Le guide de la création de Trainer

Sommaire

Part I - Introduction

Cette partie est destinée aux débutants, il est donc inutile de la lire pour après râler en disant que le niveau est trop bas, si vous avez déjà les bases.

Pré requis

MemHack (http://www.memhack.com)
TSearch (http://membres.lycos.fr/tsearch)
Trainer Making Kit (idem)
PacMania 3D (http://www.alawar.com/games/pacmania3d)
Grand Theft Auto 3 (http://www.gta3.com)
A little HexEditor (http://www.bpsoft.com)
Some good music :] (http://www.ratm.com)

Qu'est ce qu'un trainer ?

Pour résumer, un Trainer (se prononce "traîneur") est un programme de triche qui tourne en arrière plan lorsque vous jouez au jeu pour lequel il est destiné. Il vous donne un "bonus" (armes, munitions, argent, vie, objets, points...) lorsque vous appuyez sur une touche spécifique, tout en restant dans le jeu. Pour cela il y a plusieurs

moyens. Soit utiliser des combinaisons de caractères, créées la plupart du temps par les développeurs du jeu lui-même (= cheat codes), soit en modifiant les valeurs des zones mémoires spécifiques utilisées par le jeu (ce que l'on va faire).

Recherche...

Commençons par le commencement, eh oui, l'oeuf ne vient pas avant la poule, alors lançons nous dans ce travail, certes ennuyeux et plutôt fastidieux, mais nécessaire.
Soit vous êtes un paresseux irrécupérable et vous allez chercher les cheats codes sur un site spécialisé, ou encore étudier le fonctionnement d'un trainer déjà mis au point (lame), soit vous êtes un puriste et vous continuez votre (passionnante) lecture.

Nous allons commencer en douceur en essayant de tricher à ...
roulements de tambour ... *roulements de tambour* ... *PacMania3D* !
Ce shareware est disponible en téléchargement sur le site de son auteur (http://www.alawar.com/games/pacmania3d/)
Et comme outil, nous allons prendre *MemHack*, qui est léger, simple et efficace.
Vous pouvez le télécharger sur le site officiel (http://www.memhack.com).

Kay ? Let's Go !

Lancez PacMania, puis MemHack, et sélectionnez "PacMania3D" dans "Running processes".

Maintenant jouez un peu, puis arrêtez-vous après avoir avalé quelques unes de ces étranges boules blanches dont la composition chimique reste un vrai mystère pour le monde scientifique...

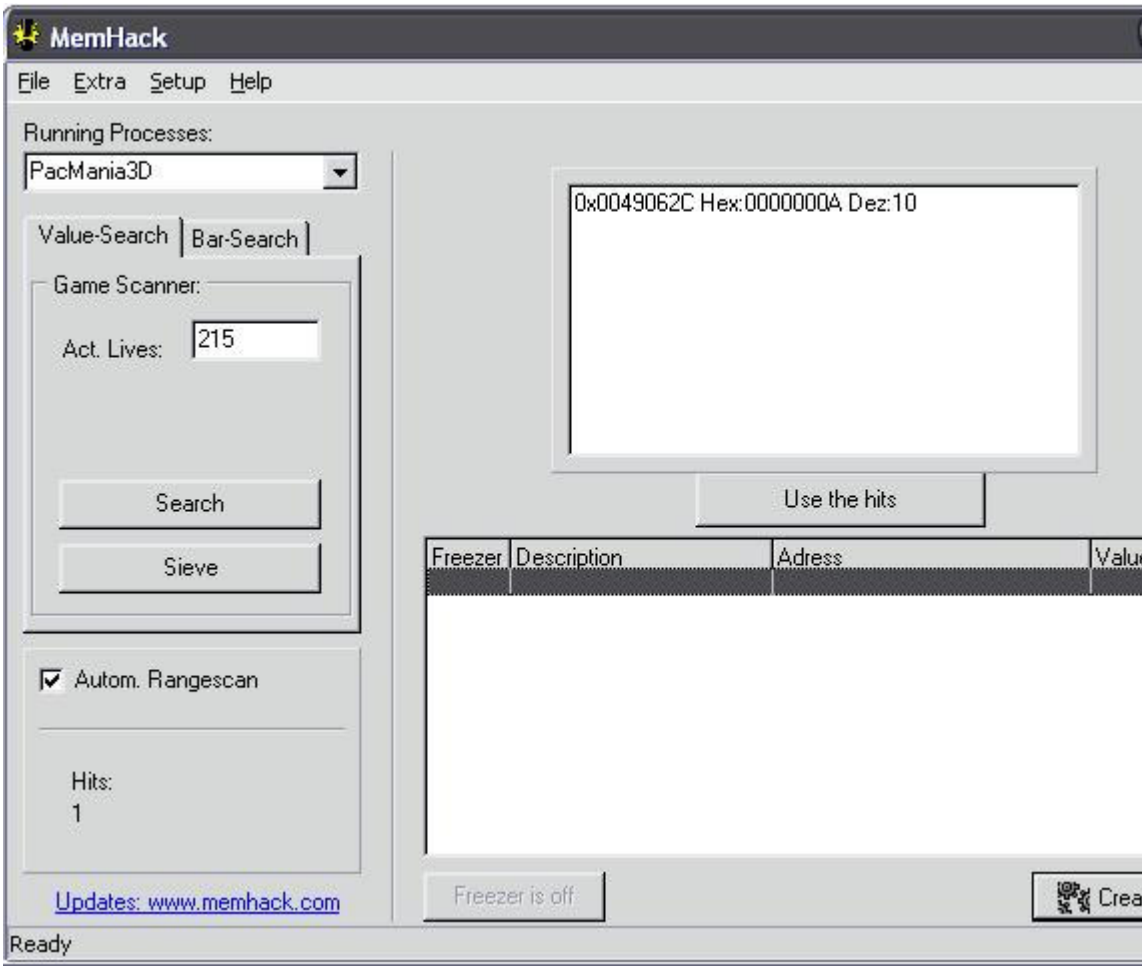
Appuyez sur Echap pour faire pause et retournez dans MemHack.
Décochez "Autom. Rangescan", puis mettez votre score dans "Act. Lives :" (pour moi c'est 205) et cliquez sur "Search".
Ne vous inquiétez pas si la recherche est un peu longue...

