看雪CrackMe2007读书笔记（实时更新）2013.06.26

原创

棋子021230 于 2013-06-26 09:04:36 发布 665 收藏
分类专栏： 软件破解实例笔记

昨天下载了个电脑闹钟的软件，看到只是加了个ASProtect壳，感觉很简单，直接ASPUnpacker脱壳，发现设置了好多暗桩，OD载入后程序直接结束。瞬间感觉自己还是太菜了，于是回过头来继续学习破解，准备把这本CHM扫一遍。当然这可能需要很长的时间，但千里之行，始于足下，加油吧！

虽说名字叫"笔记"，但为了尊重原作者，文章中不会粘很多原CHM中的代码和注释，只是记录自己认为需要补充或加深理解的东西，下面开始。

2013.6.26

1、CDQ指令：

数据扩展指令，将双字数据扩展为四字类型。
CDQ—Convert Double to Quad (386+)，该指令把edx扩展为eax的高位，也就是说变为64位。

2、有符号数除法指令IDIV

有符号数除法指令IDIV
DIV r8/m8 ;有符号字节除：AL<-AX÷r8/m8的商，
;AH<-AX÷r8/m8的余数
IDIV r16/m16 ;有符号字除：AX←DX.AX÷r16/m16的商，
;DX←DX.AX÷r16/m16的余数

3、REP指令

重复前缀指令REP(Repeat String Instruction)

重复前缀指令是重复其后的字符串操作指令，重复的次数由CX来决定。