كيف نصنع Trainer (حلقة 2)

رأينا في الدرس السابق كيفية صنع Trainer بسيط ثم كيف نصنع Trainer متقدم، ولكن تلك الطريقة لن تمكننا من صنع Trainers لألعاب كثيرة! هناك العديد من العوائق التي تواجه صانعي الـ Trainers، ولكن يجب عليك أن تعلم أن كافة صانعي التراينر في العالم مستعدون لمساعدتك، ولكن بالنسبة لك كمبتدئ نرجو أن تقوم ببعث بريد إلكتروني لمجلتنا لتشرح لنا مشكلتك ومن ثم سوف نقوم بمساعدتك!! (ask@f1-mag.com)
والآن بعودتنا إلى كيفية صنع الـ Trainer نود أن تعلم أننا سوف نحاول أن نناقش كافة المشاكل التي تواجه صانعي الـ Trainers، ولكننا لن نتمكن من سردها طبعاً في درس واحد!!!

كيفية كسر الـ DMA:

ما هو الـ DMA ؟

الـ DMA هو اختصار للـ Dynamic Memory Allocation أو توزيع الذاكرة الديناميكي، إذا كنت قد حاولت بالطريقة التي تعلمتها بالدرس السابق أن تصنع Trainer لألعاب أخرى مثل (Need For Speed Most Wanted) مثلاً فإنه عند بحثك عن عنوان الذاكرة الذي يتم فيه خزن قيمة النقود التي تجمعها خلال اللعب سوف تجد العنوان بالطريقة العادية ومن ثم سوف تقوم كما تعلمنا بتغيير القيمة التي يحملها هذا العنوان إلى $ 99999 مثلاً ولكن إذا حاولت أن تعيد تشغيل اللعبة سوف تجد أن الـ Trainer الذي صنعته لم يعد يعمل!!!! إذا لقد ذهب عملك سداً، وإن ظننت أن اللعبة تحمل عدداً محدداً من العناوين لتخزين قيمة النقود فسوف تكون مخطئاً
فما هو عمل الـ DMA في الألعاب إذا؟
كما تعلم أن أغلب الألعاب الحديثة تستحوذ على حجم كبير من الذاكرة، وقد قام مبرمجوا الألعاب بإضافة هذه الميزة إلى الألعاب لكي يقللوا من الذاكرة التي تحجزها اللعبة ولكي تصبح أسرع، في الواقع إن هذه الميزة تختلف في طريقة حجز الذاكرة فكما ذكرنا أن الألعاب عند تشغيلها تحجز قسماً من الذاكرة، ولكن ما فائدة هذه الذاكرة إذا كانت اللعبة لن تستخدم إلا ستة أو سبعة عناوين (أثناء اللعب طبعاً)!! بالطبع سوف يقوم هذا الأمر بتبطيئ الحاسب، ولذلك فإن عمل الـ DMA هو حجز عنوان من الذاكرة متى ما احتاجت الى ذلك اللعبة (أي أن العنوان لا يحجز حتى تطلب اللعبة ذلك)، أعتقد الآن أن سبب عدم عمل الـ Trainer الذي صنعته عند إعادة تشغيل اللعبة أصبح واضحاً!! إن السبب في ذلك هو أنه من الممكن أن اللعبة قد طلبت عناوين أخرى قبل العنوان الذي سوف تحجزه لوضع قيمة النقود، وبالطبع مع لعبة ضخمة مثل Need For Speed Most Wanted سوف يصبح هذا الأمر معقداً جداً.
فما العمل إذا!!!! هل هذا يعني أنه يتوجب علينا إيجاد العنوان كل مرة نلعب اللعبة!!
بالطبع لا! فلو كان هذا الأمر صحيحاً لم كان لهذه الدرس من فائدة ☺!!

البداية:

سوف تتعلم طريقة كسر الـ DMA عن طريق مثال، سوف نصنع في هذا المثال تراينر للعبة Commandos Strike Force وهي لعبة حديثة وضخمة، لن نصنع تراينر لخط الحياة هذه المرة بل لعدد الطلقات أو السكاكين التي يمكنك رميها على الأعداء.

الأدوات التي سوف تحتاجها:
بعد أن قطعنا خط المبتدئين سوف نقوم بترك برنامج Game Expert لأننا الآن في هذه المرحلة سوف نحتاج الى المزيد من القدرات في برنامج البحث عن العناوين، لذلك سوف نستخدم برنامج tSearch (يمكنك أن تستخدم برنامج Cheat Engine، ولكننا في هذا الدرس سوف نستخدم برنامج tSearch، وقد قمنا بوضع البرنامجين في القرص المرفق)

بدء العمل:
بعد أن تشغل برنامج tSearch سوف يكون شكل البرنامج كالتالي: