计算机病毒分析与防治技术

刘 真 编著

電子工業出版社

计算机病毒分析与防治技术

刘 真 编著

電子工業出版社

(京)新登字 055 号

内 容 提 要

本书是一本关于计算机病毒原理及其防治技术的实用书籍。它介绍了计算机病毒的来源、特点、危害性及其发展趋势；通过对典型病毒源代码的分析，深入地剖析了病毒寄生、传染和破坏各个环节的活动机理；从 DOS 系统出发，结合代表性病毒的分析，介绍了传染引导区、文件及综合型病毒的检测、消除和防治技术；书中对目前流传较广的约 1000 种病毒的主要特性进行综合列表；最后还具体介绍了在我国应用较多的几种主要防治病毒软件的功能与使用方法。

本书适合于计算机应用和开发人员及操作人员使用，也可作为大专院校计算机专业教材及自学用书。

图书在版编目(CIP)数据

计算机病毒分析与防治技术/刘真编著. -北京：电子工业出版社，1994.7

ISBN7-5053-2385-7

Ⅰ.计…

Ⅱ.刘…

Ⅲ.①计算机病毒-分析②计算机病毒-防治

Ⅳ.TP309

*

电子工业出版社出版

北京市海淀区万寿路 173 信箱(100036)

电子工业出版社发行　各地新华书店经销

原子能出版社照排中心排版

顺义县天竺颖华印刷厂印刷

开本：787×1092 毫米 1/16　印张：24.375 字数：550 千字

1994 年 7 月北京第 1 版　1994 年 7 月北京第 1 次印刷

印数：0,001——10,100 册

定价：20.00 元

前　言

随着计算机应用的普及，计算机病毒的蔓延对计算机系统安全的威胁也日益严重，已成为计算机系统的大敌。它不仅对计算机操作人员、各个计算机应用单位，而且对整个社会包括经济、科技、国防和安全部门都构成一种现实的威胁。因此，剖析计算机病毒的基本原理及相应的防治技术，强化计算机系统的安全可靠性已成为计算机应用领域的重要课题。

微型计算机在我国得到广泛的应用和迅速的发展。简单易学的操作系统和丰富的软件资源，使微型计算机成为人们学习、工作中的得力助手。但是自 1989 年春计算机病毒侵入我国以来，由于微机软件的盲目拷贝造成了以微机为目标的计算机病毒在我国以惊人的速度和广度流传，不少系统遭到病毒的破坏，一时间引起了许多人的困惑和恐慌。在有关部门、科研单位及大专院校的努力下，计算机病毒的肆意泛滥虽得到一定的控制，但是病毒并未被消灭，而且今后还会不断出现更新的病毒及病毒变种，将继续威胁着计算机系统。反病毒的斗争将是一个长期的任务。

本书以实用性为着眼点，在进行有关病毒的理论、病毒得以寄生、繁衍的相关系统知识的介绍和病毒源程序的分析的基础上，详尽地分析了以微型计算机为目标的若干典型病毒的特点及其检测和消除方法。希望能帮助计算机用户了解计算机病毒的共性及个性特征，学会对病毒的检测、辨识和防治方法，从而提高对典型计算机病毒的防治能力，以保证计算机系统能安全运行和使用。

本书共分 8 章和 6 个附录。第一章简单地回顾了计算机病毒的历史及有关病毒的常识；第二章介绍与计算机病毒有关的微型计算机系统的技术基础：磁盘知识，DOS 操作系统文件系统和中断系统；第三章介绍计算机病毒的构造特点、寄生原理、传播途径以及计算机病毒的交叉传染；第四章剖析若干典型的计算机病毒及其防治、消除方法；第五章分析一般计算机病毒的检测和防治技术；第六章综合说明防治病毒软件技术和防治病毒软件应具备的功能；第七章介绍目前流行的几种防治病毒的软件功能及使用方法；第八章介绍了与病毒有关的计算机工具软件简要使用方法；此外，还有常见的近千种计算机病毒的简要特征列表、有关病毒中英文名词对照、常见病毒的特征字、常见病毒的发作时间、常见传染文件型病毒传染后文件增长的字节数等 6 个附录。

本书的编写得到了单位领导及许多专家积极热情的鼓励和支持，也参考了多位专家在病毒防治工作中的经验和方法，北京大学吴良芝教授和忻宏杰同志对全书进行了审读，在此谨向他们表示衷心的感谢。由于作者水平有限，不妥之处在所难免，殷切希望广大读者批评指正。

作　者

1993.11.20

目　录

第一章　计算机病毒概述

伴随着计算机技术的发展和普及，计算机流行病菌像生物病毒侵袭人类社会一样侵袭和威胁着计算机系统，这就是计算机病毒。当人们警觉到某种病毒在周围传播，不要多久，这一地区的大多数兼容计算机就会检查到同一种病毒，大量的存储介质被感染，数据被破坏，甚至计算机系统被摧毁等等。计算机病毒悄悄地，快速地传染开，使许多计算机工作人员感到吃惊和困惑。

第一节　什么是计算机病毒

由于计算机病毒发展早期的隐蔽性、传染的快速性和种类的多样性，往往使人们还来不及给计算机病毒以十分确切的定义。在人们逐渐了解和认识计算机病毒的过程中，许多计算机工作者才从不同的角度给出了计算机病毒的定义，从而帮助人们研究和防治计算机病毒。

我们认为，计算机病毒是一种侵入计算机内部、可以自我繁殖、传播、具有破坏性的计算机程序。

迄今为止，出现在计算机领域中的计算机病毒都是人为编制的一段程序编码。它被程序设计人员或操作人员有意无意地植入某个正常程序或计算机操作系统中。然后，该病毒就依照设计者给定的指令，不断地自我复制，进行繁殖。有的病毒又以磁盘、磁带和网络作为媒介进行传播和扩散，“感染”其它的程序或系统，在一定时期或地域内广泛地流行。计算机病毒可以通过不同的途径潜伏、寄生在计算机的系统或程序中，在一定的条件下，依照其程序指令，干扰计算机的正常工作、吞食计算机的资源、甚至破坏数据或文件，严重时使计算机系统完全瘫痪。

当前，计算机病毒种类迅速增加。不同的病毒有其不同的特征。小的病毒仅有 20 条指令，不超过 56 个字节；而大的病毒可由几万条指令组成；有的病毒一进入计算机系统就大量繁殖，侵占资源，肆意破坏；但有的病毒，却长期潜伏，仅当某一条件达到时，才突然发作。这些病毒的不同特征和破坏方式是与病毒制造者的主观目的紧密相连的。但是，有些病毒的传播范围和破坏程度却是病毒制造者没有预料到和无法控制的。尤其是计算机网络系统，由于病毒借助网络传播，其传播趋势是难以预料的。在几分钟内，网络中所有运行的计算机均可能被感染。

计算机病毒是计算机技术和以计算机信息处理为中心的社会信息化进程发展到一定阶段的必然产物。

由于计算机应用，尤其是微型计算机应用的迅猛发展，计算机与人类社会各种活动密切相关。计算机已深入到国民经济各部门，商业、企业的各个角落，乃至进入家庭。微机的广泛应用和信息的自动化处理，给计算机病毒的流行，提供了适宜的环境。

由于计算机在政治，经济，军事方面所起的作用日益增大，重要性逐日提高，因而利用计

算机犯罪的引诱力也就日见增加。计算机犯罪所使用的高技术，具有可瞬时完成及可远距离控制的特点，因而不易取证，风险小而效果却不可估量。计算机病毒是计算机犯罪的一种衍生形式。计算机病毒全球性的蔓延，已经给计算机系统及其数据的安全造成了重大的损害。

随着最近十几年微型计算机的普及，针对微型计算机的病毒也借机迅速地泛滥。这是微机系统本身脆弱性的暴露和信息共享机制安全管理上的缺陷所促成的。微型计算机操作系统简单明了，软、硬件透明度好，安全措施薄弱，能够透彻了解微机内部结构的人数日益增多。因而，一部分人就利用了它本身的薄弱环节和易于攻击之处，编制或修改某些计算机病毒，并使它流传，从而使计算机病毒日益泛滥。计算机病毒问题已超出了计算机技术领域，成为一个严重的社会安全和社会道德问题。

