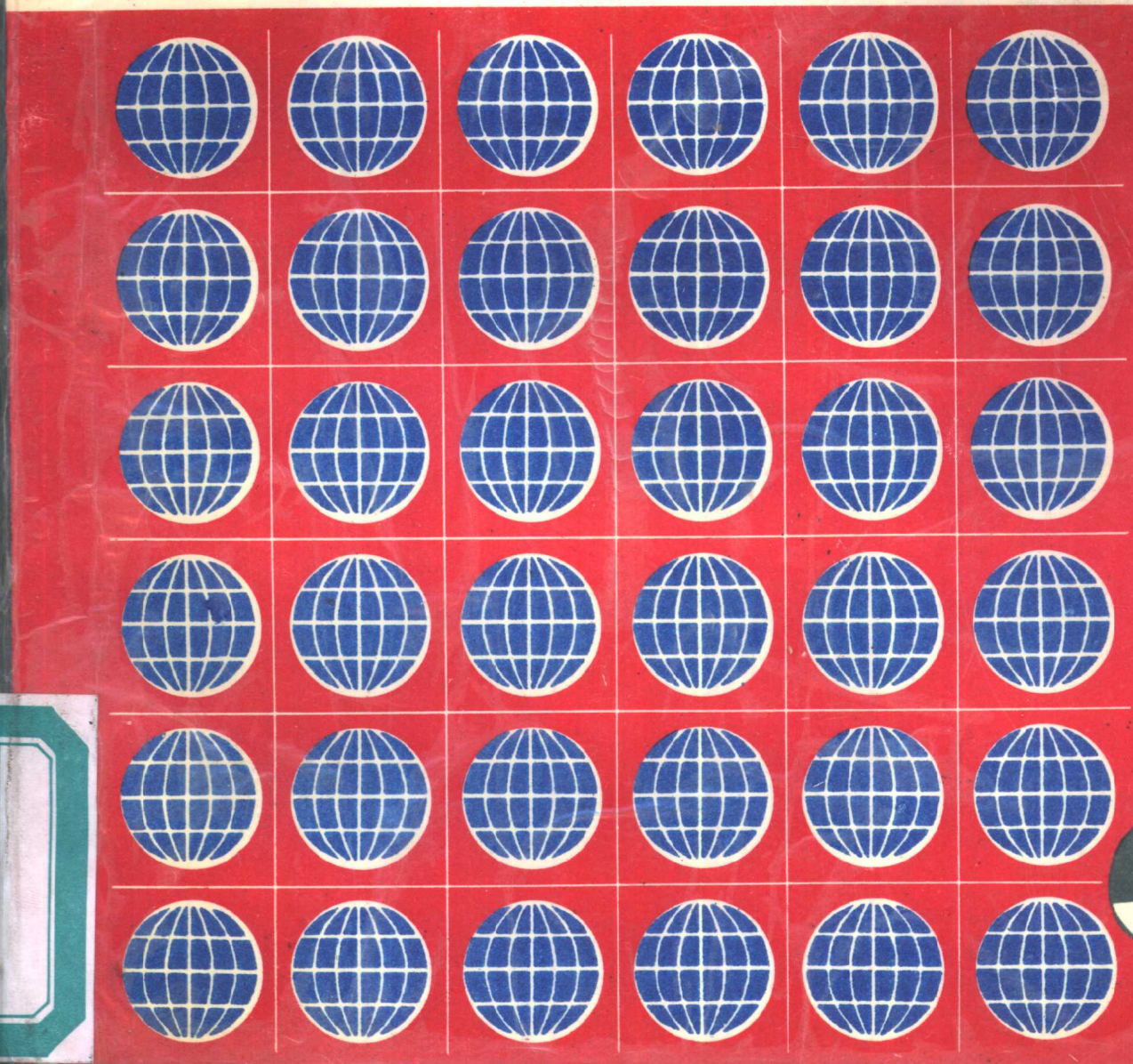
HOPE

计算机病毒防治大全

吴万钊 主编
吴万铎
黄占江 编著
宋 涵



北京希望电脑公司

计算机病毒防治大全

吴万钊　主编

吴万铎　黄占江　宋涵　编著

北京希望电脑公司

一九九一年九月

内容提要

全书分为两篇，第一篇为基础篇，介绍了计算机病毒的基本概况，DOS 操作系统的基本结构、启动过程，DOS 文件的管理机制，DOS 加载程序的过程，COM 型和 EXE 型文件的特点，硬盘的结构以及 DOS 系统中断的基础知识，动态调试程序 DEBUG 的使用方法等。第二篇为防治篇，对目前国内流行的十几种计算机病毒，如小球病毒、大麻病毒、黑色星期五病毒、巴基斯坦病毒、杨基都督病毒、磁盘杀手病毒、类大麻病毒（6.4 病毒）、1701 病毒（雨点病毒）、维也纳病毒（648 病毒）、Sunday 病毒（星期日病毒）、疯狂繁殖病毒（1575 病毒）、无名引导型病毒（2708 病毒）、V2000 病毒等，从它们的引导过程到传染机制，进行了详细的剖析，针对每一种病毒程序，给出了具体的诊断、防治的办法和实用解毒程序。在附录中介绍了常用 DOS 工具 PCTOOLS 和 Norton Utility 的使用方法，以及国内外常见的 59 种计算机病毒的特点。

