

中国科学技术大学计算机科学与技术学院

《信息安全导论》实验报告



实验题目：PE 病毒_____

学生姓名：郭耸霄_____

学生学号：PB20111712_____

完成日期：2022 年 5 月 18 日

信息与计算机实验教学中心制

2020 年 09 月

1 实验题目

PE 病毒。

2 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。

3 实验环境

1. Device: HP-Pavilion-Aero-Laptop-13-be0xxx
2. Operating System: Kubuntu 20.04(64-bit)
3. Processors: 16 × AMD Ryzen 7 5800U with Radeon Graphics
4. Virtual Machine Platform: VirtualBox6.1.32_Ubuntu r149290
5. Virtual Machine: Windows2003(32-bit) with VC9

4 实验原理

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。

5 实验步骤

5.1 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。

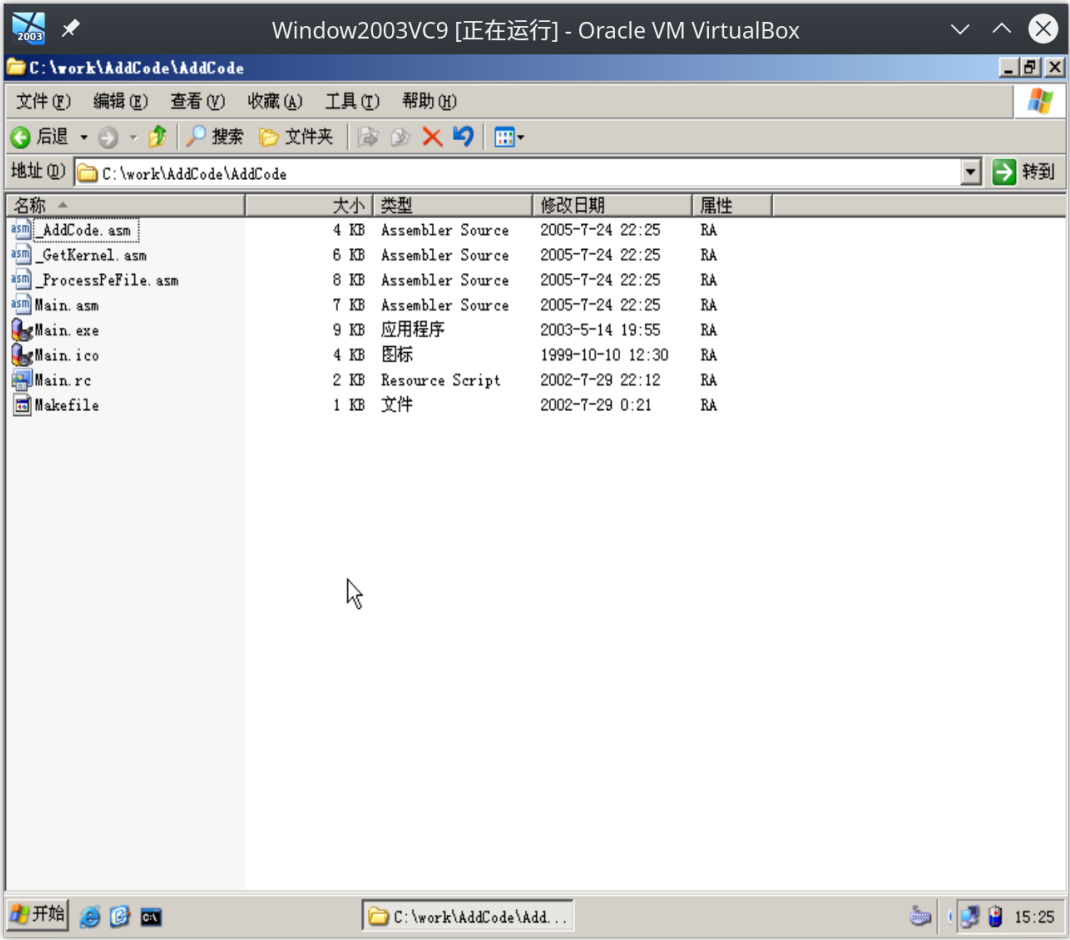


图 1: 获得的病毒样本

Main.exe 就是实现了感染功能的病毒原型程序。

5.2 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。

实 验 报 告

215 院 011 系 020 级 003 班

郭耸霄 PB20111712

2022 年 5 月 18 日

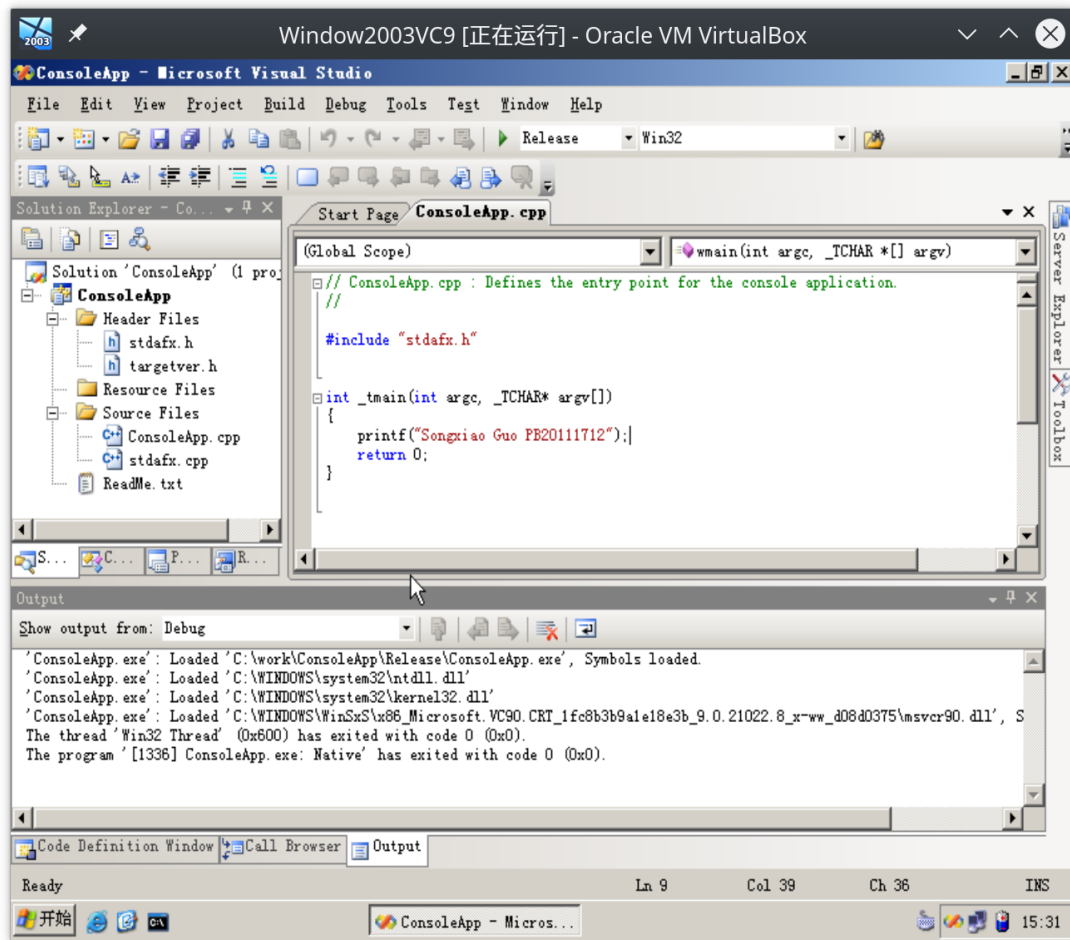


图 2: 建立的 Windows Console 工程

启动命令行，执行未感染的程序，如图 3 所示，程序正常运行。

