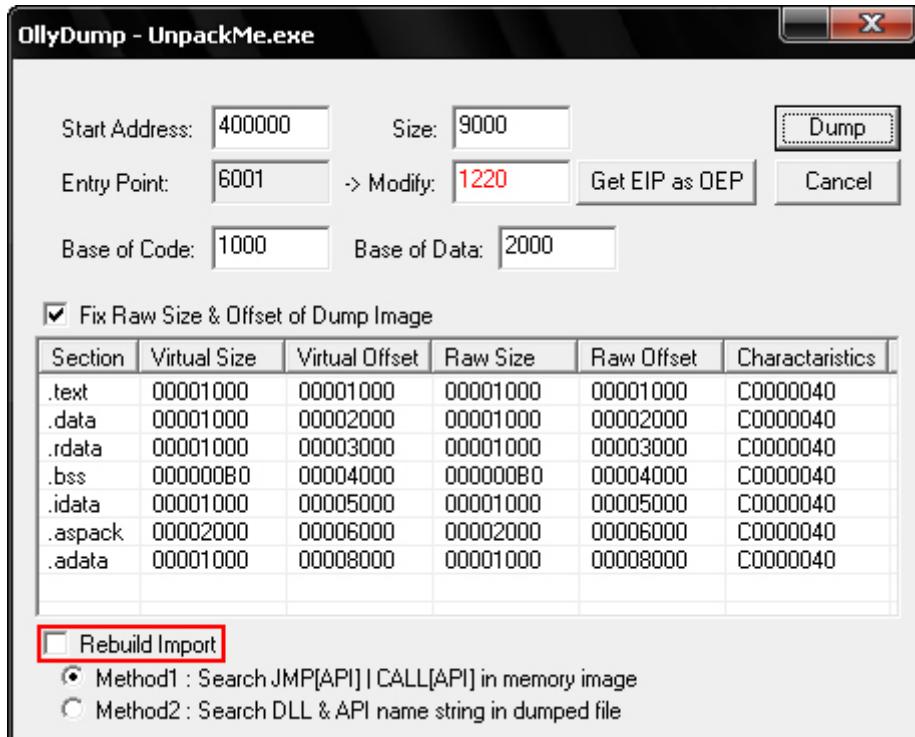
Pour l'installer, vous devez la placer dans le même répertoire qu'OllyDBG. une fois arrivé à la ligne 00401220 (qui est l'OEP) faites :

- 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"