本书分析的计算机病毒程序，基本上包括了目前国内流行的各种计算机病毒，为广大计算机用户排除计算机病毒的困扰提供了一本难得的计算机病毒防治手册。本书可作为计算机病毒防治的培训教材，也可作为大中专学生及计算机工作者的参考资料。

计算机病毒防治大全

吴万钊　主编

吴万铎　黄占江　宋涵　编著

前言

计算机病毒这一名词，人们对它已不是那么陌生了。人们对计算机病毒已有了一定的了解 。但计算机病毒的发展和传播远比人们预料的要快。不少计算机用户仍然时常受到老的和新出现的计算机病毒的困扰，有的已造成一定的损失。

那么如何有效的预防计算机病毒的侵蚀和传播，怎样消除侵蚀到系统及文件上的计算机病毒，是广大计算机用户迫切需要解决的问题。

本书集作者几年来对各种计算机病毒分析、研究的成果，参考大量国内外计算机病毒方面的有关书刊、杂志，编撰而成。本书对目前国内发现的十几种病毒从引导过程到传播机制进行了详细的分析。对每一种病毒都给出了具体的诊断、解毒的方法及步骤，并给出了一些实用解毒程序。使读者可以自行对这些病毒进行消毒、免疫处理。

在全书的编写过程中，作者力求集理论性与实用性为一体，即为想了解计算机病毒的计算机工作者提供一本有价值的参考资料，又为正受计算机病毒危害的广大计算机用户提供一些实用的诊断、解毒方法和实用解毒程序。

本书的部分内容曾在一些计算机培训班中讲授过，可作为计算机病毒防治的培训教材，是一本难得的计算机病毒防治手册，也可以作为大中专学生及科技工作者学习时参考。

本书在编写过程中，参考了大量的计算机系统方面和计算机病毒方面有关书刊杂志，在此恕不一一列举。谨向作者表示谢意。

由于作者水平有限，加之编写时间十分仓促，书中错误和遗漏之处在所难免，敬请读者和计算机同行朋友们不吝指教。

编著者

1991 年 6 月 20 日长春

目　　录

第一篇　基础篇

第一章　计算机病毒的基本概况 …… (1)
第一节　什么是计算机病毒 …… (1)
第二节　计算机病毒的起源和流行 …… (2)
第三节　计算机病毒的种类 …… (3)
第四节　计算机病毒的基本结构特点 …… (5)
第五节　计算机病毒的传播 …… (6)
第六节　计算机病毒的危害 …… (7)
第七节　计算机病毒的预防措施 …… (8)
第八节　本章小结 …… (9)
第二章　分析和防治计算机病毒必需的基础知识 …… (11)
第一节　DOS 的结构 …… (11)
一、DOS—BIOS 模块 …… (11)
二、DOS—kernel 模块 …… (12)
三、DOS—shell 模块 …… (12)
第二节　DOS 的软盘启动 …… (13)
一、DOS 启动流程 …… (13)
二、DOS 内存映象 …… (20)
第三节　DOS 引导记录 …… (20)
一、软、硬盘引导扇区 I/O 参数表 …… (20)
二、软、硬盘引导扇区基数表 …… (20)
三、引导记录块 …… (21)
第四节　DOS 文件的管理机制 …… (25)
一、文件目录表 FDT …… (26)
二、文件分配表 FAT …… (29)
三、磁盘参数表 …… (32)
第五节　DOS 加载程序的过程 …… (35)
一、COMMAND 处理命令的过程 …… (35)
二、程序段前缀控制块 PSP …… (37)
三、COM 文件映象加载 …… (40)
四、EXE 文件段重定位 …… (42)
第六节　硬盘的结构 …… (48)
一、硬盘的初始化 …… (48)
二、硬盘的结构 …… (49)
三、硬盘 DOS 分区的格式化 …… (51)
第七节　动态调试程序 DEBUG 的使用方法 …… (51)

一、DEBUG 程序的初始化 …… (51)
二、DEBUG 命令一览表 …… (52)
三、DEBUG 的使用方法 …… (52)
第八节 IBM PC 机的中断系统简介 …… (58)
一、中断的基本概念 …… (58)
二、中断向量的设置过程 …… (58)
三、与病毒程序有关的主要中断功能简介 …… (60)

