实验　PE 病毒

中国科学技术大学 曾凡平

5.1 实验目的

了解 Windows 操作系统环境下的 PE 病毒的原理，并验证病毒的危害。

5.2 实验环境

本实验使用安装了 VC9.0 的 Windows 2003 操作系统，可以利用实验 1 的虚拟机。

5.3 实验原理和步骤

本实验使用安装了 VC9.0 的 Windows 2003 操作系统，可以利用实验 1 的虚拟机。如果还没有建立虚拟机，参考实验 1 的步骤，下载、导入和设置虚拟机。

5.3.1 PE 病毒的原理

Windows 的可执行文件，如*,exe、*.dll、*.ocx 等，都是 PE(Portable Executable)格式文件，即可移植的执行体。感染 PE 格式文件的 Windows 病毒，简称为 PE 病毒。

PE 病毒中最难实现的是感染模块。感染模块其实是向 PE 文件添加可执行代码，要经过以下几个步骤：

(1) 判断目标文件是否为 PE 文件
(2) 判断是否被感染，如果已被感染过则跳出继续执行原程序程序，否则继续；
(3) 将添加的病毒代码写到目标文件中。这段代码可以插入原程序的节的空隙中，也可以添加一个新的节到原程序的末尾。为了在病毒代码执行完后跳转到原程序，需要在病毒代码中保存 PE 文件原来的入口指针。
(4) 修改 PE 文件头中入口指针，以指向病毒代码中的入口地址。
(5) 根据新 PE 文件的实际情况修改 PE 文件头中的一些信息

罗云彬在《Windows 环境下 32 位汇编语言程序设计》中给出了向 PE 文件中添加执行代码的实例。只需做少量修改就可以实现病毒的感染模块，感兴趣的读者可自行研究。