Vous devriez observer quelque-chose de ce genre :

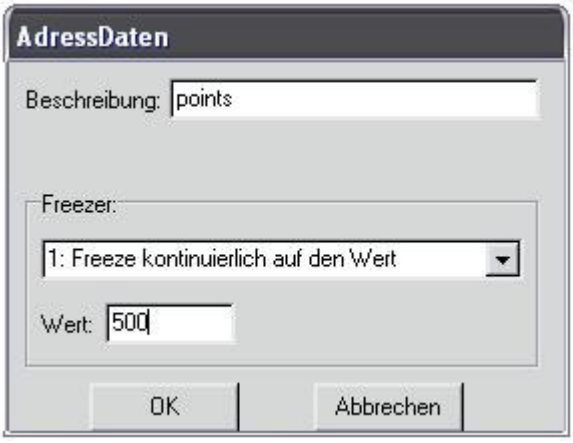
Scanning Memory: xxx
Scanning Memory: xxx
Scanning Memory: xxx
[...]
Ready

OK ? On est sur la bonne voie, mais il y a malheureusement trop de réponses, alors retournez dans le jeu et continuez à gober ces délicieuses boules blanches, puis retournez dans MemHack afin de chercher votre nouveau score (215 pour moi), mais maintenant, vous allez cliquer sur "Sieve " et non "Search".

Résultat : "Hits : 1" ! BINGO ! On la tient enfin cette fameuse adresse !!



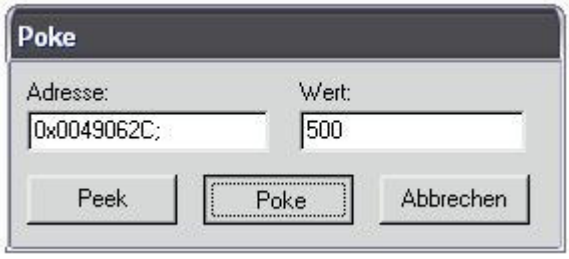
Maintenant cliquez sur "Use the hits" :



Pour ceux qui ne comprennent pas l'Allemand :
"Beschreibung" = description (facultative)
"Wert" = valeur.

Entrez 500 par exemple, puis validez. Vous obtenez ceci :

Cliquez droit sur cette ligne, puis cliquez sur "Peek & Poke" :