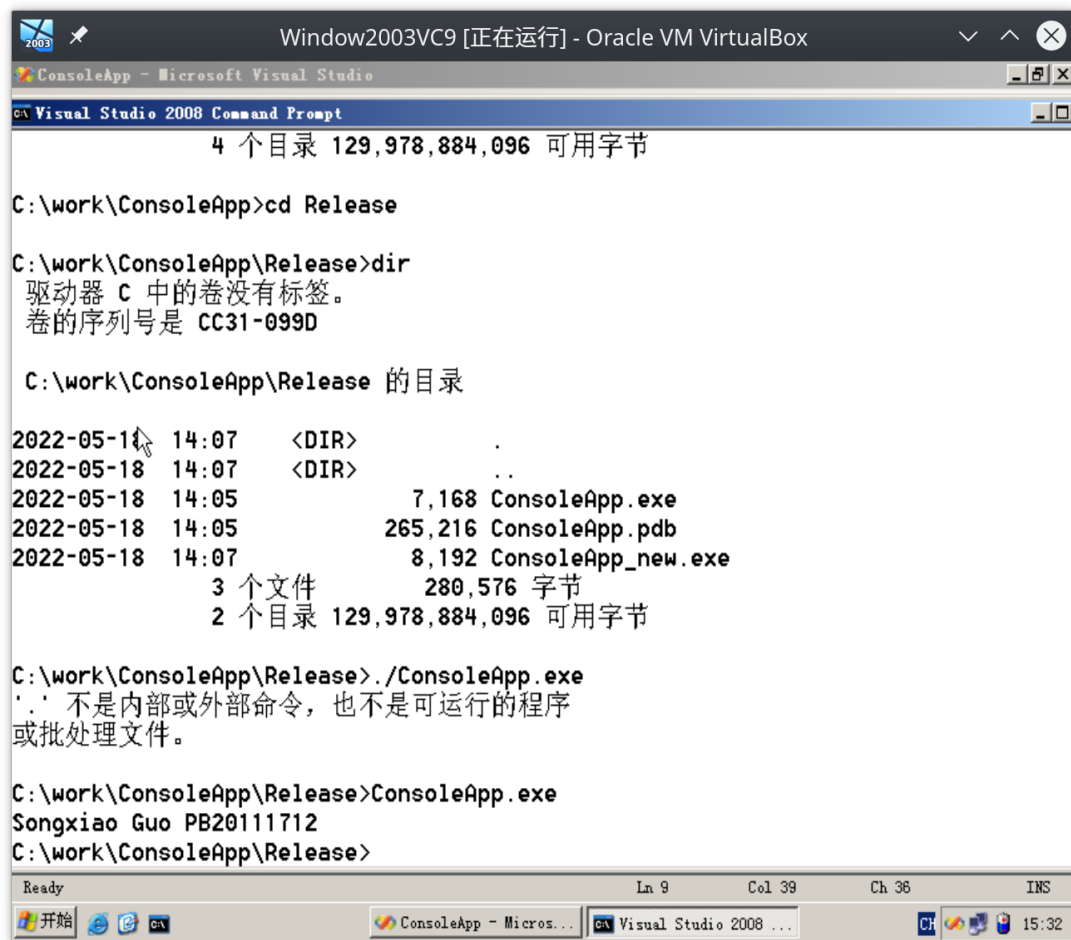


图 3: 未感染的程序正常运行

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。

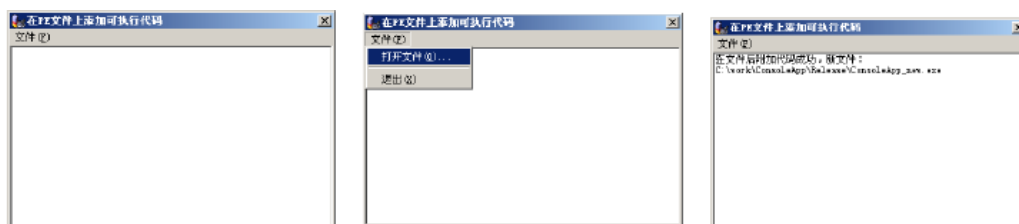


图 4: 感染程序

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、6 所示。

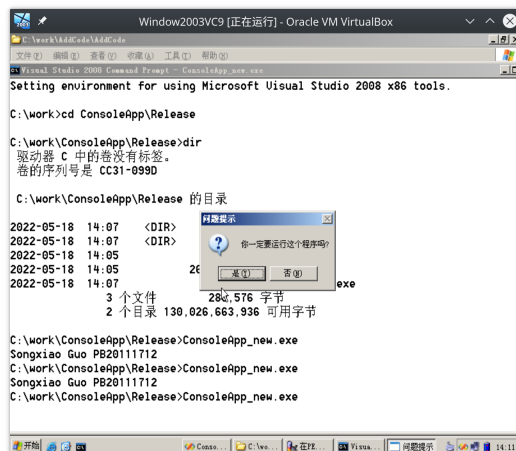


图 5: 感染后的程序先运行病毒代码

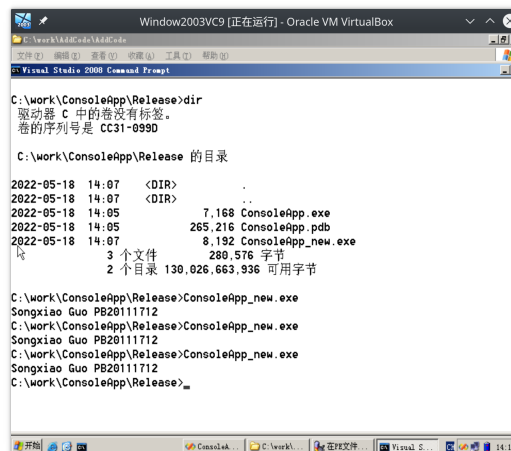


图 6: 感染后的程序再执行原来的代码

5.3 用 Visual Studio 2008 建立一个 Windows MFC Dialog based 的工程，在 Dialog 上显示我的姓名和学号。用病毒原型程序感染该可执行程序。

