**0x00 挂起进程注入原理**

挂起进程注入其实和挂起线程注入其实是一个道理，区别在于挂起进程在程序开始时候，挂起线程在程序运行中，本质上都是挂起主线程，执行写入的ShellCode，这里就不做赘述了。

实现步骤:

1. 构造ShellCode
2. CreateProcess以挂起的方式启动目标进程

3.OpenThread打开线程，SuspendThread挂起线程

4.GetThreadContext获取目标主线程线程上下文

5.SetThreadContext修改目标主线程上下文到我们写入的ShellCode处执行

6.ResumeThread恢复线程让ShellCode执行

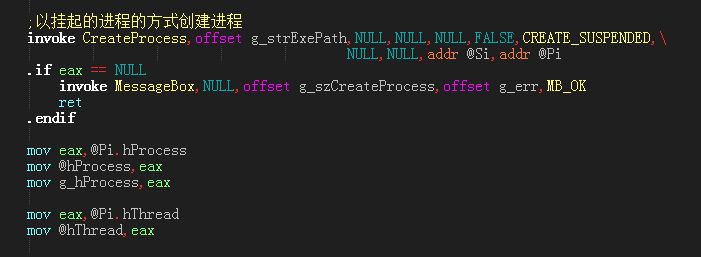
7.VirtualFreeEx扫尾释放空间

这种方式和挂起线程的方式代码编写思路几乎一样，并且更加简单方便，因为CreateProcess可以拿到目标进程的进程句柄和主线程句柄，省去了自己去拿。

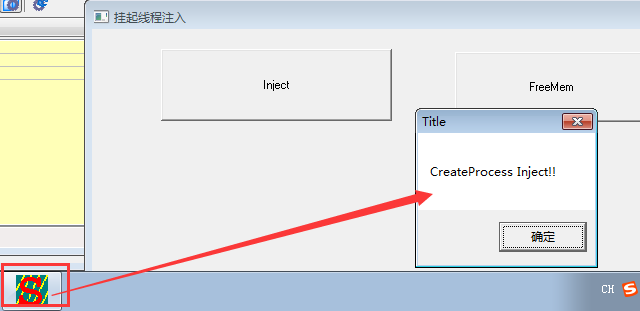
**0x01 挂起进程注入具体编程实现步骤**

由于这种方式和挂起线程注入方式的注入手段大同小异，所以只看区别部分

区别就在于使用的CreateProcess的API一口气实现了挂起主线程，拿到进程句柄，主线程句柄的操作，其他并无区别，详细请看附件代码



实验效果:



在程序启动前，弹出我们自定义的MessgeBox，注入成功