第 7 章　计算机病毒

本章简介：在介绍计算机病毒基本概念的基础之上，对计算机病毒的发展、计算机病毒的特性、计算机病毒的危害、计算机病毒的分类以及计算机病毒的传播进行了系统的讨论，使读者对计算机病毒有了一个较为全面的认识。

7.1　计算机病毒概述

计算机病毒只是一段可执行的程序代码，它们附着在各种类型的文件上，当文件从一个用户复制到另一个用户时，计算机病毒也就随之蔓延开来。计算机病毒的历史贯穿于计算机技术的发展，几乎每一个阶段都有一些代表性的病毒产生。而对每一个使用计算机的人来说，病毒都是一个无法回避的现实问题，正所谓“常在河边走，哪有不湿鞋！”，它常常给那些粗心的用户带来难以承受的损失。

7.1.1　计算机病毒的定义

关于什么是计算机病毒，我国 1994 年 2 月 18 日颁布实施的《中华人民共和国计算机信息系统安全保护条例》第二十八条中有明确的定义：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。

第一次真正的从学术上对计算机病毒进行描述的是美国计算机网络安全专家 Fred Cohen 博士。他认为：计算机病毒是一种能传染其它程序的程序，病毒常常是借助于其它应用程序，并把自身植入到其它程序中实现。这段话有以下几层含义。

1. 计算机病毒是一个程序。
2. 计算机病毒具有传染性，可以传染其他程序。
3. 计算机病毒的传染方式是修改其它程序，把自身植入到其它程序中而实现。

计算机病毒并不是自然界中发展起来的生命体，它们不过是某些人专门做出来的，具有一些特殊功能的程序或者程序代码片段。

病毒既然是计算机程序，它的运行就需要消耗计算机的 CPU 资源。当然，病毒并不一定具有破坏力，有些病毒可能只是恶作剧，例如计算机感染病毒后，只是显示一条有趣的消息或者一幅恶作剧的画面，但是大多数病毒的目的都是想方设法毁坏相关的程序或数据。

综上所述，可以从以下几个方面来理解计算机病毒的定义。首先，病毒是通过磁盘、磁带和网络等作为媒介传播扩散且能“传染”其他程序的程序。其次，病毒能够实现自身复制且借助一定的载体存在，具有潜伏性、传染性和破坏性。再者，计算机病毒是一种人为制造的程序，它不会自然产生，是精通编程的人精心编制的，通过不同的途径寄生在存储介质中，当某种条件成熟时，才会复制、传播，甚至变异后传播，使计算机的资源受到不同程度的破坏。

计算机病毒的定义在很多方面借用了生物学病毒的概念，因为它们有着诸多相似的特征，比如能够自我复制，能够快速“传染”，且都能够危害“病原体”，当然计算机病毒危害的“病原体”是正常工作的计算机系统程序或者互联网络。

近几年，随着计算机网络技术的飞速发展，计算机病毒逐渐融合了木马、网络蠕虫和网络攻击等新的技术，形成了以普通病毒、木马、网络蠕虫、移动代码和复合型病毒等形态存在的恶意代码，在政治、经济、军事等很多领域下都造成了很大的社会危害。

7.1.2 计算机病毒的发展

早在 1949 年，距离第一部商用计算机的出现还有好几年时，计算机的先驱者冯·诺依曼就在他的一篇论文《复杂自动机组织论》中，提出了计算机程序是能够在内存中进行自我复制的，即把病毒程序的蓝图勾勒出来。但当时，绝大部分计算机专家都无法想象这种会自我繁殖的程序是可能的，只有少数几个科学家默默地研究冯·诺依曼所提出的概念。十年之后，在美国电话电报公司（AT&T）的贝尔实验室中，三个年轻程序员道格拉斯·麦耀莱、维特·维索斯基和罗伯·莫里斯在工作之余想出一种电子游戏叫做“磁芯大战”。

1975 年，美国科普作家约翰·布鲁勒尔写了一本名为《震荡波骑士》的书，该书第一次描写了在现代信息社会中，计算机已成为正义和邪恶双方斗争的工具，成为当年全美最佳畅销书之一。

1977 年夏天，托马斯·捷·瑞安的科幻小说《P-1 的青春》成为美国的畅销书，轰动了科普界。作者幻想了世界上第一个计算机病毒，可以从一台计算机传染到另一台计算机，最终控制了 7000 台计算机，酿成了一场灾难，这实际上是计算机病毒的思想基础。

1983 年 11 月 3 日，弗雷德·科恩博士研制出一种在运行过程中可以复制自身的破坏性程序，伦·艾德勒曼将它命名为计算机病毒（Viruses），并在每周一次的计算机安全讨论会上正式提出，8 小时后专家们在 VAX11/750 计算机系统上运行，第一个病毒实验成功，一周后又获准进行 5 个实验的演示，从而在实验上验证了计算机病毒的存在。20 世界 80 年代起，IBM 公司的 PC 系列微机因为性能良好，价格便宜，逐步成为世界微型计算机市场上的主要机型。但是由于 IBM 的 PC 系列微型计算机自身的弱点，尤其是 DOS 操作系统的开放性，给计算机病毒的制造者提供了可乘之机。因此，装有 DOS 操作系统的微型计算机成为其攻击的主要对象。

1986 年初，在巴基斯坦的拉合尔，巴锡特和阿姆杰德两兄弟经营一家 IBM 的 PC 机及其兼容机的小商店。他们编写了 Pakistan 病毒，这是一种系统引导型病毒。该病毒在一年内流传到了世界各地，使人们认识到计算机病毒对 PC 机的影响。

1987 年 10 月，美国第一例计算机病毒（Brian）被发现。此后，病毒就迅速蔓延开来，世界各地的计算机用户几乎同时发现了形形色色的计算机病毒，如大麻、IBM 圣诞树、黑色星期五等。

1988 年 3 月 2 日，一种苹果机病毒发作。

1988 年 11 月 3 日，美国 6 千台计算机被病毒感染，造成 Internet 不能正常运行。这是一次非常典型计算机病毒入侵计算机网络的事件。迫使美国政府立即做出反应，国防部成立了计算机应急行动小组，更引起了世界范围的轰动。此病毒的作者为罗伯特·莫里斯，当年 23 岁，是在康乃尔大学攻读学位的研究生。

1989 年，全世界计算机病毒攻击十分猖狂，我国也未幸免。其中，“米开朗基罗”病毒给许多计算机用户造成极大损失。

1991 年，在“海湾战争”中，美军第一次将计算机病毒用于实战，在空袭伊拉克首都巴格达的战斗中，成功地破坏了对方的指挥系统，使之瘫痪，保证了战斗顺利进行，直到最后取得战斗的胜利。

1992 年，出现针对杀毒软件的“幽灵”病毒，如 One_Half。还出现了实现机理与以往的文件型病毒有明显区别的 DIR2 病毒。

1994 年 5 月，南非第一次多种族全民大选的计票工作，因计算机病毒的破坏停止 30 余小时，被迫推迟公布选举结果。

1996 年，出现针对微软公司 Office 的“宏病毒”。1997 年公认为计算机反病毒界的“宏病毒年”。

1998 年，全球首例破坏计算机硬件的 CIH 病毒出现，引起人们的恐慌。

1999 年 3 月 26 日，出现一种通过因特网进行传播的“美丽杀手”病毒。

1999 年 4 月 26 日，CIH 病毒在我国大规模爆发，造成巨大损失。

2000 年 5 月 4 日，一种被称为“我爱你”的爱虫病毒开始在全球各地迅速传播。该病毒起初仅是通过 Microsoft Outlook 电子邮件系统传播，邮件的主题为 I LOVE YOU，并且包含一个附件。一旦在 Microsoft Outlook 里打开这个邮件，系统就会自动复制并向地址簿中的所有邮件地址发送这个病毒。“我爱你”病毒属于一种蠕虫病毒，它与 1999 年的 Melissa 病毒非常相似。此后在网络上又接连出现 40 多种病毒变种，比如 SOUTHPARK、“母亲节”等，不仅使反病毒专家头痛不已，也使全球为此损失 100 亿美元。

2001 年完全可以被称为“蠕虫之年”。 出现的蠕虫病毒不仅数量众多，而且危害极大，感染了数百万计算机，其中典型的蠕虫包括 Nimda（尼姆达）、CodeRed（红色代码）、Badtrans（坏透了）等。

