32位文件型病毒实验报告

|  |  |  |
| --- | --- | --- |
| 组员名单 | | |
|  |  |  |
|  |  |  |

**一.【实验目的】**

(1)了解文件型病毒的基本制作原理。  
(2)了解病毒的感染、破坏机制，进-步认识病毒程序。  
(3)掌握文件型病毒的特征和内在机制。

**二.【实验内容】**

通过运行病毒程序观看各步的提示以了解病毒的内在机制。

**三.【实验环境】**

VMWare 16.2.1

Windows xp

**四.【实验素材】**

virus.rar包中包括Virus.exe(编译的病毒程序)、软件使用说明书.doc(请仔细阅读)、源代码详解.doc(对代码部分加入了部分注释)以及pll.asm(程序源代码)。Example.rar包中选择的是一个常用程序(ebookedit)安装后的安装目录下的程序，用于测试病毒程序

**五.【实验步骤】**

**第一步 环境安装**

**1.直接将 example.rar 和 virus.zip 中的virus.exe 移动进 windows xp中**

**第2步 实验过程**

1.将virus.exe 移动进 已被解压的example文件夹中，然后运行：（图1-1， 1-2 ，1-3）

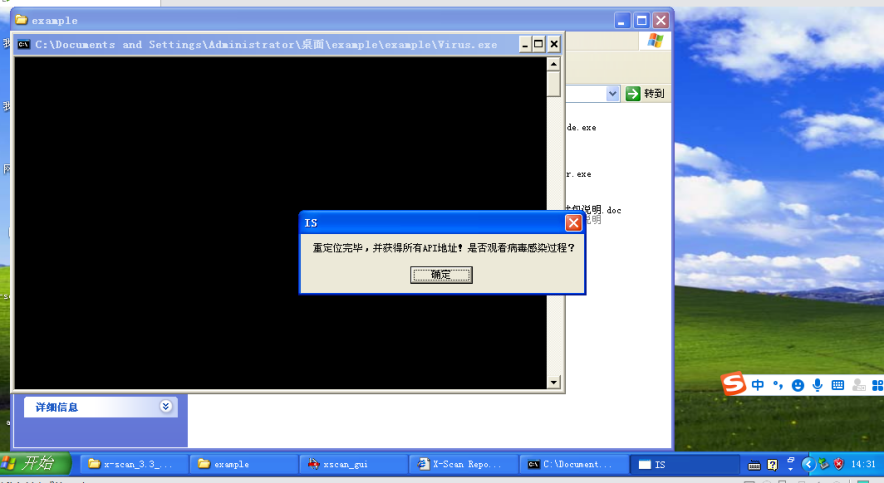


图1-1

1. 会弹出各种提示，点击“是”确认观看病毒感染过程，跟着流程走就行：

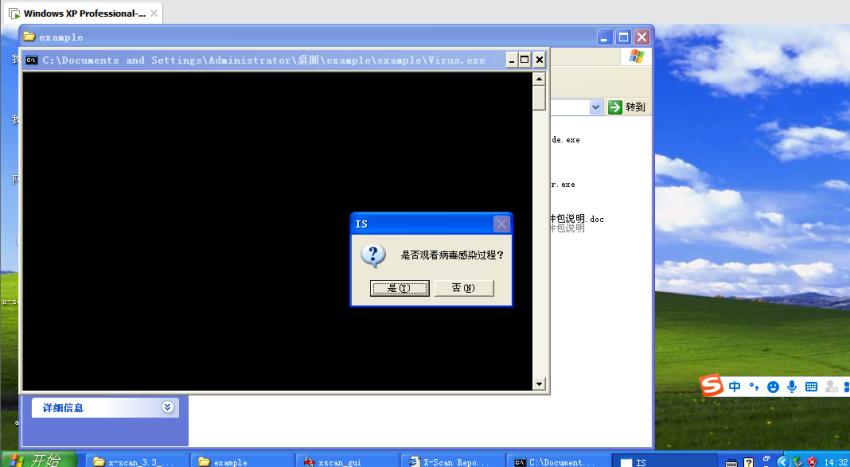


图2-1

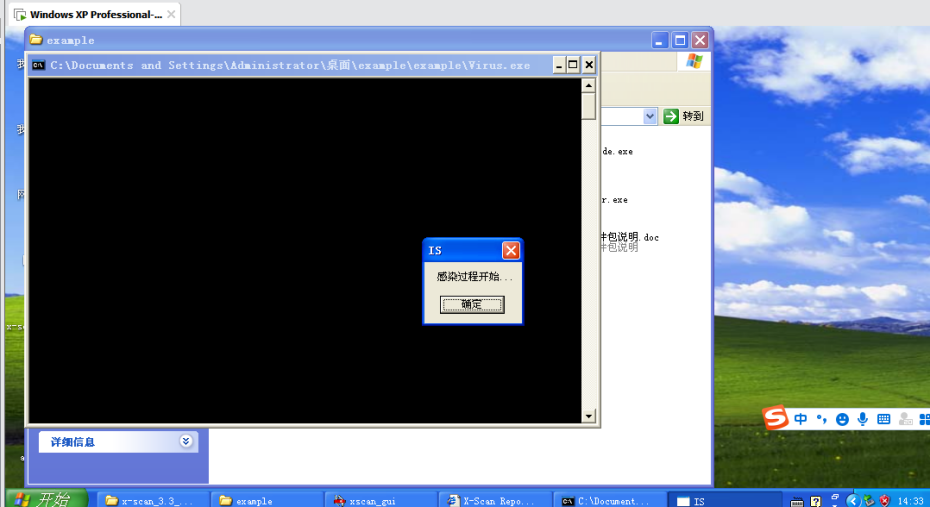


图2-2

3.开始查找本路径下所有符合感染条件的文件：

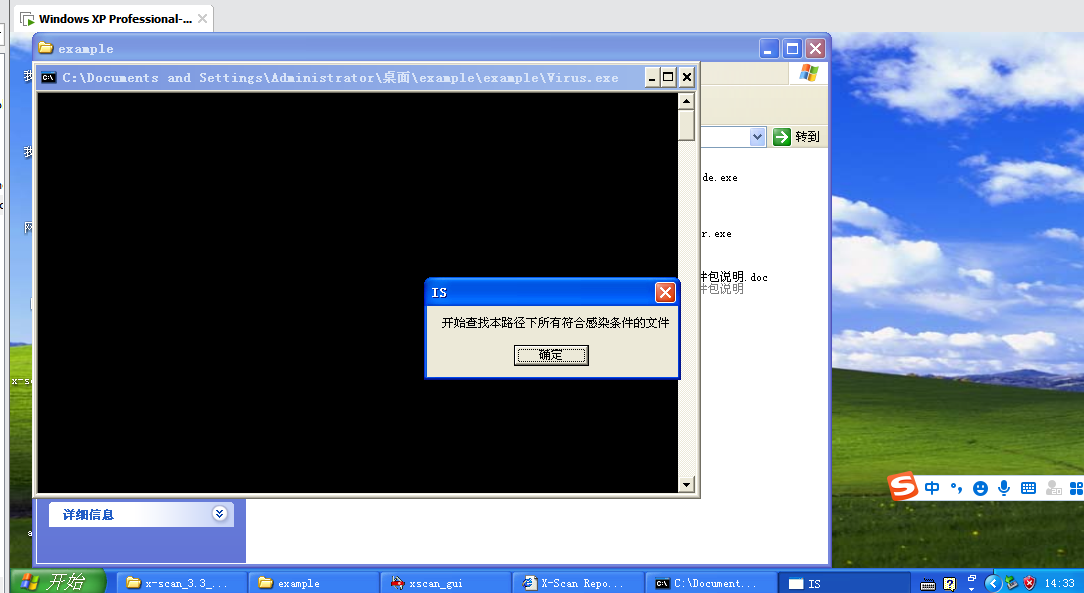


图3-1

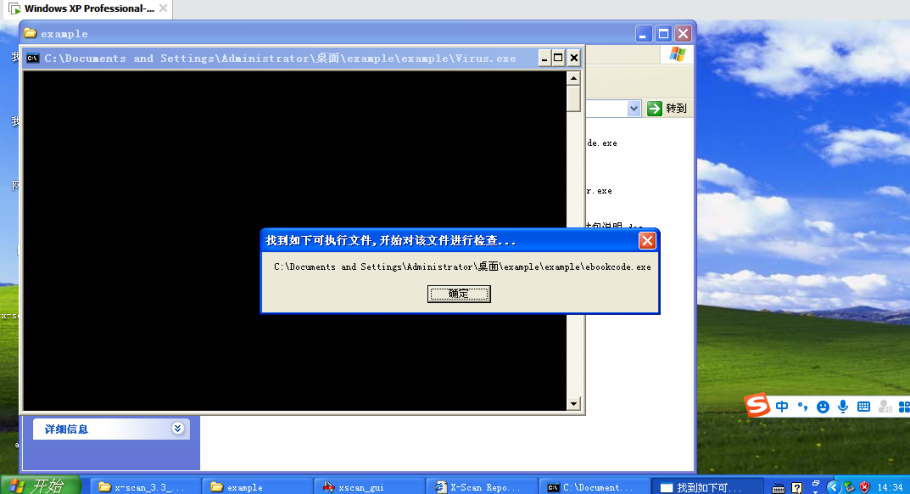


图3-2

**4.该文件未被感染，则进行感染：**

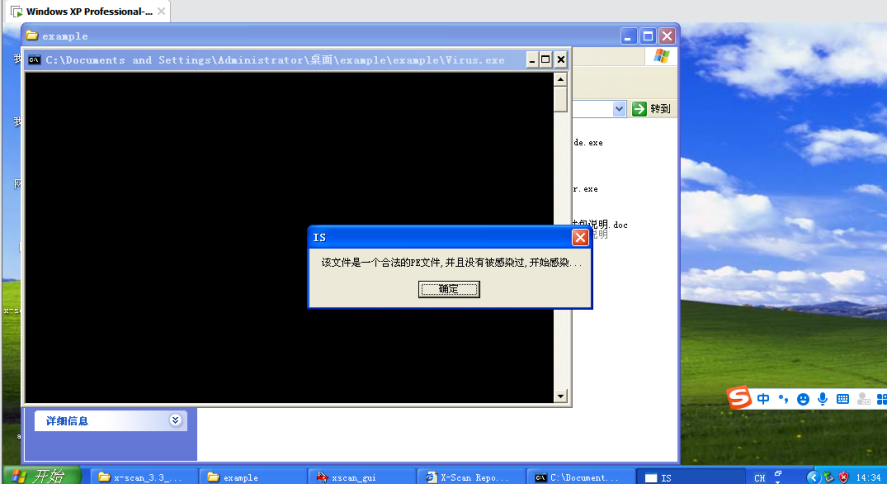


图4-1

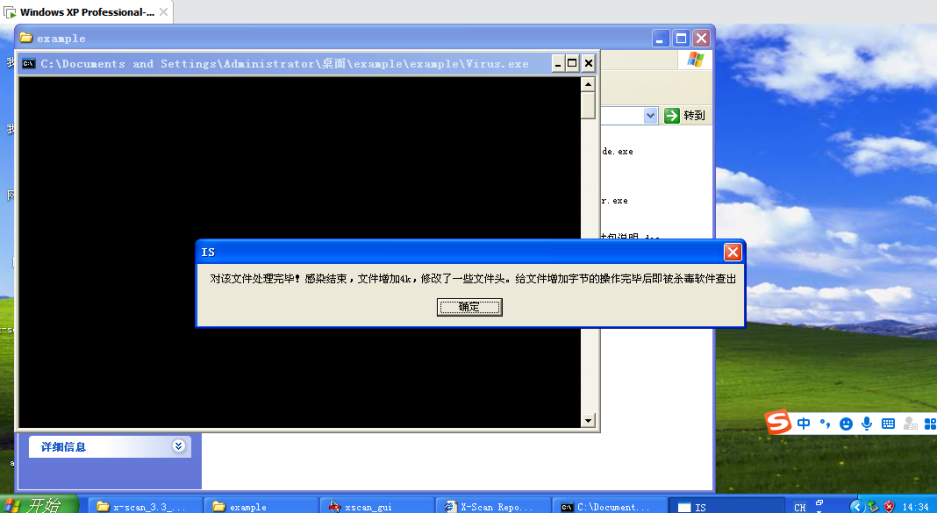


图4-2

**5.让病毒sleep一下，避免磁盘的高速运转，而被用户察觉：**

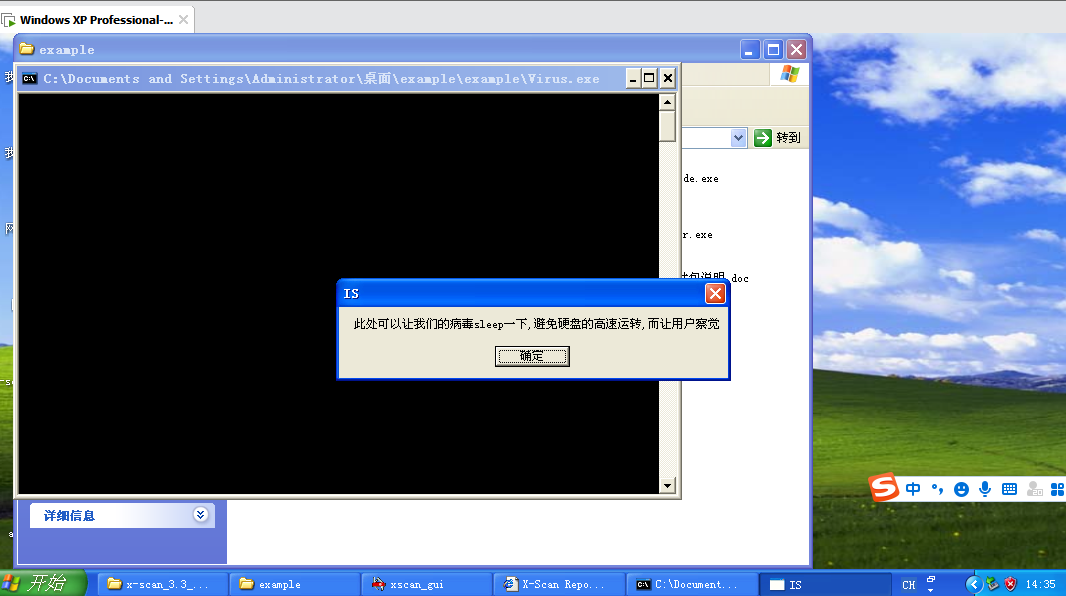