第二节　计算机病毒的产生

计算机病毒这一名词是由科普小说首先提出的。

1975 年美国科普小说作家约翰·布鲁勒尔(John Brunner)出版了一本名为："震荡波骑士"的幻想小说。该书以计算机蠕虫为主，描述了在信息社会中代表正义和邪恶的两种势力之间利用计算机展开的一场斗争。这个故事使计算机第一次成为幻想中相互攻击的重要工具。该书幻想新奇，描写生动，获得了广大读者的喜爱。继之，在 1977 年，另一个美国科普作家托马斯·杰·雷恩(Thomas·J·Ryan)的著作"P-I 的青春"更是轰动一时，在该书中作者设想出现了一种神秘的、能够自我复制的计算机程序，并称之为"计算机病毒"。该病毒在计算机之间流传，一时感染了 7000 多台计算机的操作系统，引起了极大的混乱。

科幻小说的出现是有一定的历史背景的。在那以前，许多人已发现了计算机程序可以自我复制和变异这一机理。

首先，计算机的创始人，冯·诺依曼(John Von Neumann)在世界上第一台计算机诞生后仅仅 4 年，于 1949 年就发表了"复杂自动机器的理论和结构"的论文，指出计算机程序可以在内存中进行复制即"程序复制机理"的理论。

在此之后，许多计算机人员在自己的研究工作或游戏中发展和应用了程序或软件自我复制的理论。1959 年美国 ATST Bell 实验室的 3 个年轻人，道格拉斯·麦克尔罗伊(Douglas Mcilroy)，维克特·维索特斯基(Vietor Vysottsky)及罗伯特·莫里斯(Robert Morris)利用公司机器中的核心存储器中的数据和程序来做游戏。他们通过改变磁心存储器中的代码来消毁其它的程序。这种游戏被他们称做"磁心大战"(Core war)。为此，他们设计出有自我复制能力、并在探测到敌方程序运行时能消毁其程序的程序。这个程序经过不断地改进，其威力逐渐增大，甚至发展到影响计算机 Xerox 530 机的正常运行。由于意识到这种能自我复制程序的潜在危险，磁心战被停止了，并在有关人员的默契中保守了这个秘密。直到若干年后，凯·汤普逊(Ken Thompson)在给计算机协会做的一次演讲中才泄露出去。而后，又在"科学美国人"上详细地探讨了 Core war 中可自我复制程序的原理。从此，美国有关学术界才开始了实质性的研究。

1983 年弗雷德·科恩(Fred Cohen)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，在全美计算机安全会议上提出并在 VAX 11/150 机上作了演示。在一周后，他又获准进行了实验演示，共演示了 5 个实验，由此，证实了计算机病毒的实际存在。伦·艾德勒

曼(Len Adleman)将它命名为“计算机病毒”。

随着计算机技术的发展,出现了一些热心于编制程序的计算机爱好者。尤其是年轻的学生,他们热衷于用计算机作一些恶作剧的游戏,并探索有自我复制能力的潜伏程序的奥秘。

1985 年,IBM PC 机上出现了恶意的特洛依木马(Jrojan Horse)程序 EGABTR,该程序在显示漂亮的图象效果的同时,删除磁盘上的文件。

1986 年在巴基斯坦的拉哈尔,一家出售 IBM PC 微型计算机的商店,年青的两兄弟阿姆加德(Amjad)和巴锡特(Basit),对社会上软件互相拷贝和交换产生好奇和兴趣,他们动手编制了一个计算机病毒程序,并在程序中注明了自己的姓名和地址。这就是所谓的巴基斯坦病毒。这是到目前为止,世界上唯一标注有编写者姓名和地址的病毒。该病毒程序运行时在屏幕上显示:

welcome to the Dungeon
(c) 1986 Basic & Amjad (pvt) ltd
BRAIN COMPUTER SERVICES
730 Nijam Block Allama Igbal Town
Lahore,Pakistan
Phone:430791,443248,2800530
Beware of this VIRUS
confact us for vaceination

