Crack看雪论坛加解密的一个破解案例程序

原创

Cvjark 于 2019-03-19 21:59:27 发布 1209 收藏 3

分类专栏： 逆向学习 读书笔记

本文链接：https://blog.csdn.net/weixin_43084928/article/details/88674955

逆向学习 同时被 2 个专栏收录

10 篇文章 2 订阅

订阅专栏

读书笔记

6 篇文章 0 订阅

订阅专栏

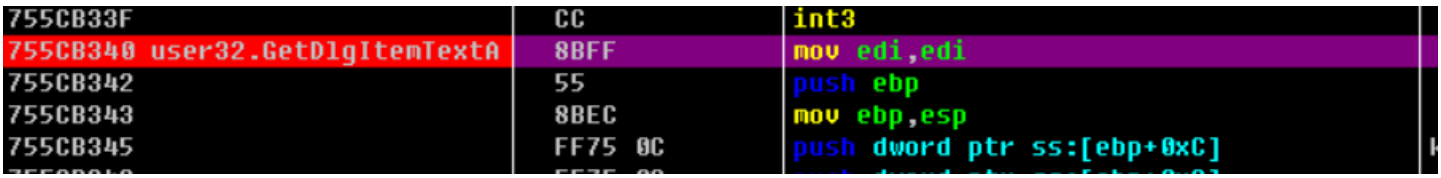
新手能力有限，文章有什么错误还请各位前辈批正，感激不尽~

运行程序，了解下程序的大概流程：

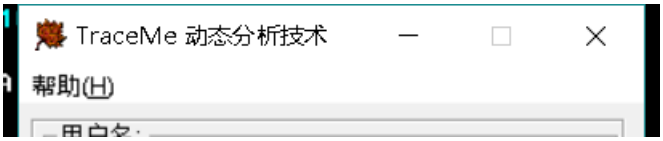
程序要求输入用户名于序列号，点击check，基于Windows的消息机制，一般都从一些API入手，读取输入的内容然后执行下一步，因此我们可以以API作为切入点：

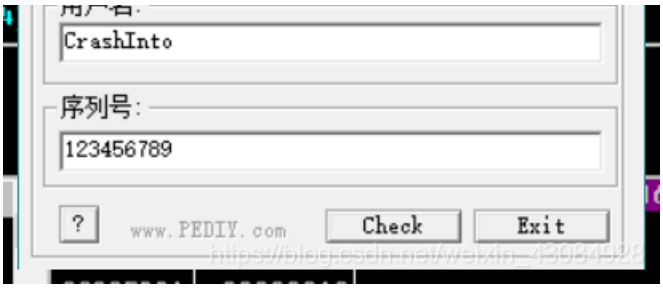
在OD中，我们可以ctrl+G检索要跟随的API表达式，读取内容一般是：GetdlgItemTest（A/W）和GetWindowsTest（A/W）

