Cours N° 8

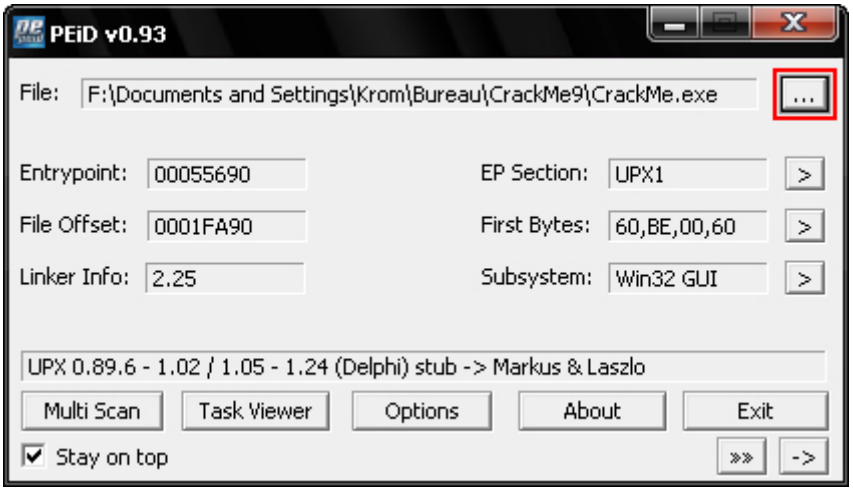
Voilà un cours qui parlera d'un sujet que vous avez peut-être déjà rencontré un jour ou l'autre, celui d'un programme qui a été compressé ou crypté. On peut le voir pour plusieurs raisons :

- Un message d'erreur nous prévient quand on désassemble le programme.
- On ne voit aucunes Strings Data References ou aucuns text dans le programme.
- On ne peut pas Débugger le programme.
- ...

Un des réflexes à prendre quand vous voulez Cracker un programme est de systématiquement l'analyser avec PEiD :

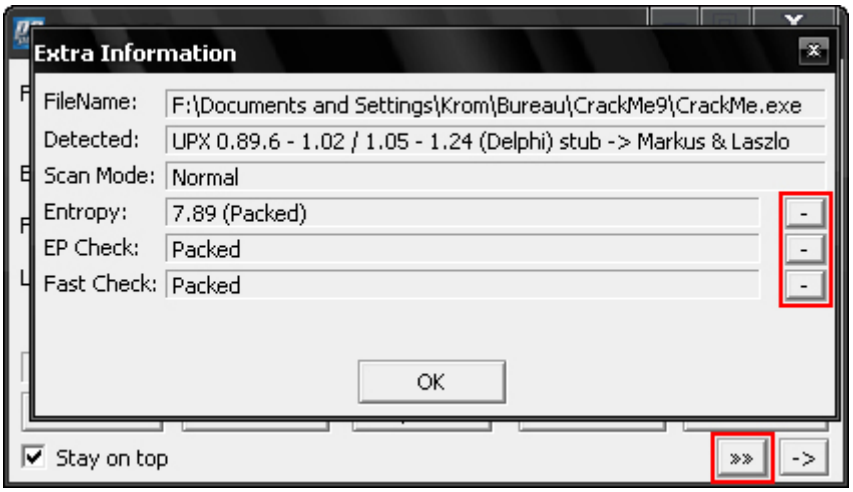
- **http://www.KromCrack.com/prog/Peid-0.93.exe**

Ouvrez PEiD et sélectionnez le programme à analyser en cliquant sur [...] en haut a droite



On voit tout de suite qu'il a été crypté par " UPX 0.89.6 - 1.02 / 1.05 - 1.24 (Delphi) stub -> Markus et Laszlo "
Si aucune protection n'a été détecté, il nous affichera soit " Nothing found * " soit le langage de programmation utilisé comme " Borland Delphi 2.0 " ou " Microsoft C++ " etc ...

Nous pouvons aussi avoir plus de détails sur le Cryptage en appuyant sur [» »] :



Maintenant que nous avons tous les détails sur le type et le nom du package, nous allons pouvoir commencer le Crack.
Pour cela, il vous faudra plusieurs outils :

- ProcDump // Il va nous servir à faire un Dump du programme ainsi qu'à modifier son OEP.
- OllyDBG // Il va nous servir à Dumper notre .exe ainsi qu'a trouver l'OEP.
- ImpRec // Il va nous servir à reconstituer l'IAT.
- CrackMe // Peut être utile à avoir non ?