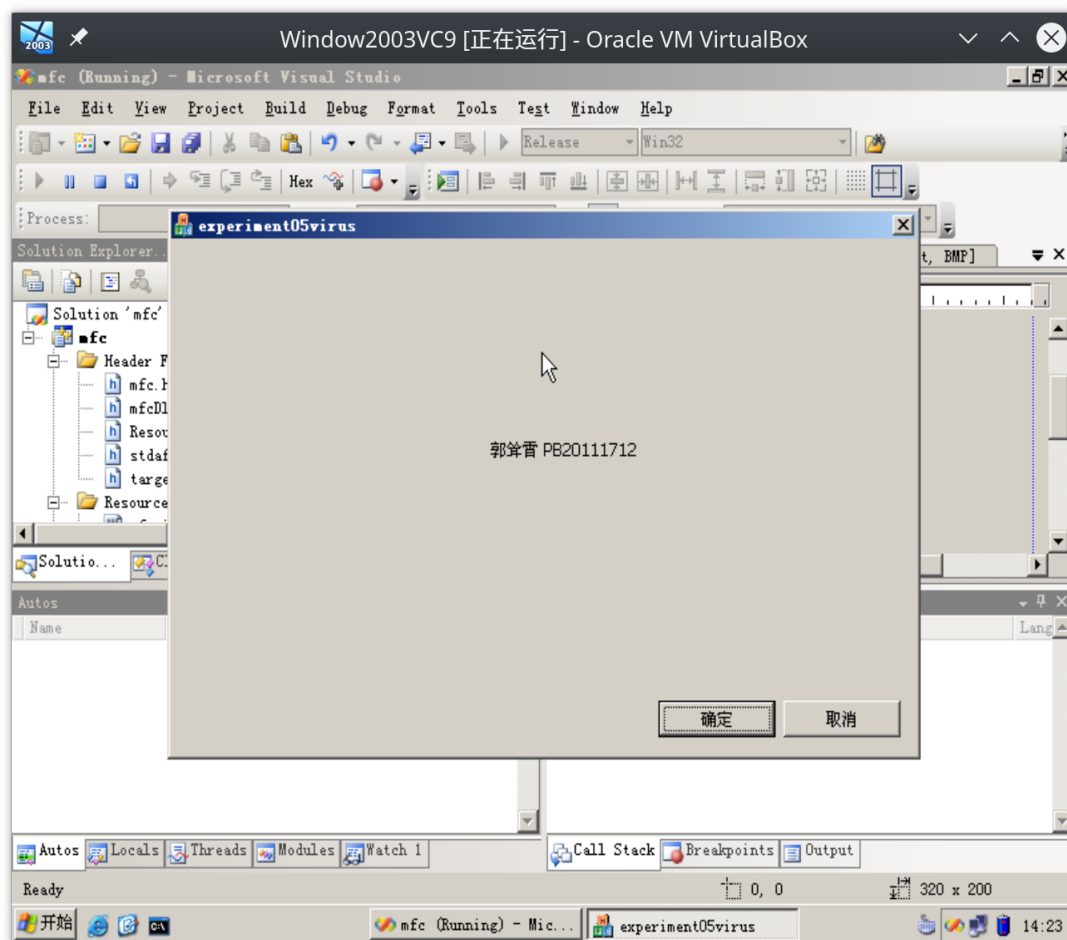


图 7: 在 Dialog 上显示我的姓名和学号

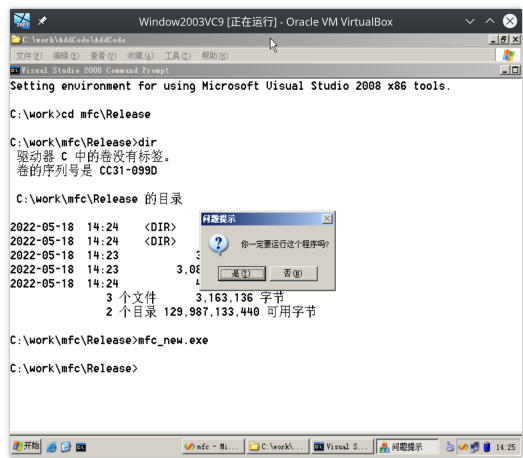


图 8: 感染后的程序先运行病毒代码

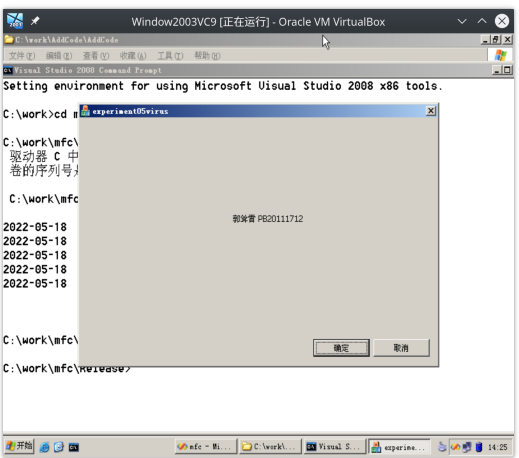


图 9: 感染后的程序再执行原来的代码

5.4 参考 myVirus.iso,用 5.3 中的感染了病毒的可执行程序 and AUTORUN.INF 制作一张光盘映像文件, 文件名为 “pb20111712.iso”。