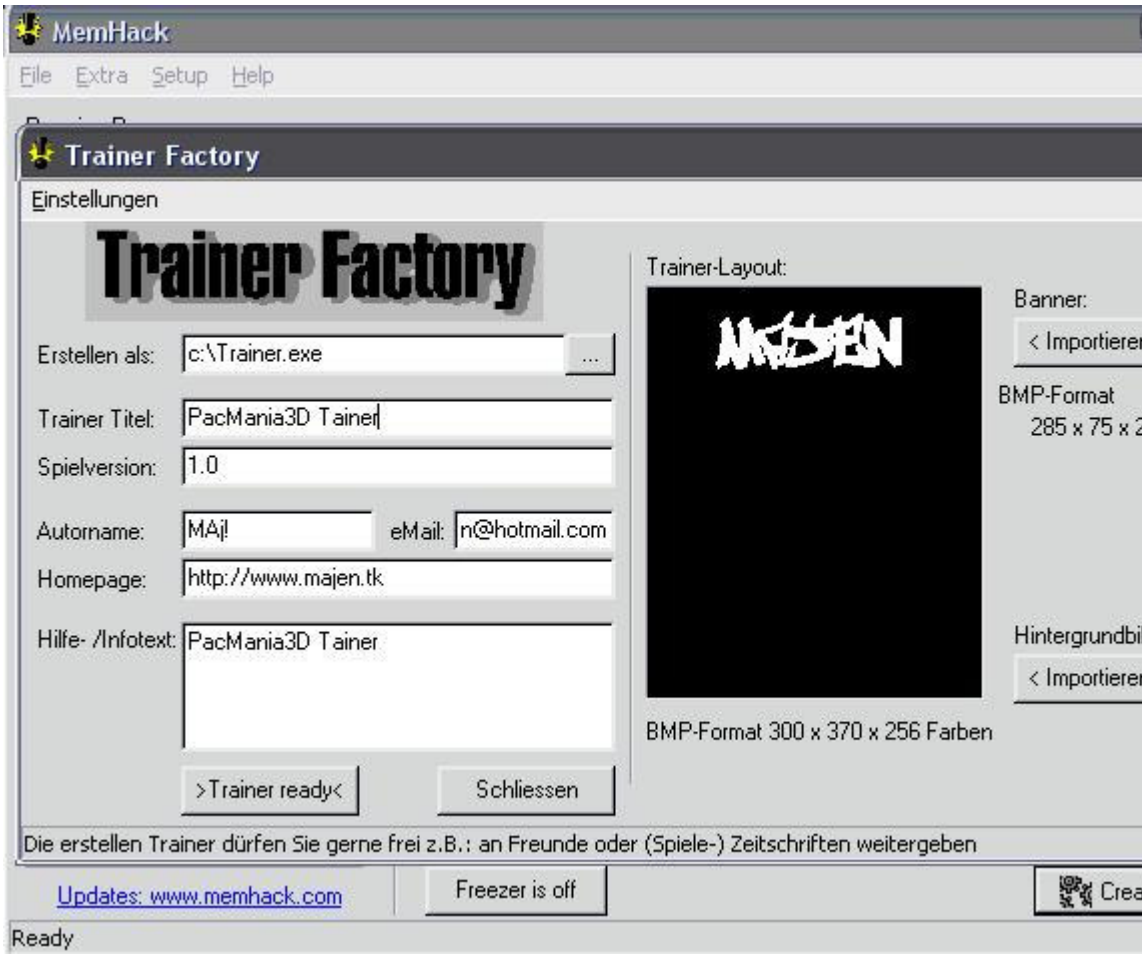
Maintenant cliquez sur "Poke" et retournez dans le jeu...

Et voilà ! Nous avons nos 500 points durement gagnés ^ _^

Note : Ce n'est pas grave si vous obtenez plusieurs adresses, le tout est de ne pas en avoir 10000 :)

Création d'un trainer

Étant donné que vous êtes probablement débutant (Newbie Game Hacker), nous allons faire simple et utiliser le créateur de trainer intégré dans MemHack :



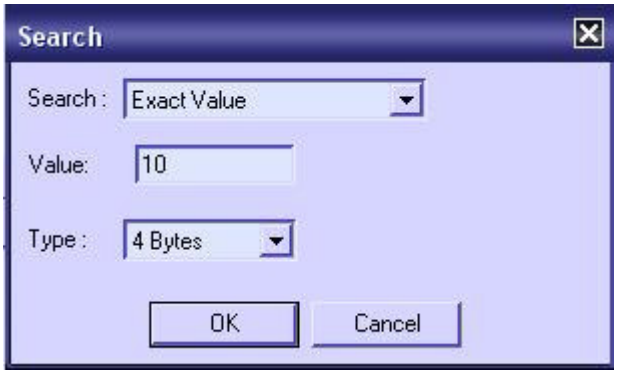
Bon ok, c'est pas le top mais c'est toujours mieux que rien, surtout si vous voulez absolument distribuer vos trainers.

Note : Ce trainer ne marchera qu'une seule fois, car nous utilisons des adresses qui changent à chaque fois (DMA).
Lisez la suite pour apprendre à créer un "vrai trainer", qui marchera à chaque fois et sur toutes les machines (Static Address).