Comment Packer / Unpacker un programme ?

Le logiciel de compression (dans ce cas c'est UPX (Ultimate Packer for eXecutables)), greffe au logiciel ce que l'on appelle une " Loader ".
Lu but de ce Loader est de modifier l'entry point du programme (Le début du code) pour que ce soit le Loader qui se lance en premier et lance par la suite le programme qu'il va décompresser.

Avant la compression :

- Début du code.
- Fin du code.

Après la compression :

- Lancement du Loader à la place du début du code.
- Décompression en RAM du programme.
- Début du code.
- Fin du code.

Voici les différentes étapes nécessaire à l'unpacking d'un logiciel. :

Recherche de l'OEP

OEP est l'abréviation de Original Entry Point, c'est à partir de cette ligne que le programme non packé va commencer. Lorsqu'un packer est présent, c'est le loader qui se chargera en premier, et qui va commander la décompression du programme. Après avoir décompressé, le Loader va jumper vers l'OEP du programme, afin que celui-ci se lance normalement.

Exemple :

- Loader.
- ...
- ...
- ...
- JMP OEP.

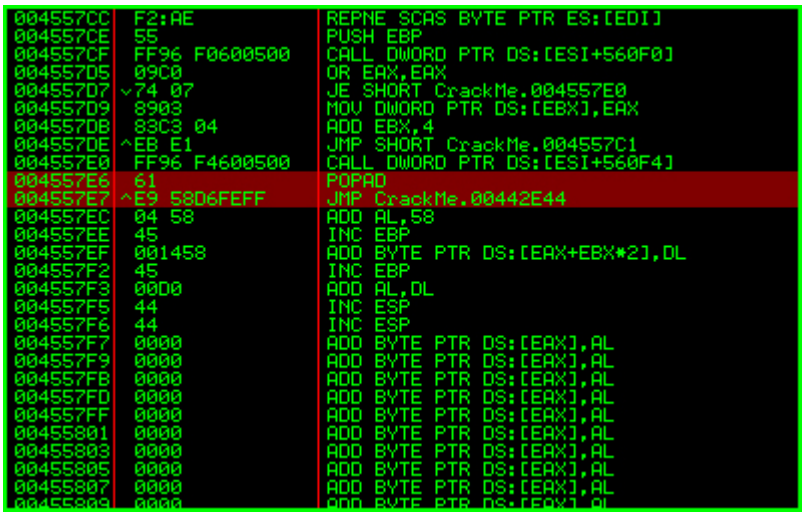
Le Dump du fichier

Un dump, c'est une étape consistant à copier partiellement ou tout un programme en mémoire Comme expliqué ci-dessus, le loader se charge de décompresser le programme en mémoire, puis de l'exécuter. Lors de cette étape, nous allons copier ce qui se trouve en mémoire après l'action du Loader, ce qui signifie que dans notre dump nous aurons (avec le Loader) notre programme décompressé.

Pour Dumper un .exe, on doit trouver Son OEP (Original Entry Point (Son Véritable Début)), pour le faire j'ai dit plus haut que le programme se lançait après le Loader. Voici comment se comporte un programme packé avec UPX :