在 2002 年新生的计算机病毒中，木马、黑客病毒以 61%的绝对数量占据头名。网络病毒越来越成为病毒的主流。

2003 年的 1 月 25 日，仅在“SQL 杀手”病毒出现的当天，我国就有 80%的网络服务供应商先后遭受此蠕虫病毒的攻击，造成许多网络的暂时瘫痪。

2003 年的 8 月 12 日，名为“冲击波”的病毒在全球袭击 Windows 操作系统，据估计可能感染了全球一、两亿台计算机，在国内导致上千个局域网瘫痪。

2005 年由国内作者编写的“灰鸽子”木马成为当年头号病毒，它危害极大，变种极多（共有 4257 个变种），是国内非常罕见的恶性木马病毒。

2006 年 11 月至今，我国又连续出现“熊猫烧香”、“艾妮”等盗取网上用户密码帐号的病毒和木马，病毒的趋利性进一步增强。网上制作和贩卖病毒、木马的活动日益猖獗，利用病毒木马技术进行网络盗窃、诈骗的网络犯罪活动呈快速上升的趋势。

2010 年 6 月，“震网”病毒成为第一个专门定向攻击真实世界中基础能源设施的“蠕虫”病毒。该病毒能够干扰位于伊朗铀浓缩工厂中的离心机保护系统，通过提高离心机转速达到破坏离心机的效果，最终导致伊朗 Natanz 铀浓缩基地至少有 20%的离心机因感染该病毒而被迫关闭。

2012 年 5 月，俄罗斯安全专家发现了“火焰”病毒，全名为 Worm.Win32.Flame，它是一种后门程序和木马病毒，同时又具有蠕虫病毒的特点。只要控制者发出指令，它就能在网络和移动设备中进行自我复制。一旦计算机系统被感染，病毒将开始一系列复杂的行动，包括检测网络流量、获取截屏画面、记录音频对话和截获键盘输入等。被感染系统中所有的数据都能通过链接传到病毒指定的服务器。“火焰”病毒是迄今为止代码最多的病毒程序，其设计结构使其几乎无法被追查到。

“震网”病毒和“火焰”病毒的问世，表明计算机病毒已发展成为具备情报获取、基础设施摧毁等作战效果的网络攻击武器，这些病毒打击目标明确，结构设计复杂，隐蔽性极强，体现了计算机病毒新的发展趋势。

2017 年 5 月，一种名为“想哭”的勒索病毒席卷全球，在短短一周时间里，上百个国家和地区受到影响。据美国有线新闻网报道，截至 2017 年 5 月 15 日，大约有 150 个国家受到影响，至少 30 万台电脑被病毒感染。

7.1.3 计算机病毒的特性

要防范计算机病毒，首先需要了解计算机病毒的特征和破坏机理，为防范和清除计算机病毒提供充实、可靠的依据。根据计算机病毒的产生、传染和破坏行为的分析，计算机病毒一般具有以下特性：非授权可执行性、隐蔽性、传染性、潜伏性、破坏性和可触发性。

1. 非授权可执行性

用户通过调用执行一个程序时，把系统控制交给这个程序，并分配给它相应的系统资源，如内存，从而使之能够运行完成用户的需求。因此程序执行的过程对用户是透明的。而计算机病毒是非法程序，正常用户是不会明知是病毒程序而故意调用执行。但计算机病毒具有正常程序的一切特性：可存储性和可执行性。它隐藏在合法的程序或数据中，当用户运行正常程序时，病毒伺机窃取到系统的控制权，得以抢先运行，然而此时用户还认为在执行正常的程序。

2. 隐蔽性

计算机病毒是一种具有很高的编程技巧、短小精悍的可执行程序。它通过粘附在正常程序或磁盘引导扇区中，或者磁盘上标为坏簇的扇区中，以及一些空闲概率较大的扇区中，也有个别的以隐含文件的形式出现，这是它的非法可存储性。病毒想法设法地隐藏自身，就是为了防止被用户察觉。

3. 传染性

传染性是计算机病毒最重要的特征，是判断一段程序代码是否为计算机病毒的依据。病毒程序一旦侵入计算机系统，就开始搜索可以传染的程序或者磁介质，然后通过自我复制迅速传播。只要一台计算机染毒，如不及时处理，那么病毒会在这台计算机上迅速扩散，其中的大量文件（一般是可执行文件）会被感染。由于目前计算机网络日益发达，计算机病毒可以在极短的时间内通过像 Internet 这样的网络传遍世界。

4. 潜伏性

计算机病毒具有依附于其他媒体而寄生的能力，这种媒体称为计算机病毒的宿主。依靠病毒的寄生能力，病毒传染给合法的程序和系统后，一般不会马上发作，而是悄悄隐藏起来，然后在用户不察觉的情况下进行传染。这样，病毒的潜伏性越好，它在系统中存在的时间也就越长，病毒传染的范围也越广，其危害性也越大。

5. 表现性或破坏性

无论何种病毒程序，一旦侵入系统都会对操作系统的运行造成不同程度的影响。即使是不直接产生破坏作用的病毒程序，也要占用系统资源（如占用内存空间、占用磁盘存储空间及系统运行时间等）。而绝大多数病毒程序要显示一些文字或图像，影响系统的正常运行，还有一些病毒程序删除文件，加密磁盘中的数据，甚至摧毁整个系统和数据，使之无法恢复，造成无可挽回的损失。因此，病毒程序的副作用轻则降低系统工作效率，重则导致系统崩溃、数据丢失。病毒程序的表现性或破坏性体现了病毒设计者的真正意图。

6. 可触发性

计算机病毒一般都有一个或者几个触发条件。满足其触发条件或者激活病毒的传染机制，使之进行传染，或者激活病毒的表现部分或破坏部分。触发的实质是一种条件的控制，病毒程序可以依据设计者的要求，在一定条件下实施攻击。这个条件可以是输入特定字符，使用特定文件、某个特定日期或特定时刻，或者是病毒内置的计数器达到一定次数等。

7.1.4 计算机病毒的危害

在计算机病毒出现的初期，提到计算机病毒的危害，往往注重于病毒对信息系统的直接破坏作用，例如格式化硬盘、删除文件数据等，并以此来区分恶性病毒和良性病毒。其实这些只是病毒劣迹的一部分。随着计算机应用的进一步发展，人们深刻地认识到凡是病毒都可能对计算机信息系统造成严重的破坏。

计算机病毒的主要危害有以下几个方面。

1. 直接破坏计算机数据信息

大部分病毒在激发时直接破坏计算机的重要信息数据，所利用的手段有格式化磁盘、改写文件分配表和目录区、删除重要文件或者用无意义的“垃圾”数据、改写文件，以及破坏

CMOS 设置等。

“磁盘杀手”病毒（DISK KILLER）内含计数器，在硬盘染毒后累计开机时间 48 小时内激发，激发的时候屏幕上显示 Warning!! Don’t turn off power or remove diskette while Disk Killer is Processing!（警告! Disk Killer 正在工作，不要关闭电源或取出磁盘），并改写硬盘数据。

2. 占用磁盘空间和对信息的破坏

寄生在磁盘上的病毒总要非法占用一部分磁盘空间。

引导型病毒的一般侵占方式是由病毒本身占据磁盘引导扇区，而把原来的引导区转移到其他扇区，也就是引导型病毒要覆盖一个磁盘扇区。被覆盖的扇区数据永久性丢失，无法恢复。

一些操作系统功能能够检测出磁盘的未用空间，文件型病毒就利用这些功能进行传染，把传染部分写到磁盘的未用部位去。所以在传染过程中一般不破坏磁盘上的原有数据，但非法侵占了磁盘空间。一些文件型病毒传染速度很快，在短时间内感染大量文件，每个文件都不同程度地加长了，就造成磁盘空间的严重浪费。

3. 抢占系统资源

除 VIENNA、CASPER 等少数病毒外，其他大多数病毒在活动时都是常驻内存的，这就必然抢占一部分系统资源。病毒所占用的基本内存长度大致与病毒本身的长度相当。病毒抢占内存，导致可用内存减少，一部分软件不能运行。除占用内存外，病毒还抢占中断，干扰系统的运行。计算机操作系统的许多功能是通过中断调用技术来实现的。病毒为了传染激发，总是修改一些有关的中断地址，在正常中断过程中加入病毒的“私货”，从而干扰系统的正常运行。

