Cracker:
“Xilisoft 3GP Video Converter 2.1.53 build-901b”

http://www.xilisoft.com/

Par:
Esp!oN Le rAvaGe /CiM
28/11/2005 - 16 :54

Objectif:

- Cracker le logiciel afin qu'il accepte touts les codes.

Matos:

- Windasm 8.93
- Editeur hexadécimal.

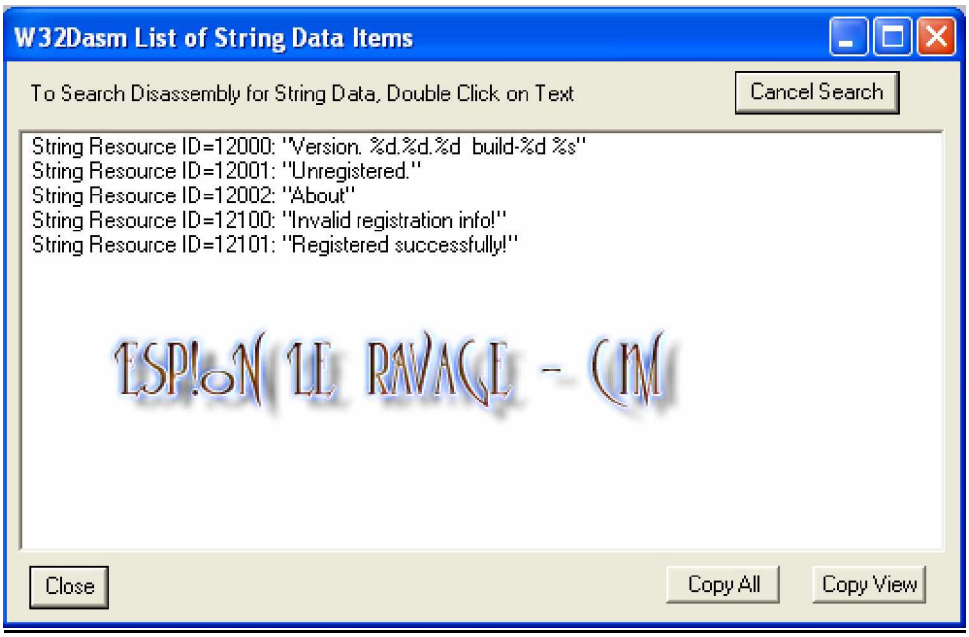
Niveau de difficulté:

- Moyen+

Do it just for fun!

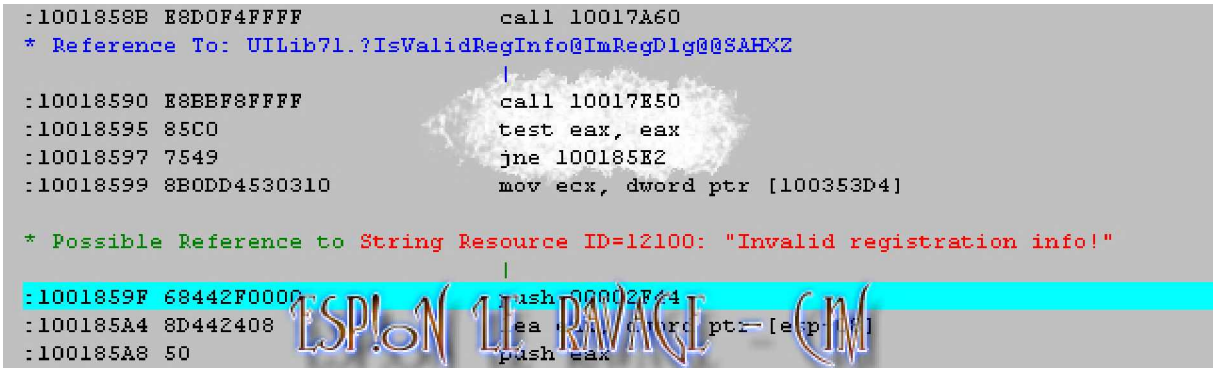
On s'attaque maintenant à un type différent (plus ou moins) de protection, car le fichier à cracker n'est pas l'exécutable lui-même, mais un fichier .dll qui va avec.

