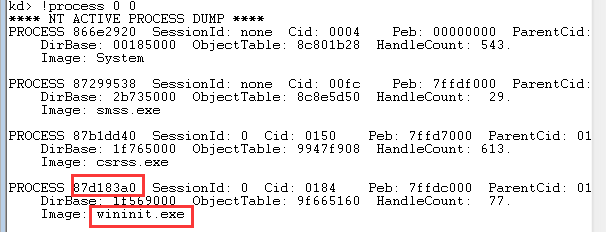
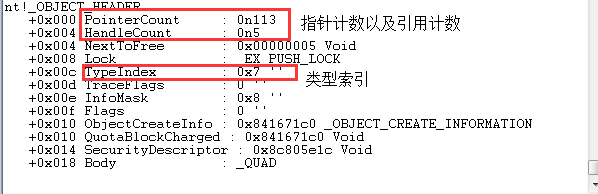
每一个内核对象，都有一个头部。

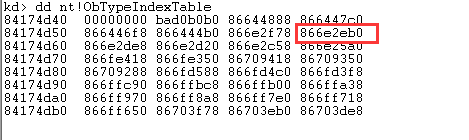
举例来说，分析一个进程对象

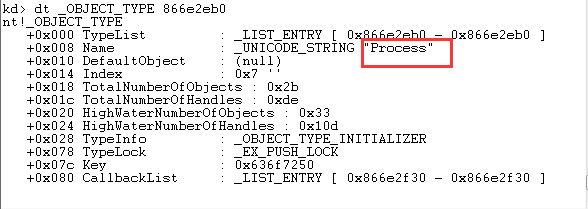


选取一个 EPROCESS地址：87d183a0



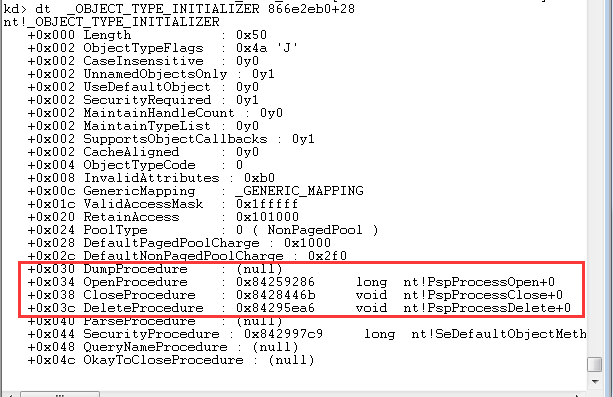
 typeIndex是ObTypeIndexTable的一个下标，索引是7。





 能够看到，对象类型是process

这里面，有一个比较重要的字段，就是\_OBJECT\_TYPE\_INITIALIZER

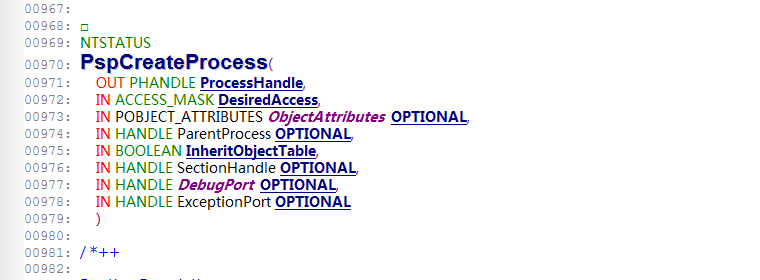


 这个结构体中，有很多函数指针，这些函数，在内核对象创建，销毁，打开，的时候会被调用。

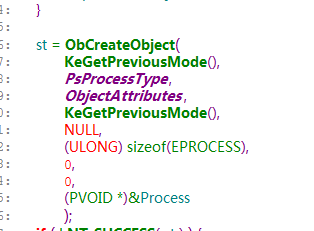
我们可以通过Hook这些函数，来控制 对象的创建，销毁，打开等操作

这种Hook，称之为Object-Hook。

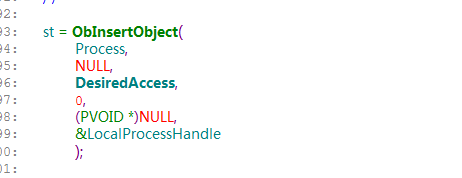
根据win2000的代码,createprocess为例子:

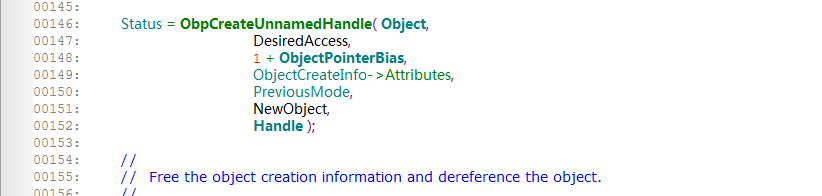


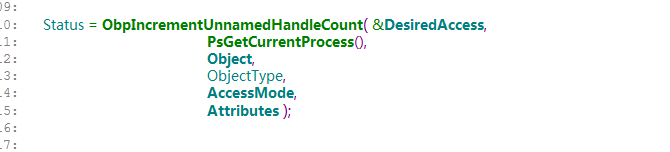
调用,但是创建对象的时候不会调用:



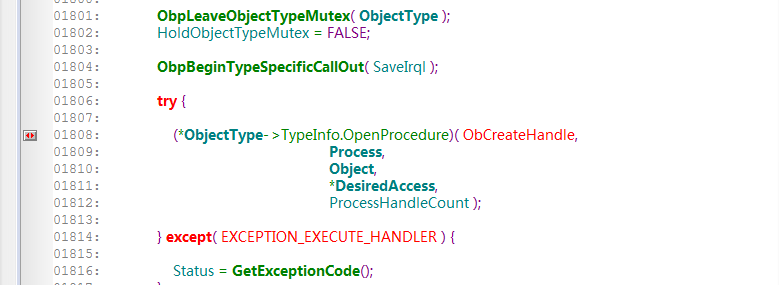
在插入进程的句柄表的时候会调用:





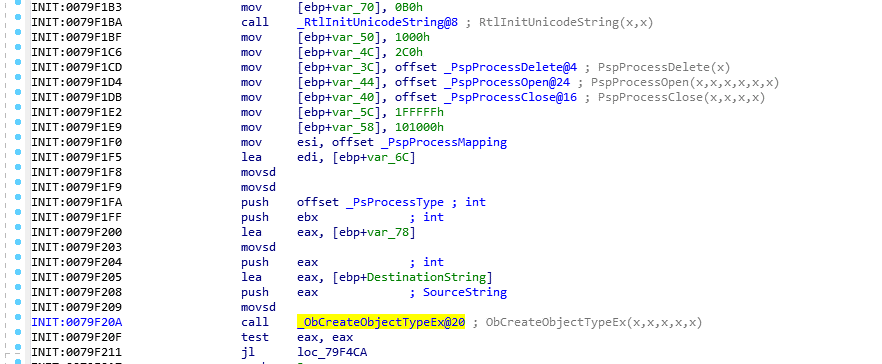


最后调用创建的回调:



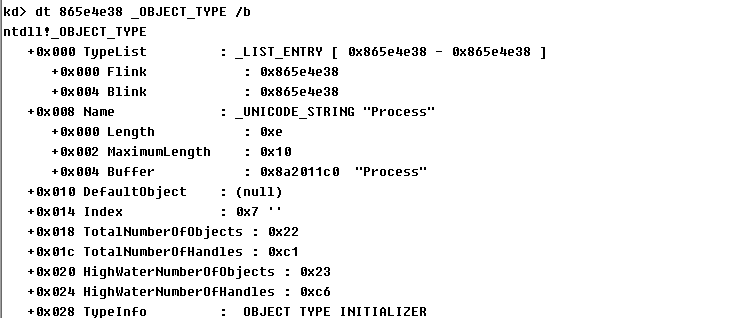
总结:其实所谓对象的hook拦截,其实对象以及创建完毕了,但是对象没法插入句柄表导致过程失败

Obj的初始化可以找到所有的回调函数的地址,直接查找ObCreateObjectTypeEx



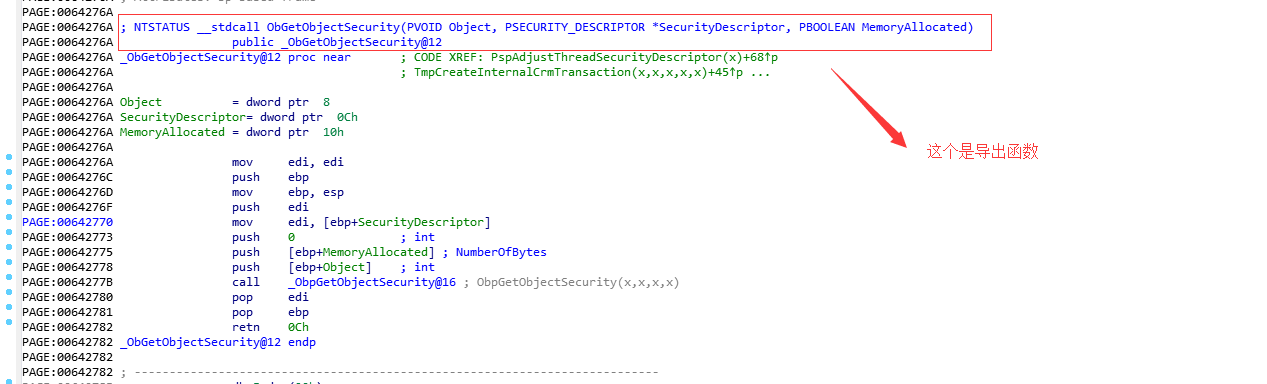


Windbg调试结果





怎么找ObpGetObjectSecurity,直接找obGetobjectSecurity,这个是个导出函数



句柄表结构:

