در ورژن جدید کافی است داخل متد **[fireObtainLicenseEvent](http://127.0.0.1/roeder/dotnet/Default.aspx?Target=code://TMW.SCL:3.17.0.0/TMW.SCL.TMWApplication/fireObtainLicenseEvent())**() را با NOP پر کنیم. آدرس را با Hex Raye Ida پیدا کرده و با یک ویرایشگر با NOP پر می کنیم

اسمبلی اصلی کامپونت TMW.SCL است.

برای استفاده از کامپوننت باید از کلاس TWMApplicationBuilder استفاده شود. این کلاس از TWMApplication نمونه می‌سازد

فیلدهای مربوط با لایسنس در کلاس TMWApplication موجود است.

برای هر ماژول مثل برای هر ماژول مثل IEC، ModBus و DNP دو فیلد bool برای کلاینت و سرور وجود دارد کافی است که این فیلدها همیشه مقدار true برگردانند تا کامپونت فکر کند لایسنس شده است.

چون دراسمبلی کدهای C++ هم وجود دارد از Reflexil+Reflector برای کرک کردن نمی توان استفاده کرد و تنها می توان از روش Byte patching استفاده کرد

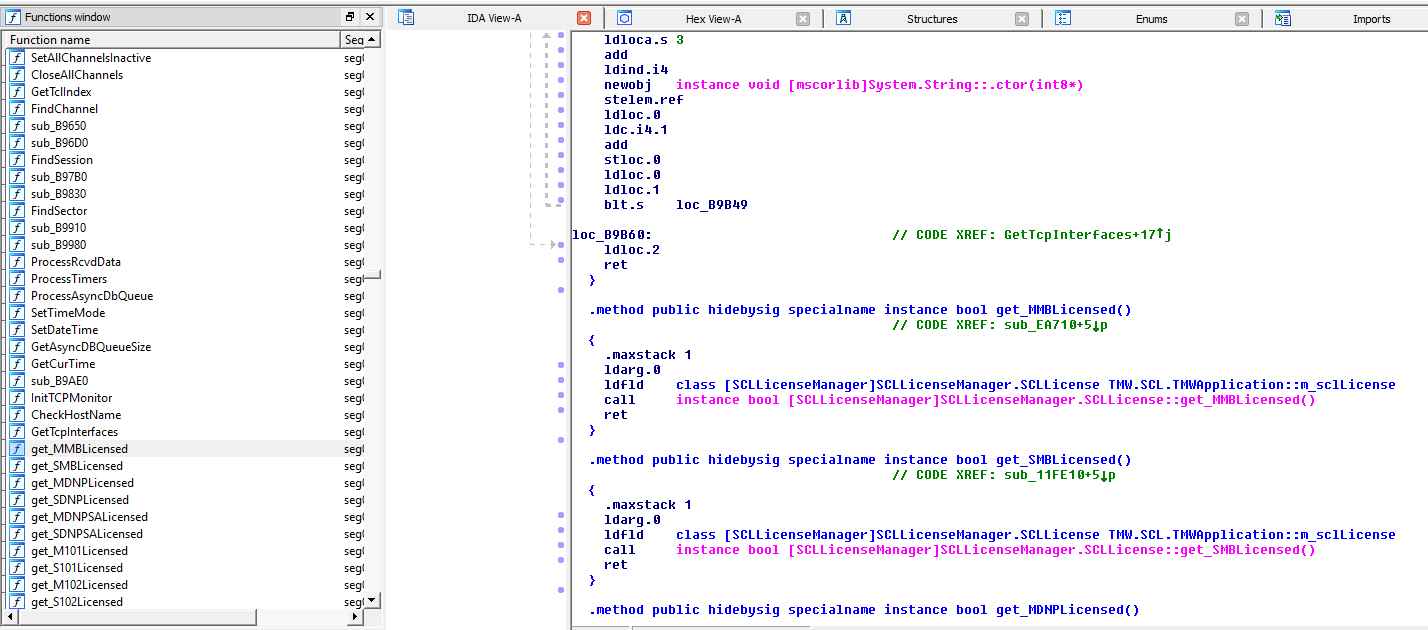
نحوه‌ی کرک

1. با استفاده از نرم افزار Hex-Rays Ida فایل اسمبلی را Disassm کرده و در FunctionWindow، کلیک می کنیم.
2. از منوی Search\Search را انتخاب کرده و M102Licensed جستجو می‌کنیم تا مکان خصیصه را پیدا کنیم.
3. سپس در FunctionWindow رو خصیصه دابل کلیک می کنیم تا مکانش در IDA View – A مشخص گردد.
4. حال تمام کدهای بدنه‌ی توابع get مربوط به پراپرتی ها را با nop پر کرده و در آخر به پشته 1 اضافه می کنیم و ret می کنیم
5. پچ به این صورت است که در پنجره Hex View آپکدها را دستکاری می کنیم