Le fichier qui nous intéresse est : " UILib71.dll ", faites une copie de ce fichier et désassemblez la, jetez un coup d'œil sur le listing :

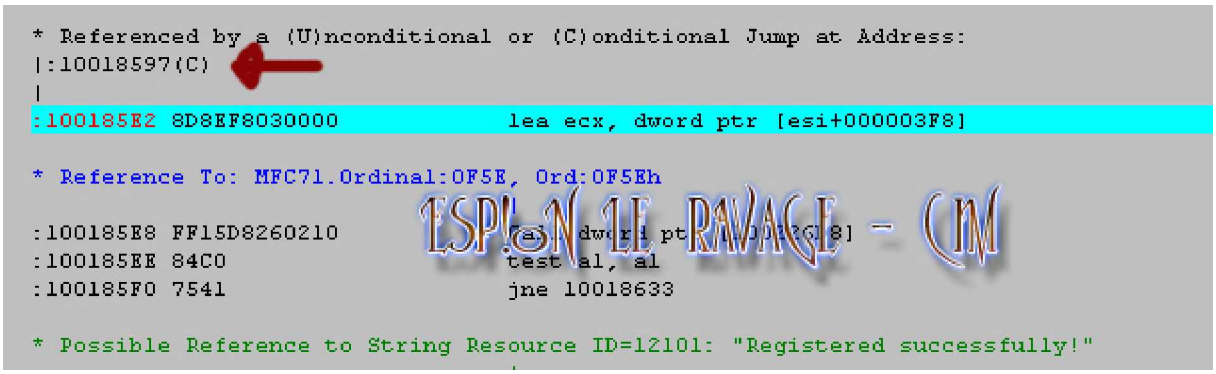


Pour un listing on ne peut pas trouver mieux : 5 ligne avec 5/5 de trucs intéressants !!

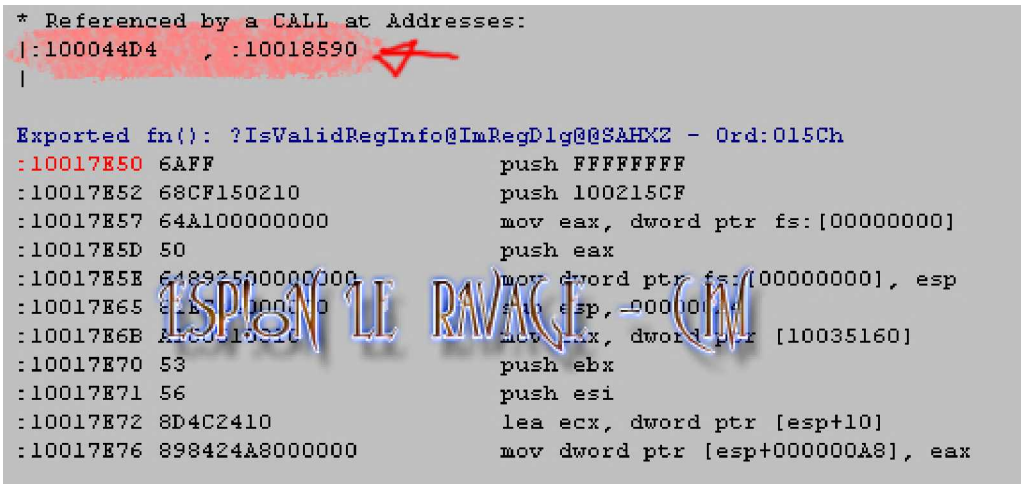
Faites un double clique sur "Invalid registration info!", vous vous trouvez maintenant ici :



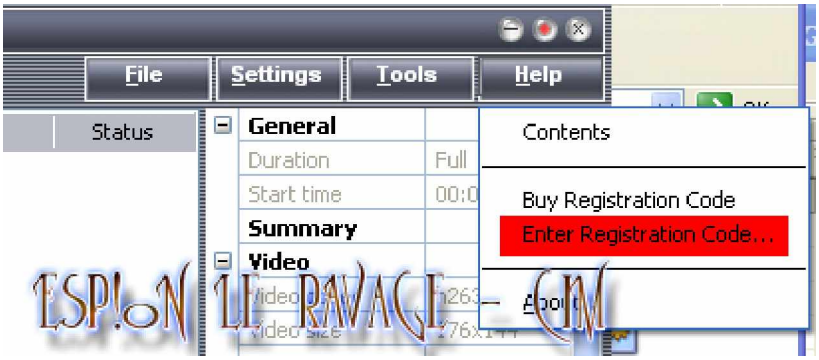
Bonne nouvelle : Call/Test/Saut (ils sont vraiment gentils les éditeurs !!) ; c'est probable à 99% que le :10018597 7549 jne 100185E2 saute vers le bon message ; suivez le pour en avoir l'esprit clair :