4. 影响计算机运行速度

病毒进驻内存后不但干扰系统运行，还影响计算机速度，主要表现在以下几点。

（1）病毒为了判断传染激发条件，总要对计算机的工作状态进行监视，这相对于计算机的正常运行状态既多余又有害。

（2）有些病毒为了保护自己，不但对磁盘上的静态病毒加密，而且进驻内存后的动态病毒也处在加密状态，CPU 每次寻址到病毒处时，都要运行一段解密程序把加密的病毒解密成合法的 CPU 指令再执行；而病毒运行结束时，再用一段程序对病毒重新进行加密。这样 CPU 额外执行数千条以至上万条指令。

（3）病毒在进行传染时，同样要插入非法的额外操作，特别是传染外部存储介质时，不但计算机速度明显变慢，而且正常的读写顺序被打乱。

5. 计算机病毒错误与不可预见的危害

计算机病毒与其他计算机软件的一大差别是病毒的无责任性。编制一个完善的计算机软件，需要耗费大量的人力和物力，经过长时间调试完善，软件才能推出。但在病毒编制者看来既没有必要这样做，也不可能这样做。很多计算机病毒都是个别人在一台计算机上匆匆编制调试后就向外抛出。反病毒专家在分析大量病毒后发现绝大部分病毒都存在不同程度的错误。

错误病毒的另一个主要来源是变种病毒。有些计算机初学者尚不具备独立编制软件的能力，出于好奇或其他原因修改别人的病毒，造成错误。

计算机病毒错误所产生的后果往往是不可预见的，反病毒工作者曾经详细指出“黑色星期五”病毒存在 9 处错误、“乒乓病毒”有 5 处错误等。但是人们不可能花费大量时间去分析数万种病毒的错误所在。大量含有未知错误的病毒扩散传播，其后果是难以预料的。

6. 计算机病毒的兼容性对系统运行的影响

兼容性是计算机软件的一项重要指标，兼容性好的软件可以在各种计算机环境下运行，

反之兼容性差的软件则对运行条件“挑肥拣瘦”，要求机型和操作系统版本等。病毒的编制者一般不会在各种计算机环境下对病毒进行测试，因此病毒的兼容性较差，常常导致死机。

7. 攻击移动智能终端系统

由于移动终端设备承载的功能日益增多和处理信息的敏感性增强，病毒对移动终端设备的危害也呈现出多样性和高威胁性，如恶意扣费、隐私窃取（聊天记录、各种支付密码等）、远程控制和诱骗欺诈等，能给用户造成经济损失等多方面危害。

8. 摧毁工业控制系统和工业基础设施

由于工业控制系统具有数据采集、设备控制和参数调节等功能，因此通过病毒攻击工业控制系统可以造成除了上述危害以外的一些攻击效果，例如，扰乱上位机监控、拒绝服务攻击控制设备，以及程序块删除与下载等，从而直接或间接对工业控制系统和工业基础设施进行损伤或摧毁。

9. 给用户造成严重的心理压力

据有关计算机销售部门统计，计算机售后用户怀疑“计算机有病毒”而提出咨询约占售后服务工作量的 60%以上。经检测确实存在病毒的约占 70%，另有 30%的情况只是用户怀疑，而实际上计算机并没有病毒。大多数用户对病毒采取宁可信其有的态度，这对于保护计算机安全无疑是十分必要的，然而往往要付出时间、金钱等方面的代价。仅仅怀疑病毒而贸然重装系统或格式化硬盘所带来的损失更是难以弥补。不仅是个人用户，在一些大型网络系统中也难免为甄别病毒而停机。总之，计算机病毒像“幽灵”一样笼罩在广大计算机用户心头，给人们造成巨大的心理压力，极大地影响了现代计算机的使用效率，由此带来的无形损失是难以估量的。

7.1.5 计算机病毒的分类

按照计算机病毒的特点及特性，计算机病毒的分类方法有许多种。因此，同一种病毒可能有多种不同的分法。

1. 按照病毒攻击的系统分类

（1）攻击 DOS 系统的病毒。这类病毒出现最早、最多，变种也最多，20 世纪出现的计算机病毒基本上都是这类病毒。

（2）攻击 Windows 系统的病毒。由于 Windows 的图形用户界面（GUI）和多任务操作系统深受用户的欢迎，Windows 已成为病毒攻击的主要对象。1998 年，出现的 CIH 病毒就是一个 Windows95\98 病毒。

（3）攻击 UNIX 系统的病毒。当前，UNIX 系统应用非常广泛，并且许多大型计算机系统均采用 UNIX 作为其主要的操作系统，所以 UNIX 病毒的出现对人类的信息处理也是一个严重的威胁。

（4）攻击移动终端系统的病毒。常见的移动终端系统有 IOS、Android 和 Symbian 等，针对每种系统现在都有多种病毒，隐私窃取和远程控制是其主要攻击目的。

（5）攻击工业控制系统的病毒。SCADA、PLC 等都是工业控制系统中常见的可攻击对象，这些担负着数据采集、设备控制等功能的系统一旦被攻击，可能会对工业设备造成严重损伤。

2. 按照病毒攻击的计算机类型分类

（1）攻击微型计算机的病毒。这是世界上传染最为广泛的一种病毒。

（2）攻击小型机的计算机病毒。小型机的应用范围是极为广泛的，它既可作为网络的一个结点机，也可以作为小的计算机网络的主机。起初，人们认为计算机病毒只有在微型计算机上才能发生而小型机则不会受到病毒的侵扰，但自 1988 年 11 月份 Internet 网络受到蠕虫（Worm）程序的攻击后，使得人们认识到小型机也同样不能免遭计算机病毒的攻击。

（3）攻击工作站的计算机病毒。近几年，计算机工作站有了较大的进展，并且应用范围也有了较大的拓展，所以不难想象，攻击计算机工作站的病毒的出现也是对信息系统的一大威胁。

（4）攻击移动终端设备的病毒。随着移动终端设备的普及，目前其数量已经达到数十亿，如此庞大的数量一旦被攻击将会造成巨大的损失。

（5）攻击工业设备的病毒。“震网”病毒的出现，使通过计算机病毒攻击工业设备成为现实，而工业设备对安全性考虑不足这一普遍现象给此类病毒提供了较大生产空间。

3. 按照病毒的链结方式分类

由于计算机病毒本身必须有一个攻击对象以实现对计算机系统的攻击，计算机病毒所攻击的对象是计算机系统可执行的部分。

（1）源码型病毒

该病毒攻击高级语言编写的程序，该病毒在高级语言所编写的程序编译前插入到源程序中，经编译成为合法程序的一部分。

（2）嵌入型病毒

这种病毒是将自身嵌入到现有程序中，把计算机病毒的主体程序与其攻击的对象以插入的方式链接。这种计算机病毒是难以编写的，一旦侵入程序体后也较难消除。如果同时采用多态性病毒技术、超级病毒技术和隐蔽性病毒技术，将给当前的反病毒技术带来严峻的挑战。

（3）外壳型病毒

外壳型病毒将其自身包围在主程序的四周，对原来的程序不做修改。这种病毒最为常见，既易于编写，也易于发现，一般测试文件的大小即可得知。

（4）操作系统型病毒

这种病毒试图把它自己的程序加入或取代部分操作系统进行工作，具有很强的破坏力，可以导致整个系统的瘫痪。圆点病毒和大麻病毒就是典型的操作系统型病毒。

这种病毒在运行时用自己的逻辑部分取代操作系统的合法程序模块，根据病毒自身的特点和被替代的操作系统中合法程序模块在操作系统中运行的地位与作用，以及病毒取代操作系统的取代方式等，对操作系统进行破坏。

4. 按照病毒的破坏情况分类

按照计算机病毒的破坏情况可分为良性和恶性两类。

（1）良性计算机病毒

良性计算机病毒是指其不包含立即对计算机系统产生直接破坏作用的代码。这类病毒为了表现其存在，只是不停地进行扩散，从一台计算机传染到另一台，并不破坏计算机内的数据。这种病毒多数是恶作剧者的产物，他们的目的不是为了破坏系统和数据，而是为了让使用染有病毒的计算机用户通过显示器或扬声器看到或听到病毒设计者的编程技术。这类病毒有小球病毒、1575/1591 病毒、救护车病毒、扬基病毒和 Dabi 病毒等。还有一些人利用病毒的这些特点宣传自己的政治观点和主张。也有一些病毒设计者在其编制的病毒发作时进行人身攻击。