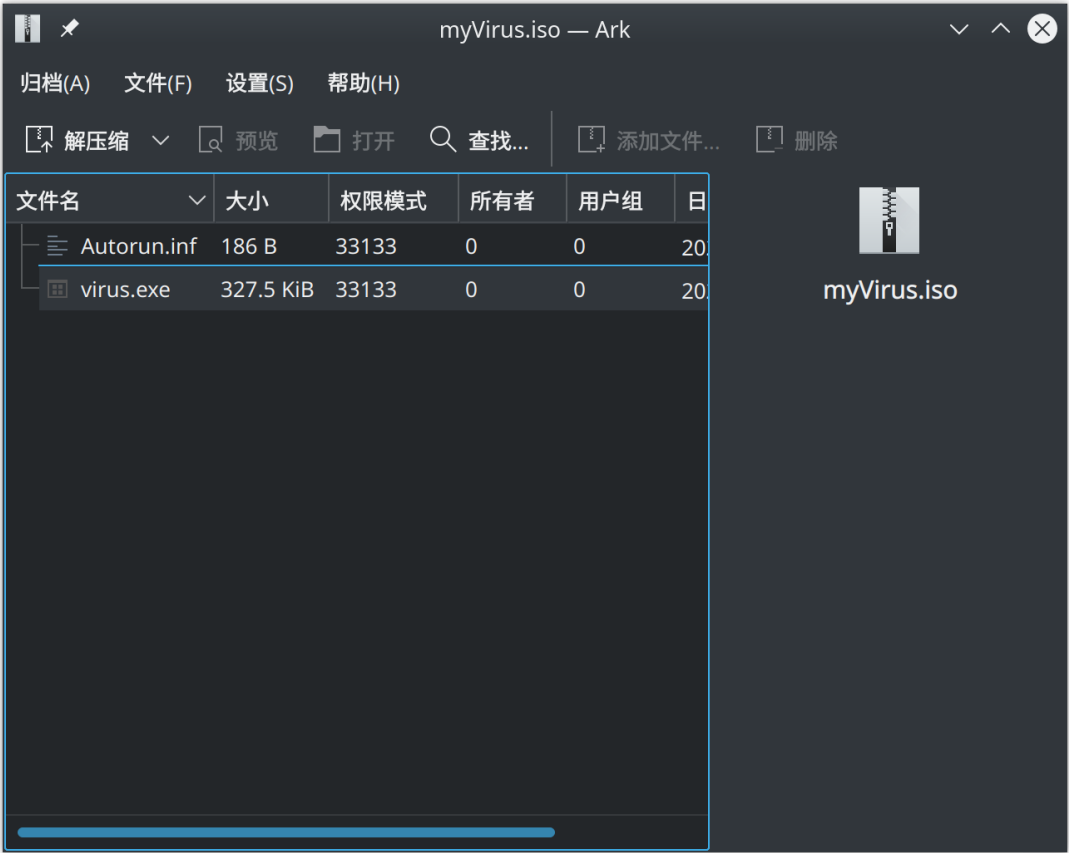


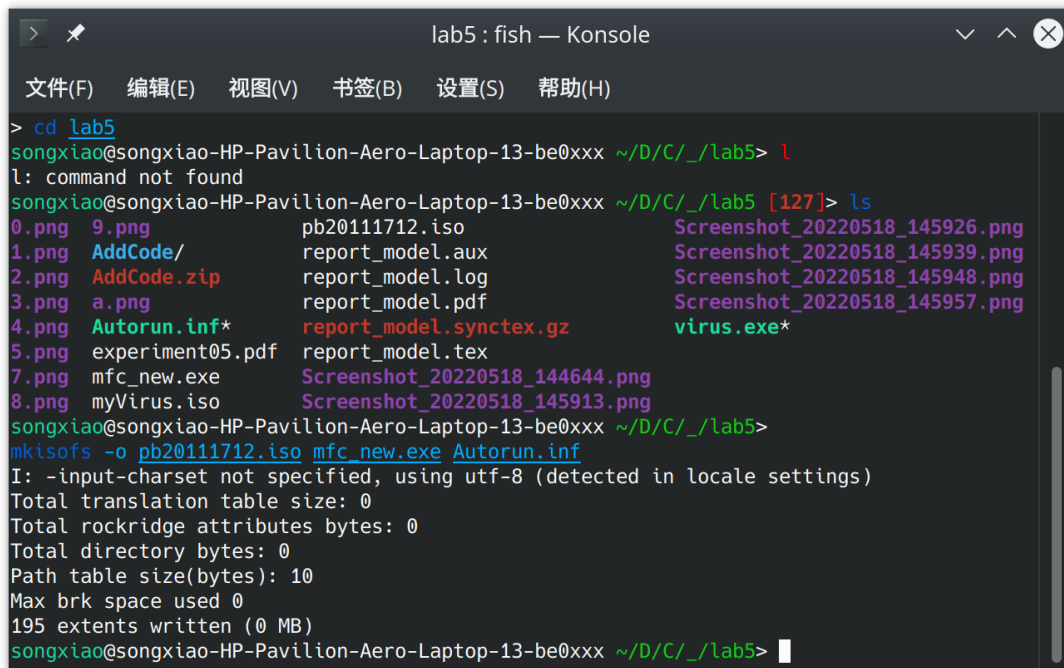
图 10: 在 myVirus.iso 中找到 AUTORUN.INF

实 验 报 告

215 院 011 系 020 级 003 班

郭耸霄 PB20111712

2022 年 5 月 18 日



```
lab5 : fish — Konsole
文件(F) 编辑(E) 视图(V) 书签(B) 设置(S) 帮助(H)

> cd lab5
songxiao@songxiao-HP-Pavilion-Aero-Laptop-13-be0xxx ~/D/C/_/lab5> l
l: command not found
songxiao@songxiao-HP-Pavilion-Aero-Laptop-13-be0xxx ~/D/C/_/lab5 [127]> ls
0.png  9.png          pb20111712.iso          Screenshot_20220518_145926.png
1.png  AddCode/        report_model.aux        Screenshot_20220518_145939.png
2.png  AddCode.zip     report_model.log        Screenshot_20220518_145948.png
3.png  a.png          report_model.pdf        Screenshot_20220518_145957.png
4.png  Autorun.inf*   report_model.synctex.gz  virus.exe*
5.png  experiment05.pdf report_model.tex
7.png  mfc_new.exe    Screenshot_20220518_144644.png
8.png  myVirus.iso    Screenshot_20220518_145913.png
songxiao@songxiao-HP-Pavilion-Aero-Laptop-13-be0xxx ~/D/C/_/lab5>
mkisofs -o pb20111712.iso mfc_new.exe Autorun.inf
I: -input-charset not specified, using utf-8 (detected in locale settings)
Total translation table size: 0
Total rockridge attributes bytes: 0
Total directory bytes: 0
Path table size(bytes): 10
Max brk space used 0
195 extents written (0 MB)
songxiao@songxiao-HP-Pavilion-Aero-Laptop-13-be0xxx ~/D/C/_/lab5>
```

