Cours de Cracking

(5ième Partie)

Mon objectif : élaborer un crack en Turbo Pascal.

1/ Le logiciel utile pour ce cours

-> Le programme à craquer : **Turbo Pascal compiler**

2/ Introduction

Nous allons maintenant apprendre a faire un crack en langage TurboPascal... Rassurer vous, aucune connaissance n'est requise pour suivre ce tutorial !! Enfin, si : ca suppose que vous sachiez cracker un prog (cf cours 4) ...

Comme je me vois mal vous apprendre a programmez en quelque leçons, je vais vous donnez un code source où vous ne modifierez que quelques lignes en fonction du crack que vous ferez :)

Commencons par la théorie : ci-Dessous, le code source du patch en question...

Tout ce qui ce trouve entre accolades en gris cela correspond à des commentaires en pascal.. Vous pouvez donc les supprimer si vous le souhaitez. Ce qui est en rouge, c'est ce qu'il faut changer c'est à dire adapater suivant votre programme ... Le reste du programme c'est le code donc n'y touchez pas si vous ne comprenez pas ce qui est écrit.

Dernière remarque : dans le texte quand vous verrez des caractères bizarres des , ou des ... c'est normal c'est pour avoir les lettres accentuées sous dos.

La version du code source est celle du 14/12/2004. Je l'ai complètement retouché (moi pifoman) au niveau du code et du graphisme et de la langue utilisée qui maintenant est le français.

3/ Le code source

--- début code ---

```
Program Crack;
Uses CRT, DOS;

Const

    FileNC               : string  = 'Start Clean 1.2';
    FileN                : String  = 'STARTCLN.EXE';
    DateCrack            : string  = '14/12/2004';
    BytesToChange        : Integer = 6;
    FileS                : LongInt = 31744;



    {On force la comparaison du faux numéro de série au vrai dans la fonction KERNEL32.lstrcmpA}
    {Il suffit d'annuler pour cela le saut après la comparaison et écrivant une suite de 6 nop}
    {La ligne de code :004011EB 0F8580000000 jne 00401271 devient donc :004011EB 909090909090 nopnopnopnopnopnop}

    A                   : Array[1..6] of Record
    A : Longint;
    B : Byte;
    End =
    (
         (A:$5EB;B:$90),
         (A:$5EC;B:$90),
         (A:$5ED;B:$90),
         (A:$5EE;B:$90),
         (A:$5EF;B:$90),
         (A:$5F0;B:$90)
    );


Var
  F     : File;
  Ch    : Char;
  I     : LongInt;

Begin

clrscr;                      {on vide l'écran}
Textcolor(3);        {couleur du texte en bleu; 8 pour avoir la couleur blanc}

Writeln('');
Writeln('                     ÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜ');
Writeln('                     Û                                   Û');
Writeln('                     Û      Crack pour ',FILENC,'   Û');
Writeln('                     Û            par Pifoman            Û');
Writeln('                     Û                                   Û');
Writeln('                     Û            le ',DateCrack,'          Û');
Writeln('                     Û                                   Û');
Writeln('                     Û          pifoman@yahoo.com        Û');
Writeln('                     Û                                   Û');
Writeln('                     ÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜÜ');
```

```
Writeln('');
Writeln('');


Assign(F,FileN);          {on assigne le fichier à la variable f}
{$I-} Reset(F,1); {$I+}   {on ouvre le fichier en lecture/écriture}


{Si le fichier exite et qu'on ne peut pas ouvrir le fichier en mode lecture/écriture}

If (IOResult <> 0) and (FSearch(FileN,FExpand(FileN))<>'') then
      begin

         Writeln('');
         Writeln('      Le fichier ',FileN,' est d,ja ouvert ou verrouill, en
,criture.');
         Writeln('');

         halt(0);

      end;



If (FSearch(FileN,FExpand(FileN))='') then

     begin

         Writeln('');
         Writeln('        Le fichier nomm, ',FileN,' n''existe pas dans ce r
,pertoire.');
         Writeln('');
         Writeln('                                Craquage abandonn,...');

         Halt(1);

     end;


If FileSize(F)<>FileS then

     begin

         Writeln('');
         Writeln('                V,rification de la taille du fichier ... ERREUR!');
         Writeln('');
         Writeln('           Le fichier nomm, ',FileN,' a une taille incorrecte !!!');
         Writeln('');
         Writeln('                    La taille attendue est de : ', FileS ,'
octets.');
         Writeln('                    La taille actuelle est de : ', FileSize(F) ,'
octets.');
         Writeln('');
         Writeln('                                Craquage abandonn,...');
         Writeln('');
         Writeln('');

         Close(F);
         Halt(1);
```

```
     end

else

     begin

          Writeln('                    ² ²ÜÜÜ        ²ÜÜßßÜÜ      ÜÜßßÜÜ²        ÜÜÜ² ²');
          Writeln('  þ ßÜÜ         ²ÜÛÛÛÛÛÛÛÛÜÜ ±²ÛÛ    ²Û   Û²    ßÛ²±
ÜÜÛÛÛÛÛÛÛÛÜ²        ÜÜß þ');
          Writeln('       ²ÛßßÜ  Ü²ÛÛÛÛÛßßß²ÛÛÛÛÜ ß  ²  ²Û² ²Û²  ²   ß ÜÛÛÛÛ²ßßßÛÛÛÛÛ²Ü
ÜßßÛ²');
          Writeln('²  þ Ü²ÛÝ  Ü²²ÛÛÛÛ       ²ß²ÛÛÜ     ÜÛ   ÛÜ     ÜÛÛ²ß²
ÛÛÛÛ²²Ü  ÝÛ²Ü þ  ²');
          Writeln('Üß  Ü²ÛÛÛ Ü²²ÛÛÛÛ            ß²ÛÜÜÜÛß     ßÛÜÜÜÛ²ß
ÛÛÛÛ²²Ü ÛÛÛ²Ü  ßÜ');
          Writeln(' ßÛÛ²ÛÛß   ß²²Ûß               ²ßß        ßß²
ßÛ²²ß   ßÛÛ²ÛÛß');
          Writeln('');
          Writeln('');

          Writeln('                   V,rification de la taille fichier ... OK');
          Writeln('');

      end;


For I := 1 to BytesToChange do

     begin
               Seek(F,A[I].A);          {on positionne le curseur de lecture sur
l'offset A[I].A du fichier F à craquer}
               Ch:=Char(A[I].B);        {on récupère la nouvelle valeur A[I].B à
affecter à cet offset}
               Blockwrite(F,Ch,1);      {on écrit cette valeur à l'offset considéré.La
valeur est sur 1 octet}

     end;

Close(F);

Writeln('');
Writeln('                    Le programme est maintenant crack,.');

end.
```