有些人对这类计算机病毒的传染不以为然，认为这只是恶作剧，没什么关系。其实良性和恶性都是相对而言的。良性病毒取得系统控制权后，会导致整个系统和应用程序争抢 CPU 的控制权，可能会导致整个系统死锁，给正常操作带来麻烦。有时系统内还会出现几种病毒交叉感染的现象，一个文件不停地反复被几种病毒所感染。因此也不能轻视良性病毒对计算机系统造成的损害。

（2）恶性计算机病毒

恶性计算机病毒是指在其代码中包含损伤和破坏计算机系统的操作，在其传染或发作时会对系统产生直接的破坏作用。这类病毒有很多，如黑色星期五病毒、火炬病毒和米开朗基

罗病毒等。当米氏病毒发作时，硬盘的前 17 个扇区将被彻底破坏，使整个硬盘上的数据无法被恢复，造成的损失是无法挽回的。有的病毒还会对硬盘做格式化等破坏性操作。因此这类恶性病毒是很危险的，应当注意防范。防病毒系统可以通过监控系统内的这类异常动作识别出计算机病毒的存在与否，或至少发出警报提醒用户注意。

5. 按照病毒的寄生方式分类

传染性是计算机病毒的本质属性，根据寄生部位或传染对象分类即根据计算机病毒的寄生方式进行分类，有以下几种。

（1）引导型病毒

引导型病毒是指寄生在磁盘引导区或主引导区的计算机病毒。这种病毒主要是用病毒的全部或部分逻辑取代正常的引导记录，而将正常的引导记录隐藏在磁盘的其它地方。这种病毒利用系统引导时不对主引导区的内容正确与否进行判别的缺点，在引导型系统的过程中侵入系统，驻留内存，监视系统运行，伺机传染和破坏。按照引导型病毒在硬盘上的寄生位置又可细分为主引导记录病毒和分区导记录病毒。主引导记录病毒感染硬盘主引导区，如大麻病毒、2708 病毒和火炬病毒等；分区引导记录病毒感染硬盘的活动分区引导记录，如小球病毒、Girl 病毒等。

（2）文件型病毒

文件型病毒是指能够寄生在文件中的计算机病毒。这类病毒程序感染可执行文件或数据文件。寄生在可执行程序中的病毒，一旦程序被执行，病毒也就被激活，病毒程序首先被执行，并将自身驻留内存，然后设置触发条件进行传染。如果这些可执行程序是操作系统的一部分，只要计算机开始工作，病毒就处在随时被触发的状态。文件型病毒感.com 和.exe 等可执行文件，如 1575/1591 病毒、848 病毒等，以及 Macro/Concept、Macro/Atoms 等宏病毒感染 DOC 文件。

（3）复合型病毒

复合型病毒是指具有引导型病毒和文件型病毒寄生方式的计算机病毒。这种病毒扩大了病毒扩大了病毒程序的传染途径，它既感染磁盘的引导记录，又感染可执行文件。当染有此种病毒的磁盘用于引导系统或调用执行染毒文件时，病毒都会被激活。因此在检测和清除复合型病毒时，必须全面、彻底地根治，如果只发现该病毒的一个特性， 把它只当作引导型或文件型病毒进行清除。虽然好像是清除了，但还留有隐患，这种经过消毒后的“洁净”系统更具有攻击性。病毒有 Flip 病毒、新世纪病毒和 One-half 病毒等。

6. 按照病毒的传播媒介分类

按照计算机病毒的传播媒介来分类，可分为单机病毒和网络病毒。

（1）单机病毒

单机病毒的载体是磁盘，常见的是病毒从 U 盘或光盘传入硬盘，感染系统，然后再传染其它 U 盘，U 盘又传染其它系统。

（2）网络病毒

网络病毒的传播媒介不再是移动式载体，而是网络通道，这种病毒的传染能力更强，破坏力更大，危害程度更高。

7.1.6 计算机病毒的传播

传播性是计算机病毒具有的巨大威胁和隐患的特点之一。计算机病毒潜伏在系统内，用户在豪不知情的情况下进行相应的操作激活触发条件，使其得以由一个载体传播至另一个载体，完成传播过程。随着计算机的广泛普及应用及互联网的飞速发展，计算机病毒的传播也从传统的常用交换媒介传播逐渐发展到通过互联网进行全球化的传播。

1. 移动式存储介质

计算机和手机等数码产品常用的移动存储介质主要包括软盘、光盘、DVD、硬盘、闪存、U 盘、CF 卡、SD 卡、记忆棒和移动硬盘等。移动存储介质以其便携性和大容量存储性为病毒的传播带来了极大的便利，这也是其成为目前主流病毒传播途径的重要原因。例如，“U 盘杀手”病毒，该病毒是一个利用 U 盘等移动设备进行传播的蠕虫病毒。Autorun.inf 文件一般存在于 U 盘、MP3、移动硬盘和硬盘各个分区的根目录下，当用户双击 U 盘等设备时，该文件就会利用 windows 自动播放功能优先运行 Autorun.inf 文件,并立即执行所要加载的病毒程序，导致破坏用户机器且遭受损失。

2．各种网络传播

（1）电子邮件

电子邮件是病毒通过互联网进行传播的主要媒介。病毒主要依附在邮件的附件中，而电子邮件本身并不产生病毒。当用户下载附件时，计算机就会感染病毒，使其入侵至系统中，伺机发作。由于电子邮件一对一、一对多的这种特性，使其在被广泛应用的同时，也为计算机病毒的传播提供了一个良好的渠道。

（2）下载文件

病毒被捆绑或隐藏在互联网上共享的程序或文档中，用户一旦下载了该类程序或文件而不进行病毒查杀，感染计算机病毒的几率将大大增加。病毒可以伪装成其他程序或隐藏在不同类型的文件中，通过下载操作来感染计算机。

（3）浏览网页

当用户浏览不明网站或误入携带木马网站后，在访问的同时，病毒便会在系统中安装病毒程序，使计算机不定期地自动访问该网站，或窃取用户的隐私信息，给用户造成损失。

（4）聊天通信工具

Q Q、MSN、微信和 Skype 等即时通信聊天工具，无疑是当前人们进行信息通信与数据交换的重要手段之一，成为网上生活必备软件。由于通信工具本身安全性的缺陷，加之聊天工具中的联系人列表信息量丰富，给病毒的大范围传播提供了极为便利的客观条件。目前，仅通过 Q Q 这一种通信聊天工具进行传播的病毒就达上百种。

（5）移动通信终端

通过移动通信终端进行病毒传播也是当前病毒发作的一种流行趋势，手机作为最典型的移动通信终端，以其高普及率及低安全防御能力成为当前一种新型病毒传播途径。具有传染性和破坏性的病毒，会利用发送的手机短信、彩信、无线网络下载歌曲、图片或文件等方式传播，由于手机用户往往在不经意的情况下接收读取短信、彩信或直接单击网址链接等方式获取信息，让病毒毫不费力地入侵手机进行破坏，甚至使之无法正常使用。

7.2　计算机病毒的检测与清除

7.2.1　计算机病毒的检测原理

根据计算机病毒的特点，要想彻底检查出计算机是否感染病毒，必须利用多种方法进行检测，主要有根据异常现象判断和利用专业查毒软件检测两种。

1. 根据异常现象初步检测

虽然不能准确判断系统感染了何种病毒，但是，可通过异常现象来判断病毒的存在。根据异常现象进行初步检测是计算机病毒清除防范十分重要的环节。计算机出现的异常现象主要包括以下几个方面。

（1）计算机运行异常：包括无法开机、开机速度变慢、系统运行速度慢、频繁重启、无故死机和自动关机等。

（2）屏幕显示异常：包括计算机蓝屏、弹出异常对话框和产生特定的图像（如小球计算机病毒）等。

（3）声音播放异常：出现非系统正常声音，如“杨基”(Yangkee)计算机病毒和中国的“浏阳河”计算机病毒。

（4）文件/系统异常：无法找到硬盘分区、文件名称等相关属性遭受更改、硬盘存储空间意外变小、无法打开/读取/操作文件、数据丢失或损坏，以及 CPU 利用率或内存占用率过高的现象。

（5）外设异常：鼠标、打印机等外部设备出现异常，无法正常使用等。

（6）网络异常：联网状态下不能正常上网、杀毒软件无法正常升级、自动弹出网页、主页被篡改、自动发送电子邮件，以及其他异常现象等。

当出现以上异常现象时，则可以初步判断计算机极有可能已经感染了病毒，需要利用专业检测工具进一步检查病毒的存在并杀毒。

2. 利用专业工具检测查毒

由于病毒具有较强的隐蔽性，所以必须使用专业工具对系统进行查毒，主要是针对包括特定的内存、文件、引导区和网络在内的一系列属性，能够准确地报出病毒名称。常见的杀毒软件基本都含有查毒功能，如瑞星免费在线查毒、360 查毒、金山毒霸查毒和卡巴斯基查毒等。

当前，查毒软件使用的最主要的病毒查杀方式为病毒标记法。此种方式首先对新病毒加以分析，编成病毒码，加入资料库中，然后通过检测文件、扇区和内存，利用标记，也就是病毒常用代码的特征，查找已知病毒与病毒资料库中的数据进行对比分析，即可判断是否中毒。其既可在系统运行时检测出计算机病毒，又能在计算机病毒出现时立刻发现。

3. 检测的主要依据

（1）检查磁盘主引导扇区

硬盘的主引导扇区、分区表，以及文件分配表、文件目录区是病毒攻击的主要目标。

引导病毒主要攻击磁盘上的引导扇区。硬盘存放主引导记录的主引导扇区般位于 0 柱面 0 磁道 1 扇区。该扇区的前 3 个字节是跳转指令（DOS 下），接下来的 8 个字节是厂商、版本信息，再向下的 18 个字节均是 BIOS 参数，记录有磁盘空间、FAT 表和文件目录的相对位置等，其余字节是引导程序代码。病毒侵犯引导扇区的重点是前面的几十个字节。

当发现系统有异常现象时，特别是当发现与系统引导信息有关的异常现象时，可通过检查主引导扇区的内容来诊断故障。方法是采用工具软件，将当前主引导扇区的内容与干净的备份相比较，如发现有异常，则很可能是感染了病毒。

（2）检查 FAT 表

病毒隐藏在磁盘上，一般要对存放的位置做出“坏簇”信息标志反映在 FAT 表中。因此，可通过检查 FAT 表，看有无意外坏簇，来判断是否感染了病毒。

（3）检查中断向量

计算机病毒平时隐藏在磁盘上，在系统启动后，随系统或随调用的可执行文件进入内存并驻留下来，一旦时机成熟，它就开始发起攻击。病毒隐藏和激活一般是采用中断的方法，即修改中断向量，使系统在适当时转向执行病毒代码。病毒代码执行完后，再转回到原中断处理程序执行。因此，可通过检查中断向量有无变化来确定是否感染了病毒。

检查中断向量的变化主要是查看系统的中断向量表，其备份文件一般为 INT.DAT。病毒最常攻击的中断有：磁盘输入/输出中断（13H），绝对读、写中断（25H、26H），以及时钟中断（08H）等。

（4）检查可执行文件

检查.com 或.exe 可执行文件的内容、长度和属性等，可判断是否感染了病毒。检查可

执行文件的重点是在这些程序的头部即前面的 20 个字节左右。因为病毒主要改变文件的起始部分。对于前附式.com 文件型病毒，主要感染文件的起始部分，一开始就是病毒代码。对于后附式.com 文件型病毒，虽然病毒代码在文件后部，但文件开始必有条跳转指令，以使程序跳转到后部的病毒代码。对于.exe 文件型病毒，文件头部的程序入口指针一定会被改变。因此，对可执行文件的检查主要是看这些可疑文件的头部。

（5）检查内存空间

计算机病毒在传染或执行时，必然要占据一定的内存空间，并驻留在内存中，等待时机再进行传染或攻击。病毒占用的内存空间一般是用户不能覆盖的。因此，可通过检查内存的大小和内存中的数据来判断是否有病毒。

通常采用些简单的工具软件，如 PCTOOLS、DEBUG 等进行检查。病毒驻留到内存后，为防止 DOS 系统将其覆盖，一般都要修改系统数据区记录的系统内存数或内存控制块中的数据。如检查出来的内存可用空间为 635KB, 而计算机真正配置的内存空间为 640KB，则说明有 5KB 内存空间被病毒侵占。

虽然内存空间很大，但有些重要数据存放在固定的地点，可首先检查这些地方，如 DOS 系统启动后，BIOS、变量和设备驱动程序等是放在内存中的固定区域内（0：4000H~0:4FF0H）。根据出现的故障，可检查对应的内存区以发现病毒的踪迹。如打印、通信和绘图等出的故障，很可能在检查相应的驱动程序时能发现问题。

（6）检查特征串

一些经常出现的病毒都具有明显的特征，即有特殊的字符串。根据它们的特征，可通过工具软件检查和搜索，以确定病毒的存在和种类。例如，磁盘杀手病毒程序中就有 ASCII 码 disk killer，这就是该病毒的特征字符串。杀毒软件一般都收集了各种已知病毒的特征字符串，并构造出病毒特征数据库，这样，在检查和搜索可疑文件时，就可用特征数据库中的病毒特征字符串逐一比较，确定被检测文件感染了何种病毒。

这种方法不仅可检查文件是否感染了病毒，并且可确定感染病毒的种类，从而能有效地清除病毒。但缺点是只能检查和发现已知的病毒，不能检查新出现的病毒，而且由于病毒不断变形与更新，老病毒也会以新面孔出现。因此，病毒特征数据库和检查软件也要不断更新版本，才能满足不同用户的使用需要。

4. 计算机病毒的检测手段

（1）特征代码法

特征代码法被早期应用于 SCAN、CPAV 等著名病毒检测工具中。国外专家认为特征代码法是检测已知病毒的最简单、开销最小的方法。

特征代码法的实现步骤如下。

1）采集已知病毒样本，病毒如果既感染.com 文件，又感染.exe 文件，对这种病毒要同时采集.com 型病毒样本和.exe 型病毒样本。

2）在病毒样本中，抽取特征代码。依据如下原则：抽取的代码比较特殊，不大可能与普通正常程序代码吻合。抽取的代码要有适当长度，一方面维持特征代码的唯一性，另一方面又不要有太大的空间与时间的开销。如果一种病毒的特征代码增长 1B，要检测 3000 种病毒，增加的空间就是 3000B。在保持唯一性的前提下，尽量使特征代码长度短些，以减少空间与时间开销。在既感染.com 文件又感染.exe 文件的病毒样本中，要抽取两种样本共有的代码。将特征代码纳入病毒数据库。

3）打开被检测文件，在文件中搜索和检查文件中是否含有病毒数据库中的病毒特征代码。如果发现病毒特征代码，由于特征代码与病毒一一对应，便可以断定，被查文件中患有何种病毒。

检测准确、可识别病毒的名称和误报警率低是特征代码法的优点，可依据检测结果，进

行解毒处理。但是，采用病毒特征代码法的检测工具，面对不断出现的新病毒，必须不断更新版本，否则检测工具便会老化，逐渐失去实用价值。病毒特征代码法对从未见过的新病毒，自然无法知道其特征代码，因而无法检测这些新病毒。另外，搜集已知病毒的特征代码，费用开销大，在网络上效率低（在网络服务器上，因长时间检索会使整个网络性能变坏）。

因此，特征代码法有以下的特点。

- 速度慢。随着病毒种类的增多，检索时间变长。如果检索 5000 种病毒，必须逐一检查 5000 个病毒特征代码。如果病毒种数再增加，检测病毒的时间开销就变得十分可观。此类工具检测的高速性，将变得日益困难。
- 误报警率低。
- 不能检查多态性病毒。特征代码法是不可能检测多态性病毒的。国外专家认为多态性病毒是病毒特征代码法的终结者。
- 不能对付隐蔽性病毒。隐蔽性病毒如果先进驻内存，后运行病毒检测工具，隐蔽性病毒能先于检测工具，将被查文件中的病毒代码剥去，检测工具其实是在检查一个虚假的“好文件”，而不能报警，被隐蔽性病毒蒙骗。

（2）校验和法

将正常文件的内容，计算其校验和，将该校验和写入文件中或写入别的文件中保存。在文件使用过程中，定期地或每次使用文件前，检查文件现在内容算出的校验和与原来保存的校验和是否一致，因而可以发现文件是否感染，这种方法称为校验和法，它既可发现已知病毒也可发现未知病毒。在 SCAN 和 CPAV 工具的后期版本中除了病毒特征代码法之外，也纳入校验和法，以提高其检测能力。

运用校验和法查病毒采用以下 3 种方式。

1）在检测病毒工具中纳入校验和法，对被查的对象文件计算其正常状态的校验和，将校验和值写入被查文件中或检测工具中，之后进行比较。

2）在应用程序中，放入校验和法自我检查功能，将文件正常状态的校验和写入文件身中，每当应用程序启动时，比较现行校验和与原校验和值，实现应用程序的自检测。

3）用校验和检查程序常驻内存,，每当应用程序开始运行时，自动比较检查应用程序内部或别的文件中预先保存的校验和。

但是，这种方法不能识别病毒类，不能报出病毒名称。由于病毒感染并非文件内容改变的唯一原因，文件内容的改变有可能是正常程序引起的，所以校验和法常常误报警。而且此方法会影响文件的运行速度。

病毒感染的确会引起文件内容变化，但是校验和法对文件内容的变化太敏感，又不能区分正常程序引起的变动，而频繁报警。用监视文件的校验和来检测病毒，不是最好的方法。这种方法遇到已有软件版本更新、变更口令和修改运行参数等，都会发生误报警。

校验和法对隐蔽性病毒无效。隐蔽性病毒进驻内存后，会自动剥去染毒程序中的病毒代码，使校验和法受骗，对一个有毒文件算出正常校验和。

因此，校验和法的优点是：方法简单能发现未知病毒，被查文件的细微变化也能发现。其缺点是：会误报警，不能识别病毒名称，不能对付隐蔽型病毒。

（3）行为监测法

利用病毒的特有行为特征来监测病毒的方法，称为行为监测法。通过对病毒多年的观察与研究，有一些行为是病毒的共同行为，而且比较特殊。在正常程序中，这些行为比较罕见。当程序运行时，监视其行为，如果发现了病毒行为，立即报警。

这些能够作为监测病毒的行为特征如下。

- 占有 INT 13H。 所有的引导型病毒，都攻击 BOOT 扇区或主引导扇区。系统启动时，当 BOOT 扇区或主引导扇区获得执行权时，系统刚刚开始工作。一般引导型病毒都

会占用 INT 13H 功能，因为其他系统功能未设置好，无法利用。引导型病毒占据 INT 13H 功能，在其中放置病毒所需的代码。

- 修改 DOS 系统内存总量。病毒常驻内存后，为了防止 DOS 系统将其覆盖，必须修改系统内存总量。
- 对.com、.exe 文件做写入动作。病毒要感染.com .exe 文件，必须对它们进行写操作。
- 病毒程序与宿主程序的切换。染毒程序运行中，先运行病毒，而后执行宿主程序。在两者切换时，有许多特征行为。

行为监测法的优点：可发现未知病毒，可相当准确地预报未知的多数病毒。行为监测法的缺点：可能误报警，不能识别病毒名称，实现时有一定难度。

（4）软件模拟法

多态性病毒每次感染都改变其病毒密码，对付这种病毒，特征代码法失效。因为多态性病毒代码实施密码化，而且每次所用密钥不同，把染毒的病毒代码相互比较，也无法找出相同的可能作为特征的稳定代码。虽然行为检测法可以检测多态性病毒，但是在检测出病毒后，因为不知病毒的种类，难以做消毒处理。

为了检测多态性病毒，可应用新的检测方法—软件模拟法。它使用一种软件分析器，用软件方法来模拟和分析程序的运行。该类工具开始运行时，使用特征代码法检测病毒，如果发现隐蔽病毒或多态性病毒嫌疑时，启动软件模拟模块，监视病毒的运行，待病毒自身的密码译码以后，再运用特征代码法来识别病毒的种类。

7.2.2 计算机病毒的清除原理

清除计算机病毒要建立在正确检测计算机病毒的基础之上。清除计算机病毒主要应做好以下工作：

（1）清除内存中的病毒。

（2）清除磁盘中的病毒。

（3）病毒发作后的善后处理。

大多数商品化的软件为保证对病毒的正确检测，都对内存进行检测。但清除内存中病毒的软件并不多，一般都要求从干净的系统盘启动后再做病毒的检测和清除工作。

清除引导区病毒时，应预先准备好正常引导程序的备份，以对付覆盖型的引导区型病毒。对主引导区表信息应该特别注意，因为一旦分区表信息被破坏，要从硬盘中提取现有分区的状况并恢复分区表比较困难。对于将引导扇区转储的引导区型病毒，只要将原引导扇区找出并回写就可以了，但在回写前要检查其有效性，不然也可能会造成破坏，使原本在带病毒的情况下尚能存取的硬盘，在清除了病毒之后反而找不到硬盘了。

除了覆盖型的文件型病毒之外，其他感染.com 型和.exe 型的文件型病毒都可以被清除干净。因为病毒是在基本保持原文件功能的基础上进行传染的，既然文件的基本功能在染毒后也能实现，只是增加了副产品—依靠文件中增加的病毒代码运行的病毒，那么反病毒软件也可以仿照病毒的方法进行传染的逆过程—将增加的病毒代码清除出被感染文件，并保持其原有的功能。但是，被覆盖型病毒感染的文件最好彻底删除，因为文件原有的部分代码已被病毒代码所取代且没有备份，从而无法恢复文件原有的功能。

7.2.3 计算机病毒的清除方法

计算机病毒的清除方法一般有人工清除法和自动清除法两种。其中，人工清除是指用户利用软件，如 DEBUG、PCTOOLS 等所具有的有关功能进行病毒清除；自动清除是指利用防治病毒的软件来清除病毒。这两种方法视具体情况可以灵活运用。虽然目前有不少防治病毒的软件，但由于病毒的多样性和软件的使用范围的局限性，不可能刚出现一种病毒就能很

快研制出一种清除和抗毒的软件。因此，掌握人工清除的方法有特别重要的意义。

人工清除的步骤是：首先用一张“干净”（无病毒感染）的 DOS 系统盘，关闭写保护，启动系统；然后判断病毒感染对象。如果是分区感染，则恢复正常的分区表；如果是 Boot 区感染，则恢复 Boot 区；如果是可执行文件感染，则对该文件消毒；最后，回收资源，如修改文件分配表（FAT）、根目录区等。

1. 文件型病毒的清除方法

在计算机病毒中绝大部分是文件型病毒。所谓“文件型病毒”是指此类病毒寄生在可执行文件上，传播的途径也是依靠可执行文件。从数学角度来讲，清除病毒的过程实际上是病毒感染过程的逆过程。通过检测工作，已经得到了病毒体的全部代码，用于还原的数据肯定在病毒体内，只要找到这些数据，依照一定的方法即可将文件恢复，也就是说可以将病毒清除。

清除文件型病毒通常按照以下步骤进行：

①分析病毒与被感染文件之间的链接方式。

②确定病毒程序是位于文件的首部还是尾部，找到病毒程序开始和结束的位置，还原被感染文件的主要部分。

③恢复被感染文件的头部参数。

感染 com 文件的病毒会把 com 文件的头 3B 替换为病毒程序，并且把这 3B 保存在病毒体中。恢复时，就要从病毒体中找出这 3B，用来替换文件头中的病毒程序。

exe 文件被病毒感染后，文件头中的 CS、TP、SS、SP 等字段会被病毒修改，与被感染的 com 文件一样，这些字段的原有值被存放在病毒体中。特别要注意的是，有些病毒会先把这些值加密或变形，然后再存储。找出这些参数后，恢复文件头中的 CS、IP、SS、SP 等字段的值。另外，清除文件中的病毒后，文件的长度会变短，因此需要修改文件头中的长度参数。最后，把恢复后的内容写入文件。在这一过程中，因为不包括病毒体，文件长度会变短，只要把文件的正常内容写入文件病毒体就会被清除。

2. 引导型病毒的清除方法

（1）引导型病毒的清除原理

①引导型病毒感染时的攻击部位有硬盘主引导扇区和硬盘或软盘的 Boot 扇区。为保存原主引导扇区、Boot 扇区，病毒可能随意地将它们写入其他扇区，而毁坏这些扇区。

②硬盘主引导扇区染毒是可以修复的。恢复步骤如下：

用无毒软盘启动系统。寻找一台同类型、硬盘分区相同的无毒机器，将其硬盘主引导扇区写入一张软盘；或者病毒感染前硬盘主引导扇区有备份，将备份的主引导扇区写入一张软盘。将此软件插入染毒机器，将其中采集的主引导扇区数据写入染毒硬盘，即可修复。

③硬盘、软盘 Boot 扇区染毒也可以修复。解决办法就是寻找与染毒盘相同版本的无毒系统软盘，执行 SYS 命令，即可修复。

④引导型病毒如果将原主引导扇区或 Boot 扇区以覆盖的方式写入根目录区，被覆盖的根目录区将被完全破坏，不可能修复。

⑤如果引导型病毒将原主引导扇区或 Boot 扇区以覆盖的方式写入第一 FAT 时，第二 FAT 未破坏，则可以修复。可将第二 FAT 复制到第一个 FAT 中。

⑥一般情况下，引导型病毒占用的其他部分存储空间，只有采用“坏簇”技术和“文件结束簇”技术占用的空间需要收回。

（2）DEBUG 清除引导型病毒

在检测到磁盘被引导型病毒感染后，清除病毒的基本思想是用正常的系统引导程序覆盖引导扇区中的病毒程序。

如果在病毒感染以前，预先阅读并保存了磁盘主引导区和 DOS 引导扇区的内容，就很

容易清除病毒。可以用 DEBUG 把保存的内容读入内存，再写入到引导扇区，于是引导扇区中的病毒被正常引导程序所替代。

假设 MBR.dat 和 Boot.dat 分别保存的是硬盘的主导扇区和 DOS 引导扇区的内容，长度为 512B，则按以下步骤执行：

A>DEBUG

一 N MBR.DAT

一 L 7C00

一 N Boot.DAT

一 L7 E00

一 A 100

XXXX：0100 MOV AX，0301

XXXX：0103 MOV BX，7C00

XXXX：0106 MOV CX，0001

XXXX：0109 MOV DX，0080

XXXX：010C INT 13

XXXX：010E INT 3

XXXX：010F

一 G

一 W 7E00 2 0 1

一 Q

如果没有保留引导扇区的信息，则清除其中的病毒比较困难。对于那些把引导扇区的内容转移到其他扇区中的病毒，需要分析病毒程序的引导代码，找出正常引导扇区内容的存放地址，把它们读入内存，再按上面的方法写到引导扇区中。这将要花费较多的时间。

而对于那些直接覆盖引导扇区的病毒，则必须从其他微机中读取正常的引导程序。具体做法是：先从没有被病毒感染的微机硬盘中读取主引导扇区内容，其中含有主引导程序和该硬盘的分区表。将其写入被病毒感染的硬盘主引导区，然后把写入的主引导程序和本硬盘的分区表连接，把连接后的内容写入内存。

假设从未被感染的微机硬盘中读取主引导扇区，存放在 A 盘的 MBR.dat 中：

A>DEBUG

一 A100

XXXX：0100 MOV AX，0201

XXXX：0103 MOV BX，7C00

XXXX：0106 MOV CX，0001

XXXX：0109 MOV DX，0080

XXXX：010C INT 13

XXXX：010E INT 3

XXXX：010F

一 G

一 NA：MBR

一 R CX

0200

一 W 7C00

一 Q

这样已经得到了一张带有正常主引导扇区的软盘，下面要做的就是把这些内容写入被病

毒感染的硬盘。在带有病毒的计算机上，用“干净”的系统盘启动，然后进入 DEBUG：

A>DEBUG

一 A100

XXXX：0100 MOV AX，0201

XXXX：0103 MOV BX，7C00

XXXX：0106 MOV CX，0001

XXXX：0109 MOV DX，0080

XXXX：010C INT 13

XXXX：010E INT 3

XXXX：010F

一 G

一 NA：MBR

一 L 7E00

0200

一 M 7E00 L IBE 7C00

一 A100

XXXX：0100 MOV CX，0301

XXXX：0103

一 G=100

一 Q

以上介绍的是清除硬盘主引导扇区病毒的方法。对于硬盘 DOS 引导扇区中的病毒，可以用和硬盘上相同版本的 DOS（从软盘）启动，再执行 A:\>SYS C：命令传送系统到 C 盘，即可清除硬盘 DOS 引导扇区的病毒。

3. 宏病毒的清除方法

宏病毒是一类主要感染 Wod 文档和文档模板等数据文件的病毒。宏病毒是使用某个应用程序自带的宏编程语言编写的病毒，目前国际上已发现 3 类宏病毒：感染 Word 系统的 Word 宏病毒、感染 Excel 系统的 Excel 宏病毒和感染 Lotus Ami Pro 的宏病毒。目前，人们所说的宏病毒主要指 Word 和 Excel 宏病毒。

与以往的病毒不同，宏病毒有以下特点：

（1）感染数据文件：宏病毒专门感染数据文件，彻底改变了人们的“数据文件不会传播病毒”的错误认识。

（2）多平台交叉感染：宏病毒冲破了以往病毒在单一平台上传播的局限，当 Word、Exce 这类软件在不同平台（如 Windows、Windows NT/2000、OS/2 和 Macintosh 等）上运行时,会被宏病毒交叉感染。

（3）容易编写：以往病毒都是以二进制的计算机机器码形式出现，而宏病毒则是以人们容易阅读的源代码形式出现，所以编写和修改宏病毒比以往病毒更容易。

（4）容易传播：别人送一篇文章或发一封电子邮件给你，如果它们带有病毒，只要打开这些文件，计算机就会被宏病毒感染了。此后，打开或新建文件都可能带上宏病毒，这导致了宏病毒的感染率非常高。

感染了宏病毒后，同样可以用防治计算机病毒的软件来查杀，如果手头一时没有病毒防治软件的话，对某些感染 word 文档的宏病毒也可以通过手工操作的方法来查杀的。

4. 网络病毒清除方法

网络病毒主要指通过互联网络进行传染的病毒，互联网络指的是传染渠道，就病毒本身而言，可能包括文件型病毒、引导型病毒等多种病毒，所以这里所说的清除方法是针对网络，

主要是局域网这一特殊传染环境的各种针对性措施：

（1）立即使用 BROADCAST 等命令，通知所有用户退网，关闭文件服务器。

（2）用带有写保护的、“干净”的系统盘启动系统管理员工作站，并立即清除本机病毒。

（3）用带有写保护的“干净”的系统盘启动文服务器，系统管理员登录后，使用 DISABLE LOGIN 等命令禁止其他用户登录。

（4）做好系统及文件备份工作。将文件服务器的硬盘中的重要资料备份到干净的软盘上。但千万不可执行硬盘上的程序，也千万不要往硬盘中复制文件，以免破坏被病毒搞乱的硬盘数据结构。

（5）用最新的病毒防治软件扫描服务器上所有卷的文件，尝试恢复或删除被病毒感染的文件，重新安装被删文件。

（6）用病毒防治软件扫描并清除所有可能染上病毒的软盘或备份文件中的病毒。

（7）用病毒防治软件扫描并清除所有的有盘工作站硬盘上的病毒。

（8）对于已经误删除、丢失的数据或文件，可以尝试使用数据恢复软件进行恢复。

（9）特别对于上网的用户来说，一定要及时的下载并安装系统补丁程序。

（10）特别对于非计算机专业的使用人员，一定要尝试安装使用高端的安全卫士，来对你的电脑或网络定期不定期进行基本的维护工作。

（11）通过网络进行下载或者浏览信息时，尝试登陆官方网站或者大型的门户网站去进行相关的操作，尽量不去或者少去一些不知名的网站或者色情、暴力、反动的网站。

（12）及时关注系统的运行状态，对于异常进程、不用的端口以及不经常使用的部分服务功能及时的进行关闭操作。

（13）及时地清除异常系统启动项，以及系统目录中的异常文件。

（14）在确信病毒已经彻底清除后，重新启动网络和工作站。如有异常现象，请网络安全与病毒防治专家来进行下一步处理。

7.2.4 病毒和防病毒技术的发展趋势

如今，防范与解决计算机病毒已是迫在眉睫，但想要防范计算机病毒，首先要对计算病毒进行系统的了解，才能控制、预防和清除计算机病毒。

1. 计算机病毒的发展趋势

近年来，随着互联网的高速发展，病毒也进入了加狂和泛滥的阶段，目前计算机病毒的发展主要体现出在以下 4 个方面。

（1）病毒的种类和数量迅速增长。

2010 年，据江民反病毒中心、江民全球病毒监预警系统和江民客户服务中心联合统计的数据，截止到 2010 年 6 月 30 日，共截获新增各种计算机病毒（样本）数总计（包括木马、后门、广告程序、间谍木马、脚本病毒、漏洞病毒和蠕虫病毒）7584737 个，其中新增木马（样本）4454277 个，新增后门（样本）623791 个，新增广告程序（样本）223639 个，新增漏洞病毒（样本）166359 个，其他病毒（样本）1063255 个，各种新型病毒及变异还在不断变化。