图 11: 用 mkisof 制作光盘映像文件

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

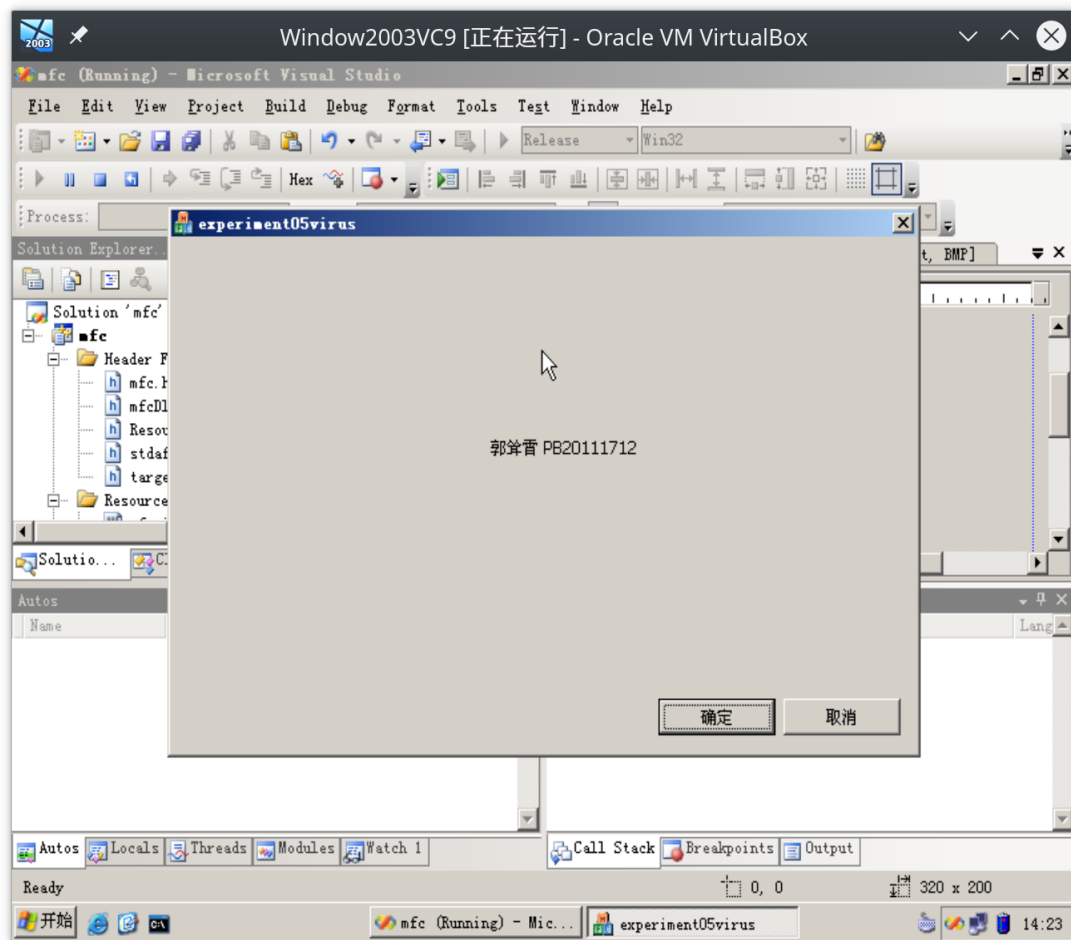


图 12: AutoRun 病毒在双击盘符后的效果

实 验 报 告

215 院 011 系 020 级 003 班

郭耸霄 PB20111712

2022 年 5 月 18 日

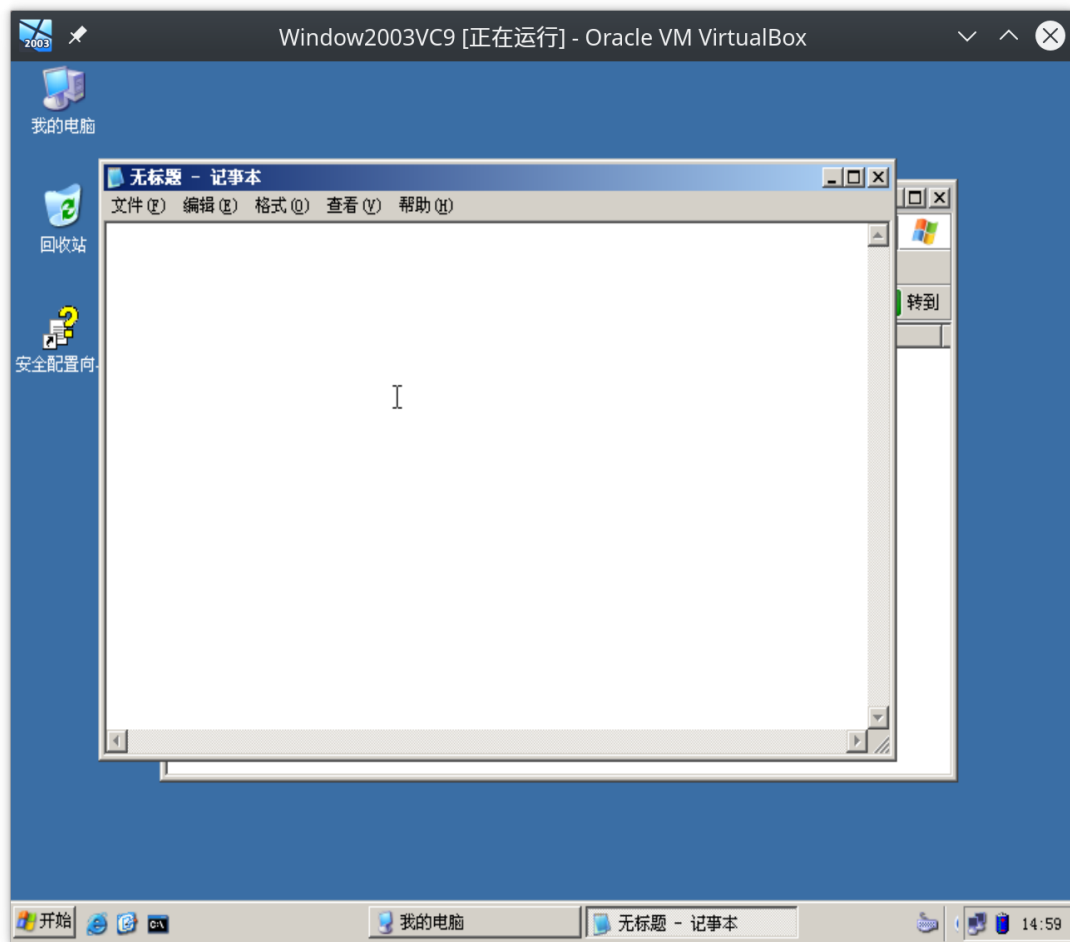


图 13: AutoRun 病毒在自动播放后的效果