C'est exact, maintenant revenez d'où vous venez et entrez dans le call à l'adresse « 10018590 » :

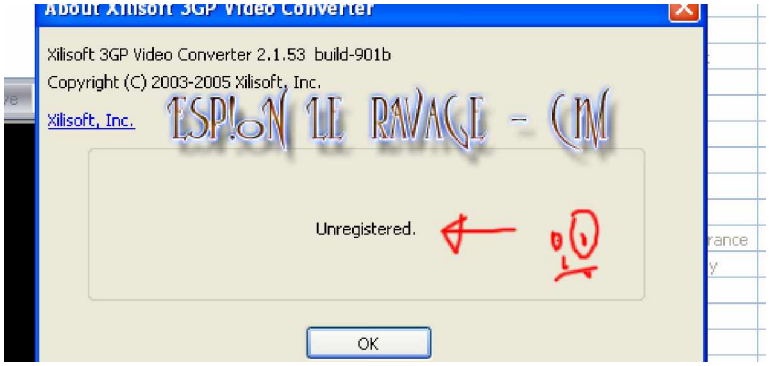


Remarquez (et rappelez vous aussi) d' abord que cette routine est appelée par DEUX call, mais ce n'est pas important à ce stade. Ce qu'il faut faire maintenant c'est de forcer ce call à ce terminer avant de faire la routine, le seul moyen et de mettre un 'ret' à la place du Push, donc notez l'offset de ce push (17E50) puis chargez votre fichier "UILib71.dll" (pas la copie mais le fichier d'origine, car la copie est déjà utilisée par windasm) ensuite changez 6A par C3, enregistrez puis testez :

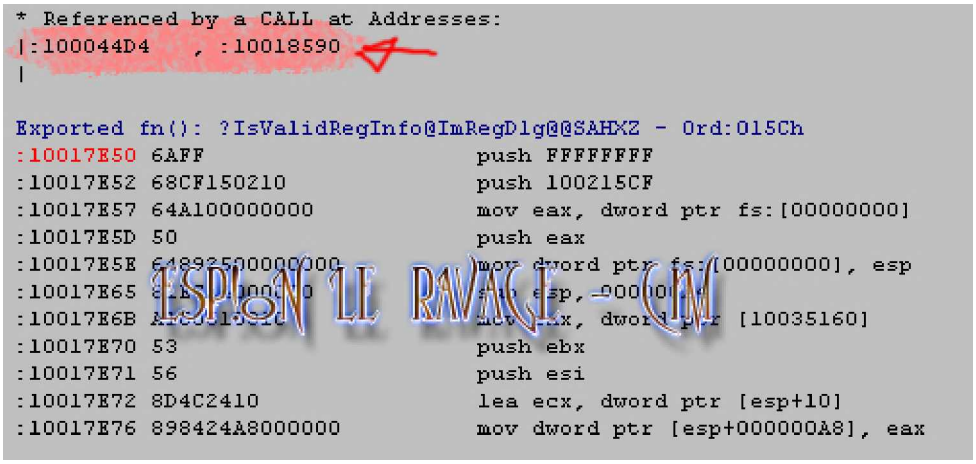


Entrez un nom et n'importe quel serial, validez et ça marche :

