

بسم الله الرحمن الرحيم
السلام عليكم ورحمة الله وبركاته

العنوان : كيفية اصطياد او اقتناص السيريال نمبر من البرامج [Reverse Engennering]
الكاتب : Hakker – EgY Coders Team

اهلا بكم جميعا ان شاء الله في هذه الورقة سوف اشرح كيفية اصطياد و اقتناص السيريال نمبر من البرامج التي تطلب سيريال نمبر وكسرها بمنتهى السهولة .

الادوات المستخدمة :

- 1- برنامج OllyDbg
- 2- البرنامج المراد كسرة (AD Stream Recorder)

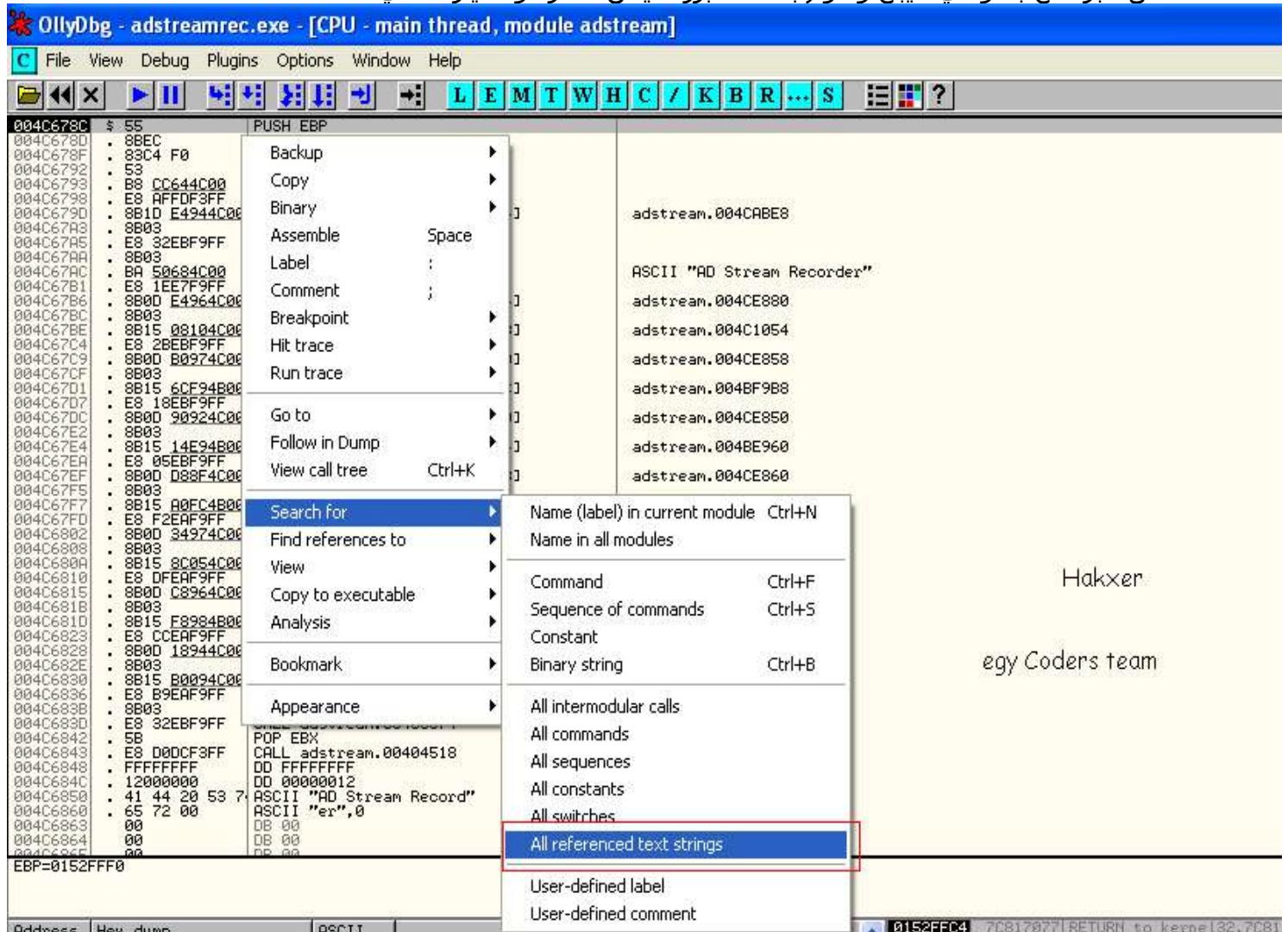
في البداية هنشغل البرنامج وندخل على منطقة ال Registration او الرегистر (التسجيل) ونقوم بكتابة بيانات خاطئة لنستخرج محتوى ال MessageBox كما تشاهدون في الصورة