实 验 报 告

215 院 011 系 020 级 003 班

郭耸霄 PB20111712

2022 年 5 月 18 日

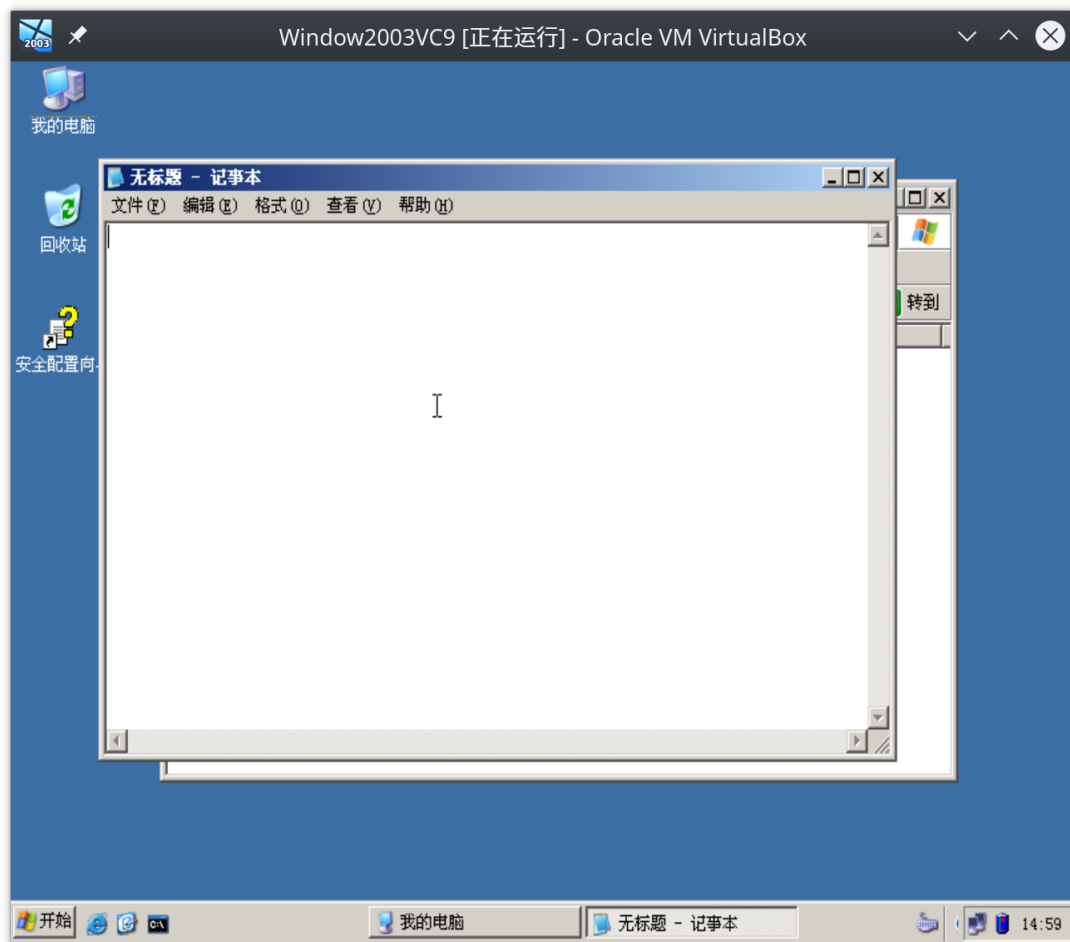


图 14: AutoRun 病毒在 MyExplore 后的效果

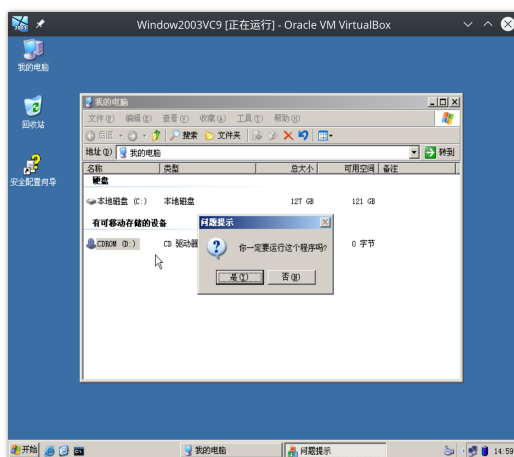


图 15: AutoRun 病毒在 Open 后的效果

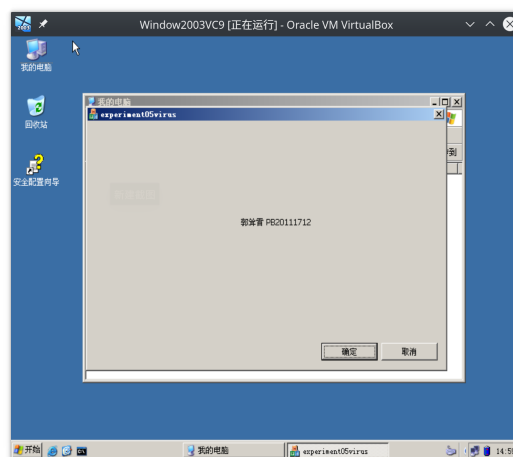