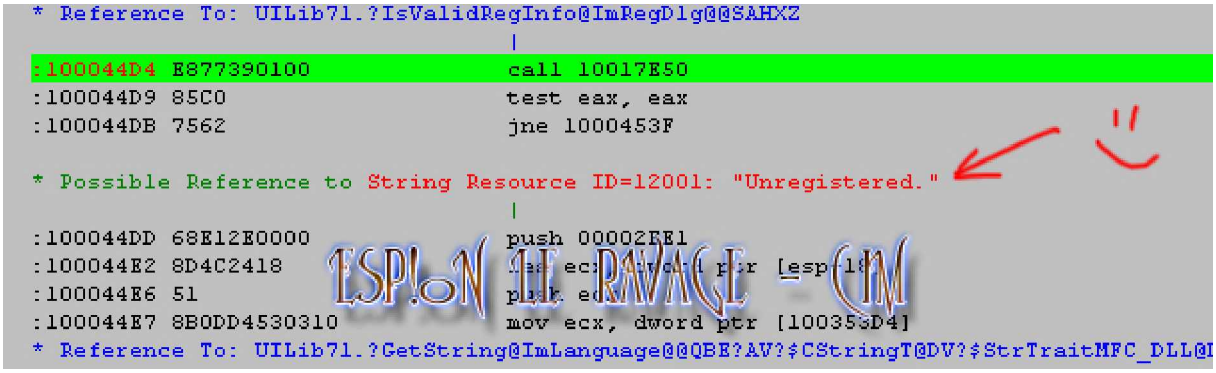
Théoriquement on a terminé, mais c'est pas vraiment le cas : regardez le coté '*About*' :



Merde alors !! Tout ce qu'on a fait c'est détourner le message d'erreur… mais il nous reste une petite astuce (hihihi… !) : vous vous rappelez du deuxième call ?



Allez y jetez un coups d'œil (adresse:100044D4) :

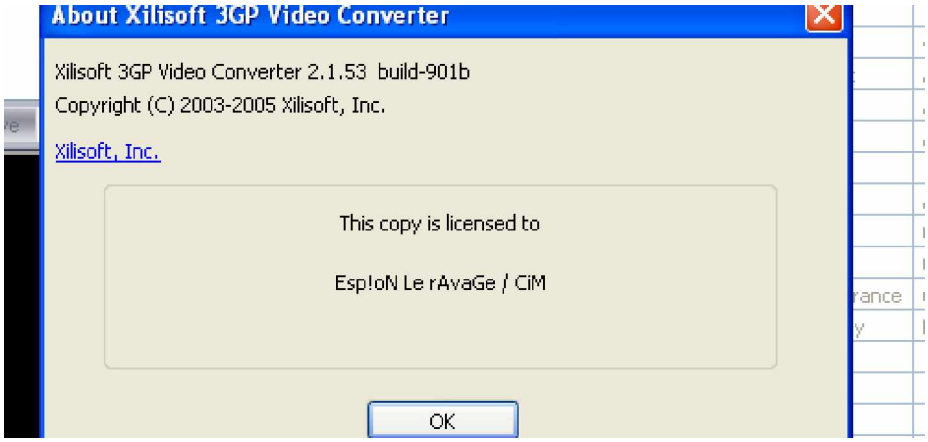


Et surprise : Le 'Unregistered' apparaît !! Donc le ret qu'on a mis à la place du push pour détourner le message d'erreur influence aussi l'apparition de cet 'Unregistered' seule solution : empêcher ce call d'avoir lieu ! Pour faire, notez son offset (*44D4*) et changez à l'aide de votre éditeur hexadécimal : E877390100 par 9090909090 (90 = nop = pas d'opérations) ; enregistrez et testez… pas grand-chose : dans *About* on voit toujours 'Unregistered'.

Le seul suspect qui reste c'est le jne :

:100044DB 7562 jne 1000453F

Si ce saut ne se fait pas, le programme continu sa route et nous affiche « Unregistered », que faut-il faire à votre avis ? IL FAUT A TOUT PRIS QU'IL AIE LIEU CE SAUT !!! Comme cela le programme sautera le 'Unregistered' ; notez son offset (*44DB*) changez 75 par EB (EB= JMP = saute toujours !) ; enregistrez et testez, voilà le résultat :



Maintenant on peu dire que le programme est cracké.

Recapitulatif:

Changements effectués:

- 6A par C3 (offset 17E50)
- E877390100 par 9090909090 (offset *44D4*)
- 75 par EB (offset *44DB*)

انتهى والحمد لله

Esp!oN Le rAvaGe/CiM Le 28/11/2005 -- 18 :25