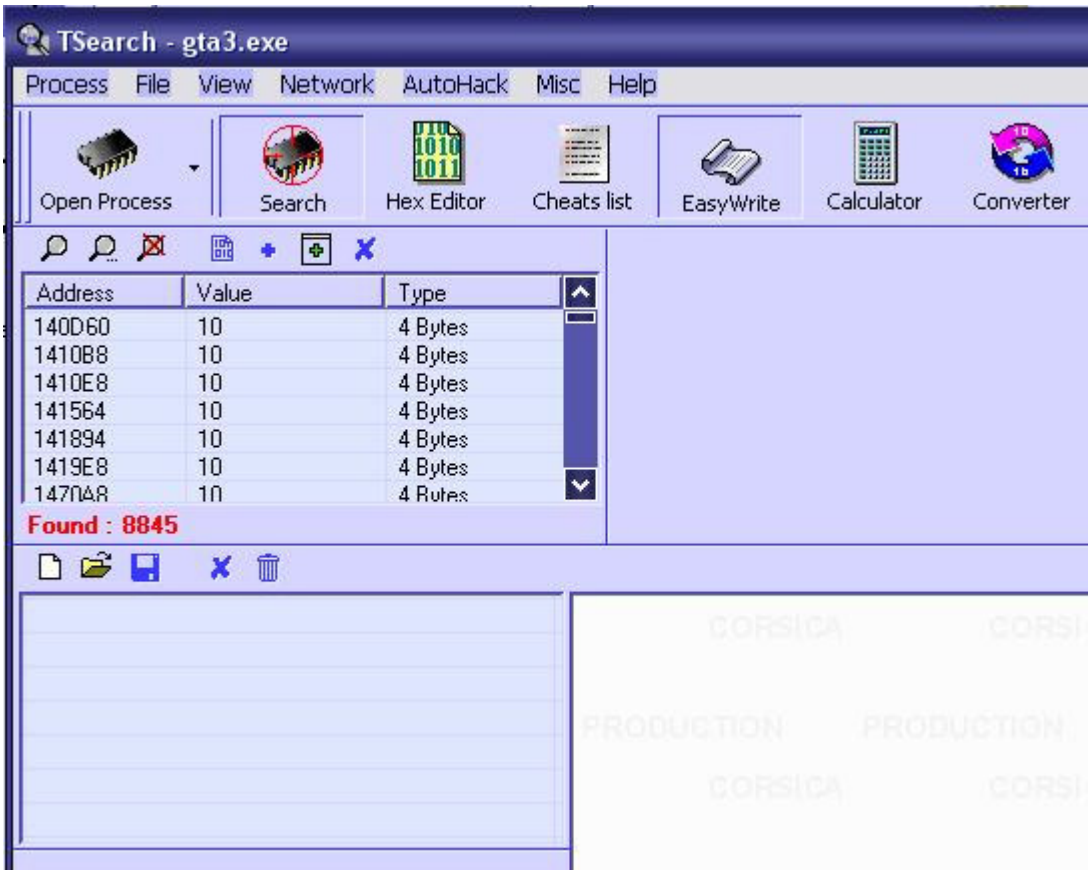
Part II - Dynamic memory allocation (DMA)

Dans la première partie, nous avons vu comment rechercher et utiliser des adresses que l'on pourrait qualifier de temporaires (DMA), maintenant nous allons chercher celles du mythique GTA3 avec *TSearch*, un outil beaucoup plus puissant que vous pourrez acquérir sur le site de son auteur (http://membres.lycos.fr/tsearch).
Lancez le jeu, repérez un type armé et allez lui causer... Prenez son arme, appuyez sur Alt+Tab pour revenir à Windows, puis lancez TSearch.

Sélectionnez GTA3 dans "Open Process" puis cliquez sur l'icône avec la loupe pour chercher le nombre total de munitions que nous avons, c'est-à-dire **10** (0+10).

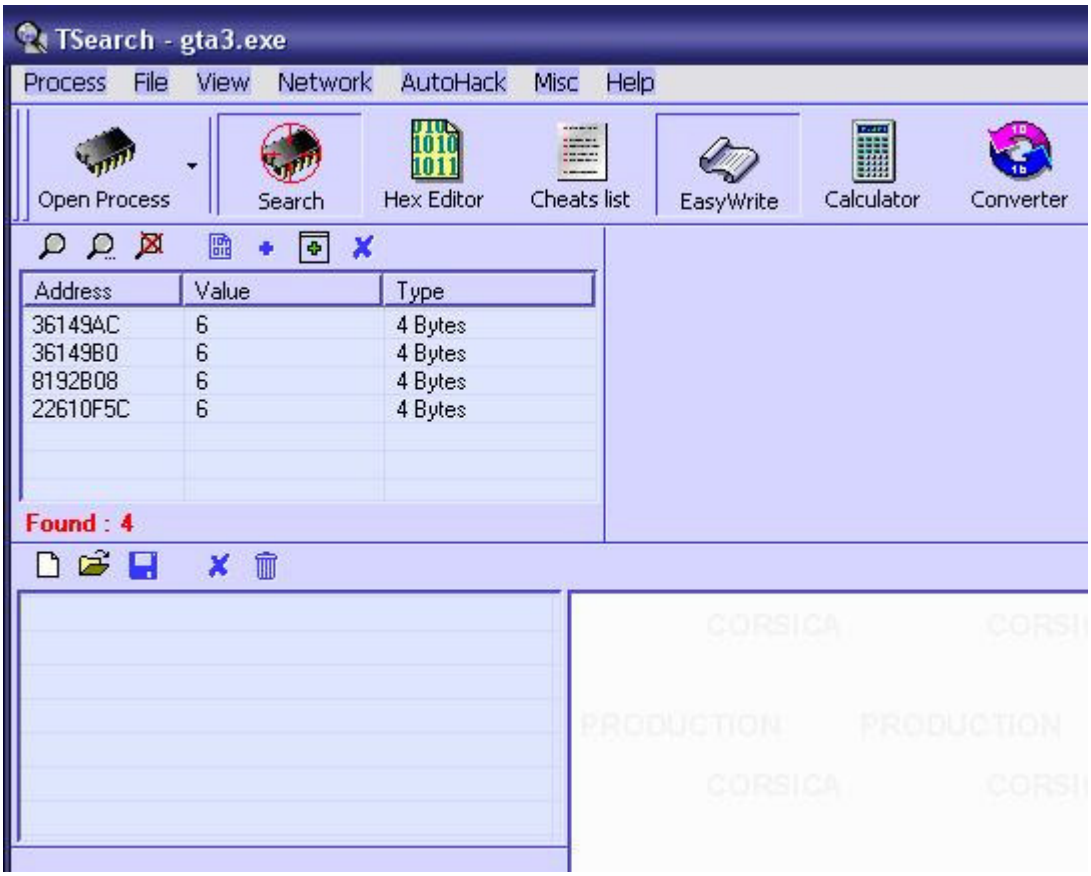


Vous obtenez quelque chose comme ceci :



