第3章 计算机病毒防治

3.1 实验基础

3.1.1 计算机病毒概述

计算机病毒是一种人为制造的，侵入计算机系统、寄生于应用程序或系统可执行部分，并可以自我复制、传播，具有激活性、攻击性的程序代码。病毒是计算机技术发展的必然产物。病毒大多不以文件形式存在，寄生在合法程序上，可以是引导程序、可执行程序、Word文档等。

病毒的发展速度非常迅速。1980年IBM PC成为主流，其自身和DOS的弱点给病毒攻击造成可乘之机。1987年，实战病毒Brain出现。1988年底，首例在我国国家统计部门发现小球病毒感染。1992年，多态型病毒出现。1995年，出现能够变换自身代码的变形病毒。据统计，1989年1月计算机病毒种类不过100种，1990年1月已超过150种，1990年12月超过260种，目前计算机病毒总数超过6万，并以每天超过200个的速度诞生。

病毒有多种分类方法。按照传染目标可以分为引导型、文件型、混合型。按照破坏性可以分为良性病毒和恶性病毒。

病毒具有如下特征：刻意编写人为破坏、主动传染性、自我复制、扩散传播、隐藏性、可激活性、不可预见性。

计算机病毒可以通过不可移动的计算机硬件设备、移动存储设备、计算机网络、点对点通信系统和无线通信系统等多种途径进行传播。

计算机病毒程序是为了特殊目的而编制的，它通过修改其他程序而把自己复制进去，并且传染该程序。一般来说，计算机病毒程序包括三个功能模块：引导模块、传染模块和破坏模块。这些模块功能独立，同时又相互关联，构成病毒程序的整体。

引导模块的功能是借助宿主程序，将病毒程序从外存引进内存，以便使传染模块和破坏模块进入活动状态。另外，引导模块还可以将分别存放的病毒程序链接在一起，重新进行装配，形成新的病毒程序，破坏计算机系统。传染模块的功能是将病毒迅速传染，尽可能扩大染毒范围。病毒的传染模块由两部分组成：条件判断部分和程序主体部分，前者负责判断传染条件是否成立，后者负责将病毒程序与宿主程序链接，完成传染病毒的工作。病毒编制

者的意图，就是攻击破坏计算机系统，所以破坏模块是病毒程序的核心部分。破坏模块在进行各种攻击之前，首先判断破坏条件是否成立，只有条件全部满足时，破坏模块才开始其破坏活动。

现代计算机病毒具有以下流行特征：

（1）攻击对象趋于混合型；

（2）同时感染系统引导区和可执行文件；

（3）采用反跟踪技术；

（4）增强隐蔽性；

（5）避开修改中断向量值，直接修改中断服务子程序；

（6）请求在内存中的合法身份，通过正常的内存申请进行合法驻留；

（7）维持宿主程序的外部特性，如控制文件显示属性或针对系统引导区的读操作提供正确内容给用户；

（8）不使用明显的感染标志，使被感染文件的标志复杂化，难以识别；

（9）病毒体繁衍不同变种。

目前杀毒软件中采用的技术主要有以下几种：

（1）病毒扫描程序：在文件和引导记录中搜索病毒的程序。只能检测出它已经知道的病毒。操作简单，耗时，适用于简单病毒。

（2）内存扫描程序：扫描内存以搜索内存驻留文件和引导记录中的病毒。发现后用一块未感染的软盘引导启动，病毒即被从内存清除。

（3）完整性检查程序：计算机在未感染状态，取得每个可执行文件和引导记录的信息指纹，存放于硬盘的数据库中，用于验证原来记录的完整性。缺点是对已经被病毒感染的系统再使用这种方法，可能遭到蒙骗，不能对新文件进行有效的检查。

（4）行为监视器：内存驻留程序，实时监测病毒和其他有恶意的损害活动并通知用户。可以防止新的、未知的病毒在计算机上传播。可能会影响一些活动与病毒相像的合法程序。不需要进行频繁的更新以保持有效。其缺点是无法监测出慢性病毒，因为这种病毒感染时不会主动调用系统服务。行为监视程序可以监测到的病毒种类有特定性。只有在病毒开始作用时，行为监视程序才能够监测病毒。

