

بسم الله الرحمن الرحيم
السلام عليكم ورحمة الله وبركاته

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

اهلا بكم جميعا ان شاء الله في هذه الورقة سوف اشرح كيفية اصطياد و اقتناص السيرياتل نمبر من البرامج التي تطلب سيرياتل نمبر وكسرهما بمنتهى السهولة .

الادوات المستخدمة :

1- برنامج OllyDbg

2- البرنامج المراد كسره (AD Stream Recorder)

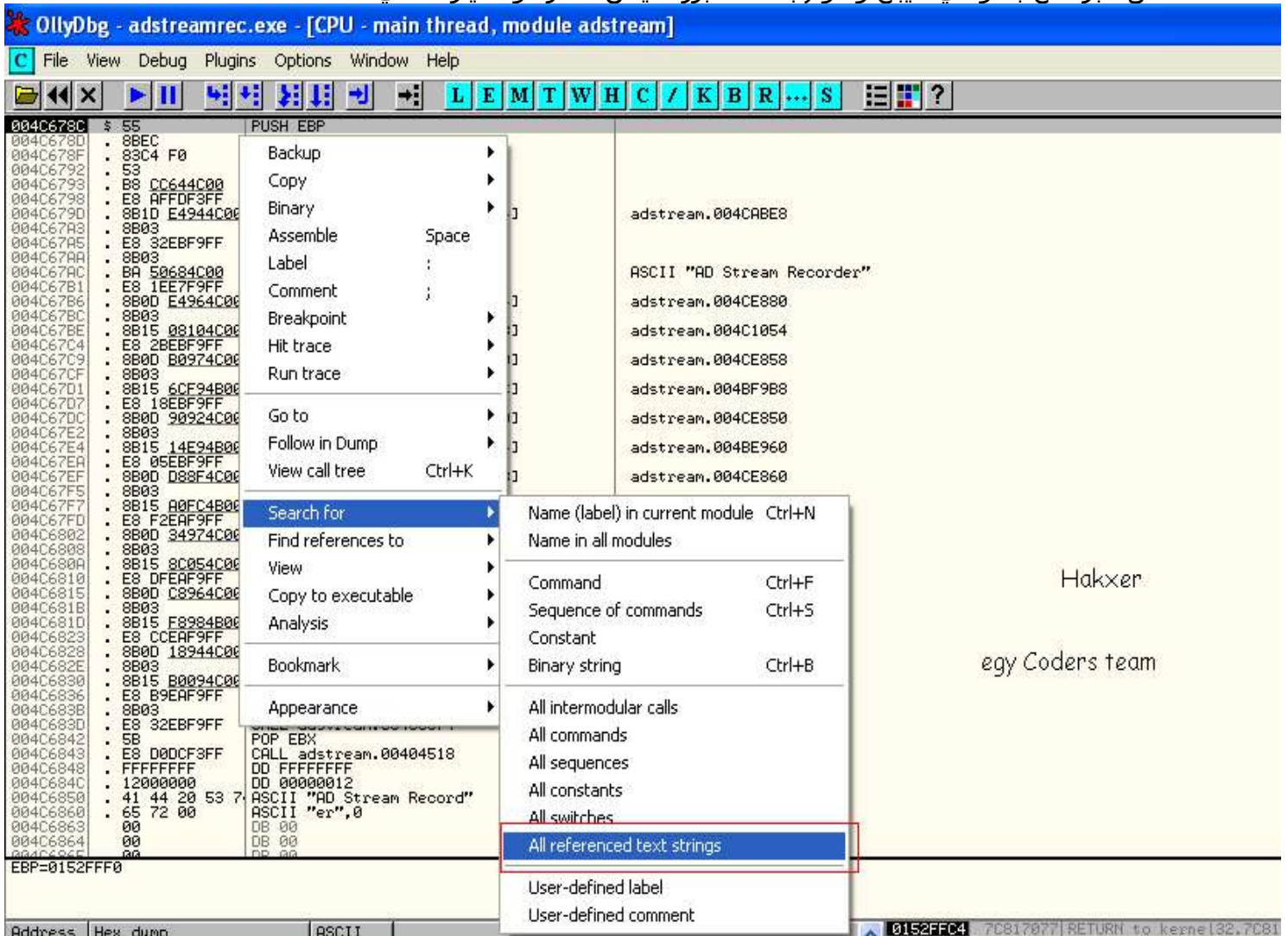
في البداية هنشغل البرنامج وندخل على منطقة ال Regestration او الريجستير (التسجيل) ونقوم بكتابة بيانات خاطئة لنستخرج محتوى ال MessageBox نقوم بالتالي كما تشاهدون في الصورة