第二篇 防治篇

第三章 小球病毒 …… (66)
第一节 小球病毒的表现形式 …… (66)
第二节 小球病毒的传染途径 …… (67)
第三节 小球病毒的组成 …… (67)
第四节 小球病毒的机理 …… (68)
一、病毒程序的自举部分 …… (68)
二、病毒程序的传播部分 …… (68)
三、病毒程序的表现部分 …… (68)
第五节 小球病毒程序的分析 …… (69)
一、病毒程序引导部分的分析 …… (69)
二、病毒程序传播部分的分析 …… (71)
第六节 小球病毒的诊断 …… (77)
一、用 CHKDSK 检查 …… (77)
二、用 DEBUG 检查 …… (77)
三、用 PCTOOLS 检查 …… (78)
四、用其它检查方法判定 …… (79)
五、激活病毒程序检查法 …… (79)
第七节 小球病毒的消除和免疫 …… (79)
第八节 小球病毒具有反免疫功能 …… (83)
第九节 小球病毒的变种简介 …… (84)
第十节 实用的小球病毒解毒程序 …… (85)
第十一节 本章小结 …… (88)
第四章 大麻病毒 …… (89)
第一节 大麻病毒的表现形式 …… (89)
第二节 大麻病毒的组成 …… (89)
第三节 大麻病毒的传染途径 …… (91)
第四节 大麻病毒对不同磁盘的破坏作用 …… (92)
第五节 大麻病毒程序的分析 …… (93)
一、病毒程序引导部分的分析 …… (94)
二、病毒程序传播部分的分析 …… (98)
第六节 大麻病毒的诊断 …… (100)

一、软盘上大麻病毒的诊断 …… (100)
二、硬盘上大麻病毒的诊断 …… (101)
三、计算机系统中大麻病毒的诊断 …… (101)
第七节 大麻病毒的消除 …… (102)
一、用 DEBUG 消除大麻病毒 …… (102)
二、用程序实现对大麻病毒的检测和消除 …… (104)
第八节 大麻病毒与小球病毒的特点比较 …… (106)
第九节 大麻病毒与小球病毒构成的复合病毒分析 …… (107)
第十节 本章小结 …… (107)
第五章 巴基斯坦病毒 …… (109)
第一节 巴基斯坦病毒的表现形式 …… (109)
第二节 巴基斯坦病毒的传播 …… (109)
第三节 巴基斯坦病毒的组成 …… (110)
第四节 巴基斯坦病毒的工作机理 …… (110)
第五节 巴基斯坦病毒程序的分析 …… (111)
一、病毒程序引导部分的分析 …… (112)
二、病毒程序传播部分的分析 …… (115)
第六节 巴基斯坦病毒的诊断 …… (118)
第七节 巴基斯坦病毒的消除 …… (120)
第八节 使软盘对巴基斯坦病毒具有免疫能力 …… (125)
第九节 本章小结 …… (126)
第六章 黑色星期五病毒 …… (127)
第一节 黑色星期五病毒的表现形式 …… (127)
第二节 黑色星期五病毒程序的组成 …… (127)
一、引导驻留部分 …… (128)
二、传播部分 …… (128)
三、破坏部分 …… (129)
第三节 黑色星期五病毒的传染机制 …… (129)
第四节 黑色星期五病毒程序的分析 …… (131)
一、引导驻留部分 …… (131)
二、传播部分 …… (137)
第五节 黑色星期五病毒的诊断方法 …… (145)
一、检查系统中是否感染有病毒 …… (145)
二、检查文件上是否感染了病毒 …… (145)
第六节 黑色星期五病毒的消除 …… (146)
一、消除系统中的病毒 …… (146)
二、消除文件上的病毒 …… (148)
三、介绍一个解毒的软件 …… (150)
第七节 本章小结 …… (151)

第七章　磁盘杀手病毒 …… (152)
第一节　磁盘杀手病毒的表现形式 …… (152)
第二节　磁盘杀手病毒的组成 …… (152)
一、引导部分 …… (152)
二、传播部分 …… (153)
三、破坏部分 …… (153)
第三节　磁盘杀手病毒的传染 …… (153)
第四节　磁盘杀手病毒独特的破坏判别条件 …… (153)
第五节　磁盘杀手病毒程序的分析 …… (154)
一、病毒程序引导部分的分析 …… (154)
二、病毒程序传播部分的分析 …… (161)
第六节　磁盘杀手病毒的诊断 …… (165)
一、检查系统中是否感染有病毒 …… (165)
二、检查软、硬盘上是否感染有病毒 …… (165)
第七节　磁盘杀手病毒的消除 …… (167)
第八节　本章小结 …… (169)
第八章　杨基都督病毒 …… (170)
第一节　杨基都督病毒的表现形式 …… (170)
第二节　杨基都督病毒的组成 …… (170)
一、病毒程序的引导部分 …… (170)
二、病毒程序的传播部分 …… (170)
三、病毒程序的表现部分 …… (172)
第三节　杨基都督病毒的传染过程 …… (173)
第四节　杨基都督病毒程序的分析 …… (173)
一、引导部分的分析 …… (173)
二、传播部分的原理分析 …… (177)
第五节　杨基都督病毒的诊断 …… (185)
一、对系统中染有病毒情况的诊断 …… (185)
二、对文件上染有病毒情况的诊断 …… (186)
第六节　杨基都督病毒的消除 …… (186)
一、用 DEBUG 解毒 …… (186)
二、用过滤法消除文件上的病毒 …… (187)
第七节　本章小结 …… (187)
第九章　类大麻病毒 …… (189)
第一节　类大麻病毒的表现形式 …… (189)
第二节　类大麻病毒的组成 …… (190)
第三节　类大麻病毒程序的分析 …… (191)
一、病毒程序引导过程的分析 …… (191)
二、病毒程序传播部分的分析 …… (195)

