逆向笔记3--常见的逆向调试方式

原创

Sezangel 于 2019-11-05 20:05:26 发布 1405 收藏 3

分类专栏： 逆向

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/weixin_43046297/article/details/102922564

版权

逆向 专栏收录该内容

14 篇文章 2 订阅

订阅专栏

根据软件调试经验，这里列举了我个人总结出来的一些常用的软件调试方案

1.nop法

nop法通过用于跳过序列号验证机制，得到最后的成功结果，关键是我们要找到序列号判定的函数，如何找到这个函数，常用的方法有以下几个：

1.利用字符串查找法，右键，查找，引用的字符串，查找判断失败或者成功弹出的字符串，从而向上，找到判定函数的位置，之后再跟进调试。

2.利用调用模块查找法，右键，查看调用的模块，尤其是对于要输入验证码的程序，常见的模块调用有：

GetDlgItemTextA（GetDlgItemTextW）

GetWindowTextA（GetWindowTextW）（当然这是对于调用windows API函数的代码），有一些程序编写的代码语言，决定了其链接库调用的函数名称不是这些，需要我们查找具体函数名

3.ctrl+N，可以直接查找所有的函数调用表，进而查找我们所需要下断的函数

2.修改代码结构法

修改代码结构法通常用于清楚nag窗口，或者用于防止OD调试（通过恶意修改代码结构方法防止我们调试程序）

比如：1.改变AddressofEntryPoint，从而直接把nag窗口弹出的代码段跳过

比如：2.程序员编写程序时采取的方法，将sizeofcode字段恶意变长，我们可以通过修改为正常值的方法，从而实现调试，发现程序有采取这种方法时，我们不仅要关注sizeofcode，还要关注：SizeofInitialzedData、Baseofcode、Baseofdata。。。。。类似结构

3.修改寄存器数值法

这种方法也通常用于破解软件、跳过序列号验证机制、跳过nag窗口，比如在条件跳转指令前，存在test ax，ax代码，这时在该验证代码之前，可以人工修改ax的值，进而改变后续跳转指令。

4.强制改变跳转指令法

这种方法也是通常用于破解软件、跳过序列号验证机制、跳过nag窗口的等等，可以将条件跳转指令改为强制跳转指令，或者将跳转条件相反的指令互相修改，从而达到目的。

5.内嵌补丁法

内嵌补丁方法就是在程序的代码区块，利用没有用的代码区域，添加我们所需要的代码，比如我们需要让程序执行某个我们自己想要执行的代码段，可以利用jmp，跳转到我们编写内嵌补丁的区段，执行完代码后，jmp回原代码执行指令，即可实现我们需要的功能。

6.堆栈查看法

在调试代码的过程中，比如我们弹出了nag窗口，或者正在执行验证操作，如何查看此时代码调用的函数？
1.可以暂停函数，选择面板K，查看此时调用的函数
2.查看L，可以看程序的日志文件，里面可以看到代码的执行过程以及函数相关的调用。
3.利用看雪论坛提供的ollyuni.dll插件，还可以查看各种跳转指令的位置

7.通过程序资源查找关键指令

可以利用软件exescope，可以加载程序，并且查看程序内的资源，将程序加载入程序，到资源–对话框：可以看到所需分析的对话框或者关键部位的对应编号，因此可以在OD中查找指令：push+编号，下断，进而进行后续分析

8.反调试软件破解

1.多态病毒类
2.防OD调试的关键函数