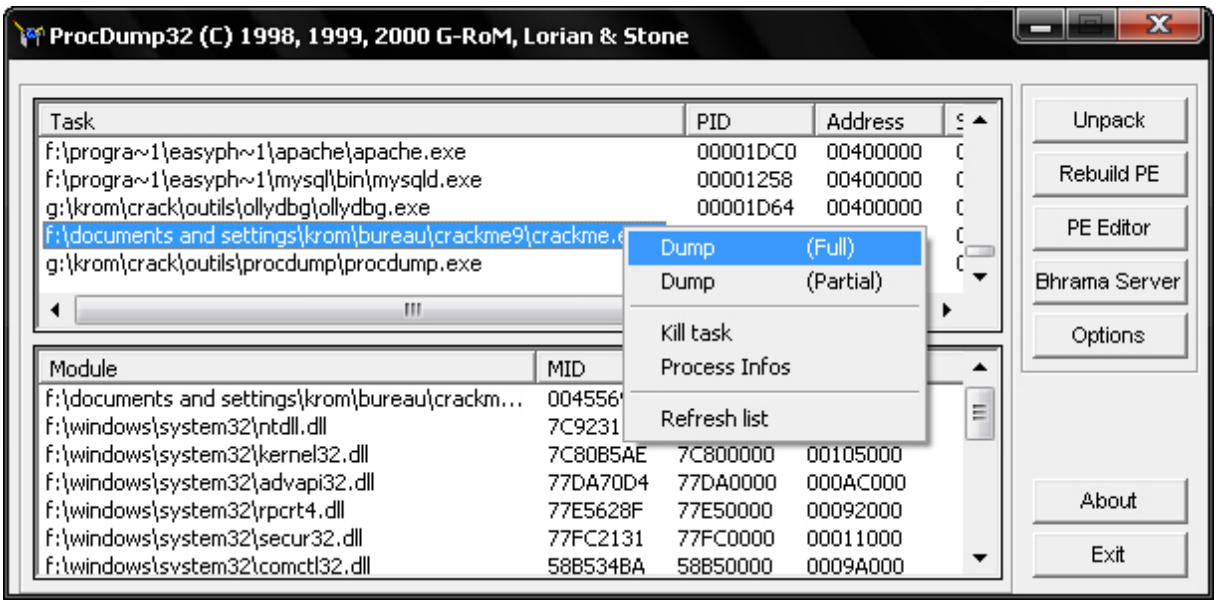
- PUSHAD
- ...
- ...
- POPAD
- JMP OEP

Donc, pour trouver son OEP qui est, après le Loader, il faut don trouver le POPAD car c'est après celui-ci qu'il y aura un saut vers le Début et nous connaîtrons enfin sa véritable adresse ;)
Dans ce Crack-me le POPAD est en fin de Code, nous voyons maintenant que l'adresse de L'OEP est 00442E44 car il y a le JMP qui pointe dessus !



Maintenant, mettez un BreakPoint avec F2 sur le " JMP CrackMe.00442E44 " et lancez le programme avec F9. Pourquoi faire ça ? Parce que maintenant nous savons que le programme est totalement décompressé car nous somme sur la dernière ligne du Loader.

Pour faire le Dump, ouvrez ProcDump.exe (en ayant bien pris soin d'avoir lancé le CrackMe jusqu'au " JMP CrackMe.00442E44 " avec OllyDBG), allez ensuite dans le bas de la liste ->> Clique droit sur le processus ->> Dump (Full).

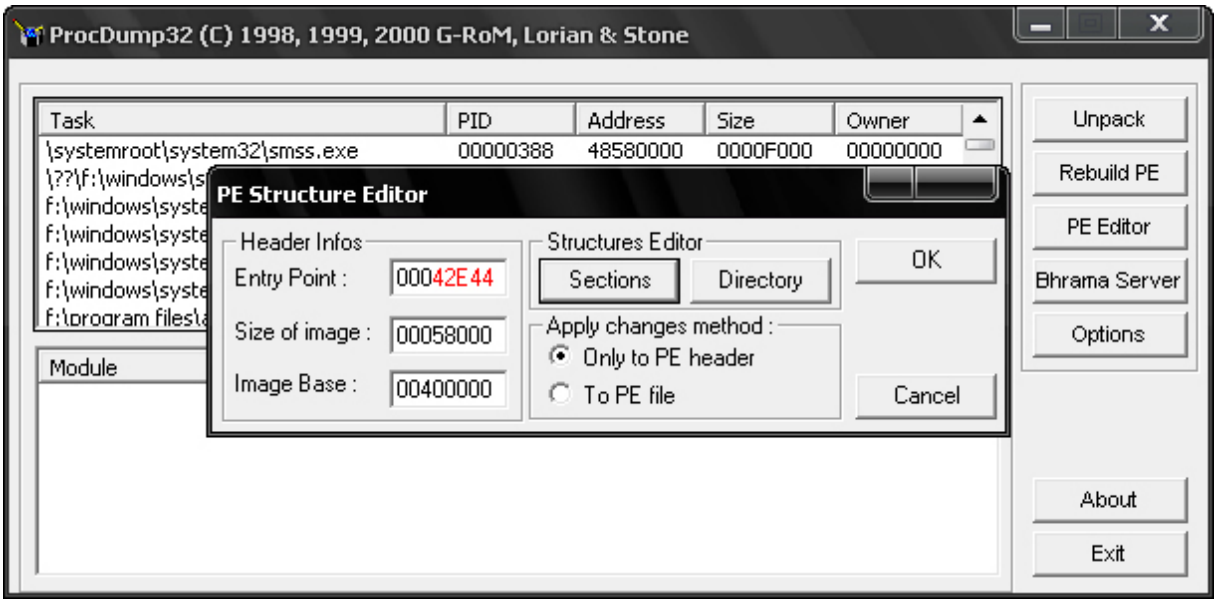


Enregistrez-le sous " CrackMe_Dump.exe ". Souvenez-vous bien de l'adresse 00442E44 qui est en fait l'OEP.