Arg ! Nous avons beaucoup trop de résultats pour pouvoir en faire quelque chose !
Retournez dans le jeu, allez montrer votre nouveau joujou (je parle du pistolet, hein!) à un autre bonhomme (eh oui, car le premier n'est logiquement plus en état de l'admirer, si vous avez bien fait votre boulot...)

OK ? Maintenant, cherchez (icône avec la loupe et les 3 petits points) le nombre de munitions qu'il vous reste.
Pour moi, c'est **6** (0+6).



Ah ! 4 résultats, nettement mieux, non ?

Recommencez l'opération autant de fois que nécessaire pour trouver cette fameuse adresse...
Pour moi, c'est **36149B0**, mais elle sera différente chez vous car je le répète, c'est une adresse attribuée de façon dynamique.

Une fois trouvée, cliquez sur "Cheats list", puis double-cliquez dessus pour qu'elle apparaisse dans le tableau d'à coté.
Sélectionnez la nouvelle ligne, cliquez droit puis "Edit" :

Créons une "Hotkey"; cliquez sur "Set", puis sur "Click here to set", pressez la touche de votre choix (F5 pour moi), sélectionnez "Set value" pour l'action et mettez **1000** comme valeur, puis validez.

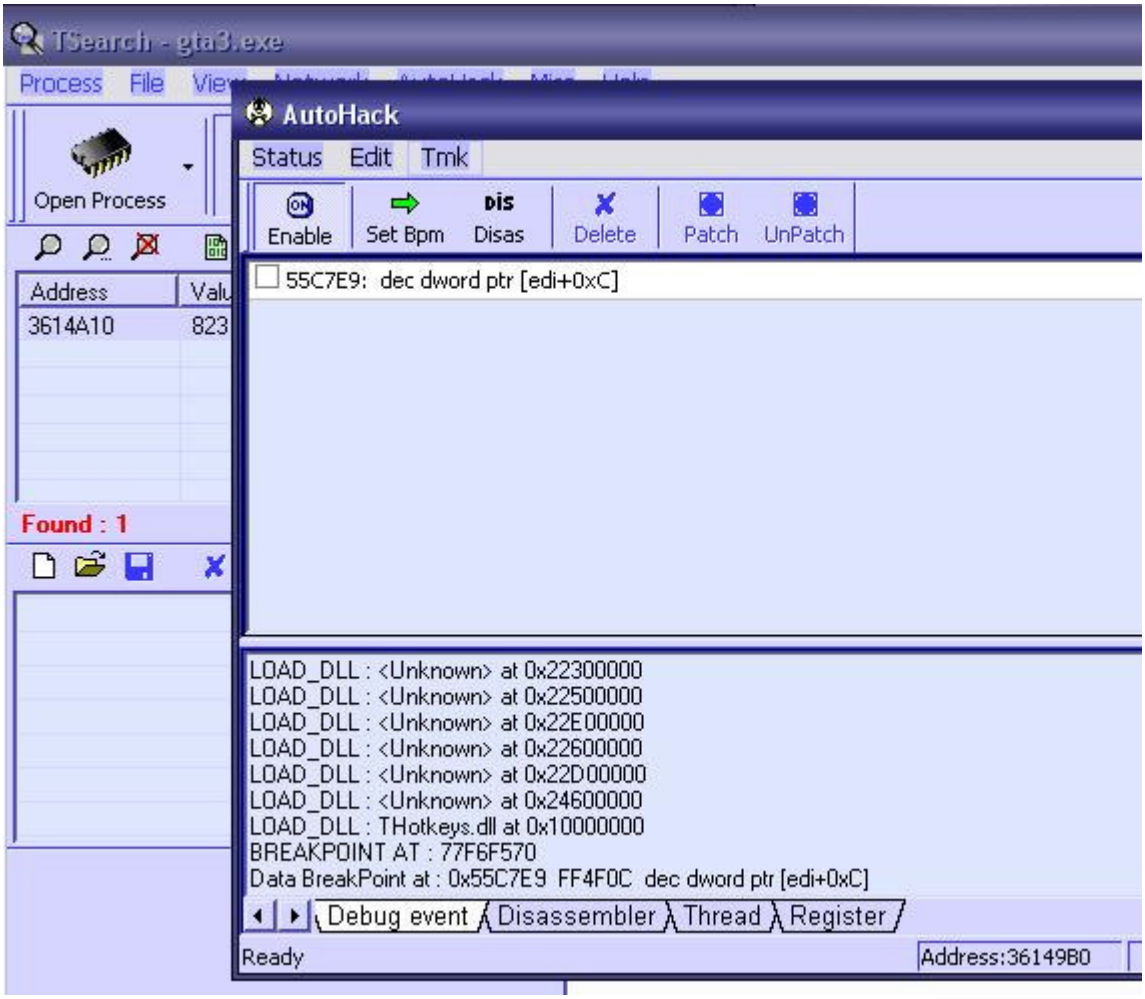
Maintenant, lorsque vous appuyerez sur la touche choisie pendant la partie, vous aurez 1000 balles :)

Retournez dans le jeu et amusez-vous bien...

