



计算机安全与维护

Windows系统安全问题排查 基础课后实验



实验一 熊猫烧香病毒感染与清除

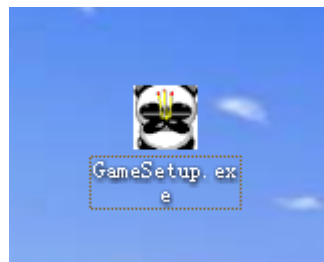
• 熊猫烧香病毒介绍

- 病毒名称：熊猫烧香，Worm.WhBoy.（金山称），Worm.Nimaya.（瑞星称）
- 病毒别名：尼姆亚，武汉男生，后又化身为“金猪报喜”，国外称“熊猫烧香”
- 病毒类型：蠕虫病毒，能够终止大量的反病毒软件和防火墙软件进程。
- 影响系统：Win 9x/ME、Win 2000/NT、Win XP、Win 2003、Win Vista
- 发现时间：2006年10月16日
- 来源地：中国武汉东湖高新技术开发区关山



实验一 熊猫烧香病毒感染与清除

- 熊猫烧香病毒的可执行文件
— 双击该文件后，病毒开始执行





实验一 熊猫烧香病毒感染与清除

- 执行后系统的感染情况（具体情况查看视频录像）
 - 病毒运行后，会把自己拷贝到
C:\WINDOWS\System32\Drivers\spo01sv.exe
 - 病毒建立一个计时器以6秒为周期在磁盘的根目录下生成setup.exe（病毒本身）和autorun.inf，并利用AutoRun Open关联使病毒在用户点击被感染磁盘时能被自动运行
 - 搜索感染所有.EXE/.SCR/.PIF/.COM文件，将感染目标文件和病毒溶合成一个文件（被感染文件贴在病毒文件尾部）完成感染



实验一 熊猫烧香病毒感染与清除

- 病毒会添加自启动项
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Runsvchshare 键值为
C:\WINDOWS\System32\Drivers\spoclsv.exe
- 每隔一秒，关闭开启的任务管理器和注册表编辑器等安全窗口
- 每隔六秒，删除安全软件在注册表中的键值
- 关闭系统进程和安全软件进程



实验一 熊猫烧香病毒感染与清除

- 熊猫烧香病毒的手工清除

- 手工清除过程中使用了IceSword软件工具

- 由于病毒原因无法直接查看系统的进程和对注册表进行编辑，所以借助IceSword工具来手工清除

- 清除步骤（实际演示查看视频录像）

- 找到病毒进程spo01sv.exe，并强制结束

- 删除注册表中的病毒启动项

- HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run的键值

- "svcshare=C:\WINDOWS\System32\Drivers\spo01sv.exe"



实验一 熊猫烧香病毒感染与清除

- 删除所有盘符根目录下的病毒文件：setup.exe和autorun.inf
- 删除病毒的本体文件
C:\WINDOWS\System32\Drivers\ spo01sv.exe
- 系统重启后，查看之前的注册表启动项位置，系统进程和病毒文件都已经被清除，不再生成
- 运行任务管理器和注册表编辑器也可以正常使用