كما ترون المظلل باللون الاحمر هو السيريال نمبر المطلوب الجزء الاول منه والجزء الثاني والمظلل باللون الازرق هي محتوى ال MessageBox والتي هي : ! Incorrect Code :

الى الاسفل

حسنا الان نحفظ هذه الرسالة ونذهب الى صديقنا ال اوللي ديج للقيام بتنقية البرنامج
نشغل البرنامج بالاوللي ديج ونقوم بالضغط بزر الايمان للفارة واختيار التالي



حسنا الان ظهر لنا ال MessageBox نقوم بعمل بحث عن الكلمة التي وجدناها في ال
والتي هي : !Incorrect Code

004C02C1 PUSH adstream.004C0384 ASCII "Control1"
004C02F8 MOV EAX,adstream.004C0398 ASCII "Incorrect Code!"
004C0304 MOU EAX,adstream.004C03B0 ASCII "Thank you for using"

Hakxer - egypt coders team

كما تشاهدون لقد وجدنا الجملة التي نبحث عنها حسنا

الان نضغط نقرتين double click

هنا البداية ولقد وضعنا break point عليها عن طريق الضغط على F2

Hakixer - EgY
Coders Team

[Timeout = 200. ms
Sleep]

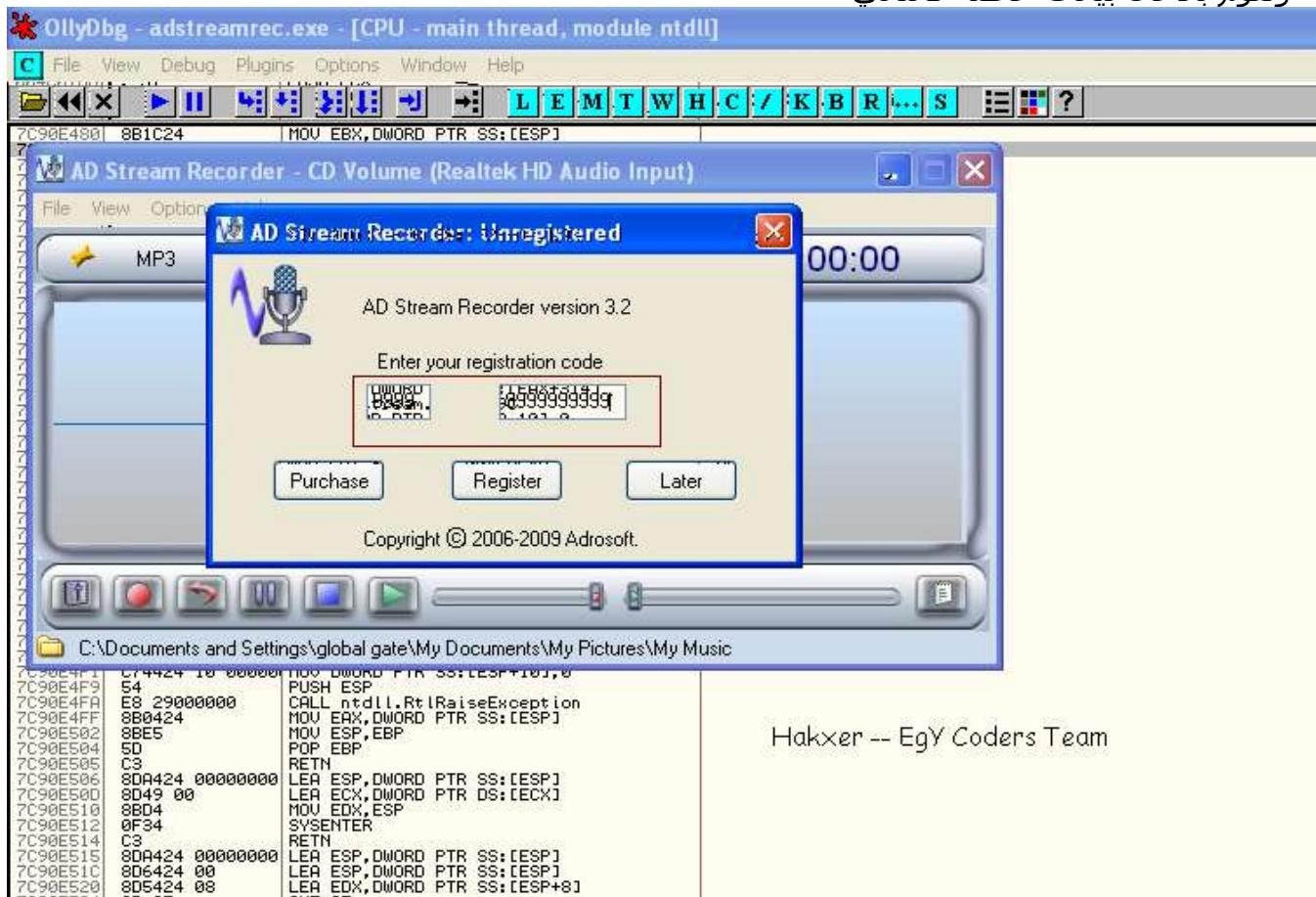
```

004C01E0 55 PUSH EBP
004C01D1 . 8BEC MOV ECX,ESP
004C01D3 . 33C9 XOR ECX,ECX
004C01D5 . 51 PUSH ECX
004C01D6 . 51 PUSH ECX
004C01D7 . 51 PUSH ECX
004C01D8 . 51 PUSH ECX
004C01D9 . 51 PUSH ECX
004C01D9 51 PUSH ECX
004C01DB . 51 PUSH ECX
004C01DC . 51 PUSH ECX
004C01DD . 53 PUSH EBX
004C01DE . 56 PUSH EDI
004C01E0 . 57 PUSH EDI
004C01E0 8945 FC MOV DWORD PTR SS:[EBP-4],EAX
004C01E3 . 33C0 XOR EAX,EAX
004C01E5 . 55 PUSH EBP
004C01E6 . 68 4B034C00 PUSH adstream.004C034B
004C01E6 64:FF30 PUSH DWORD PTR FS:[EAX]
004C01EE . 64:8920 MOV DWORD PTR FS:[EAX],ESP
004C01F1 . 68 C8000000 PUSH 0C8
004C01F6 . 8B05 90DAF4FF CALL JMP.&kernel!32.Sleep>
004C01FE . 8B45 EC MOV EDX,DWORD PTR DS:[EBP-10]
004C0201 . 8B00 14030000 MOV EAX,DWORD PTR DS:[EBP-10]
004C0202 . 8B80 14030000 MOV EAX,DWORD PTR DS:[EAX+314]
004C0207 . E8 9953F8FF CALL adstream.0044559C
004C020C . 837D F0 00 CMP DWORD PTR SS:[EBP-10],0
004C0210 . ~0F84 02010000 JE adstream.004C0318
004C0216 . C745 F8 320000 MOV EDI,DWORD PTR SS:[EBP-8],32
004C021D . BF 488C4C00 MOV EDI,adstream.004C8C48
004C0222 > 8D55 EC LEA EDX,DWORD PTR SS:[EBP-14]
004C0225 . 8B45 FC MOV EAX,DWORD PTR SS:[EBP-4]
004C0228 . 8B80 14030000 MOV EAX,DWORD PTR DS:[EAX+314]
004C0233 . E8 6953F8FF CALL adstream.0044559C
004C0236 . 8B45 EC MOV EAX,DWORD PTR SS:[EBP-14]
004C0237 . 50 PUSH EDI
004C0239 . 8D45 E8 LEA EDX,DWORD PTR SS:[EBP-18]
004C023C . 8BD7 MOV EDI,EDI
004C0241 . E8 AF46F4FF CALL adstream.004648F0
004C0241 . 8B55 EC MOV FNX.DWORD PTR SS:[EBP-18]