Correction du PE

Le PE contient certaines informations sur le fichier. L'information qui va nous intéresser avec UPX, c'est l'OEP, en effet, UPX modifie l'OEP d'origine pour le remplacer par celui de son Loader, et comme maintenant nous avons le Dump (c'est-à-dire un fichier .exe contenant entre autres le programme décompressé) il nous suffit de remplacer l'OEP du Loader par celui du programme, pour qu'au lancement de celui-ci ce soit réellement le programme qui soit lancé et pas le Loader, devenu inutile.

C'est dans cette étape que nous allons modifier l'OEP. Réouvrez ProcDump.exe, allez cette fois dans " PE Editor " et sélectionnez " CrackMe_Dump.exe ". Une nouvelle fenêtre s'affiche et c'est dans la case " Entry Point " que nous allons mettre notre adresse 00442E44. (En fait nous n'allons mettre que 42E44 car ce n'est que les 5 derniers chiffres qui comptent) :

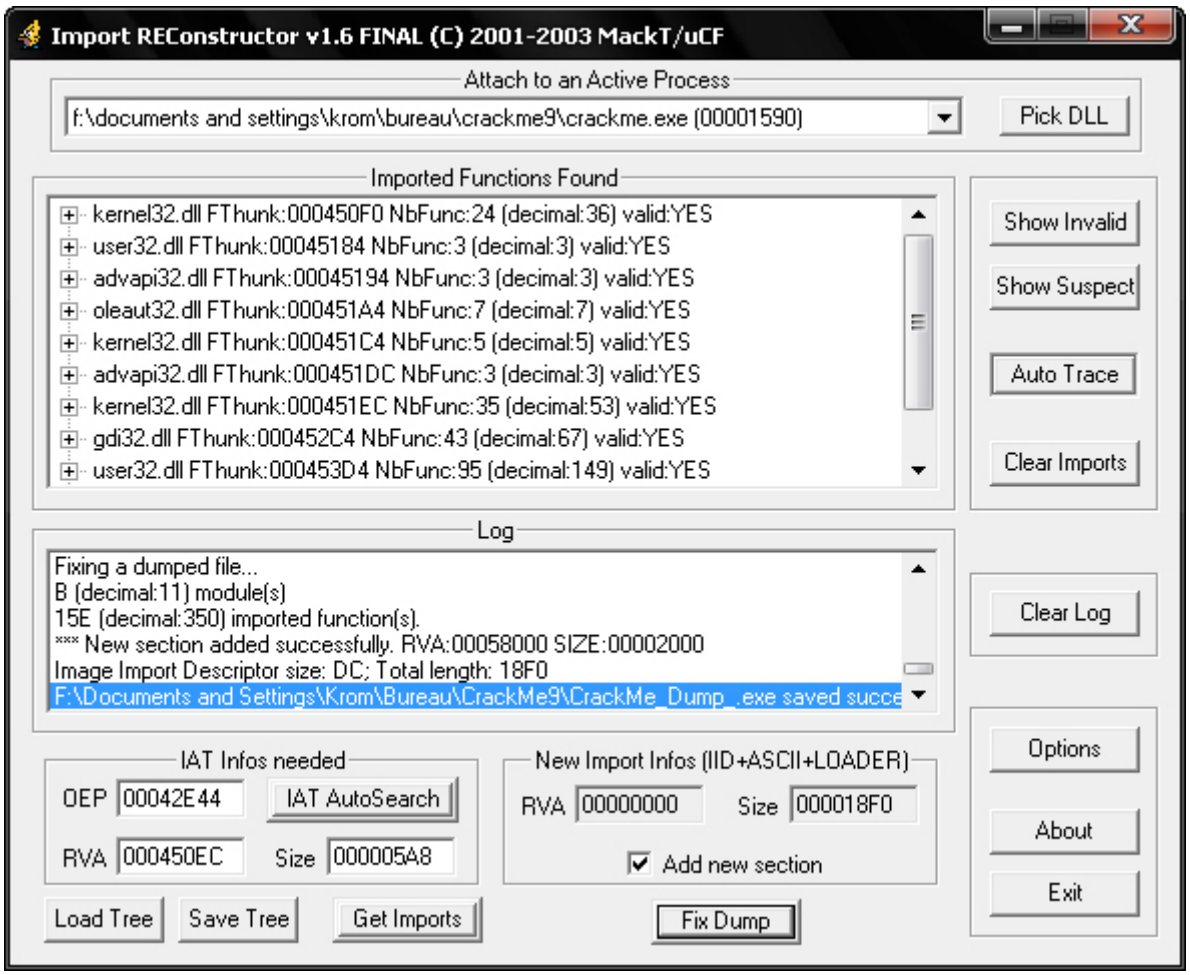


Ensuite fermez la fenêtre en cliquant sur " OK ".