图5-1

**6.病毒还可以继续感染本目录下的其他exe文件，但因为步骤基本相同遂不记录：**

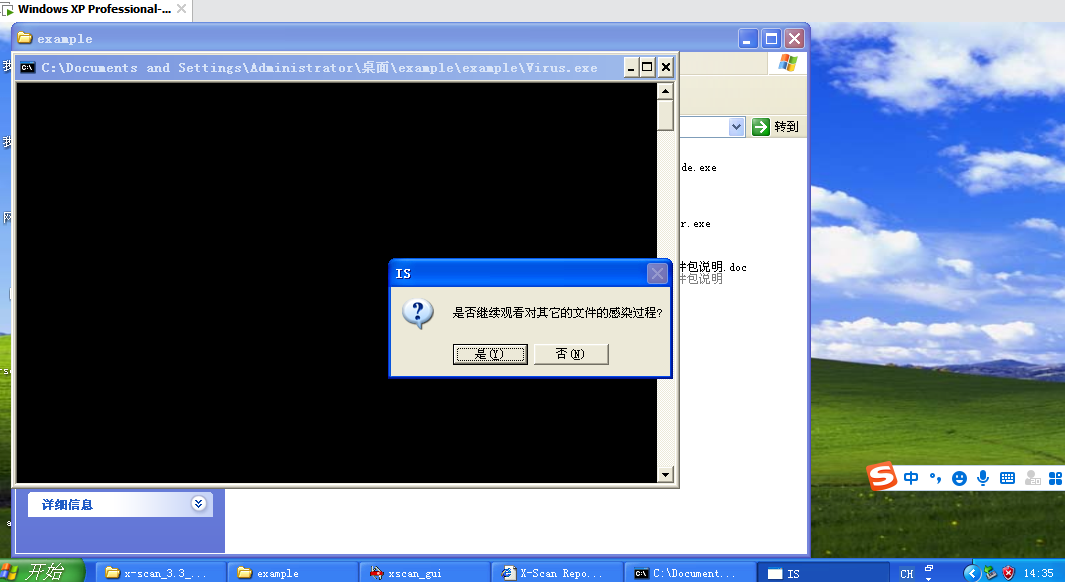


图6-1

**7.验证刚刚感染的exe文件是否成功被感染，点击ebookcode.exe 文件后发现弹出病毒文件virus.exe 所写的MessageBoxA函数:**

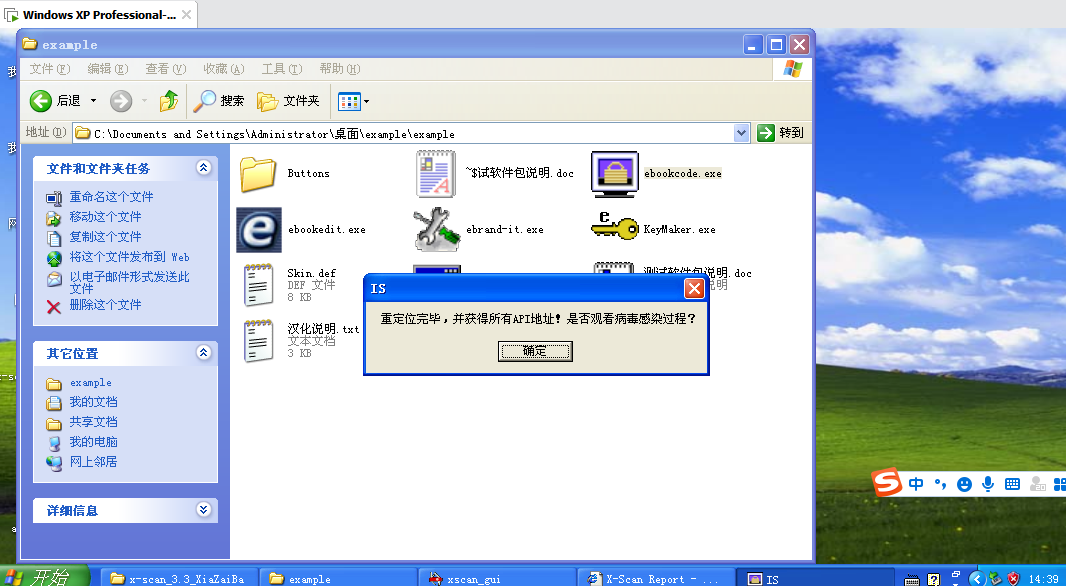


图7-1

发现成功被感染，实验完成。

**六.【源码分析】**

**1.PE结构示意图（图 7-1）：**

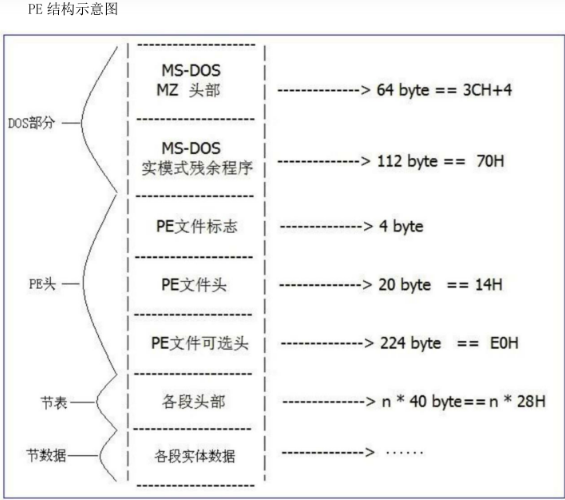


图6-1

**2.个别功能模块说明：（图 6-3）：**

**（1）显示msg模块,实际中可替换为攻击模块。**

**SingleTest  proc    szMsg                           ;for debug**

**pushad**

**push    0h**

**lea     eax,[ebx+offset