5.3.2 验证 PE 病毒的步骤

(1) 获得病毒样本

从课程网站下载 AddCode.zip，解压缩到 C:\Work，所看到的信息如图 1 所示

bjhuangustc.edu.cn

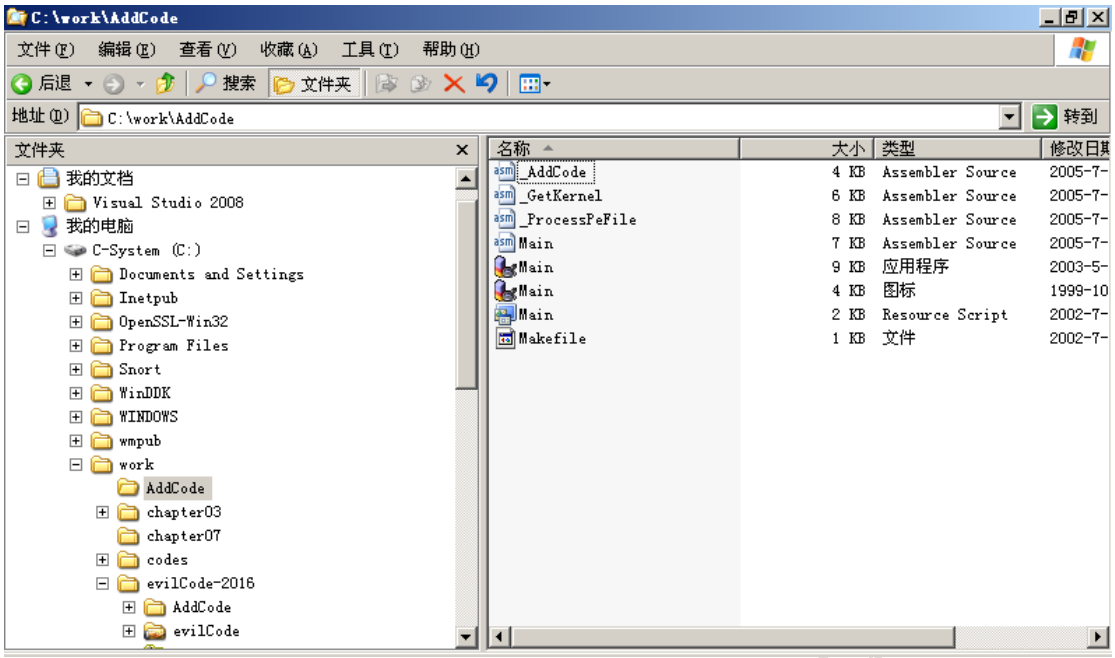

图 1 AddCode 的内容

Main.exe 就是实现了感染功能的病毒原型程序。

(2) 感染命令行程序

启动 Visual Studio 2008，建立一个 Windows Console 工程，在命令行上输出你的姓名和学号，如图 2 所示。

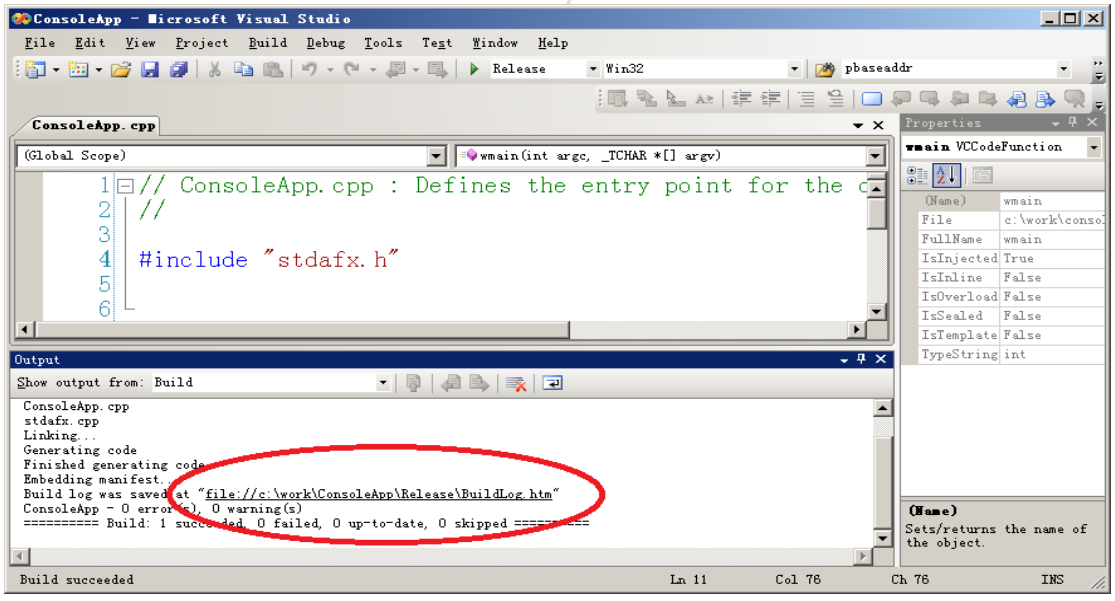

图 2 命令行程序

启动命令行，执行未感染的程序，如图 3 所示，程序正常运行。

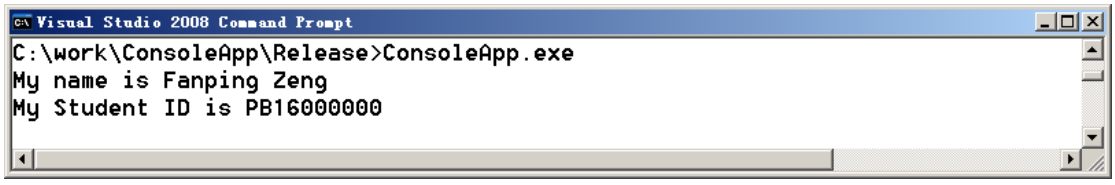

图 3 程序正常运行

启动病毒程序 main.exe，从文件菜单选择要感染的程序，如图 4 所示。

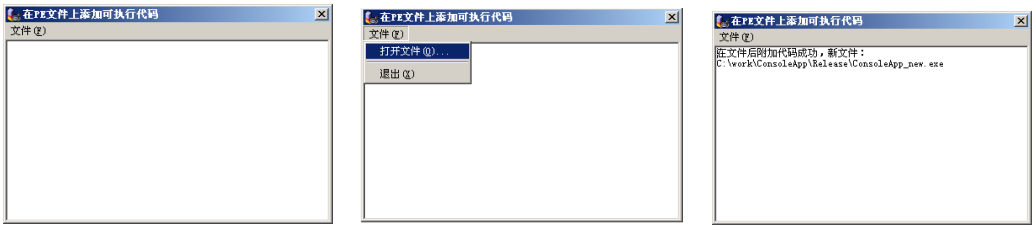

图 4 感染命令行程序