（2）病毒传播手段呈多样化、复合化趋势

根据第九次全国信息网络安全状况与计算机病毒疫情调查报告的调查结果和研究分析，可以发现：计算机病毒木马本土化趋势加剧，变种速度更快、变化更多，潜伏性和隐蔽性增强、识别更难，与防病每软件的对抗能力更强，攻击目标明确，趋利目的明显。因此，计算机用户账号密码被盗现象日益增多。病毒木马传播的主要渠道是网页挂马和移动存储介质，其中网页挂马出现复合化趋势。

（3）病毒制作技术水平不断攀升

病毒制造者不断推进病毒的制造技术，不断推出病毒的新变种，利用新的技术手段隐藏自身进程，通过不断更新的技术终止杀毒软件的运行，逃避杀毒软件对于病毒的查杀，达到传播有害程序、破坏数据文件、非法窃取利益的目的。更值得关注的是，2008 年以来，大部分主流病毒技术都进入了驱动级，开始与杀毒软件争抢系统驱动的控制权，从而控制杀毒软件，致使很多杀毒软件功能失效。

（4）病毒的危害日益增大

越来越多的木马和病毒破坏计算机系统、造成死机、蓝屏、数据丢失，以及窃取用户账号密码等，给用户造成巨大的损失和破坏。“熊猫烧香”等病毒迅速在互联网上疯狂肆虐，被感染的计算机数量增长，严重威胁着个人用户和企业用户的信息安全。

2. 防病毒技术的发展趋势

随着实时监控技术的日益发展完善，能够达到监控文件、邮件、网页、即时通信、木马修改注册表和隐私信息维护的目的。但随着病毒制造者不断推出新变种，防病毒技术也取得了一定的进步和突破，由被动防御向主动防御转变势在必行。这是因为，如果用户不及时网络病毒库进行更新，会滞后于病毒制造者及病毒发作时间，加之近年网络新兴病毒频发，反病毒领域知识已经认识到必须由被动使用杀毒软件向主动防御新型病毒转变。所以，云概念、云计算、云安全和云杀毒等新兴概念应运而生。

云安全（Cloud Security）计划是网络时代信息安全的最新体现，它融合了并行处理、网格计算和未知病毒行为判断等新兴技术和概念，通过网状的大量客户端对网络中软件行为的异常进行监测，获取互联网中木马及恶意程序的最新信息，传送到服务器端进行自动分析和处理，再把病毒和木马的解决方案分发到每一个客户端。病毒库不再保存在本地，而是保存在官方服务器中，在扫描时和服务器交互后，做出判断是否有病毒。依托“云安全”进行杀毒能降低升级的频率，降低查杀的占用率，并可以极大地减小本地病毒数据库的容量。

云安全技术应用的最大优势在于，识别和查杀病毒不再仅仅依靠本地硬盘中的病毒库，而是依靠庞大的网络服务，实时进行采集、分析和处理。整个互联网就是一个巨大的“杀毒软件”，参与者越多，每个参与者就越安全，整个互联网就会更安全。

本章小结

本章主要讲述了以下内容:

计算机病毒的基本概念，主要介绍了什么是计算机病毒，以及对计算机病毒的理解。

计算机病毒的发展历程，主要介绍了从最早的计算机病毒是如何产生的，直到 2017 年勒索病毒的出现等一系列发展历程。

计算机病毒的特性，主要介绍了计算机病毒的非授权可执行性、隐蔽性、传染性、潜伏性、表现性或破坏性、可触发性等特性。

计算机病毒的危害，主要介绍了直接破坏计算机数据信息、占用磁盘空间和对信息的破坏、抢占系统资源、影响计算机运行速度、计算机病毒错误与不可预见的危害、计算机病毒的兼容性对系统运行的影响、攻击移动智能终端系统、摧毁工业控制系统和工业基础设施、给用户造成严重的心理压力。

计算机病毒的分类，主要介绍了计算机病毒按照病毒攻击的系统分类、按照病毒攻击的计算机类型分类、按照病毒的链结方式分类、按照病毒的破坏情况分类、按照病毒的寄生方式分类、按照病毒的传播媒介分类等几种分法。

计算机病毒的传播，主要介绍了计算机病毒借助于移动式存储介质的传播和各种网络方式的传播。

计算机病毒的检测原理，主要介绍了根据异常现象初步检测和利用专业工具检测查毒两种检测方法，以及检测的主要依据，还有计算机病毒的检测手段。

计算机病毒的清除方法，主要介绍了文件型病毒的清除方法、引导型病毒的清除方法、宏病毒的清除方法、网络病毒清除方法。

计算机病毒和防病毒技术的发展趋势。

习题一

1. 填空题

（1）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_____或者_____代码。

（2）计算机病毒按照传播媒介来分类，可分为单机病毒和_____病毒。

（3）计算机病毒传播的两个主要途径是_____和互联网络。

（4）计算机病毒的检测方法主要有根据_____和利用专业查毒软件检测两种方法。

（5）_____病毒可以寄生在可执行文件上，传播的途径也是依靠可执行文件进行。

2. 简答题

（1）简述计算机病毒的定义和特征。

（2）简述计算机病毒的分类。

（3）试举例说明生活中计算机病毒是如何传播的？

（4）如何检测局域网中的计算机病毒？

参考文献

[1] 王秋爽，钱松岭，董玉琦. 信息技术学生实验课程教学实验研究——以初中《计算机病毒与防治》单元为例[J]. 中国电化教育, 2015(4):31-35.

[2] 杨志成. 电子阅览室计算机病毒的防治[J]. 农业图书情报学刊, 2004, 16(11):197-198.

[3] 景铭, 郭剑. 计算机网络安全[J]. 管理学家：学术版, 2014(6).

[4] 丁勇. 密码学与信息安全简明教程[M]. 电子工业出版社, 2015.

[5] 刘京菊. 网络安全技术及应用[M]. 机械工业出版社, 2012.

[6] 贾铁军. 网络安全技术及应用实践教程[M]. 机械工业出版社, 2019.

[7] 张惠. 计算机病毒发展趋势及防护工作研究[J]. 网络安全技术与应用, 2018, No.209(05):4-5.

[8] 林翰. 浅谈计算机病毒发展趋势及其防范措施[J]. 计算机光盘软件与应用, 2013(11):136-137.

[9] 刘杰杰. 计算机病毒的发展趋势分析及防控策略探究[J]. 科技展望, 2017, 27(3).

[10] 王国旭, 万凯. 计算机病毒的发展趋势与防治[J]. 江西广播电视大学学报, 2014(3):92-94.

[11] 曾键, 赵辉. 一种基于 N-Gram 的计算机病毒特征码自动提取方法[J]. 计算机安全, 2013(10):2-5.

[12] 李惠先, 封二英. 一种基于人工免疫和代码相关性的计算机病毒特征提取方法[J]. 科技展望, 2015(22):204-215.

[13] 刘金莲. 浅析计算机病毒的特点及检测方法[J]. 现代职业教育, 2016(29).

[14] 李昌, 陈金花. 浅析计算机病毒特点及传播危害[J]. 电子制作, 2013(6):248-248.
[15] 郑士芹. 现代计算机病毒特征与防治策略[J]. 电脑编程技巧与维护, 2015(22):95-96.
[16] 李丽. 计算机病毒原理及其检测探析[J]. 电子技术与软件工程, 2014(13):241-241.
[17] 基于集合的划分与覆盖的计算机病毒检测研究[D]. 河北工业大学, 2014.
[18] 王立达. 计算机病毒智能检测技术研究[J]. 中小企业管理与科技(下旬刊), 2012(1):279-280.
[19] 付忠勇. 计算机网络安全教程[M]. 清华大学出版社, 2017.
[20] 梅华威, 张铭泉. 基于 BP 神经网络的手机病毒检测方法[J]. 计算机应用与软件, 2010, 27(7):283-284.