szIS]**

**push    eax**

**mov     eax,szMsg**

**push    eax**

**push    0h**

**call    [ebx+lpMessageBox]**

**popad**

**ret**

**SingleTest endp**

图6-3

如 MessageBoxA函数：**（图 6-4）：**

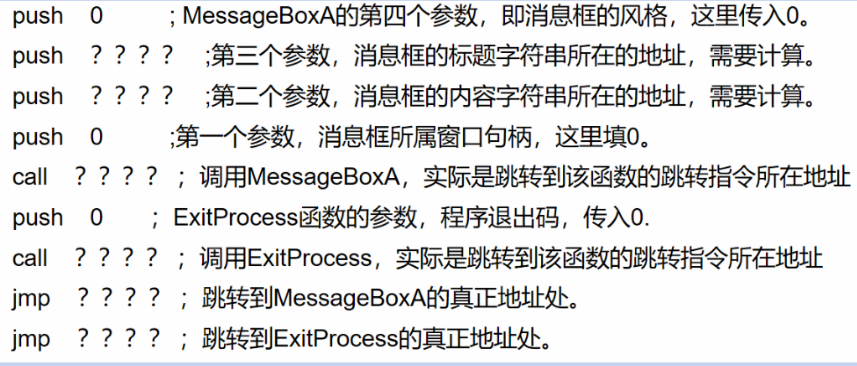


图6-4

**（2）文件处理模块,调用了windows api 的 CreateFileA 函数,其余调用windows api的操作与调用 CreateFileA 的方法相同（图 6-5）：**

**ProcessFile     proc    File:dword**

**；――――――――――――――――――――――――――――――――――――――**

**；对文件进行处理，参考文献**

**；――――――――――――――――――――――――――――――――――――――**

**pushad**

**push    [ebx+dwOldEip]**

**push        0h          ;NULL**

**push        00000020h   ;FILE\_ATTRIBUTE\_ARCHIVE**

**push        3h          ;OPEN\_EXISTING**

**push        0h          ;NULL**

**push        1h+2h       ;FILE\_SHARE\_READ or FILE\_SHARE\_WRITE**

**push        80000000h+40000000h ;GENERIC\_READ or GENERIC\_WRITE**

**push        File**

**call            [ebx+lpCreateFileA]**

**cmp         eax,-1                                  ;-1 is invalid**

**je          RT**

图6-5

Windows api函数库中的说明：（图 6-6）：



图6-6

**7.【实验总结】**