运行感染后的程序 ConsoleApp_new.exe。可以观察到，启动该程序后先运行了病毒代码（一个对话框），然后再执行原来的代码。如图 5 所示。

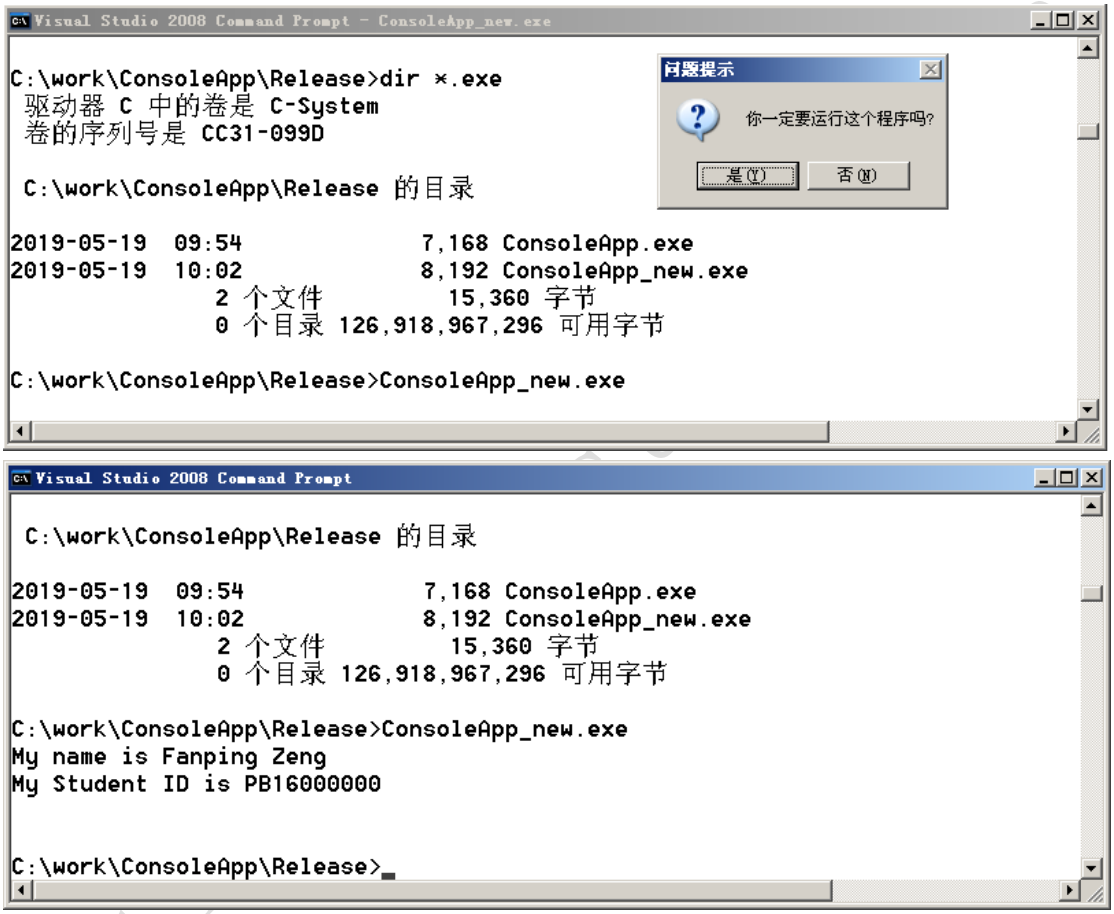

图 5 感染了病毒程序的运行过程

5.4 做实验并写实验报告，并提交光盘映像文件

（1）用 Visual Studio 2008 建立一个 Windows MFC Dialog based（Resource Language 选择中文（中国），选择 Use MFC in a static library）的工程，在 Dialog 上显示你的姓名和学号（如下图）。用病毒原型程序感染该可执行程序。

（2）参考 myVirus.iso，用（1）中的感染了病毒的可执行程序和 AUTORUN.INF 制作一张光盘映像文件（iso 文件），文件名为“学号.iso”。

（3）将制作好的光盘映像文件加载到 Windows 2003 操作系统，参考下图，验证 AutoRun 病毒在双击盘符、自动播放、MyExplore、Open 后的效果。

提示：可以用 ubuntu Linux 的 mkisofs 制作光盘映像文件。