```

بعدما وضعنا الـ Break Point – Toggle البرنامج من الزر الموجود فوق (>)

ونقوم بادخال بيانات خاطئة كالتالي



ندخل كمثال 9999999999999999 مثل ما هو في الصورة ونضغط على Register ونقوم بعملية التتبع
وعملية التتبع نقوم بها بالضغط على F8 ومراقبة المكدس (Stack)
حسنا نتتبع الى ان نجد الجزء الاول من السريال

004C0241 . 8B55 E8 MOV EDX,DWORD PTR SS:[EBP-18]
 004C0244 . 58 POP EAX
 004C0244 . 0A298314

hakixer - egy coders team

عند 004C0244 لاحظ المكدس ماذا اضيف له انظر الصورة

0152F27C	0A298314	ASCII "9999"
0152F280	0152F5E8	Pointer to next SEH record
0152F284	004C034B	SE handler
0152F288	0152F2B8	
0152F28C	0152F434	
0152F290	0043E994	Entry address
0152F294	01BAE618	
0152F298	00000000	
0152F29C	00000000	
0152F2A0	0A298328	ASCII "1014"
0152F2A4	0A298314	ASCII "9999"
0152F2A8	0A298300	ASCII "9999"
0152F2AC	00000000	
0152F2B0	00000032	
0152F2B4	01BA37BC	
0152F2B8	0152F3F8	
0152F2BC	00446B42	RETURN to adstream.00446B42
0152F2C0	01BAE618	
0152F2C4	0043E9B5	RETURN to adstream.0043E9B5 from adstream.00446AD8
0152F2C8	0152F434	
0152F2CC	0043EAA9	RETURN to adstream.0043EAA9 from adstream.00403AB4
0152F2D0	01BAE618	
0152F2D4	004469A7	RETURN to adstream.004469A7
0152F2D8	0152F434	
0152F2DC	0152F434	
0152F2E0	01BAE618	
0152F2E4	7E418896	user32.GetWindowLongW

نقوم بحفظة

Hakixer - egypt coders
Team

انظر لقد وجدنا " 1014 " انه الجزء الاول من السيريال ولو قمنا بالتتابع للتغير القيمة وظهرت لنا سيريالات جديدة مثلا تتبع مرة اخرى سيظهر لك " 1530 " حسنا وجدنا الجزء الاول من السيريال يتبقى الجزء الثاني هكذا الحال ايضا مع الجزء الثاني لكن رکز اکتر D:

المهم وجدنا السيريال الثاني ولقد حصلت على اثنين

1222364893
1270287066

طيب الان تعالا نجرب في البرنامج



تمت العملية بنجاح وتم تسجيل البرنامج الى الابد: D:

انتهت الورقة الى هنا

الكاتب : Hakixer – EgY Coders Team