Note : Vous devrez recommencez cette opération à chaque nouvelle partie, car l'adresse changera toujours !

Part III - Static address

Allez dans le menu "AutoHack" et cliquez sur "Enable debugger" afin d'activer le débugger puis cliquez droit sur la ligne contenant l'adresse dynamique et cliquez sur "AutoHack".
Retournez dans le jeu, tirez un coup (je parle toujours du pistolet, hein :)) et retournez dans TSearch.
Affichez la fenêtre AutoHack (Menu "AutoHack" -> "AutoHack window") :



Bingo ! Nous venons de trouver notre "Static address" (**55C7E9**). Elle nous servira à faire le trainer, puisqu'elle ne **change jamais**.

Code désassemblé :

```
--------------------------------------
0055c7e9  dec dword ptr [edi+0xC]   ;  <- notre adresse
0055c7ec  cmp dword ptr [edi+0x4],0x0
0055c7f0  jnz short 0x0055C80D
0055c7f2  cmp dword ptr [edi],0x9
...
--------------------------------------
```

Maintenant, allez dans le menu "TMK" (comprenez "Trainer Making Kit"), puis "Button script" :

```
--------------------------------------
Tmk button script
Copy and Past into tmk using ctrl+V
Ex: Patched script for a ON button
and Unpatched script for a OFF button

Patched script:
Poke 55C7E9 90 90 90

UnPatched script:
Poke 55C7E9 FF 4F 0C
--------------------------------------
```

Note : 90 = No Operation (NOP)

OK ? Notez ceci quelque part, nous en aurons besoin pour la suite...

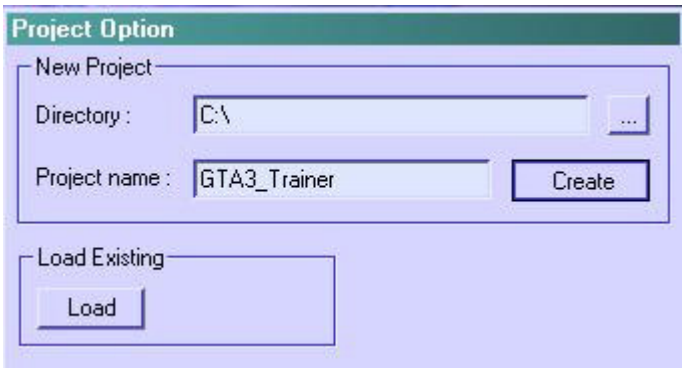
Part IV - Création d'un trainer

Le moment crucial est arrivé. La création du trainer ... *roulements de tambour* ... ("oh ****** il va pas recommencer ça !") ... Serez-vous capable de programmer un trainer pour exploiter ce que vous venez de découvrir !? *roulements de tambour* ... Nan bon, j'déconne, mais c'est tout de même une partie plutôt délicate et souvent difficile à assimiler, enfin tout dépend de votre position par-rapport à la programmation.
C'est pourquoi, j'ai décidé de diviser cette partie en deux sous partie. La première pour les débutants (Newbie Game Hacker) qui ne savent pas programmer et la deuxième pour les Delphistes :)

Trainer Making Kit

Commencez par télécharger ce magnifique outil si vous ne l'avez pas encore (quelle honte :)).
Il est disponible sur le site de TSearch (http://membres.lycos.fr/tsearch/), eh oui, encore un tool signé Corisa Inc !

Une fois téléchargé et installé, créez un nouveau projet comme ceci :



Placez des composants sur la feuille et donnez lui un peu de style (clique droit sur le composant à modifier => "Properties")

OK ? Maintenant cliquez droit sur le bouton pour activer le cheat, puis allez dans "Write memory actions" et rentrez le code que TSearch nous avait donné (cf. "Patched script"), puis cliquez sur "Apply" :

Même procédé pour le bouton désactiver.

Note : Je vous conseille de créer une HotKey ("Properties" => "Key"), ainsi, nous pourrons activer et désactiver le trainer à note guise, et ceci depuis le jeu, sans devoir à chaque fois revenir à Windows.

Maintenant allez dans l'onglet "Build Settings" en bas à gauche. Choisissez"gta3.exe" dans la liste des processus (le jeu doit être lancé), et mettez un nom pour "Exe Name" (par exemple "GTA3 Trainer").