他们把载有此病毒的软盘送给了一个朋友,至此造成了巴基斯坦病毒在全球的流传。

1987 年 5 月,帕金斯·坦尼电脑公司为了防止公司非法复制软件产品而制造的病毒在美国“普罗威斯顿日报”编辑部的计算机上显示信息:“欢迎进入土牢,请小心病毒……”

1987 年 12 月 IBM 公司的计算机网络由一份电子邮件传入了“圣诞节蠕虫程序”。每当用户显示内容时,病毒程序就以链式反应方式自我复制,最后导致网络拥挤,使部分计算机被迫停止运行。

1988 年 3 月,潜伏于苹果机中的病毒发作。被广泛感染的苹果机都停止了工作,并显示信息:“向所有苹果电脑的使用者宣布世界和平的消息”,以此庆祝苹果机的生日。

1988 年 11 月 2 日美国康乃尔(cornell)大学研究生 23 岁的罗伯特·莫里斯(Robert Morris)制造的蠕虫事件,则是一起震憾全世界的“计算机病毒侵入网络的案件”。这个事件是计算机病毒演化过程中的一个重要转折点。该事件迫使美国政府立即作出反应,国防部成立了计算机应急行动小组。该事件发生后,美国报纸和电视台立即作了报导,使“计算机病毒”第一次成为国际社会的新闻热点。

莫里斯设计的病毒程序约有 6000 字节,可在 UNIX 环境下窃取口令字,并冒充合法用户将病毒程序拷贝到远程计算机中。病毒程序利用美国最大的计算机网络 Inter Net 网上的 Sendmail 程序进入计算机。这个病毒程序切断系统的安全功能,并把一段程序复制到另一台机器上,这段程序经编译和运行,再侵夺机器上的二进制命令和文件,连续复制和传播病毒程序。罗伯特·莫里斯设计的病毒实际上是钻了 UNIX4.3 的漏洞。根据 UNIX 专家的分析,病毒以 3 种途径侵入系统:

通过 Berkelgy UNIX 4.3 “Sendmail” 中的程序故障,使调试位呈通态;

在“Finger”程序中一部分使缓冲器过载,使它对病毒程序的另一部分进行编译和连接;

通过获取口令进入系统。

计算机病毒侵入后通过 Inter Net 网络不断扩散，直接影响 SUN 和 VAX 系统的运行。

莫里斯病毒侵入的 Inter Net 网络包括 5 个计算机中心和 12 个地区节点，连接着政府、大学和研究所共 250000 台计算机。该网中连接着 3 个主要网络：美国国防部高级研究计划局网络，军用网络和国家科学基金会网络。从 11 月 2 日上午 5 时病毒开始运行到下午 5 时，约有 6000 台与 Inter Net 网络连接的计算机，包括国家航天航空局，军事基地和主要大学的计算机停止了运行。直接经济损失达 9600 万美元。莫里斯本人被判 3 年缓刑，罚款 1 万美元，并罚做 400 小时的社会服务。

莫里斯病毒程序利用了 UNIX 操作系统的漏洞侵入系统。值得注意的是，该病毒程序虽然并不"恶意"地删除文件和破坏数据。但它无限制的繁殖抢占了大量的时间和空间资源。当发现网络超载后，莫里斯本人也失去了对程序的控制能力，已经没有办法制止机器上发展的状态。

莫里斯蠕虫事件引起了美国和世界计算机界的震惊，各国计算机专家及社会各界纷纷发表评论，至此，计算机病毒和计算机安全问题开始提到日程上来。

计算机病毒继续在世界上蔓延。尤其是一些恶性病毒的制造，更是对计算机系统的恶意攻击和破坏。

1987 年秋在以色列的希伯莱大学发现的"黑色星期五"病毒就是它们的代表。该病毒传染所有的可执行文件。按原计划黑色星期五病毒将在 1988 年 5 月 13 日(星期五)破坏该大学 1500 台微机系统的运行，恶意地破坏和删除磁盘中所有的可执行文件。该病毒因为快速侵占内存空间而在激活前被发现。但是，黑色星期五病毒程序的缺陷经过某些修改后成为目前在全球流行的恶性计算机病毒。它的触发条件仍是"13 日星期五"。1989 年 10 月 13 日，尽管国际社会已向各国发出了警告，一些国家的计算机仍遭到感染和破坏，因此，许多人称 10 月 13 日为世界计算机病毒流行日。