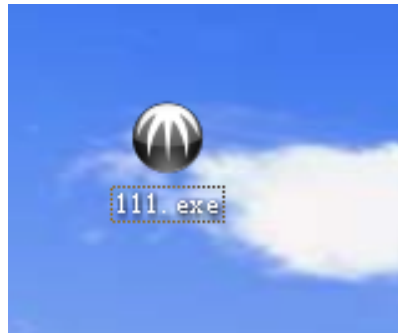


实验二 浏览器劫持病毒感染与清除

- 浏览器劫持病毒介绍

- 病毒程序运行后，会劫持一些购物网站，当进入这些网站时，会自动的跳转到病毒指定的其他购物网址，页面十分相似或者雷同

- 病毒本体运行文件为exe文件





实验二 浏览器劫持病毒感染与清除

- 分析和清除该病毒所用的工具
 - IceSword，用来查看进程，删除病毒文件
 - OllyDbg，查看病毒文件的源汇编码，分析病毒的运行机制



实验二 浏览器劫持病毒感染与清除

- 病毒执行后的感染情况（具体情况查看视频演示）
 - 病毒程序运行后，会在360的安装文件夹下生成两个文件：c:\Program Files\360\explore.exe和c:\Program Files\360\XXY.DLL
 - c:\Program Files\360\explore.exe作为进程在后台运行，c:\Program Files\360\XXY.DLL在浏览器启动时作为模块加载
 - 打开浏览器，开启一些比较热门的购物网站时，浏览器会自动的跳转到病毒指定的类似或者雷同的网站，迷惑用户和消费者



实验二 浏览器劫持病毒感染与清除

- 软件内部通过大量的网站地址的劫持和跳转来达到访问伪造网站的目的



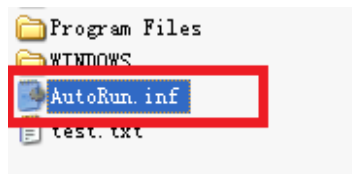
实验二 浏览器劫持病毒感染与清除

- 病毒的手动清除（实际演示查看视频录像）
 - 使用IceSword工具删除111.exe和explore.exe两个进程
 - 使用IceSword强制卸载浏览器进程中加载的XXY.DLL模块
 - 删除360目录下的两个病毒文件：c:\Program Files\360\explore.exe和c:\ProgramFiles\360\XXY.DLL
 - 重启电脑后，浏览器上网恢复正常



实验三 Autorun文件病毒的防范与删除

- Autorun.inf文件是电脑中比较常见的，作用是在双击磁盘时可以自动运行指定的文件
- 病毒和木马可以借由此方式达到自动运行的目的，尤其在移动设备中



	文件夹
	文件夹
1 KB	安装信息
0 KB	文本文档



实验三 Autorun文件病毒的防范与删除


- Autorun文件的指令格式

[AutoRun]	//表示AutoRun部分开始
Icon=X:\“图标”.ico	//给X盘一个图标
Open=X:\“程序”.exe或者“命令行”	//双击X盘执行的程序或命令
shell\“关键字”=“鼠标右键菜单中加入显示的内容”	//右键菜单新增选项
shell\“关键字”\command=“要执行的文件或命令行”	//选中右键菜单新增选项执行的程序或者命令



实验三 Autorun文件病毒的防范与删除

- 编辑好的AutoRun文件
- 双击盘符，右键“菜单”和右键“资源管理器”都会启动记事本程序



```
[autorun]
open=c:\windows\notepad.exe
shell\open=打开(&0)
shell\open\Command=c:\windows\notepad.exe
shell\open\Default=1
shell\explore=资源管理器(&x)
shell\explore\Command=c:\windows\notepad.exe
```



实验三 Autorun文件病毒的防范与删除

- 右键“打开”“资源管理器”都会启动记事本程序





实验三 Autorun文件病毒的防范与删除

- 在Autorun文件的内部修改打开的程序路径，可以在打开设备时自动运行病毒程序

```
AutoRun.inf - 记事本
文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

[autorun]
open=c:\windows\notepad.exe
shell\open=打开(&O)
shell\open\Command=c:\windows\notepad.exe
shell\open\Default=1
shell\explore=资源管理器(&X)
shell\explore\Command=c:\windows\notepad.exe
```