3.1.2　计算机病毒防治概述

防治计算机病毒应重在预防。一方面在思想上重视，管理上到位；另一方面依靠防杀计算机病毒软件。计算机病毒防治根本在于完善操作系统的安全机制。

单机用户进行病毒防范的简单有效的方法是选择一个功能完善的单机版计算机病毒软件，该软件应能满足：

- 拥有计算机病毒检测扫描器；
- 实时监控程序；
- 未知计算机病毒的检测；
- 压缩文件内部检测；
- 文件下载监视；

- 计算机病毒清除；
- 计算机病毒特征代码库升级；
- 重要数据备份；
- 定时扫描设定；
- 支持 FAT32 和 NTFS 等多种分区格式；
- 关机时检查软盘；
- 计算机病毒检测率较高。

个人用户还可以从以下方面进行病毒防护工作：

- 检查 BIOS 设置，将引导次序改为硬盘先启动；
- 安装较新的正式版本的防杀计算机病毒软件并经常升级；
- 经常更新计算机病毒特征代码库；
- 备份系统中重要的数据和文件；
- 在 Word 中，打开“提示保存 Normal 模板”，将 Normal. dot 文件的属性改为只读；
- 对外来的光盘、软盘和下载的软件都应该先进行查杀病毒再使用；
- 启用防杀病毒软件的实时监控功能。

3.2 实 验 项 目

3.2.1 宏病毒

1. 实验目的

理解宏病毒的概念、病毒机制、传播手段以及预防措施。

2. 实验原理

宏(Macro)是微软公司出品的 Office 软件包中所包含的一项特殊功能。微软公司设计此项功能的主要目的是给用户自动执行一些重复性的工作提供方便。它利用简单的语法，把常用的动作写成宏，用户工作时就可以直接利用事先编写好的宏自动运行，以完成某项特定的任务，而不必反复重复相同的工作。微软的 Word Visual Basic for Applications(VBA)是宏语言的标准。宏病毒正是利用 Word VBA 编写的一些宏，是一种寄存在文档或模板中的计算机病毒。一旦打开含有宏病毒的文档，其中的宏就会执行，宏病毒被激活，转移到计算机中并驻留在 Normal 模板上。以后所有自动保存的文档都会感染上这种宏病毒。

预防宏病毒有以下几种基本的方法。

(1) 防止执行自动宏：可以通过在 DOS 提示符下输入指令“WinWord. exe/m DisableAutoMacro”来防止打开 Word 文档时执行自动宏。另外，在打开或关闭文档时按下 Shift 键可以使文档不执行任何自动宏。

(2) 保护 Normal 模板：可以采取以下几种方法对 Normal 模板进行保护。提示保存 Normal 模板；设置 Normal 模板的只读属性；设置密码保护；设置安全级别；按照自己的习惯设置 Normal 模板并进行备份，当被病毒感染时，使用备份模板覆盖当前模板。

(3) 使用 DisableAutoMacro 功能。

3. 实验环境

运行 Windows 操作系统的主机,安装 Windows Office 软件和 Windows Visual Studio 或者 Windows Visual Studio. Net 编程环境。

4. 实验内容

(1) 手工创建一个 DOC 文档,在该文档的工程下增加一个宏病毒模块 VBS。

(2) 观察执行下述动作后,哪些 Word 中已经存在 VBS:

① 新建一个文档,随机输入若干字符,然后关闭。

② 打开一个已经存在的文档,编辑若干字符,然后关闭。

③ 把上述两个文档复制到一个移动存储设备上,然后到另一台主机上去打开它们,然后关闭。

(3) 按照宏病毒的预防方法配置主机,防范宏病毒攻击。

5. 实验步骤

(1) 打开菜单项“工具”|“宏”|“录制新宏”,为文档添加新宏,如图 3.1 所示。

(2) 打开菜单项“工具”|“宏”|“宏”,观察文档中包含的宏,如图 3.2 所示。

图 3.1　为文档添加新宏

图 3.2　查看文档中包含的宏

(3) 打开“工具”|“选项”|“安全性”,对它的属性进行安全设置,如图 3.3 和图 3.4 所示。

(4) 在 Normal. dot 中增加 AutoExec 自动宏,使用 DisableAutoMacro 宏:

```
Sub AutoExec()
WordBasic.DisableAutoMacros True
End Sub
```