随着微型计算机在我国的普及，计算机病毒也逐渐流传开来。1988 年底在国家统计部门发现了小球病毒。该病毒侵入计算机后在屏幕上显示跳动的小球，发生跳撞后又不断地反射。它使机器运行速度明显地下降。尤其在 CCDOS 中文情况下它造成屏幕上下滚动，小球布满全屏幕，机器运行速度变慢，很快造成死机。由于缺乏防治措施，小球病毒迅速在我国流传。国家统计局下属省、市、县级的统计部门近 3000 台微机均受到感染。1989 年夏季，国家统计局召开病毒防治研讨会并采取检测、防治措施后，小球病毒仍禁而不止。更有甚者，在我国境内出现了大量小球病毒的变种。目前计算机病毒仍在中国大地蔓延，品种逐渐增多，病毒变种也逐渐增多，朝着破坏性大的恶性病毒发展。同时，由于软件输入的增加，国外流行的最新计算机病毒也在我国逐渐发现并且迅速蔓延。

第三节　计算机病毒的来源

从上面叙述的计算机病毒发展的历史可以看出，计算机病毒是人为制造出来的，是人们为着各种目的所编制的计算机程序。病毒制造者按着各自的意图，编制出一个能自我复制的、有不同破坏性的程序，并使其流传，造成了当今世界上方兴未艾的计算机病毒冲击浪潮。根据计算机病毒制造人员主观目的的自我表现和病毒程序传播中的客观效果，可将计算机病毒的来源分为几类：

1. 游戏和恶作剧

一些计算机爱好者和大学的学生们对计算机技术及其应用有着特殊的兴趣。一般说来，他们大多具有较好的计算机知识基础。为了开发自己的智能或者表现自己的才华，他们制造恶作剧的能大量自我复制的病毒程序，并使它在社会上流行。这类病毒程序在计算机屏幕上显示不同种类的图形或者玩笑性的警句。这种程序一般破坏性不大，也易于发现。但由于程序不断复制自己，从而侵占了系统的存储空间，因此也给计算机的正常运行造成一定程度的危害。

2. 软件自我保护

某些软件设计者或软件公司所开发的软件产品没有得到法律的正当保护，许多产品被非法拷贝，使其利益受到损害。为了保护自身的利益和给复制者以报复性的惩罚，他们在自己的软件系统中藏入可以自我复制，并带有破坏性的病毒程序。有的计算机俱乐部的成员将自己开发的应用程序公布在计算机网络中的公告板(BBS)上，欢迎大家选用，但使用者需邮寄使用费。否则，暗藏在应用程序中病毒程序机制就会像定时炸弹一样爆发，造成"占便宜者"的计算机系统的破坏。这种情况愈演愈烈，甚至发展到用计算机病毒来进行敲诈勒索。例如，1989 年 12 月肯尼亚一些银行和企业因使用了由伦敦寄来标有"爱滋病信息磁盘"字样的软盘没有付给要求的款项相继染上病毒，使计算机磁盘文件遭到严重破坏，有的计算机陷入瘫痪。

3. 蓄意破坏

某些组织和个人旨在攻击和摧毁计算机信息系统和计算机系统而制造的病毒，就是一种蓄意破坏行动。例如前面提到的，1987 年在以色列希伯莱大学出现的黑色星期五病毒就是其雇员在被辞退时故意制造的。它针对该大学的计算机系统，一旦激活将彻底摧毁该系统，是破坏性极大的恶性病毒。由于计算机病毒潜在的威胁性被越来越多的人所认识，计算机病毒已成为某些人使用的新的恐怖手段。我国国内已发现破坏性很大名叫"中国炸弹"的计算机病毒，表明制造、传播计算机病毒已为成为计算机犯罪的衍生形式。