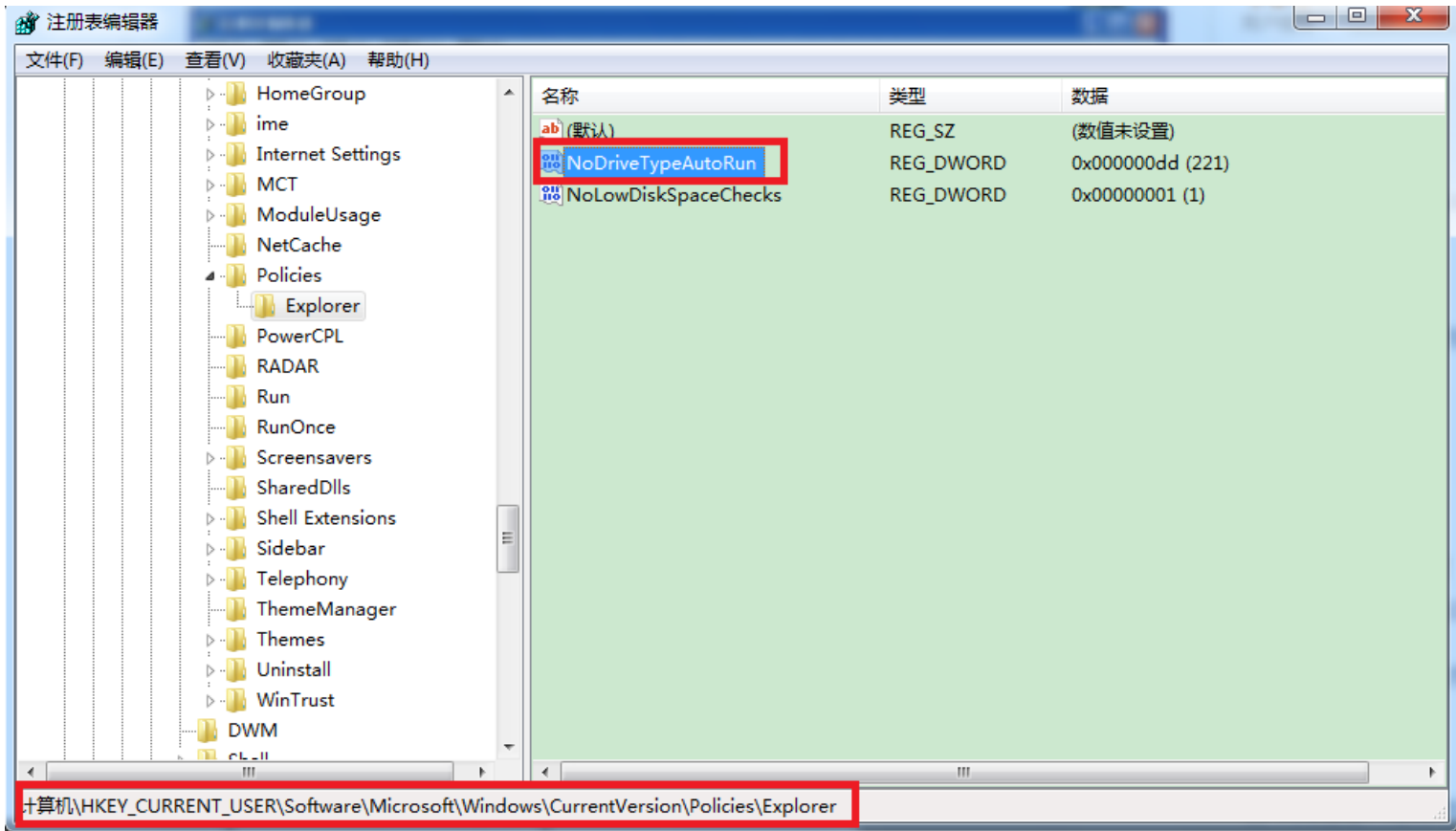
实验三 Autorun文件病毒的防范与删除

- Autorun病毒的防范
- 打开设备的方法：
 - 在电脑的地址栏中输入路径
 - 单击文件夹图标，从树型目录打开
 - 从开始菜单打开资源管理器，从树型目录打开