图 16: AutoRun 病毒在 Open 后的效果

6 实验总结

现象 0 在虚拟机上制作好的 mfc_new.exe 文件无法通过共享文件夹传到主机。

问题 0 Windows2003 (32-bit) 虚拟机安装 VirtualBox 增强功能失败。

实 验 报 告

215 院 011 系 020 级 003 班

郭耸霄 PB20111712

2022 年 5 月 18 日

解决方案 0 使用 ftp 协议传输文件。

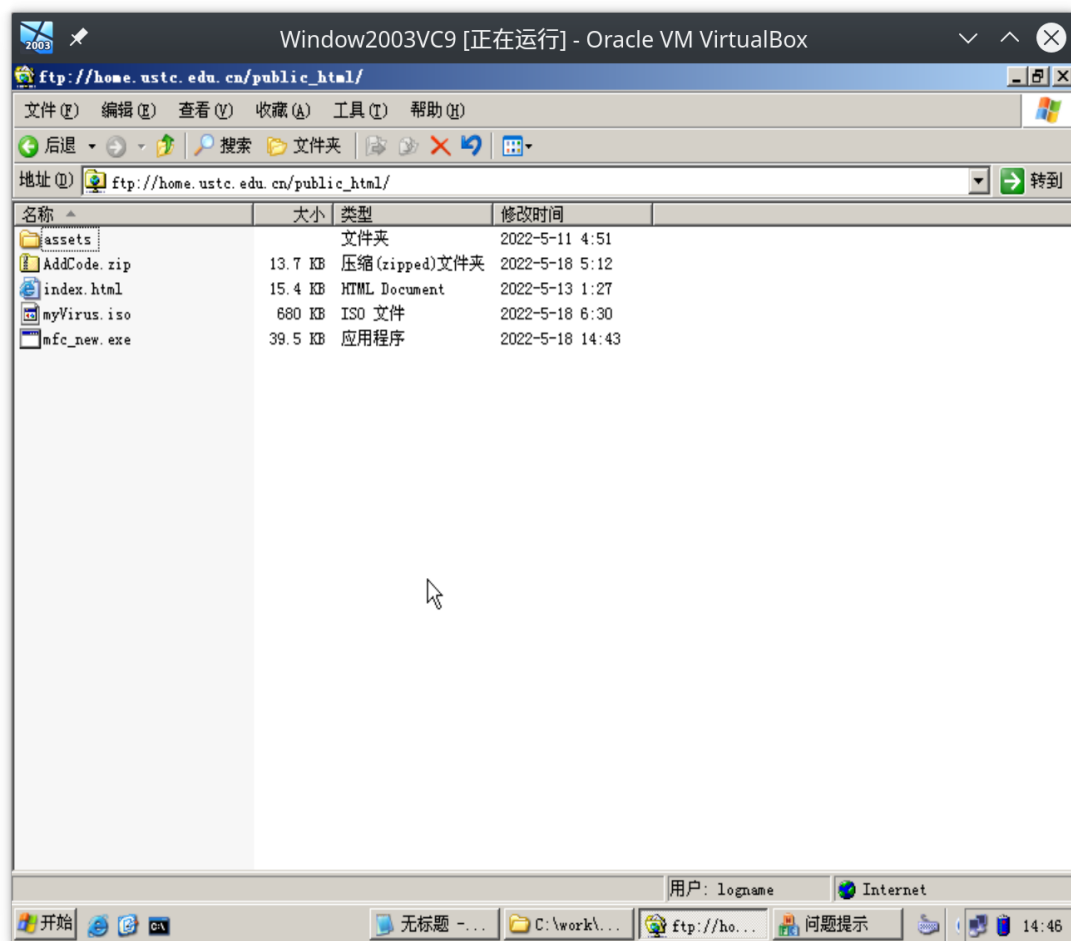


图 17: 使用 ftp 传输文件