第四节　类大麻病毒的诊断……（197）
第五节　类大麻病毒的消除……（199）
一、用 DEBUG 消除类大麻病毒 ……（199）
二、检测和消除类大麻病毒的实用程序 ……（200）
第六节　类大麻病毒与大麻病毒的特性比较……（204）
第七节　本章小结……（204）
第十章　维也纳病毒的分析与防治 ……（205）
第一节　维也纳病毒的特点……（205）
第二节　维也纳病毒的引导和传播方式……（205）
第三节　维也纳病毒的检测……（211）
第四节　消除维也纳病毒的方法……（212）
第五节　本章小结……（213）
第十一章　2708 系统引导型病毒的分析与防治……（214）
第一节　2708 病毒程序的特点 ……（214）
第二节　2708 病毒程序的引导过程 ……（217）
一、由软盘引导 ……（217）
二、由硬盘引导 ……（217）
三、引导过程的分析 …… ……（217）
第三节　2708 病毒程序的传播方式 ……（219）
第四节　2708 病毒的诊断 ……（221）
第五节　消除 2708 病毒 ……（222）
一、消除硬盘上的 2708 病毒 ……（222）
二、消除软盘上的 2708 病毒 ……（224）
第六节　本章小结……（224）
第十二章　Sunday 病毒的分析与防治 ……（225）
第一节　Sunday 病毒的表现形式 ……（225）
第二节　Sunday 病毒程序的组成 ……（225）
一、引导部分 ……（225）
二、表现部分 ……（225）
三、传播部分 ……（226）
第三节　Sunday 病毒程序引导过程和传播方式分析 ……（228）
一、Sunday 病毒程序引导过程分析 ……（228）
二、Sunday 病毒程序传播方式分析 ……（234）
第四节　Sunday 病毒程序的诊断方法 ……（243）
一、检查系统中是否感染有 Sunday 病毒 ……（243）
二、检查文件上是否感染有 Sunday 病毒 ……（243）
第五节　Sunday 病毒的消除 ……（244）
一、消除后缀为 COM 型文件上的 Sunday 病毒 ……（244）
二、消除后缀为 EXE 型文件上的 Sunday 病毒 ……（244）

第六节　本章小结…… (245)
第十三章　1701 病毒的分析与防治 …… (246)
第一节 1701 病毒程序的特点 …… (246)
第二节　1701 病毒程序的组成 …… (246)
一、1701 病毒程序的引导过程 …… (246)
二、1701 病毒程序的传染过程 …… (246)
三、1701 病毒程序独特的表现形式 …… (247)
第三节　1701 病毒程序引导过程和传播方式分析 …… (249)
一、1701 病毒程序引导过程的分析 …… (249)
二、1701 病毒程序传播方式的分析 …… (255)
第四节　1701 病毒的诊断方法 …… (261)
一、系统中含有 1701 病毒的诊断 …… (261)
二、文件中含有 1701 病毒的诊断 …… (261)
第五节　1701 病毒的消除方法 …… (262)
第六节　介绍一个对 1701 病毒进行免疫的程序 …… (263)
第七节　本章小结…… (265)
第十四章　1575 病毒的分析与防治 …… (266)
第一节　1575 病毒的特点 …… (266)
第二节　1575 病毒独特的引导方式 …… (266)
第三节　1575 病毒的传播特点 …… (269)
第四节　1575 病毒程序的引导过程和传播方式分析 …… (270)
第五节　1575 病毒程序的诊断方法 …… (290)
一、系统被 1575 病毒程序感染的诊断 …… (290)
二、文件上染有 1575 病毒的诊断 …… (290)
第六节　对 1575 病毒的免疫 …… (290)
第七节　对 1575 病毒的解毒方法 …… (290)
一、对 COM 型文件的解毒方法 …… (290)
二、对 EXE 型文件的解毒方法…… (291)
第八节　本章小结…… (291)
第十五章　V2000 病毒的分析与防治 …… (292)
第一节　V2000 病毒的特点 …… (292)
第二节　V2000 病毒的引导过程分析 …… (292)
第三节　V2000 病毒传播过程分析 …… (301)
第四节　V2000 病毒的诊断 …… (317)
一、系统中存在 V2000 病毒的诊断 …… (317)
二、文件中感染有 V2000 病毒的诊断 …… (317)
第五节　消除文件中感染的 V2000 病毒 …… (317)
一、消除 COM 型文件中的 V2000 病毒 …… (318)
二、消除 EXE 型文件中的 V2000 病毒 …… (318)

第六节　本章小结……（319）
附录一　介绍几种系统工具软件的使用方法……（320）
一、PCTOOLS 工具软件的使用方法……（320）
二、Norton Utility 工具软件……（321）
附录二　世界上流行的 59 种计算机病毒简介……（324）
附录三　与计算机病毒有关术语注释……（333）
附录四　计算机病毒名称中英文对照表……（345）
参考文献……（346）