4. 军事目的

电子计算机已成为现代军事系统的重要组成部分。许多事实表明：武器的自动化程度越高，计算机所占的比重就越大。海湾战争是以计算机为中心的高技术武器的一次实战试验。海湾战争的经验使人们进一步认识到，在现代化军事系统的装备、指挥、控制、管理等等方面，计算机都起着影响全局的作用。其中计算机软件是最活跃的因素，甚至是决定一切的主要因素。为取得未来战争的胜利，军事对垒的双方，一方面要加强本营垒中计算机的安全性和可靠性；另一方面要千方百计干扰和破坏对方的计算机系统，包括使用计算机病毒破坏对方的计算机软件系统，削弱对方的战斗力。伴随着军队越来越依赖于电子武器及其指挥和控制系统，计算机病毒可以用来从事电子对抗战的说法逐渐被许多人接受。由于下一代武器和作战系统均是由计算机软件控制的，计算机病毒便成为一种巨大的威胁。而目标捕获，战场管理和有关作战的连网计算机系统，都将是未来"计算机病毒"的主要攻击目标。

根据 1990 年 5 月来自纽约的消息，美国军队悬赏摧毁敌人电子系统的计算机病毒研制者。军方对竞争军用计算机病毒获胜者将提供 55 万美元的研制费用。悬赏来的计算机病毒可以用来摧毁军用通信线路和控制系统，传递有意错报的信息，病毒可用来改变敌方向战斗部队传递信息的通信卫星软件，可通过无线电通信系统潜入敌方的计算机系统，等等。据此

人们预料，计算机病毒很可能在将来被用于军事目的，成为军事电子对抗战的重要手段和工具。计算机病毒将变为一种新式武器。

第四节　计算机病毒的特点

从上面讨论的几种主要计算机病毒的来源可以看出，计算机病毒是人们为了达到一定的目的，所编制并令它广泛传播的一段计算机程序。就目前所发现的计算机病毒来说，其主要特点是：

一、传　染　性

类似生物界的“病毒”，传染性是计算机病毒的一个重要特性。一个计算机病毒能够主动地将自身的复制品或变种传染到系统中其它程序上，也就是说，计算机病毒的传染性在于计算机病毒的强再生机制。病毒程序一旦进入系统，就与系统中的程序链接在一起。并在运行这一被感染程序时，在系统中开始搜索能进行传染的其它程序，并把病毒自身或变种复制到其它程序上，从而达到再生的目的。经过不断地传染，再生，该病毒的副本不断地增加，使该计算机病毒迅速地扩散到磁盘存储器和整个计算机系统。计算机病毒可以传染一个微机系统，一个局部网络，一个大型计算机网络以及一个多用户系统。

一台微型计算机一旦感染上计算机病毒，病毒不仅在本系统中很快地扩散并实施破坏作用，使系统丧失正常运行的能力，而且被感染的计算机即成为该病毒流行的一个传染源，构成对同类计算机或兼容系统的一个威胁。通过计算机系统数据共享的途径，如网络连接或磁盘拷贝，病毒会不断地扩散，波及整个地区乃至形成世界性的蔓延。

在大型信息系统和计算机网络的工作环境下，计算机病毒传染的速度越快，则病毒程序对系统的破坏性就越大。

病毒程序的传染性反映了病毒程序最本质的特征。严格说来，一个程序若没有传染、再生机制，就不能叫做计算机病毒。

二、破　坏　性

计算机病毒对计算机系统的正常运行都具有一定的破坏性。所谓破坏性，不仅仅是指破坏系统，删除或修改数据，而且也包括占用系统资源，干扰机器运行等等。

从计算机病毒设计者的主观意图和病毒程序对计算机系统的破坏程度来看，已发现的计算机病毒大致可分成恶作剧和恶性病毒两类：

1. 恶作剧类型

这类病毒的制作者一般仅为了取乐和炫耀自己的技巧，所编病毒程序不破坏系统和数据。如 IBM 圣诞树病毒，可令计算机在圣诞节时显示问候的话语，并在屏幕上显示圣诞树的图象。除占用一定系统开销外，对系统破坏性小。有些人将这种形式的病毒称为良性病毒，确切地讲，应称为破坏性较小的病毒。