实验三 Autorun文件病毒的防范与删除

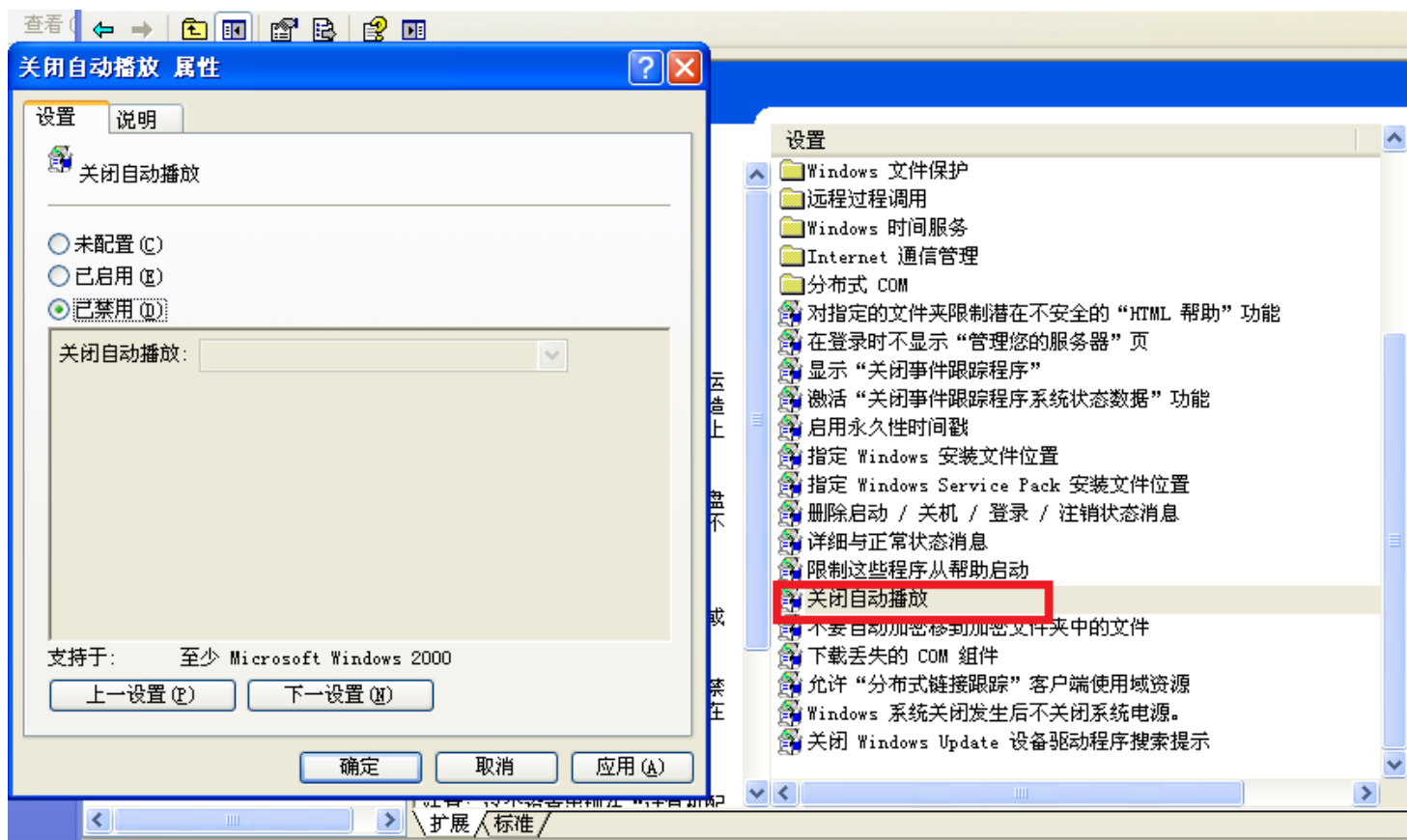
- 从注册表键关闭自动播放





实验三 Autorun 文件病毒的防范与删除

- 在组策略编辑器中关闭自动播放选项





实验三 Autorun文件病毒的防范与删除

- 使用DOS命令的批处理文件
 - 创建文件cleanAutorun.bat，在文件中添加指令
 - del /f /a:h x:\autorun.inf
 - 删除指定盘符的Autorun文件



实验三 Autorun 文件病毒的防范与删除

• Autorun 的手动删除

——一般来讲，Autorun 的文件都是有隐藏属性的，
修改显示隐藏文件，之后手动删除