这个例子是：GetdlgItemTextA

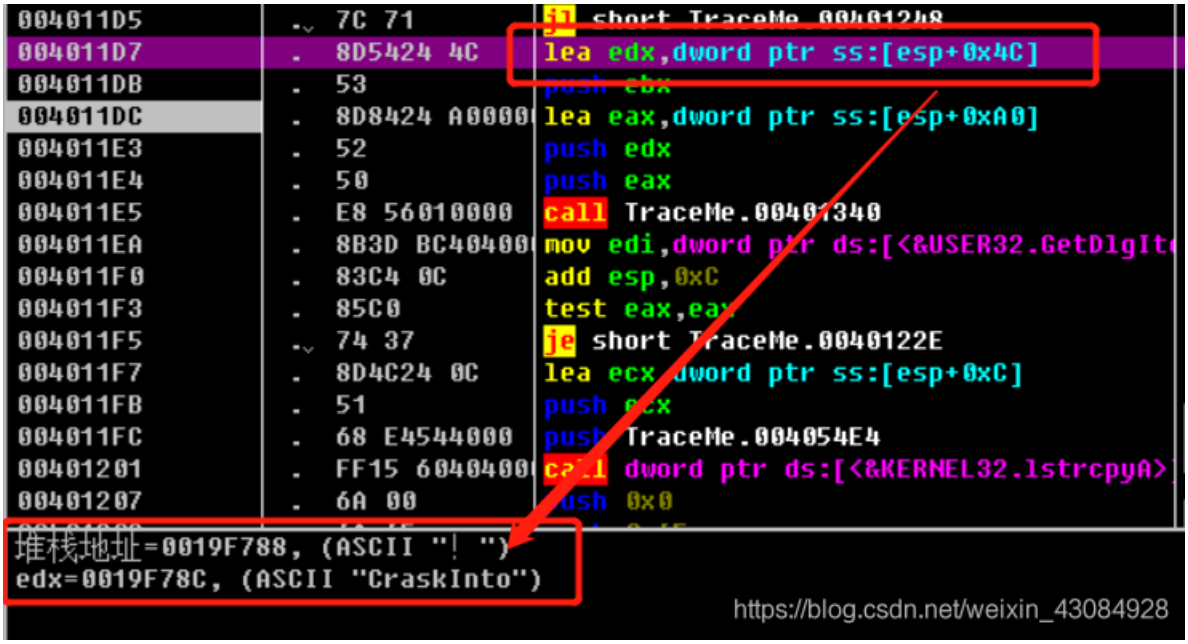


在这个位置下断：F9，我们停在这里，此时回到程序界面，输入信息

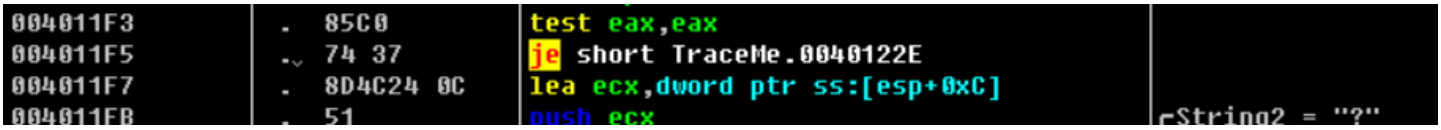




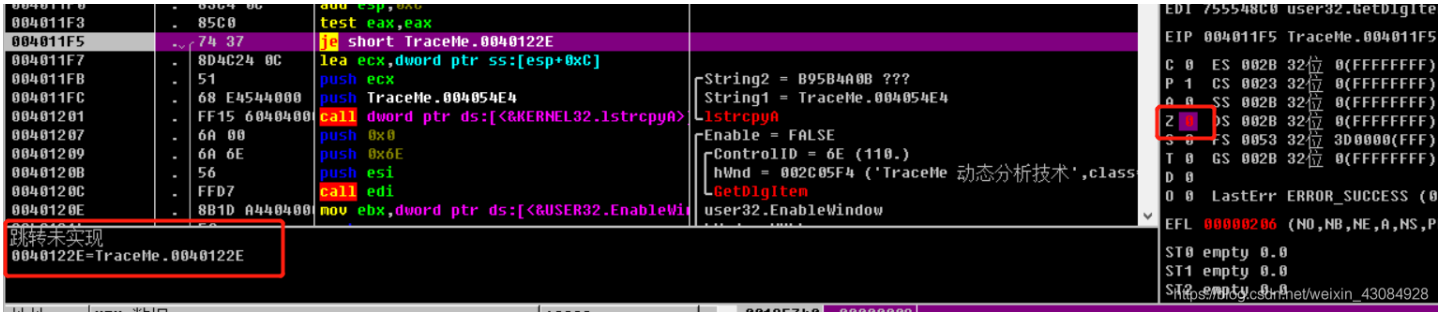
点击check，持续单步，留意消息框，会有惊喜：



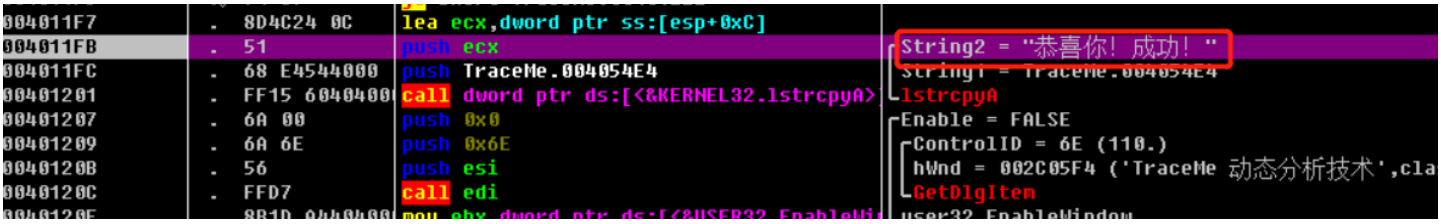
按照约定俗成，韩式调用返回通常把结果放在EAX中，即便长度不够的话，也还是会吧内容放在内存，取首地址放在EAX中，



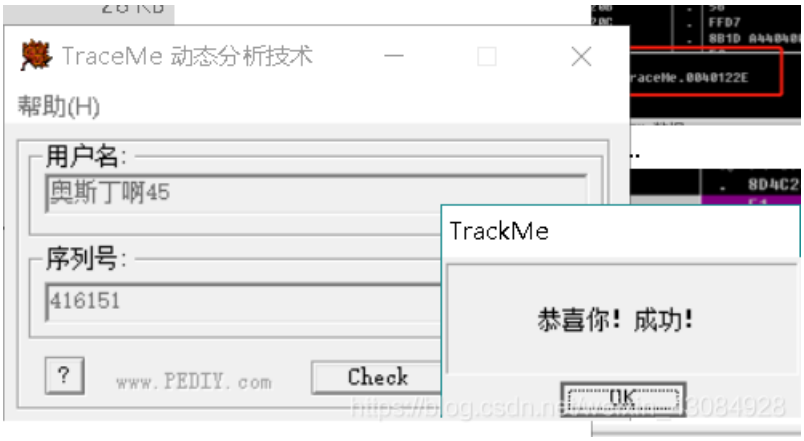
这里做了校验函数结果的条件控制跳转，我们让它取反，改Z标志位…



F8执行…



实现暴力破解，我们直接可以填充那个条件跳转指令用nop代替...然后保存到文件...：



少了校验判断，我们输入什么都会出现成功的信息...

程序下载链接 提取码：s237