---------- Fin code ----------

---------- Rendu graphique ----------

---------- Fin rendu graphique

3/ Explications du code

Au final, on s'appercoit qu'il n'y a que 3 endroits a modifier en fonction du patch qu'on veut faire. Ce sont les 3 premiers blocs de code où l'on fixe les paramètres du programme comme son nom sa taille en octets, la taille du tableau des offsets / valeurs et les offset / valeurs eux-mêmes. C'est pas sorcier et à mon avis, c'est a la portée de tout ceux qui veulent apprendre ..

Bon, maintenant qu'on a vu la théorie, passons a la pratique !
On va créer un crack pour le logiciel que nous avons cracké dans le 1er cours...
Deja, on peut préparé les infos dont on a besoin pour faire le crack :

Le code à modifier en rouge.

- Le nombre de changements = **6** car on remplace 0F 84 80 00 00 00 par 90 90 90 90 90 90.
  J'ai ajouté des espaces entre les bytes pour la clarté du code mais ils n'existent pas.
- Les offsets où on a fait les changements (à droite le byte d'origine) (*cf cours 4*) :

  5EB =>> 0F
  5EC =>> 84
  5ED =>> 80
  5EE =>> 00
  5EF =>> 00
  5F0 =>> 00

- Pour chaque offset, la nouvelle valeur qu'on veut mettre : **90**
- Le nom du fichier EXE qu'il faut cracké, en version DOS : **STARTCLN.EXE**
- La version du programme et son nom complet : **StartClean v1.2**

Pour le code :

- Une accolade { introduit un commentaire et une accolade } ferme un commentaire en pascal.
- Un bloc d'instruction est encadré par la séquence de début begin la séquence de fin end.
- WriteIn affiche du texte à l'écran.