第一篇　基础篇

随着计算机科学技术的飞速发展，计算机的应用越来越广泛，微型计算机开始普及并逐步进入家庭。随之而来，曾经还是幻想的计算机病毒也作为一种活生生的事实出现在人们的面前，并已破坏了众多的计算机系统，造成重大的经济损失，从而对整个计算机系统构成了严重的威胁。

计算机病毒的出现，给社会——不仅仅是计算机工作者，而且包括政府、法律等部门以及各级领导乃至普通的工作人员敲响了警钟。一种新的利用计算机作为犯罪工具的高技术犯罪正成为日益严重的社会问题。

本篇在第一章里较详细地介绍了计算机病毒的基本概况，以使读者能对计算机病毒有一个初步的了解，并介绍了一些简单的预防措施。在第二章里，详细介绍了分析和防治计算机病毒所必要的基础知识，为在第二篇中分析和防治常见的各类计算机病毒打下一个良好的基础。

第一章　计算机病毒的基本概况

第一节　什么是计算机病毒

简单地说，计算机病毒是一种特殊的计算机程序。因为这种特殊的程序，它能象微生物学所称的病毒一样，在计算机系统中繁殖、生存和传播，并象微生物学中的病毒对动植物体带来疾病那样，这种特殊的计算机程序可以对计算机系统资源造成严重的破坏。所以人们就借用了这个微生物学名词，来形象地描述这种特殊的计算机程序，并称之为“计算机病毒”(Computer virus)。

目前，对计算机病毒尚没有一个确切的定义。美国计算机安全专家 Frederick Cohen 博士将计算机病毒定义为：计算机病毒是一个能传染其它程序的程序，病毒是靠修改其它程序，并把自身的拷贝嵌入到其它程序中而实现的。B. W. Burnham 认为：计算机病毒是一种能够使其自身的拷贝插入(通常以非破坏方式)到某个接受拷贝的程序中(或宿主程序中)的指令序列。这些定义都从一定的角度阐述了计算机病毒的概貌，但这似乎还不够，仅仅是说明了计算机病毒的一些形式。

在美国，对计算机病毒采用狭义定义，即计算机病毒为：能自我繁殖并向无毒的计算机系统扩散的加密性指令集；而在日本，则较多采用广义的定义，即计算机病毒为：不断滋长的且危及越来越多的计算机系统工作的程序或指令集。

国内对计算机病毒的研究还刚刚起步，各类书刊中对此也有一些报道和阐述，但也还没有一个为大家所公认的明确定义。不过人们对计算机病毒已不是那么陌生了，对于它的传染性和破坏性都有了一定的了解。

计算机病毒一般是一段程序，或一组指令，它们具有如下特点：

(1)隐蔽性

计算机病毒都是一些可以直接运行或间接运行的具有高超编程技巧的程序，它常隐藏在操作系统的引导扇中，可执行程序或数据文件中，以及磁盘上某些被标记为坏簇的扇区中，不易被人们察觉和发现。

(2)传染性

病毒程序一进入到计算机系统中，就开始寻找其进行感染的其它程序或存储信息的媒介。通过自我复制，它很快地传播到整个系统或软、硬盘上。病毒可以传染一个局部网络、一个大型计算机中心或者一个多用户系统。病毒的传染性是计算机病毒的再生机制，是衡量一种程序是否为病毒的首要条件，它是构成计算机病毒程序的重要条件之一。

(3)潜伏性

编制巧妙的病毒程序，可以在几天、几周甚至几个月、几年内隐蔽在合法文件之中，悄悄地进行传播和繁殖，而不被人们发觉。在此期间，只要计算机系统工作，就会传染病毒，使得编制的程序和数据文件的备份等可能染上病毒，而成为病毒的“携带者”。计算机病毒的潜伏性与传染性相辅相成。潜伏性越好，其在系统中存在的时间就会越长，病毒的传染范围也就会越大。

(4)可触发性

计算机病毒一般都有一个或若干个触发条件：或者是触发其传染，如在一定的条件下激活一个病毒的传染机制，使之进行传染；或是在一定条件下激活计算机病毒的表现部分或破坏部分，表现其自身的存在或破坏系统中及软、硬盘上的数据。触发条件可以是外界的，也可以是系统内部的。但对病毒本身而言，触发条件都是外部因素，一种病毒只是设置一定的触发条件。这个触发条件由外部因素提供，通过病毒自身的判断功能来实现。触发的实质是一种条件控制。一个病毒程序可以按照设计者的要求，在某个点上激活并对系统发起攻击。攻击是否进行，可以与多种情况联系起来，如指定的某个时间、日期、特定的用户识别标志符的出现、特定文件的出现、某一文件使用的次数等等。

(5)表现性或破坏性

病毒程序的最终目的是要干扰系统，破坏数据，因此它一定要表现其自身的存在。这主要体现在：占用系统资源(如占据内存空间，占据软、硬盘空间，以及系统运行时间等)，破坏系统中的数据文件，干扰程序的正常运行，甚至摧毁整个系统。病毒程序的表现性或破坏性，体现了病毒程序设计者的真正目的，这是构成计算机病毒的第二个重要条件。由于病毒程序的破坏性带来严重的危害，因此，越来越受到人们的关注。

