

بسم الله الرحمن الرحيم  
السلام عليكم ورحمة الله وبركاته

العنوان : كيفية اصطياد او اقتناص السيريال 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 السيريال نمبر من البرامج التي تطلب سيريال نمبر وكسرهما بمنتهى السهولة .

الادوات المستخدمة :

1- برنامج OllyDbg

2- البرنامج المراد كسره ( AD Stream Recorder )

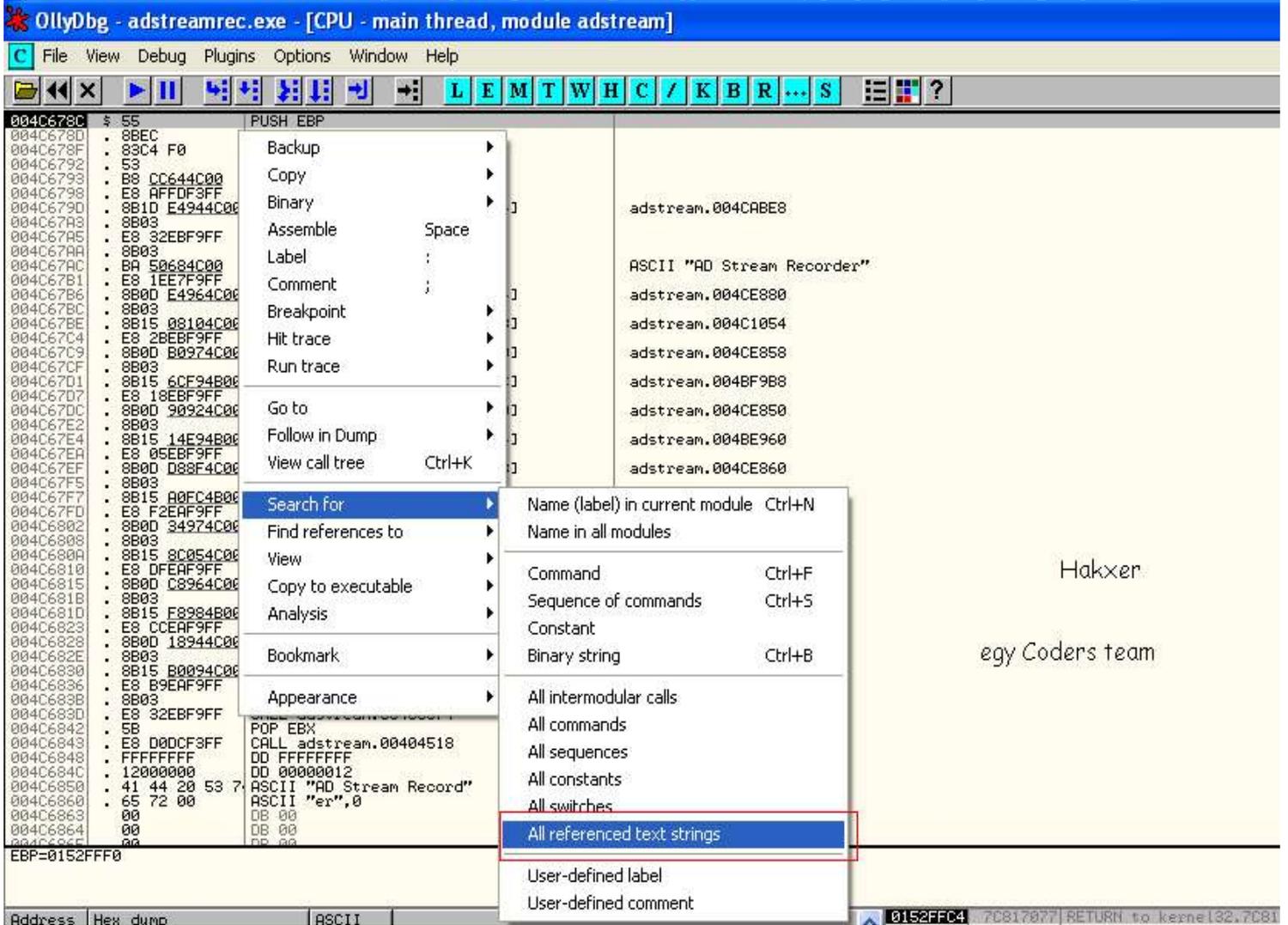
في البداية هنشغل البرنامج ندخل على منطقة ال Regestration او الريجستير ( التسجيل ) ونقوم بكتابة بيانات خاطئة لنستخرج محتوى ال MessageBox نقوم بالتالي كما تشاهدون في الصورة



كما ترون المظلل باللون الاحمر هو 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 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



```

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 سيريلات 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