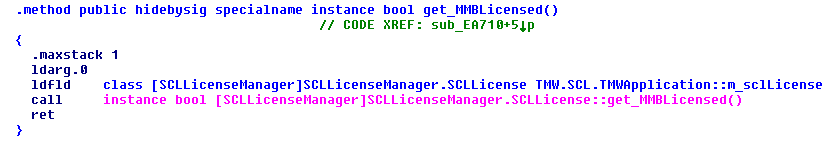
# Important Opcodes (ref. http://en.wikipedia.org/wiki/List\_of\_CIL\_instructions)

|  |  |  |  |
| --- | --- | --- | --- |
| 0x00 | nop | Do nothing (**N**o **op**eration). | Base instruction |
| 0x2A | ret | Return from method, possibly with a value. | Base instruction |
| 0x17 | ldc.i4.1 | Push 1 onto the stack as int32. | Base instruction |
| 0x28 | call <method> | Call method described by method. | Base instruction |
| 0x16 | ldc.i4.0 | Push 0 onto the stack as int32. | Base instruction |

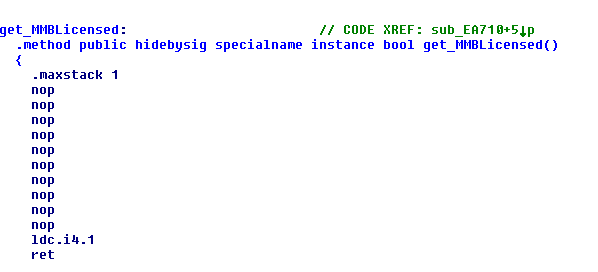
تصاویر زیر مراحل را نشان می دهند



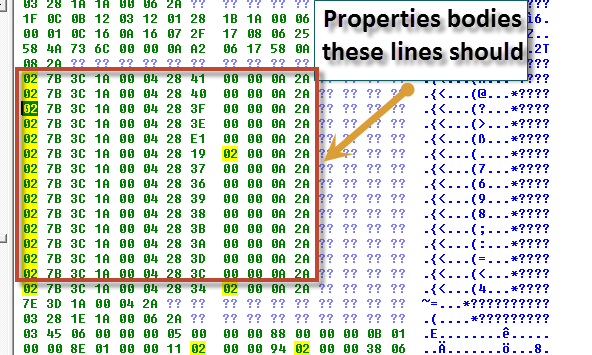
نحوه پیدا کردن Property



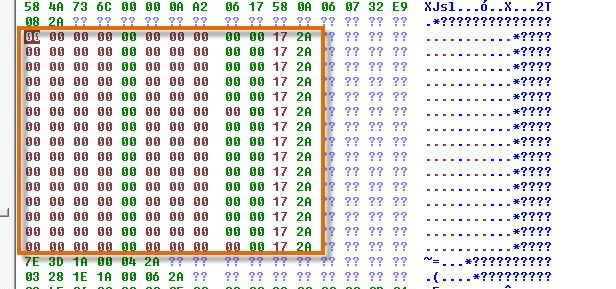
MMBLicensed Property body before patching



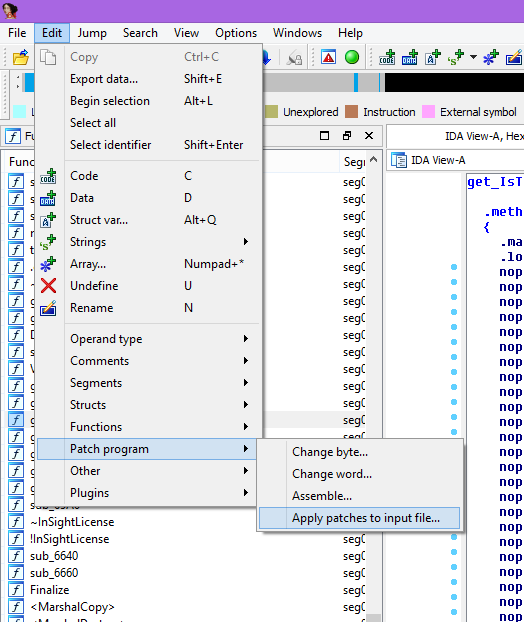
MMBLicensed Property body after patching



Properties body before pachting (Hexview (opcodes))



Property body after pachting (Hexview (opcodes))

در آخر تغییرات داده شده را با استفاده از منوی زیر در فایل ذخیره می کنیم 

و با استفاده از یک Hex Editor از این کار مطمئن می شویم که تغییرات در فایل اعمال شده اند.