第二节　计算机病毒的起源和流行

一般认为计算机病毒的发源地在美国。1977 年夏季，美国的 Thomas. J. Ryan 出版了一本科幻小说，名叫《The Adolescence of P－1》。在这本书中，作者构思出了世界上第一个计算机病毒。这种病毒能从一个计算机到另一个计算机传染流行，能控制 7000 台计算机的操作系统。

早在 60 年代初期，美国电报电话公司贝尔研究所里的一群年轻研究人员，常常做完工作后，留在实验室里饶有兴趣地玩一种他们自己创造的计算机游戏。这种被称作“达尔文”的游戏很有刺激性。它的玩法是，由每个人编一段小程序，输入到计算机中运行，相互展开攻击，设法毁灭别人的程序。这种程序就是一种计算机病毒的雏形，然而当时人们并没有意识到这一点。

真正的计算机病毒，通常认为是十年前首先产生在贝尔研究所，当时是因为工作失误无意中造出了计算机病毒。但是，也有人认为，大约在同一时期，首先是施乐公司帕洛阿尔托研究所的研究人员在试验开发中，制造出了计算机病毒。从那时起，一些软件开发人员和一些恶作剧者，为了显示自己高超的技艺或存心开玩笑，陆续制造了不少计算机病毒。

计算机界真正认识到计算机病毒的存在是在1983年。在这一年的11月3日的计算机安全学术讨论会上，美国计算机安全专家 Frederick Cohen 博士首次提出了计算机病毒的概念，随后获准进行实验演示。当天，专家们首先在运行 UNIX 操作系统的 VAX11/750 机上实验，成功地验证了第一个计算机病毒，一周后，又演示了另外五个实验。在5次实验中，计算机病毒使计算机系统瘫痪所需的时间平均为30分钟。由此证实了计算机病毒的存在，并证明计算机病毒可以在短时间内实现其对计算机系统的破坏，且可以迅速地向外传播。

实际上，计算机病毒的广泛传染始于1987年，在1988年才开始得到人们的重视。尤其是在1988年11月3日以后，计算机病毒才逐步为计算机界人士所了解。

1988年11月3日，美国最大的计算机网络 Internet 网络遭到了计算机病毒的攻击，该网络中约有6200台基于 UNIX 系统的 VAX 系列小型机及 SUN 工作站都染上了病毒，计算机用户的损失约9200多万美元。从此，国际计算机领域掀起了一个谈论计算机病毒的高潮。

自计算机病毒开始传播以来，仅三年多的时间，就出现了数十种病毒（不包括同类病毒的变种），并传遍了整个世界，世界各地均有受计算机病毒危害的恶性事件的报道。我国在这场世界性计算机病毒的传播中，也未能幸免。1989年4月西南铝厂首先报告发现小球病毒。之后在各地陆续报告发现计算机病毒。

目前，国内发现的计算机病毒，主要是攻击 IBM PC 机及其兼容机的，大约有十几种。其中传播最广的是小球病毒，并且这种病毒已产生了十余种变种。其次是大麻病毒、黑色星期五病毒、巴基斯坦病毒。另外也已发现了雨点病毒、杨基都督病毒、磁盘杀手病毒、音乐病毒等的传播。

由于到目前为止，我国计算机网络系统尚处在形成时期，还未达到国家级大网的水平，现在仍是一些部门级的小 LAN 或 3+COM 网络 Ethernet，所以，目前计算机病毒在我国的蔓延，主要是通过不同计算机之间软盘资源的共享，即主要靠软盘介质进行传播，这也就相应地限制了计算机病毒的传播速度和范围。由于我国软件应用的现状，尽管计算机病毒的传播途径比较单一，但其传播的范围还是比较广的。在国际计算机病毒的浪潮中，国内也必将受到冲击。各种在国外出现的病毒，也会在国内相继出现，且各种病毒的影响情况也是很难预料的。

第三节　计算机病毒的种类

在计算机病毒产生并发展的短短几年中，计算机病毒种类增加之多实在令人惊叹！

就计算机病毒产生的后果而言，一般将计算机病毒分为良性病毒和恶性病毒两大类。

所谓良性病毒，是指那些只是为了表现自己而并不破坏系统数据，只占用系统 CPU 资源或干扰系统工作的一类计算机病毒。这类病毒多数是恶作剧者的产物，他们的目的不是为了对系统的数据进行破坏，而是为了让使用这种被传染了病毒的计算机系统的用户，通过屏幕显示的方式，知晓病毒设计者的编程技术、技巧方法和超群的才华。如小球病毒、巴基斯坦病毒等，就属于这一类病毒。应该指出的是，这类病毒在一定程度上对系统也有破坏作用（或称副作用）。

恶性病毒是指那些一旦发作就破坏系统的数据、删除文件或格式化操作盘以及使系统处于瘫痪状态等一类计算机病毒。如黑色星期五病毒、磁盘杀手病毒等。这类病毒的目的在于人为地破坏计算机系统的工作和系统中数据，其破坏力和带来的严重危害是无法估量的。

