看雪学院-OllyDBG入门系列（二）笔记

原创

Cytosine 于 2017-02-04 15:10:45 发布 1029 收藏
分类专栏： 笔记_看雪学院OD入门系列 解密 逆向 OllyDBG 文章标签： Note OllyDBG 逆向

本文链接：https://blog.csdn.net/Cytosine/article/details/54863306


笔记_看雪学院OD入门系列 同时被 3 个专栏收录
3 篇文章 0 订阅
订阅专栏


解密
5 篇文章 0 订阅
订阅专栏


逆向
6 篇文章 0 订阅
订阅专栏

OllyDBG 入门系列（二）一字串参考 笔记

原作地址：**http://bbs.pediy.com/showthread.php?threadid=21308**

作者：**CCDebuger**

软件破解的一般流程

拿到一个软件先别接着马上用 OllyDBG 调试，先运行一下，有帮助文档的最好先看一下帮助，熟悉一下软件的使用方法，再看看注册的方式：

如果是序列号方式可以先输个假的来试一下，看看有什么反应，也给我们破解留下一些有用的线索。

如果没有输入注册码的地方，要考虑一下是不是读取注册表或 Key 文件（一般称 keyfile，就是程序读取一个文件中的内容来判断是否注册），这些可以用其它工具来辅助分析。

如果这些都不是，原程序只是一个功能不全的试用版，那要注册为正式版本就要自己来写代码完善了。

获得程序的一些基本信息后，还要用查壳的工具来查一下程序是否加了壳，若没壳的话看看程序是什么编译器编的，如 VC、Delphi、VB 等。这样的查壳工具有 PEiD 和 FI。有壳的话我们要尽量脱了壳后再来用 OllyDBG 调试，特殊情况下也可带壳调试。