Note : Ne mettez pas l'extension ".exe" car le proggy le fait automatiquement.

Tout est prêt ? Il est temps de compiler votre projet !
Allez dans le menu "Build", puis "Build you project" (j'ai laissé la faute mais je sais que ça devrait être "your" et non "you")

Et voilà, nous avons notre trainer prêt à l'emploi !
Par défaut, il se trouve dans le dossier *"C:\Program Files\Trainer Maker Kit*".

Pas mal le résultat, non ?

Vous pouvez télécharger mon projet et l'exécutable ici, si vous voulez y jeter un coup d'oeil :)

Programmation

Je vais vous faire un petit exemple (toujours avec GTA3) pour avoir les munitions illimitées lorsqu'on presse CRTL+ F1 pendant une partie...

Pour cela, nous allons utiliser Borland Delphi et les API (**A**pplication **P**rogramming **I**nterface) suivantes :

// Pour détecter les touches pressées :
GetAsyncKeyState(*virtual-key code*);
// Pour trouver la fenêtre du jeu :
FindWindow(*address of class name, address of window name*);
// Pour récupérer l'ID :
GetWindowThreadProcessId(*handle of window, address of variable for process identifier*);
// Pour ouvrir le processus :
OpenProcess(*access flag, handle inheritance flag, process identifier*);
// Pour écrire dans la mémoire :
WriteProcessMemory(*handle of process whose memory is written to, address to start writing to, address of buffer to write data to, number of bytes to write, actual number of bytes written*);
// Pour fermer l'handle :
CloseHandle(*handle of object to close*);

[Delphi] ---------- Begin ----------

```
unit Unit1;

interface

uses
  Windows, Messages, SysUtils, Variants, Classes, Graphics, Controls, F
  Dialogs, StdCtrls, ExtCtrls;

type
  TForm1 = class(TForm)
    Timer1: TTimer;
    procedure FormCreate(Sender: TObject);
    procedure Timer1Timer(Sender: TObject);

  private
    { Private declarations }
  public
    { Public declarations }
  end;

// Variables

var
  Form1 : TForm1;
  Fentr : integer;
  PrcID : integer;
  ProID : integer;
  Opnpr : integer;
  Wrtpr : cardinal;
  Buf   : pchar;
  NumberOfBytes : byte;
  PokeValue     : dword;
  PokeAddress   : dword;

implementation

{$R *.dfm}
```

```
procedure TForm1.FormCreate(Sender: TObject);
begin
  Timer1.Interval := 1;           // Défini l'intervalle du timer à 1 m
  Timer1.Enabled  := True;        // Lance le timer...
end;

procedure TForm1.Timer1Timer(Sender: TObject);
begin
// Si l'utilisateur presse CTRL+F1...
if (GetAsyncKeyState(VK_F1) <> 0) and (GetAsyncKeyState(VK_CONTROL) <>
 begin
  PokeAddress   := $55C7E9;       // Adresse
  PokeValue     := 99;            // Valeur à 'injecter'
  NumberOfBytes := 1;             // Nombre de byte à écrire
  Fentr := FindWindow(nil,'GTA3');
  PrcID := GetWindowThreadProcessId(Fentr,@ProID);
  Opnpr := OpenProcess(PROCESS_ALL_ACCESS,False,ProID);
  GetMem(Buf,1);
  Buf^  := Chr(PokeValue);
  WriteProcessMemory(Opnpr, ptr(PokeAddress),Buf,NumberOfBytes,Wrtpr);
  FreeMem(Buf);
  closehandle(Opnpr);
 end;

end.
```

[Delphi] ------------------------------ End ------------------------------

Et voilà, c'est tout pour le code ! Pas si difficile que ça finalement, non ?