6. 实验报告与要求

根据上面介绍的各项实验要求,详细观察记录宏病毒执行感染前后的变化,给出分析报告。

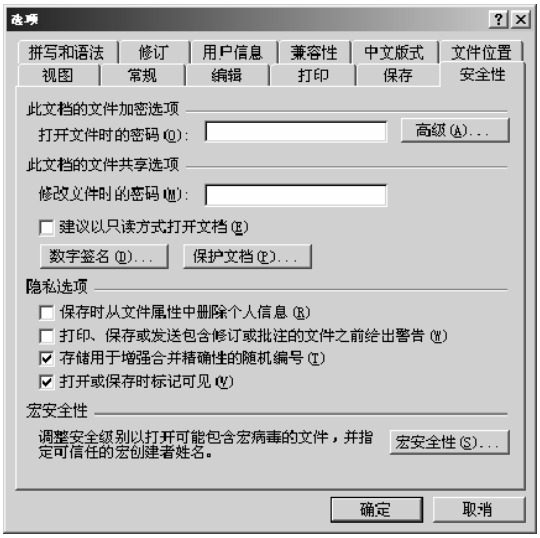

图 3.3 设置宏安全性

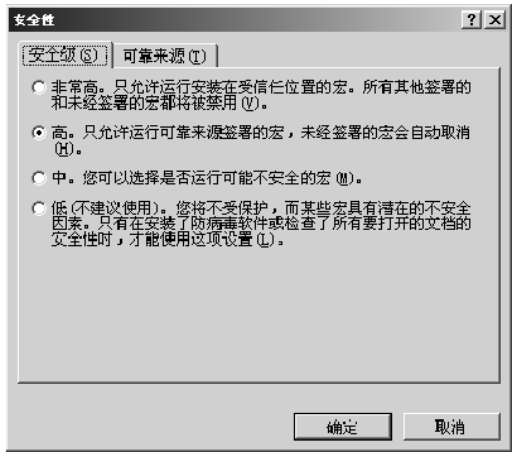

图 3.4 设置宏安全级别

7. 实验分析与讨论

脚本病毒的病毒原理、传播机制与宏病毒比较有何异同，如何进行防范。

8. 注意事项

禁止所有宏的执行可以从根本上防治宏病毒，但这是不现实的，因为用户有时需要使用自己编制的一些宏。禁止自动宏的执行，可以保证用户在安全启动 Word 文档后，进行必要的宏病毒检查，从而达到防治宏病毒的目的。

3.2.2 防病毒软件使用

1. 实验目的

了解防病毒软件基本工作原理，掌握防病毒软件配置和使用方法。

2. 实验原理

目前大多数防毒软件都提供了丰富的安全功能，不同的产品功能会有所不同。用户安装好防毒软件后，应了解其详细的使用方法，对其进行适当的设置，使之充分发挥作用，更好地满足个人的安全需求。

3. 实验环境

运行 Windows 操作系统的主机，安装 McAfee 的 VirusScan 反病毒软件。

4. 实验内容

（1）启用各监控模块；

（2）启用访问控制；

（3）更新病毒库并设置自动更新计划；

（4）对磁盘进行病毒扫描。

5. 实验步骤

（1）打开“VirusScan 控制台”对话框，对访问保护、缓冲区溢出保护、电子邮件扫描等功能进行启用，并打开各属性页进行设置，如图 3.5～图 3.10 所示。

