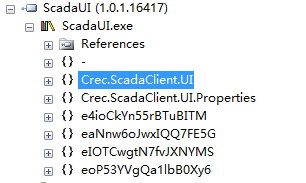
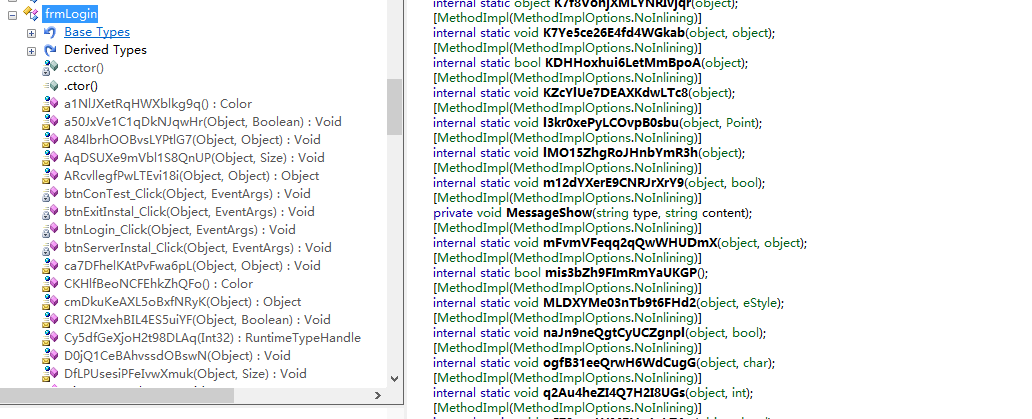
大家好,前段时间做数据分析,需要解析对方数据,而数据文件是对方公司内部的生成方式,完全不知道它是怎么生成的. 不过还好能拿到客户端(正好是C#开发)所以第一件事就是用Reflector编译,但是没有想象的那么简单,看看反编译结果





代码已经混淆了,方法体内部处理也看不见 ,怎么办喃?

**现在就来说说反混淆(剥壳)那些事**

目前比较常用的混淆(加壳)有Dotfuscator,MaxToCode,Xenocode,Them[IDA](http://www.52pojie.cn/thread-108580-1-1.html).

反混淆的工具有很多Dedot ,DePhe,XeCoString等,但是这些只能剥对应算法,今天重点推荐一个工具 De4Dot

De4Dot支持多种反混淆.Dotfuscator,MaxToCode这两种是网友测试的,Xenocode是我测试的,

官方介绍支持:

* Agile.NET (aka CliSecure)
* Babel.NET
* CodeFort
* CodeVeil
* CodeWall
* CryptoObfuscator
* DeepSea Obfuscator
* Dotfuscator
* .NET Reactor
* Eazfuscator.NET
* Goliath.NET
* ILProtector
* MaxtoCode
* MPRESS
* Rummage
* Skater.NET
* SmartAssembly
* Spices.Net
* Xenocode

源码:

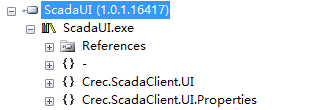


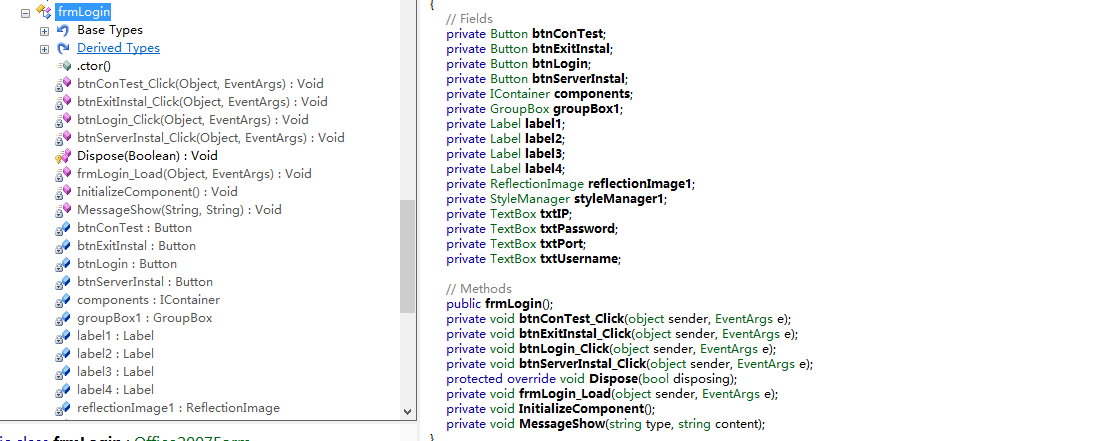
可以看出de4dot确实能剥很多算法的壳,很强大!

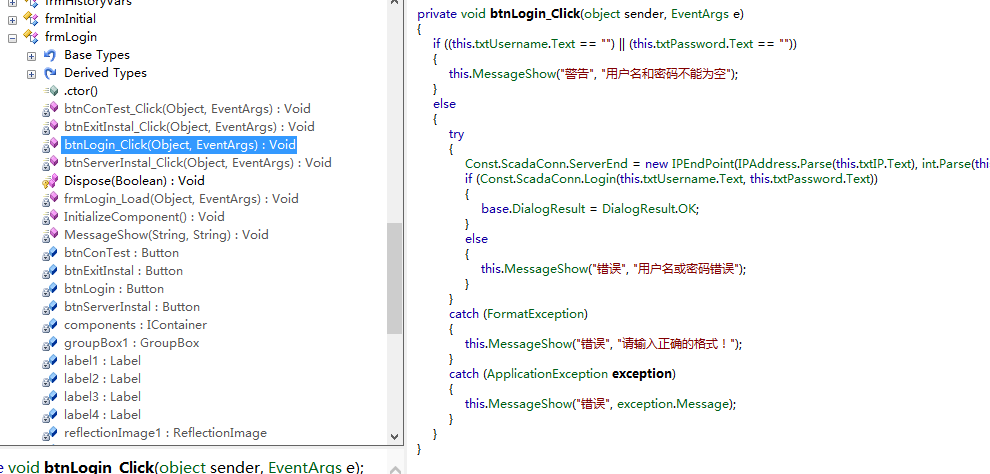
现在来试试



它在我指定文件同目录下生成了 X-cleaned.(exe/dll) 文件,我们在用Reflector来解析一下







成功了,是不是应该欢呼一下. 如果有更强大的工具,求通知!

大家发现没,现在这个客户端是需要登录的,而我没有账户密码,而我想进去怎么办?

本篇只是过渡用,主要是下一篇,如何修改对方dll,跳过登录过程,所谓的破解

如果有兴趣的朋友想了解核心算法,可以去官网下来看<https://bitbucket.org/0xd4d/de4dot/overview> 开源的

发现问题 请留言,如果喜欢请推荐一下,

转载请注明出处! 谢谢

来源： <<http://www.cnblogs.com/jio92/p/de4dot.html>>