




# 170527 逆向-CrackMe(4)

原创

奈沙夜影  于 2017-05-27 16:38:13 发布  344  收藏

分类专栏: [CrackMe](#)

版权声明: 本文为博主原创文章, 遵循 [CC 4.0 BY-SA](#) 版权协议, 转载请附上原文出处链接和本声明。

本文链接: <https://blog.csdn.net/whklhjh/article/details/72782509>

版权



[CrackMe 专栏收录该内容](#)

83 篇文章 2 订阅

订阅专栏

1625-5 王子昂 总结《2017年5月27日》【连续第238天总结】

A. CrackMe(4)

B. 先拖到PEiD, 无壳, 是Delphi

打开, 是一个没有按钮的序列号验证

拖入OD, 因为没有按钮, 也就无法查找MSGBOX的API

直接查找字符串, 发现成功提示

跟过去, 看一下上下文, 下断点

找到了关键跳转和前一条判断“cmp dword ptr ds:[esi+0x30c], 0x85”

把关键跳转NOP掉即爆破成功

序列号算法则非常麻烦:

按照上一个的经验, 向上翻到头, 开始跟

在尝试中发现这一段代码是在点击图片框的时候开始运行的

逐行运行下去, 发现这一段提取了Name, 进行了一番运算, 但是没有跟关键判断有关的部分

关键判断是该数据是否等于85, 推测应该在前方某处进行判断, 使得该数据等于85, 但是没有找到

无奈, 查writeup

综合3个和自己尝试得到最终结果:

使用Dede Dark来对Delphi反编译更有效, OD对于其常常很无奈

这个程序有三个关键流程, 在Dede中可以看到这3个事件: chkcode,click,dbclick

在chkcode的代码中可以看到Dede标注好的函数名, 有许多strcat, 记下内存地址, 进入OD进行跟踪

首先，修改序列号文本时会触发chkcode，进行验证码判断，为"黑头Sun Bird"+(len(Name)+5)+"dseloffc-012-OK"+Name"

。如果校验成功，则将[esi+0x30c]的值设置为3e

然后，双击图片框会触发dbclick，如果该值为3e，则修改为85

最后，单机图片框触发click，如果该值为85，则成功

中间夹杂着许多无关的获取Name，计算等等

总的来说，序列号的算法很简单，但是中间的流程比较复杂，OD往往跟不到完整过程，比如双击图片框这个事件在给单击下了



C. 明日计划

CrackMe(5)



[创作打卡挑战赛](#) >

[赢取流量/现金/CSDN周边激励大奖](#)