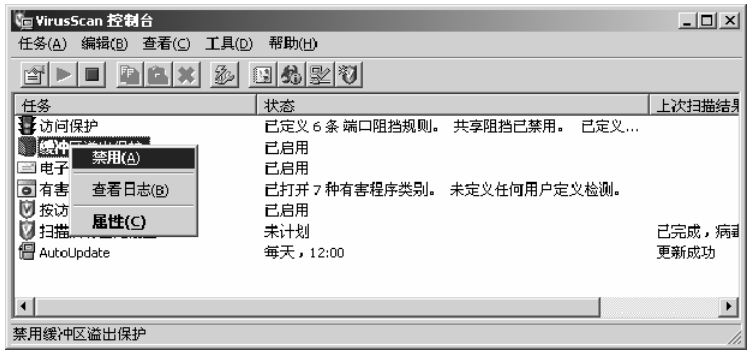

图 3.5　对防病毒软件各功能进行启用设置

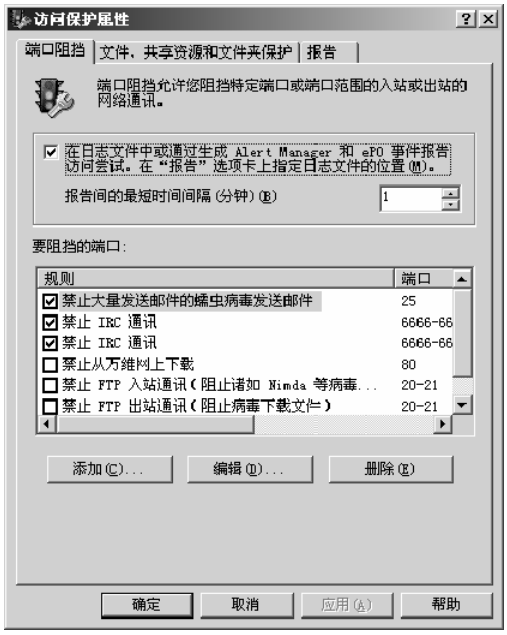

图 3.6　设置访问保护功能的端口阻挡属性

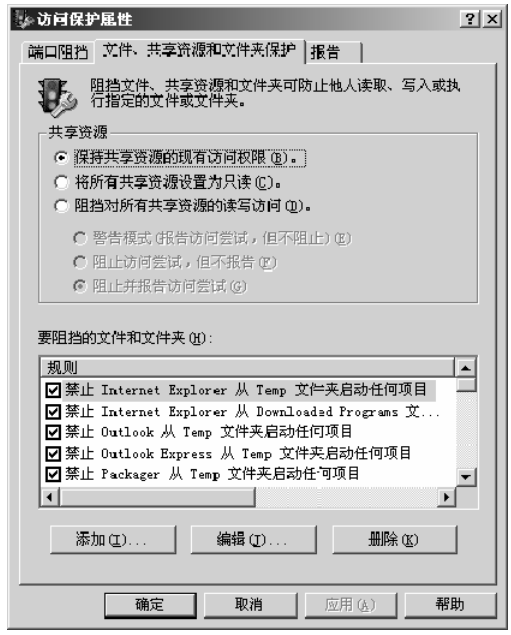

图 3.7　设置访问文件安全属性

图 3.8 设置访问日志保护属性

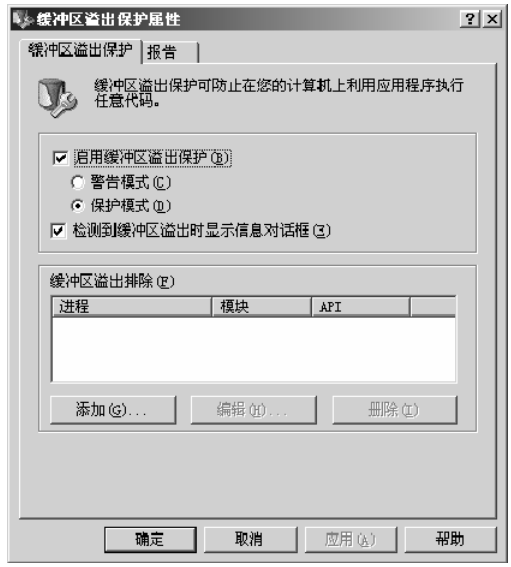

图 3.9 设置缓冲区溢出保护属性

(2)“按访问扫描”是一种实时保护模块,用户应将其开启。可以在控制台窗口选中该模块右键选择“开启”选项,或者右击桌面右下角 VirusScan 图标,进行设置,如图 3.11 和图 3.12 所示。