2. 恶性病毒型

病毒设计者的目的在于明确地破坏系统中的某些目标，从而破坏系统的正常运行。因而，这些病毒对计算机系统的破坏力是很大的，所造成的后果是极其严重的。最常见的恶性

病毒往往是消除或破坏数据，删除文件，对磁盘进行格式化等。这类计算机病毒可以中断大型计算机中心的工作，使某个计算机网络处于瘫痪，造成灾难性的损失。

计算机病毒的破坏性反映了病毒设计者的目的。但是任何病毒都是一种可执行的程序，病毒程序运行时，均要占用 CPU 时间和内存空间，降低系统正常工作的效率。恶作剧类的病毒程序要表现自己，必然要干扰系统的正常工作，打乱屏幕的显示。病毒程序的传播又大量消耗系统存储资源。因此，广义而言，任何病毒都是有害的。

根据病毒大规模扩散的情况和计算机病毒朝恶性病毒发展的趋势来看，强调指出病毒的破坏性是十分必要的。首先，任何类型的病毒都要占用系统的开销，干扰和破坏系统的正常运行。病毒对系统的破坏程度，不完全取决于设计者的目的，还取决于病毒运行的系统环境。例如前面叙述的，侵入美国 Inter Net 网络的莫里斯蠕虫程序，虽然该程序并不主动删除文件和破坏数据，却给美国最大的计算机网络造成巨大损失。再者，任何计算机病毒都是对计算机系统的非授权侵入，是对计算机系统安全工作的威胁，是一种违法行为。

三、隐　蔽　性

计算机病毒程序设计者为了使病毒程序达到非法进入计算机系统并进行广泛传播的目的，必须要在病毒程序表现之前设法隐蔽病毒本身。为了不被轻易的发现，一些广为流传的病毒都将自己隐藏在其它合法文件之中。病毒本身没有文件名，在列文件目录时也不被显示出来，尽量避免引起工作者的注意。

计算机病毒程序一般都短小精悍。因为病毒程序的设计者往往是程序设计技巧较高并且熟悉计算机内部结构的人员，他们能够设计出精致小巧的程序。由于程序短小，易于隐藏，病毒程序就不易被人察觉和发现。

当计算机病毒进入系统并进行传染时，源病毒经自我复制产生的病毒副本或变种往往使用前后链接或插入的方式隐藏在可执行文件或数据文件中。有的病毒能采取分散或多处隐藏的方式，而当病毒潜伏的程序体被合法调用时，病毒程序也合法投入运行，并将分散的程序部分在所非法占用的存储空间里进行装配，从而构成一个完整的病毒体投入进行状态。

四、潜　伏　性

病毒程序侵入系统后，一般不立即活动，需要等待一段时间，待外部条件成熟时才起作用。这就是病毒程序的潜伏性。一个编制精巧的病毒程序，可以在几周，几个月，甚至几年内进行传播和再生而不被发现。在此期间，系统的磁盘驱动器可能不断地复制病毒程序，制成病毒的副本或变种并传送到各部位，使它们感染病毒。因此，病毒的传染性与病毒的潜伏性有很大的关系。病毒程序编制得越精巧，它的潜伏期越长，则该病毒相对的传染性就越大。

所谓潜伏期是指病毒从外部设备（如磁盘驱动器）随寄生的合法程序进入系统，到病毒的破坏或表现部分开始作用时止的一段时间。病毒进入系统的时间，我们虽不能精确判定，但计算机病毒的潜伏期是可以判定的。因病毒所寄生的合法程序执行的时间可以精确判定。特定病毒的潜伏期越长，那么它的潜伏性就越好，这样病毒的传染作用可在较长的时间内发挥作用，其传染的范围也就相应地扩大。