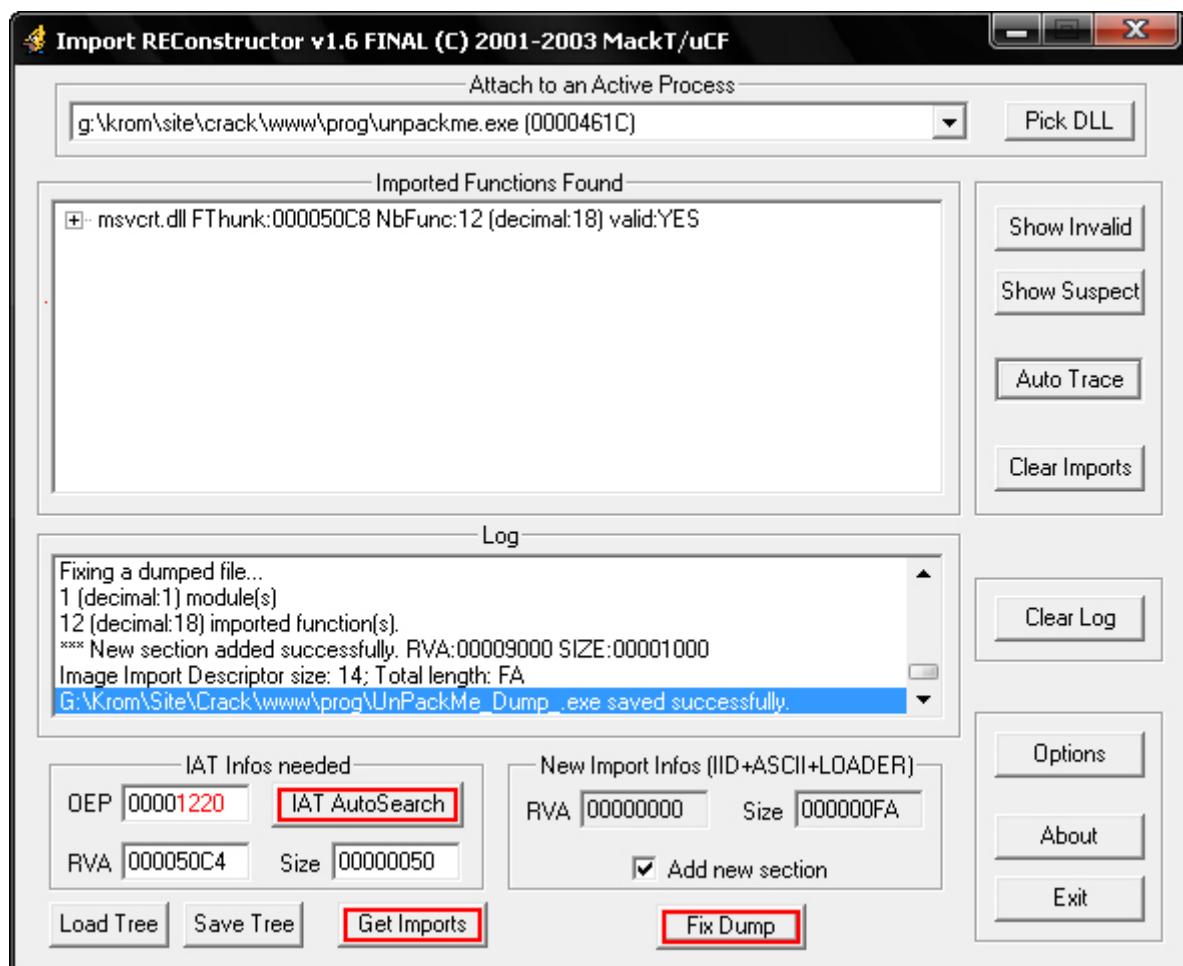


Si vous essayez de l'ouvrir, Windows va vous renvoyer une erreur 0xc0000005 car vous n'avez pas encore reconstituer l'IAT



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    ; 89EC    SUB ESP,18
00401296    ; 89E4    AND ESP,FFFFFF0
00401297    ; B8 00000000 MOV ERX,0
0040129E    ; 89C9    ADD ERX,0F
004012A1    ; 89C9    ADD ERX,0F
004012A4    ; C1E8    SHR ERX,4
004012A7    ; C1E0    SHL ERX,4
004012A9    ; 8945    MOV DWORD PTR SS:[EBP-8],ERX
004012A0    ; 8845    MOV ERX,DWORD PTR SS:[EBP-8]
004012B0    ; E8 FB040000 CALL UnPackMe.004017B0
004012B5    ; E8 96010000 CALL UnPackMe.00401450
004012B8    ; C745 FC 000000 MOV DWORD PTR SS:[EBP-4],0
004012C1    ; C70424 003040 MOV DWORD PTR SS:[ESP],UnPackMe.00403000
004012C8    ; E8 F3058000 CALL <JMP.&msvct.printf>
004012CD    ; C70424 043040 MOV DWORD PTR SS:[ESP],UnPackMe.00403000
004012D4    ; E8 E7058000 CALL <JMP.&msvct.printf>
004012D9    ; C70424 583040 MOV DWORD PTR SS:[ESP],UnPackMe.00403050
004012E0    ; E8 D8058000 CALL <JMP.&msvct.printf>
004012E5    ; C70424 AC0040 MOV DWORD PTR SS:[ESP],UnPackMe.004030A0
004012EC    ; E8 CF050000 CALL <JMP.&msvct.printf>
004012F1    ; C70424 583040 MOV DWORD PTR SS:[ESP],UnPackMe.00403050
004012F8    ; E8 C3050000 CALL <JMP.&msvct.printf>
004012FD    ; C70424 043040 MOV DWORD PTR SS:[ESP],UnPackMe.00403000
00401304    ; E8 B7050000 CALL <JMP.&msvct.printf>
00401309    ; C70424 FD0040 MOV DWORD PTR SS:[ESP],UnPackMe.004030F0
00401318    ; E8 AB050000 CALL <JMP.&msvct.printf>
00401315    ; 8045 FC LEA ERX,DWORD PTR SS:[EBP-4]
00401318    ; 894424 04 MOV DWORD PTR SS:[ESP+4],ERX
0040131C    ; C70424 183140 MOV DWORD PTR SS:[ESP],UnPackMe.00403110
00401323    ; E8 88050000 CALL <JMP.&msvct.scanf>
00401328    ; 8170 FC 510CD0 CMP DWORD PTR SS:[EBP-41],8000C51
0040132F    ; JNZ SHORT UnPackMe.0040133F
00401331    ; C70424 1C3140 MOV DWORD PTR SS:[ESP],UnPackMe.00403110
00401338    ; E8 83050000 CALL <JMP.&msvct.printf>
0040133D    ; E8 0C JMP SHORT UnPackMe.0040134B
0040133F    ; > C70424 3C3140 MOV DWORD PTR SS:[ESP],UnPackMe.00403130
00401346    ; E8 75050000 CALL <JMP.&msvct.printf>
0040134B    ; > C70424 583140 MOV DWORD PTR SS:[ESP],UnPackMe.00403150
00401352    ; E8 69050000 CALL <JMP.&msvct.printf>
00401357    ; C70424 5E3140 MOV DWORD PTR SS:[ESP],UnPackMe.00403150
0040135E    ; E8 3D050000 CALL <JMP.&msvct.system>
00401363    ; E8 00000000 MOV ERX,0
00401368    ; C9 LEAVE
00401369    ; C3 RETN
0040136A    ; 90 NOP
0040136B    ; 90 NOP
0040136C    ; 90 NOP
0040136D    ; 90 NOP
004013EE    ; 90 NOP

```

printf
 printf
 printf
 printf
 printf
 printf
 printf
 ASCII 0A,"Entrez le "
 printf
 ASCII "%d"
 scanf
 ASCII "Bo - Yeah ! Bon mot de passe ;)"
 printf
 ASCII "Bo - Non, essaie encore ..."
 printf
 ASCII "oooo"
 printf
 ASCII "PAUSE"
 system

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](#) à **Admin@KromCrack.com** ou en parler sur [le forum](#) :

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