Part V - Patching

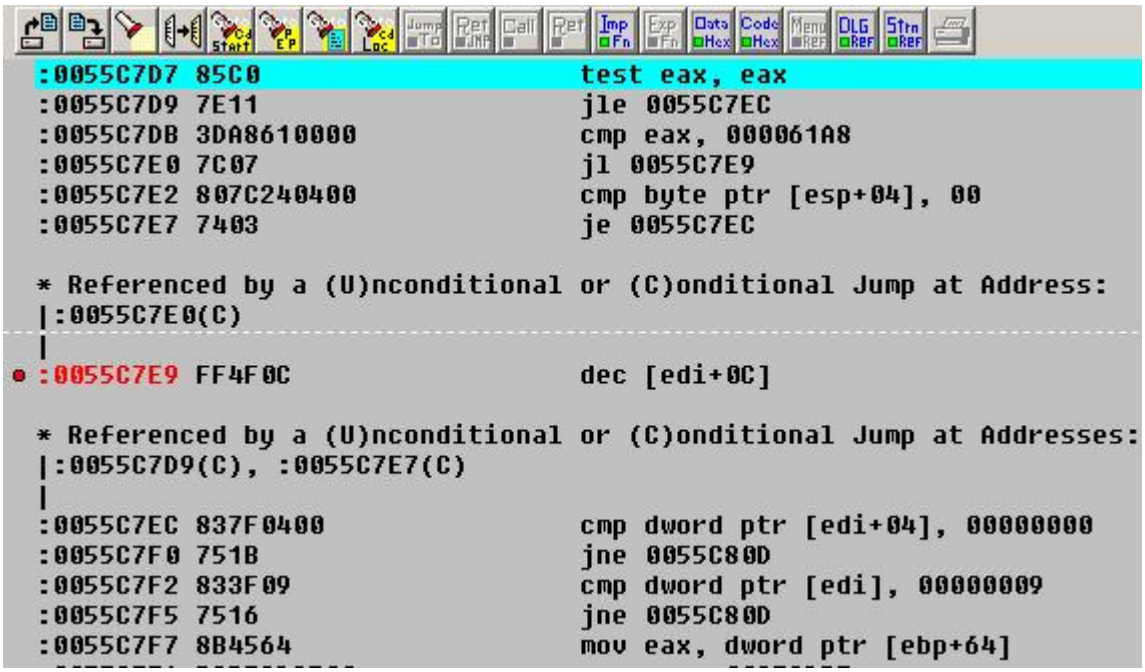
Voici une autre méthode, plus directe et donc plus violente qui s'adresse aux "gros-bourrins-de-base" pour tricher à un jeu. L'avantage est qu'il n'y a pas besoin de créer un trainer et de le lancer à chaque fois que l'envie de tricher vous prend... Alors, comme le dit le titre, nous allons directement patcher l'exécutable du jeu, une fois l'adresse statique trouvée.

Nous allons reprendre l'exemple des munitions illimitées, alors commencez par désassembler l'exécutable de GTA III (gta3.exe), avec W32Dasm par exemple.

C'est un peu long (exe>2mo!), mais vous ne serez pas déçu(e) :)

Une fois ceci accompli, allez à l'adresse que nous avait donné TSearch, c'est-à-dire **55C7E9**, sans trop vous attarder les diverses choses surprenantes que vous pourriez trouver, du genre :

```
-------------------------------------
* Possible StringData Ref from Data Obj ->"FUCKFUCKFUCK"
|
:0040A32D 6814C45E00 push 005EC414
:0040A332 E879BAFFFF call 00405DB0
:0040A337 59 pop ecx
...
-------------------------------------
```



Note : Cette étape est facultative si vous connaîssez déjà l'adresse où l'on va patcher.

Nous allons nopper le FF4F0C pour virer la vilaine décrémentation (dec) à l'adresse **55C7E9** (@Offset 0015C7E9), en le remplacent tout simplement par 909090 (3 NOP) avec l'éditeur hexadécimal de votre choix (personnellement, j'utilise Hex WorkShop) :

```
3060 006A 2F50 E875 0002 0083 7F08 007E|0`.j/P.u.......~
03FF 4F08 8B47 0C85 C07E 113D A861 0000|..O..G...~.=.a..
7C07 807C 2404 0074 0390 9090 837F 0400|..|$..t......_...
751B 833F 0975 168B 4564 B9BE CD95 00FF|u..?.u..Ed......
3560 3060 006A 3450 E833 0002 00C7 4704|5`0`.j4P.3....G.
0100 0000 837F 0800 7579 837F 0C00 7510|........uy....u.
83C4 28B0 015D 5F5E 5BC2 0800 8D44 2000|..(..]_^[....D .
C747 0402 0000 008B 0750 E891 8700 008B|.G.......P......
```

Plus fort encore, remplacez FF4F0C par FF470C afin d'incrémenter (++) au lieu de décrémenter (--). Ainsi, vous gagnerez une balle à chaque coup tiré ! C'est vraiment le monde à l'envers hehe...

OK ? Maintenant enregistrez l'exécutable, et jouez :-)

Note : N'oubliez pas de faire une sauvegarde, car même si vous réussissez à le patcher correctement, ça peut très vite devenir laçant de toujours gagner...

Part VI - Conclusion

Bon bah voilà, c'est *déjà terminé*... J'espère que vous avez compris le principe, que vous vivrez longtemps et heureux et surtout que vous ferez beaucoup de petits trainers... blablabla...
Si vous avez une question intelligente, une remarque, une correction à apporter ou quoi que ce soit d'important, laissez-moi un mail @ majen (at)hotmail(dot)com.

Greetz (aucun ordre spécifique)

BliZZard, The Analyst, Corisa (nice tools d00d!), Isis, Gang'Star, Nix, BlackWizzard, Frog-man, Netix, Lunatique, Nope, Apotec, Clad Strife, Valdeux, Entity, Crackanos, Charlie, Copyright, Thalis ... et tous les potes que j'ai oublié, mais ils se reconnaîtront aisément :)

Links

http://www.majen.tk
http://www.vngamecenter.com
http://www.trainerscity.com
http://www.gamehacking.com
http://www.extalia.com
http://www.megagames.com
http://cdeath.zoomph.net/gamerzgrim
http://membres.lycos.fr/tsearch
http://geocities.com/smil0r26
http://mytestpage.coolfreepages.com
...

Version 0.2 / Dec 2002 / (c) Majen