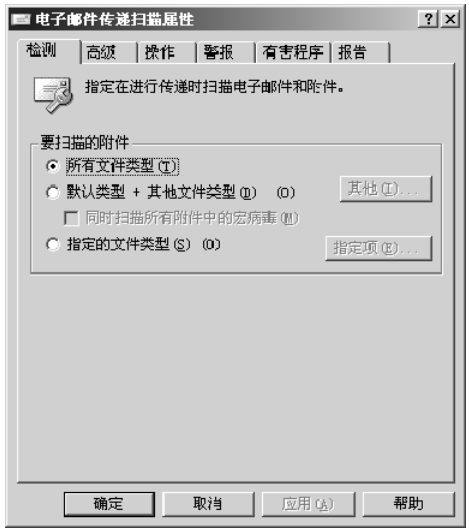

图 3.10 设置电子邮件扫描属性

图 3.11 设置按访问扫描属性

(3) 打开 AutoUpdate 属性窗口,单击“立即更新”按钮,对杀毒软件和病毒库同时进行在线更新,单击“计划”按钮,可以制订更新计划,如图 3.13～图 3.15 所示。

图 3.12　设置按访问扫描计划

图 3.13　设置自动更新功能

图 3.14　设置自动更新计划

(4) 在控制窗口中打开，或右击桌面右下角 VirusScan 图标，选择“按需扫描…”选项，进行打开设置，如图 3.16 和图 3.17 所示。

6. 实验报告与要求

根据上面介绍的各项实验要求，使用杀毒软件对机器进行病毒查杀，详细观察记录执行结果，评价该杀毒软件的优缺点，提交分析报告。

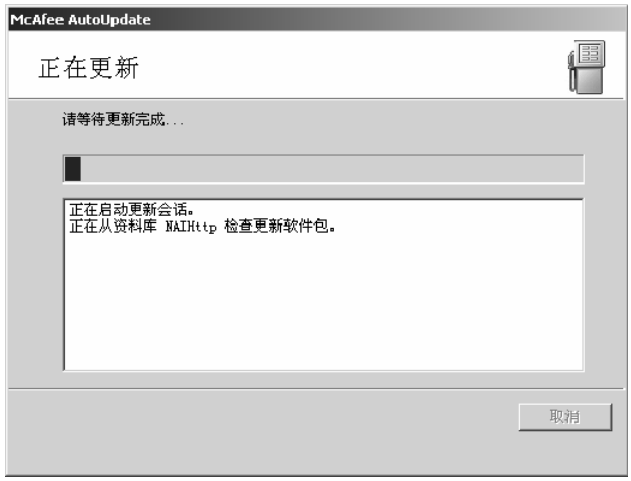

图 3.15　系统进行自动更新

图 3.16　启动按需扫描功能

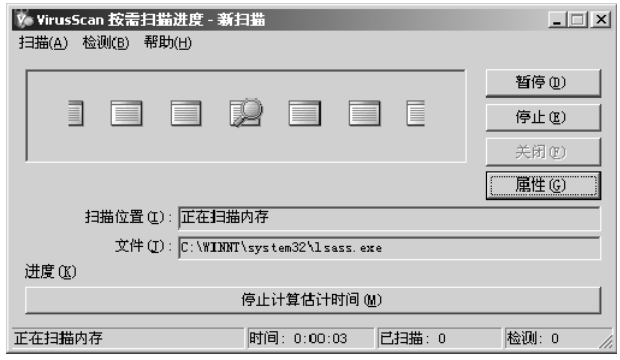

图 3.17　对系统进行扫描

7. 实验分析与讨论

作为个人用户，除了使用防病毒软件，还应该采取哪些措施来防范病毒。市场上国内外商品化防毒软件很多，各种产品分别具有哪些特点，应该如何根据用户需要进行选择。

8. 注意事项

不同类型的防毒软件操作界面和使用方法都有不同，但核心功能是基本一致的。用户在使用不同的防毒软件时，可以首先从本实验提出的几个方面进行基本设置，同时考虑自己的需求对辅助功能模块进行选用。