OD打补丁

补丁点

在非对抗下，一般选择`call`、`jmp`指令上进行操作（最好操作的点）

直接跳和间接跳

- 直接跳
  - `call MeaageBox`直接跳往函数的第一条指令处，有兼容性问题（没有`jmp`跳表作中转）
  - 跳表即为**IAT**表（Import Address Table）
- 间接跳
  - `call ds:[MessageBox]`跳往**IAT**表的表项的地址处

注

VS编译器使函数以16字节对齐，中间填充`int 3`或者`nop`

OD的右键 —— **显示模块名称**，会显示程序**显示调用**的模块名称都会在里面，**隐式调用**（`LoadLibrary`）不会在

病毒分析：

病毒四要类：**文件操作类**、**网络传输类**、**注册表操作类**、**内核操作类**

不属于以上四种直接白名单

PE下数两行半，程序入口点