Bien maintenant, il va falloir créer le fichier ".exe" grâce au compilateur... Là aussi, c'est très simple : lancer

notepad et faites un copier / coller du code qui se trouve entre les ---début--- et ---fin--- du code précédent et enregistrez le fichier sous le nom crack.pas (pas comme pascal).Ensuite faites glisser le fichier crack.pas sur le programme TPC.EXE ...

Un fichier .EXE est automatiquement généré à partir du code source !

Alors là, si le compilateur vous dit qu'il y a une erreur, ça peut venir de plusieurs endroits :
D'abord, vérifiez que vous n'avez pas mis de virgule a la dernière ligne des offset.

Ensuite, assurer vous d'avoir bien compté le nombre de changement et de l'avoir indiquer au debut du crack et a la fin du crack...Enfin, regardez si vous n'avez pas mis une apostrophe dans les "Writeln"...
Normalement, ce sont ces erreurs qui reviennent le plus souvent...
Si vous avez un autre problème, essayez de revoir ligne à ligne votre code source...

Ensuite, il vous faudra patcher ce crack avec TPPATCH.EXE , fournit en meme temps que TPC...
Procedez de la meme maniere que pour generer le crack.exe :

Normalement, ya un truc en allemand qui vous dit "Fertig "...ben ca veut dire que ca a marché :).

Pourquoi est-ce qu'on a patcher le crack ?

Parceque le Pentium 2 bug avec le Turbo Pascal...Et le remède, eh bien c'est TPPATCH.EXE ... ;)

Voila, c'est fini, vous pouvez maintenant distribuer votre crack sur Internet...
Enfin, assurez au moins qu'il fonctionne bien en le testant sur une version "saine" du programme à cracker.

Pour vous entraînez, essayer de faire le patch du 3eme cours. Vous pouvez aussi essayer de faire les patches correspondant à l'annulation des JE et des JNE (cf cours 4)...

En attendant de voir d'autres methodes de cracking dans le second numero de notre e-zine, entraînez vous a appliqué ce que nous avons deja expliqué...

Et n'oubliez pas que pour apprendre, rien ne vaut la pratique !

Remarques finales (pifoman) :

1/ Si vous êtes sous windows XP et que vous lancez le fichier CRACK.EXE il s'ouvre et se ferme automatiquement sans qu'on ait le temps de voir quoi que ce soit. Pour empêcher cela 2 solutions.

-> Faites un raccourci sur CRACK.EXE avec clic droit -> Créer un raccourci.
Cliquez droit sur le raccourci crée et faites propriétés -> programme -> décochez la case "Fermer en quittant".

-> Annuler toutes les fermetures automatiques des fenêtres dos en cliquant droit sur le fichier C:\WINDOWS_default et en et faisant propriétés -> programme -> décochez la case "Fermer en quittant ".

2/ Le précédent code source de smeita provoquait une erreur inattendue "File not found" quand STARTCLN.EXE était verrouillé en écriture. En effet STARTCLN.EXE était distribué dans le zip avec l'attribut lecture seule qui était la cause de l'erreur. J'ai corrigé le code de smeita ce qui fait que maintenant si vous mettez le fichier en lecture seule (clic droit dessus->propriétés) il vous dira que le fichier STARTCLN.EXE est bien verrouillé en écriture. J'en ai profité pour retirer l'attribut lecture seule dans le zip de STARTCLN.EXE.

3/ Le rendu graphique présenté plus haut est celui en cas de succès de la procédure de craquage.L'image en forme de vague disparaît dès qu'une erreur est rencontrée pour laisser la place au texte de l'erreur.Il y a 3 niveaux d'erreurs gérés par le programme :

-> Le fichier à craquer nommé FileN est déja ouvert ou verrouillé en écriture ce qui empêche d'écrire sur le fichier à patcher.

-> Le fichier à craquer n'existe pas dans le répertoire courant.

-> Le fichier à craquer est de taille différente par rapport à celle attendue.