كما ترون المظلل باللون الاحمر هو السيرياتل 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 دييج للقيام بتنقيح البرنامج
نشغل البرنامج بالاوللي دييج ونقوم بالضغط بزر الايمن للفارة واختيار التالي



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

```

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

```

Hakxer - egy coders team

كما تشاهدون لقد وجدنا الجملة التي نبحث عنها حسنا

الان نضغط نقرتين double click

004C01D1	004C01D1	PUSH EBP
004C01D3	004C01D3	MOV EBP,ESP
004C01D5	004C01D5	XOR ECX,ECX
004C01D6	004C01D6	PUSH ECX
004C01D7	004C01D7	PUSH ECX
004C01D8	004C01D8	PUSH ECX
004C01DA	004C01DA	PUSH ECX
004C01DB	004C01DB	PUSH ECX
004C01DC	004C01DC	PUSH ECX
004C01DD	004C01DD	PUSH ECX
004C01DE	004C01DE	PUSH ESI
004C01DF	004C01DF	PUSH EDI
004C01E0	004C01E0	MOV DWORD PTR SS:[EBP-4],EAX
004C01E3	004C01E3	XOR EAX,EAX
004C01E6	004C01E6	PUSH EBP
004C01E8	004C01E8	PUSH adstream.004C034B
004C01EE	004C01EE	PUSH DWORD PTR FS:[EAX]
004C01F1	004C01F1	MOV DWORD PTR FS:[EAX],ESP
004C01F6	004C01F6	PUSH 0C8
004C01F8	004C01F8	CALL <JMP.&kernel32.Sleep>
004C01FE	004C01FE	LEA EDX,DWORD PTR SS:[EBP-10]
004C01FE	004C01FE	MOV EAX,DWORD PTR SS:[EBP-4]
004C0201	004C0201	MOV EAX,DWORD PTR DS:[EAX+314]
004C0207	004C0207	CALL adstream.0044559C
004C020C	004C020C	CMP DWORD PTR SS:[EBP-10],0
004C0210	004C0210	JE adstream.004C0318
004C0216	004C0216	MOV DWORD PTR SS:[EBP-8],32
004C021D	004C021D	MOV EDI,adstream.004C0C48
004C0222	004C0222	LEA EDX,DWORD PTR SS:[EBP-14]
004C0222	004C0222	MOV EAX,DWORD PTR SS:[EBP-4]
004C0222	004C0222	MOV EAX,DWORD PTR DS:[EAX+314]
004C0227	004C0227	CALL adstream.0044559C
004C022B	004C022B	MOV EAX,DWORD PTR SS:[EBP-14]
004C022E	004C022E	PUSH EAX
004C022E	004C022E	LEA EAX,DWORD PTR SS:[EBP-18]
004C022E	004C022E	MOV EDI,EDI
004C023C	004C023C	CALL adstream.004048F0
004C0241	004C0241	MOV DWORD PTR SS:[EBP-18]

هنا البداية ولقد وضعنا
break point
عليها عن طريق الضغط على
F2
Hakxer - EgY
Coders Team

Timeout = 200. ms
Sleep
ASCII 04,"1014"

بعدما وضعنا ال Toggle - Break Point نقوم بتشغيل البرنامج من الزر الموجود فوق (>)

ونقوم بادخال بيانات خاطئة كالتالي

AD Stream Recorder: Unregistered
AD Stream Recorder version 3.2
Enter your registration code
9999999999999999
Purchase Register Later
Copyright © 2006-2009 Adrosoft.

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

004C0241	004C0241	MOV EDX,DWORD PTR SS:[EBP-18]	0A298314
004C0241	004C0241	POP EAX	
004C024E	004C024E	CALL adstream.00404090	

hakxer - egy coders team

عند 004C0244 لاحظ المكس 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 01BA0618
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 01BA0618
0152F2C4 0043E9B5 RETURN to adstream.0043E9B5 from adstream.00446AD8
0152F2C8 0152F434
0152F2CC 0043EAA9 RETURN to adstream.0043EAA9 from adstream.00403AB4
0152F2D0 01BA0618
0152F2D4 004469A7 RETURN to adstream.004469A7
0152F2D8 0152F434
0152F2DC 0152F434
0152F2E0 01BA0618
0152F2E4 7E4188A6 user32.GetWindowLongW

```

نقوم بحفظه

Hakxer - egy coders
Team

انظر لقد وجدنا " 1014 " انه الجزء الاول من السيريال ولو قمنا بالتتبع لتغيرت 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 ركز اكثر 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 : Hakxer – EgY Coders Team