就计算机病毒的寄生方式来说，一般将计算机病毒分为四种类型：

(1) 操作系统型(Operating System Viruses)

这种病毒也称为系统引导型。这种类型病毒的特点是：当系统引导时，病毒程序被装入内存，同时获得对系统的控制权，对外传播病毒，并在一定的条件下发作，施行破坏。一般情况下，病毒侵入到系统中及向外传播，都是悄悄完成的，难以被用户觉察。此类病毒如小球病毒、大麻病毒、磁盘杀手病毒等。

(2) 外壳型(Shell Viruses)

这类病毒是将其自身包围在系统可执行文件的周围，对原来的文件不作修改。运行该可执行文件时，病毒程序首先被执行，并将进入到系统中，获得对系统的控制权。再按同样的方式将病毒程序传染到其它在该系统下执行的文件中去。这类病毒较多，也较容易编写。如黑色星期五病毒、雨点病毒、杨基都督病毒等。

(3) 源码型(Source Code Viruses)

这种病毒在高级语言(如 FORTRAN PASCAL 等)编写的源程序被编译之前，就插入到源程序中，经编译后，成为合法程序的一部分。这是一种以合法身份存在的病毒程序。由于这种病毒专门攻击高级语言编写的源程序，而各类高级语言众多，因此这种病毒一旦传播开来，对计算机系统也将构成严重的威胁。

(4) 入侵型(Intrusive Viruses)

这种病毒是将其自身侵入到现有程序之中，使之变成合法程序的一部分。这种病毒较难编写，但病毒侵入到程序体内后，也很难删除，清除这种病毒很容易破坏原有的程序。

在计算机网络上传播的病毒，按照广义计算机病毒概念有以下几类：

(1) 蠕虫(Worm)

蠕虫是一种短小的程序，这种程序使用未定义过的处理器来自行完成并行处理。这种程序常驻于一台或多台机器中，并有重定位的能力。如果它检测到网络中的某台机器未被占用，就把自身的一个拷贝发送到那台机器。每个程序都能把自身的拷贝重新定位于另一台机器中，并能识别它的这个拷贝副本所占领的机器是哪一台。它可以在网络中连续高速地复制自己，长时间地占用系统资源，使系统负担过重，最后造成网络瘫痪。

(2) 逻辑炸弹(Logic Bomb)

这是一种当满足某些触发条件(如时间、地点、字符串、特定名字等)时，而发作引起破坏的程序。逻辑炸弹是由编写程序的人有意设置的，它有一个“定时器”，由编写程序的人设置，不到时间，不触发，具有一定的潜伏期。一旦发作，则对计算机数据进行破坏。

(3) 特洛伊木马(Trojan Horse)

它是一种外表上很有吸引力而且显得很可靠的程序，往往出现在网络的电子告示牌上。当使用者通过网络将其引入到自己的计算机以后，使用一段时间或运行一定次数后，便会发生巨大的故障，对系统造成破坏。

(4) 陷井入口(Back Door)

这是由程序的开发者有意安排的。当程序进入计算机网络里时，实际运行后只有开发者自己掌握操作的秘密，使该程序完成某种事情，而其他人则往往进入子程序死循环或其岐路。

(5) 细菌(Germ)

这是一种可不断在系统上传染自身,以占据计算机系统存贮器的程序。这一程序进入网络后,不断繁殖填满了整个网络的存储系统,使得整个网络必须关机之后,清除所有由这一程序繁殖的子孙程序之后,才能使网络系统恢复正常运行。

第四节 计算机病毒的基本结构特点

计算机病毒本身是在一种计算机中执行的程序,它必然要利用现存的计算机系统软件和硬件资源,作为其生存、繁殖和扩散的保障。现代计算机系统的硬件环境和软件环境,决定了计算机病毒的结构。计算机病毒的制造者就是根据计算机系统的软、硬件环境,抓住计算机系统的薄弱环节,来构造其病毒程序的。

通过对目前国内出现的各类计算机病毒程序的分析,各类计算机病毒大部分都由三部分组成,即引导部分、传播部分和表现(或破坏)部分(以下统称为表现部分)。个别病毒尚没有表现部分。比如大麻病毒、巴基斯坦病毒等。

驻留在传播介质上如(软、硬盘上)的计算机病毒的结构,可形象地用图(1—1)表示:

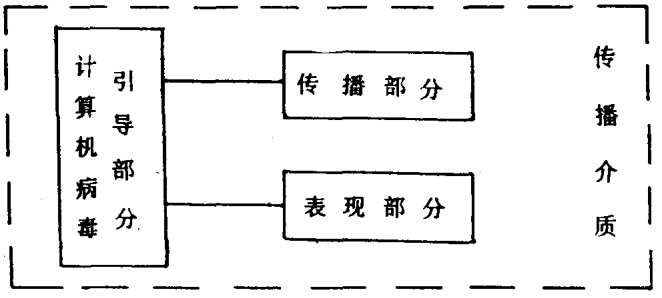


图 1—1 传播介质上计算机病毒的结构

此时计算机病毒的传播部分和表现部分是依附在引导部分上的,它们必须由引导部分带入计算机系统后,才能表现其各自的作用。这时的病毒处在静止状态,尚不具备向外传染和破坏的能力。

