9.2 计算机病毒

9.2.1 病毒的定义与特点

1994年出台的《中华人民共和国计算机安全保护条例》对病毒的定义是：计算机病毒，是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据，影响计算机使用，并能自我复制的一组计算机指令或者程序代码。

目 录
上一页
下一页
结 束
返 回

9.2.1 病毒的定义与特点

计算机病毒具有如下特点：

1）可执行性

2）破坏性

3）传染性

4）潜伏性

5）针对性

6）衍生性

7）抗反病毒软件性

目 录
上一页
下一页
结 束

9.2.2 病毒的传播途径

（1）通过计算机网络进行传播。现代网络技术的巨大发展已使空间距离不再遥远，“相隔天涯，如在咫尺”，但也为计算机病毒的传播提供了新的“高速公路”。传统的计算机病毒可以随着正常文件通过网络进入一个又一个系统，而新型的病毒不需要通过宿主程序便可以独立存在而传播千里。毫无疑问，网络是目前病毒传播的首要途径，从网上下载文件、浏览网页、收看电子邮件等，都有可能会中毒。

（2）通过不可移动的计算机硬件设备进行传播，这些设备通常有计算机的专用ASIC芯片和硬盘等。这种病毒虽然极少，但破坏力却极强，目前没有较好的监测手段。

（3）通过移动存储设备来进行传播，这些设备包括优盘、移动硬盘等。光盘使用不当，也会成为计算机病毒传播和寄生的“温床”。

（4）通过点对点通信系统和无线通道传播。比QQ连发器病毒能通过QQ这种点对点的聊天程序进行传播。

目 录
上一页
下一页
结 束
返 回

9.2.3 病毒的类型

计算机病毒可分类方式很多，主要列举以下几种：

1．按照计算机病毒存在的媒体进行分类：病毒可以划分为网络病毒、文件病毒和引导型病毒。

2．按照计算机病毒传染的方法进行分类：可分为驻留型病毒和非驻留型病毒。

3．按照计算机病毒的破坏能力进行分类：可划分为无害型、无危险型、危险型、非常危险型。

4．按照计算机病毒特有的算法进行分类：可以划分为伴随型病毒、蠕虫型病毒、寄生型病毒、

目 录
上一页
下一页
结 束

9.2.4 几种常见的计算机病毒

1.蠕虫病毒

蠕虫病毒（**Worm**）是一类常见的计算机病毒，源自第一种在网络上传播的病毒。

病毒的前缀是**Worm**。这种病毒的公有特性是通过网络或者系统漏洞进行传播，很大部分的蠕虫病毒都有向外发送带毒邮件，阻塞网络的特性。如冲击波（阻塞网络）、小邮差（发带毒邮件）等。

蠕虫病毒的一般防治方法是：使用具有实时监控功能的杀毒软件，并及时更新病毒库，同时注意不要轻易打开不熟悉的邮件附件。

目 录
上一页
下一页
结 束
返 回

2. 木马病毒和黑客病毒

木马病毒因古希腊特洛伊战争中著名的“木马计”而得名，其前缀是**Trojan**，黑客病毒的前缀一般为**Hack**。木马病毒的公有特性是通过网络或者系统漏洞进入用户的系统并隐藏，然后向外界泄露用户的信息，而黑客病毒则有一个可视的界面，能对用户的电脑进行远程控制。木马、黑客病毒往往是成对出现的，即木马病毒负责侵入用户的电脑，而黑客病毒则会通过该木马病毒来进行控制。现在这两种类型都越来越趋向于整合了。

木马病毒的传播方式主要有两种：一种是通过**E-mail**，控制端将木马程序以附件的形式夹在邮件中发送出去，收信人只要打开附件系统就会感染木马；另一种是软件下载，一些非正规的网站以提供软件下载为名，将木马捆绑在软件安装程序上，下载后，只要一运行这些程序，木马就会自动安装。

对于木马病毒防范措施主要有：用户提高警惕，不下载和运行来历不明的程序，对于不明来历的邮件附件也不要随意打开。

目 录
上一页
下一页
结 束

3. “熊猫烧香”病毒

“熊猫烧香”其实是一种蠕虫病毒的变种，是蠕虫和木马的结合体，而且是经过多次变种而来的。由于中毒电脑的可执行文件会出现“熊猫烧香”图标，所以被称为“熊猫烧香”病毒。用户电脑中毒后可能会出现蓝屏、频繁重启以及系统硬盘中数据文件被破坏、浏览器会莫名其妙地开启或关闭等现象。同时，该病毒的某些变种可以通过局域网进行传播，进而感染局域网内所有计算机系统，最终导致企业局域网瘫痪，无法正常使用。

目 录
上一页
下一页
结 束

熊猫病毒

该病毒主要通过浏览恶意网站、网络共享、文件感染和移动存储设备（如优盘）等途径感染，其中网络共享和文件感染的风险系数较高，而通过Web和移动存储感染的风险相对较低。该病毒会自行启动安装，生成注册列表和病毒文件。

对于“熊猫烧香”病毒的防范措施有：加强基本的网络安全防范知识，培养良好的上网习惯；及时更新系统补丁；为系统管理账户设置复杂无规律的密码；关掉一些不需要却存在安全隐患（如139、445等）的端口；关闭非系统必须的“自动播放”功能等

目 录
上一页
下一页
结 束

4.“火焰”病毒

“火焰”病毒的全名是**Worm.Win32.Flame**，它是一种后门程序和木马病毒，同时还具有蠕虫病毒的特点。只要其操作者发出指令，它就能够在网络和移动设备中进行自我复制。电脑系统一旦被感染，病毒就可以发起一系列的行动，包括监测网络流量、获取截屏画面、记录音频对话和截获键盘输入等。被火焰病毒感染的系统中所有的数据都能通过链接传到病毒指定的服务器，这样操作者就可以掌握这些数据。

“火焰”的设计非常复杂，它能够逃避**100** 种防毒软件。感染该病毒的电脑会自动分析它自己的网络流量规律，自动录音，记录用户密码和键盘敲击的规律，将用户浏览网页、通讯通话、帐号密码以至键盘输入等记录及其他重要文件发送给远程操控病毒的服务器。

火焰病毒被认为是到目前为止规模最大的和最为复杂的网络攻击病毒，它被用作网络武器并已经攻击了多个国家，其复杂性和功能性已经超过其他任何已知的网络武器，尽管它早在**2010** 年**3** 月就开始活动，但直到卡巴斯基实验室发现之前，没有任何的安全软件将其检测到。

目 录
上一页
下一页
结 束

5.脚本病毒

脚本病毒的前缀是Script。脚本病毒的公有特性是使用脚本语言编写，通过网页进行的传播的病毒，如红色代码（Script.Redlof）。脚本病毒还会有前缀VBS、JS（表明是何种脚本编写的），如欢乐时光（VBS.Happytime）、十四日（Js.Fortnight.c.s）等。

目 录
上一页
下一页
结 束

6.宏病毒

宏病毒其实也是脚本病毒的一种，由于它的特殊性，因此单独算成一类。宏病毒的前缀是Macro，第二前缀是Word、Word97、Excel、Excel97其中之一。凡是只感染Word 97及以前版本Word文档的病毒采用Word97作为第二前缀，格式是Macro.Word97；凡是只感染Word 97以后版本Word文档的病毒采用Word作为第二前缀，格式是Macro.Word；凡是只感染Excel 97及以前版本Excel文档的病毒采用Excel97作为第二前缀，格式是Macro.Excel97；凡是只感染Excel 97以后版本Excel文档的病毒采用Excel作为第二前缀，格式是Macro.Excel；依此类推。该类病毒的公有特性是能感染Office系列文档，然后通过Office通用模板进行传播。

目 录
上一页
下一页
结 束

7.震网病毒

震网病毒又名Stuxnet 病毒，是一个席卷全球工业界的病毒，世界上首个网络“超级武器”，已经感染了全球超过45 000 个网络，伊朗遭到的攻击最为严重。震网病毒主要利用Windows 系统的漏洞，通过移动存储介质和局域网来进行传播，它利用了微软视窗操作系统之前未被发现的4 个漏洞。“震网”病毒不会通过窃取个人隐私信息来牟利，该病毒应该出自情报部门。因为它的打击对象是全球各地的重要目标，所以它被一些专家定性为全球首先投入实战舞台的“网络武器”。在对软件进行反编译后，计算机安全专家发现震网病毒的结构非常复杂，因此它应该是一个受国家资助的高级团队研发的。这种病毒可以破坏世界各国的化工、发电和电力传输企业所使用的核心生产控制电脑软件，并且代替该软件来控制工厂的其他电脑。

目 录
上一页
下一页
结 束

9.2.5 病毒的预防

预防计算机病毒，应该从管理和技术两方面进行。

1）从管理上预防病毒

计算机病毒的传染是通过一定途径来实现的，为此必须重视制定措施、法规，加强职业道德教育，不得传播更不能制造病毒。另外，还应采取一些有效方法来预防和抑制病毒的传染。

目 录
上一页
下一页
结 束

从管理上预防病毒

（1）谨慎地使用公用软件或硬件。

（2）任何新使用的软件或硬件（如磁盘）必须先检查。

（3）定期检测计算机上的磁盘和文件并及时消除病毒。

（4）对系统中的数据和文件要定期进行备份。

（5）对所有系统盘和文件等关键数据要进行写保护。

目 录
上一页
下一页
结 束

2）从技术上预防病毒

从技术上对病毒的预防有硬件保护和软件预防两种方法。

任何计算机病毒对系统的入侵都是利用RAM提供的自由空间及操作系统所提供的相应的中断功能来达到传染的目的，因此，可以通过增加硬件设备来保护系统，此硬件设备既能监视RAM中的常驻程序，又能阻止对外存储器的异常写操作，这样就能实现预防计算机病毒的目的。

目 录
上一页
下一页
结 束

2）从技术上预防病毒

软件预防方法是使用计算机病毒疫苗。计算机病毒疫苗是一种可执行程序，它能够监视系统的运行，当发现某些病毒入侵时可防止病毒入侵，当发现非法操作时及时警告用户或直接拒绝这种操作，使病毒无法传播。

目 录
上一页
下一页
结 束

9.2.6 病毒的清除

如果发现计算机感染了病毒，应立即清除。通常用人工处理或反病毒软件方式进行清除。

人工处理的方法有：用正常的文件覆盖被病毒感染的文件；删除被病毒感染的文件；重新格式化磁盘等。这种方法有一定的危险性，容易造成对文件的破坏。

目 录
上一页
下一页
结 束

用反病毒软件对病毒进行清除是一种较好的方法。常用的反病毒软件有瑞星、卡巴斯基、NOD32、NORTON、BitDefender等。特别需要注意的是，要及时对反病毒软件进行升级更新，才能保持软件的良好杀毒性能。