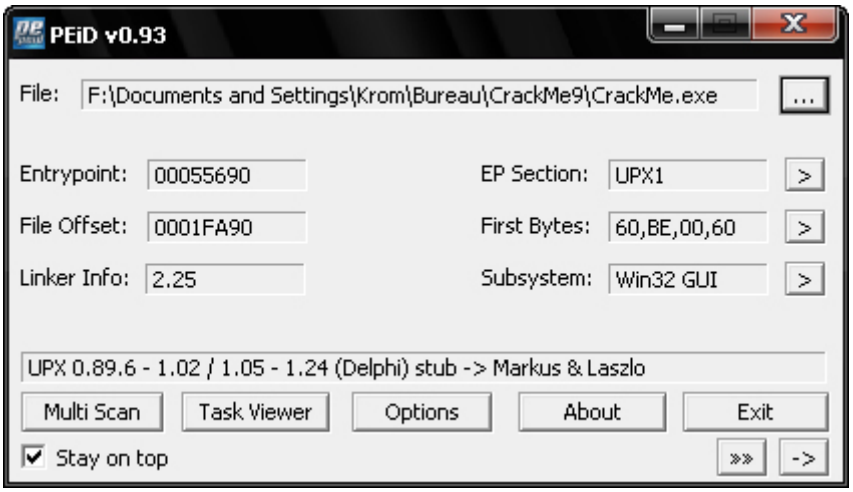
Reconstruction de l'IAT

L'IAT c'est en fait la table des imports, en fait c'est un tableau qui récapitule les .dll utilisées par le programme, ainsi que leurs adresses et celles des fonctions utilisées. On doit le faire car sinon le programme va planter, car il va chercher des noms et des adresses à certains endroits du code et nous, avec notre Dump, on a changé ces adresses.
Marche à suivre :

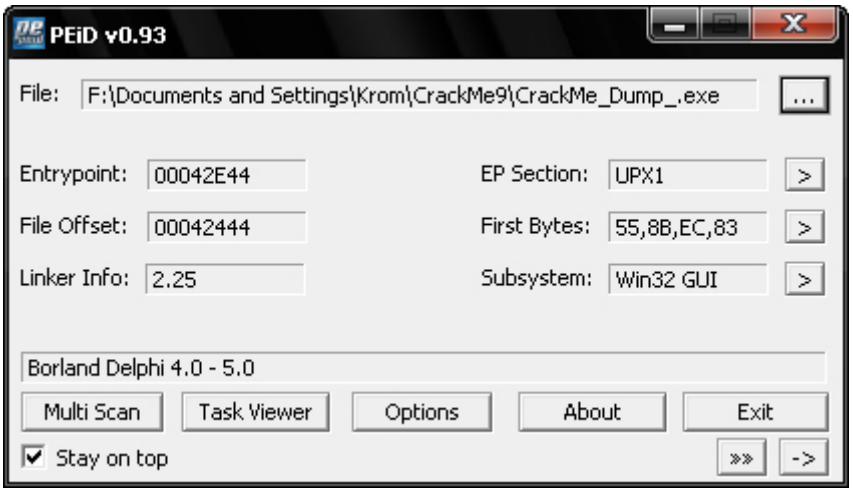
1) Lancez le CrackMe qui est Packé.
2) Sous " Attach to an active process " Sélectionnez CrackMe.exe
3) Modifiez l'OEP sous " IAT Infos needed ".
4) Cliquez sur " IAT Autosearch " et le programme vous indique qu'il a trouvé quelque chose.
5) 5) Cliquez sur " Get Imports " et ImpRec vous donne les fonctions importées.
6) On clique sur " Fix Dump " et une fenêtre s'ouvre. On va chercher notre Dump de tout à l'heure (CrackMe_Dump.exe) et on clique sur OK. ImpRec vient de reconstruire l'IAT de notre Dump.
7) Le programme final est enregistré sous " CrackMe_Dump_.exe "



Avant :



Après :



Maintenant vous pouvez essayer de Cracker ce CrackMe ;)

Le Pass est : " 12011982 "

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/**