计算机病毒进入到系统后,病毒的结构发生了变化,传播部分和表现部分均直接与系统打交道,控制或干扰系统的某些工作。此时的结构如图(1—2)所示:

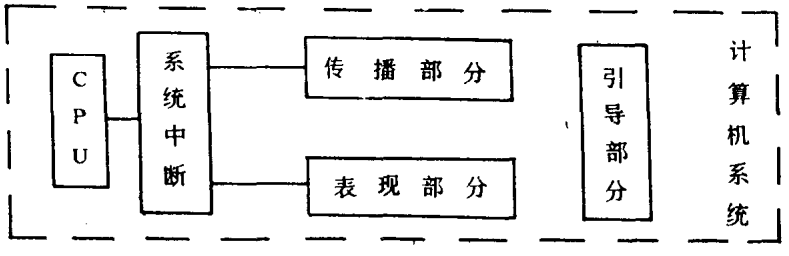


图 1—2 进入系统后,计算机病毒的结构

这时病毒程序已从静态转变为动态,并开始向外传播病毒,当满足触发条件后,其表现部分发作,干扰系统的正常工作,有的甚至删除操作盘中的文件(如黑色星期五病毒),而磁盘杀

手病毒发作时，除了将操作盘上数据全部破坏外，还使计算机系统处于瘫痪状态。

病毒程序的传播部分和表现部分，在其处于静止状态时，与引导部分紧密相联，并依赖于引导部分侵入到计算机系统中。它们之间的关系是相辅相成的。没有引导部分，其它两部分不能进入到系统中，当然也就无从对系统及文件进行破坏。只有引导部分，而没有其它部分，则该病毒不能向外传播，没有繁殖力，它充其量只能算作一个破坏程序。

一个病毒程序的引导模块，主要是将整个病毒程序送入到计算机系统中，完成病毒程序的安装。对于含有较长代码的病毒程序（如小球病毒一类，因病毒程序被分作两部分在介质中存放），则要首先实现两部分病毒程序的合并，然后再进行安装。在此之后，引导程序还要修改系统的中断向量，使之分别指向病毒程序的传播部分和表现部分。这样就使病毒程序的这两部分由静态转变为动态，并脱离引导模块，直接与计算机系统打交道。最后，引导模块还要执行原来系统正常的引导工作（对操作系统型病毒而言），或执行被调入内存的可执行文件（对外壳型病毒而言）。这样在用户看来，计算机仍在"正常"地工作，而丝毫觉察不到病毒的入侵。

病毒程序的传播模块完成将病毒程序向其它的网络、软、硬盘等介质上传染的工作，担负着向外扩散病毒的任务。该模块一般包括两部分。一部分是传播条件判断部分，对满足条件的介质施行传染；另一部分是传染部分，完成将整个病毒程序传至被攻击的目标上。一个程序具有传染能力，是判断其为计算机病毒的先决条件。正是其传染性，才使得病毒程序得以生存、繁殖。病毒程序的传播过程只是在读、写盘操作瞬间，人们是很难发现的。

病毒程序表现模块的作用，体现了该病毒设计者的真正目的。恶作剧者所编写的计算机病毒的表现模块，只是为了表现病毒自身的存在，并以此来宣扬设计者的才华，或通过这种表现而导致对计算机效率的降低，从中求得乐趣。而作为恶毒攻击者，他所编写的计算机病毒的表现部分，其主要作用是对系统的数据进行破坏。

表现模块也分为两部分。第一部分为触发判断条件，根据这一部分来确定病毒程序是否对计算机系统进行破坏。这个触发条件，就象定时炸弹一样构成了对系统数据的严重威胁。而这种破坏判断机制所要满足的条件越多，则病毒的潜伏性就越小。比如黑色星期五病毒发作条件为：不是 1987 年，且为 13 日和星期五三个条件，这样的条件较易被人们人为地破坏，而使病毒失去发作的机会。第二部分为表现部分工作段，具体地体现病毒制造者的目的，实施对系统的破坏。

第五节　计算机病毒的传播

计算机病毒依靠其传播载体的携带才得以迅速地传播。目前病毒的传播载体主要有下列三种：

（1）　网络传播载体

在计算机网络中，每一个分计算机系统要通过与主计算机系统之间的通讯线路实现系统中数据的共享，这个网络中各系统之间的通讯线路就构成了病毒传播的载体，使得病毒能够在网络中传播。

（2）　磁性介质传播载体

这种传播载体主要有磁盘和磁带，特别是软磁盘，由于它存储容量大，操作方便，体积小，便于携带，所以被广泛采用。病毒程序如果隐藏在软盘中，随着该软盘被拷贝复制，或在不同的计算机系统中使用，病毒就被传播出去。国内微型计算机上的病毒传染，主要就是由软盘作为