计算机病毒及其防治

杨大全　编著

东北工学院出版社

计算机病毒及其防治

杨大全　编著

东北工学院出版社

1991　沈阳

内容简介

本书结合作者多年教学和科研经验，在综合国内外计算机病毒及其防治研究的最新成果基础上，全面论述了计算机病毒的原理、症状、诊断、预防和处理等基本知识。包括计算机病毒起源，传播机制和预防措施，国内流行的病毒扫描程序及消毒软件，病毒的检测和诊治，手工检测与处理病毒的工具软件，典型病毒剖析，防治病毒的方法和途径，病毒的交叉感染等。并对和病毒有关的 DOS 技术，磁盘结构知识等也深入浅出的做了介绍，是广大计算机用户了解病毒，检测病毒和消除病毒的必备书，也可供高等学校师生参考使用。

计算机病毒及其防治

杨大全　编著

东北工学院出版社出版发行

（沈阳市文化路 3 号巷 11 号）　沈阳 7212 印刷厂印刷

（辽新出许字 89032 号）

开本：787×1092　1/16　印张：13.75　字数：349 千字

1991 年 8 月第 1 版　1991 年 8 月第 1 次印刷

印数：1～7100 册

责任编辑：战志民　责任校对：张德喜

封面设计：唐敏智　版式设计：高志武

ISBN 7-81006-353-7/TP・15　定价：6.80 元

前　言

随着计算机事业的高度发展，随着计算机的广泛普及和应用，计算机已深入到人类社会生活的各个方面，今天我们几乎看不到没有计算机参与的高科技领域。就在人们惊叹计算机给人类进步和社会文明带来巨大成就时。一个幽灵——计算机病毒出现了。

计算机病毒的出现给计算机应用事业带来了阴影，并造成了巨大的经济损失。什么是计算机病毒？怎样防治它？则是计算机界的共同呼声。本书结合作者对多种病毒的剖析和研究，并综合了计算机病毒防治研究的最新成果，较全面的叙述了计算机病毒的原理、症状、诊断、预防和处理。全书共由十章组成。第 1 章叙述了计算机病毒的起源、特性和传播现状。第 2 章介绍计算机病毒的传播机制和预防措施，并对病毒进行分类。第 3 章介绍了国内流行的病毒扫描程序 SCAN. EXE 及各种消毒软件。第 4 章介绍了检测和诊治计算机病毒所需要的预备知识。第 5 章对于手工检测与处理病毒的工具软件做简要介绍，其中包括 DEBUG、PCTOOLS 和 NORTON UTILITY。第 6 章对国内的常见典型病毒逐个进行剖析并给出诊治方法。第 7 章探讨了通用防治病毒的方法和途径。第 8 章对计算机病毒的交叉感染进行了分析，并对最常见的病毒交叉感染提出了行之有效的解毒步骤。第 9 章介绍了 INTERNET 网络事件，最后一章提供某些病毒程序的部分功能清单及相应的编程技巧，供读者编写自己的应用程序时借鉴。

郑重教授对本书的编写给于鼓励和大力支持，表示衷心的感谢。崔占东同志和笔者一起剖析多个病毒样本，并参加编写了第 10 章，燕玉堂同志对本书的出版给予了大力帮助；辛军、刘雪玲同志帮助打印书稿，一并表示感谢。

此外，本书的编写和出版还得到下列同志的热情帮助，他们是邵光、张理、佟大地、张光明、张哈京、林立等。在此谨向这些曾关心和帮助本书的同志表示衷心的感谢。

因时间紧，成书仓猝，加之水平有限，书中难免有一些错误和不妥之处，敬请读者批评指正。

作者

1990. 9. 9

目　录

第 1 章　计算机病毒的起源、特性、传播现状

1.1　计算机病毒的起源

随着计算机的普及和应用，计算机已深入到人类社会生活的各个方面，今天我们几乎看不到没有计算机参与的科技领域，计算机给人类进步和社会文明所带来的巨大冲击，就象当年蒸气机和电的发明所带来的震撼一样。正当计算机应用事业向前蓬勃发展的时刻，一个幽灵——计算机病毒悄然出现了。计算机病毒的影响和破坏在我们身边几乎到处可见，但我们真正考察计算机病毒的起源时却没有一个准确的答案。关于计算机病毒的种种起源说主要有以下几方面：

（1）恶作剧起源说

一批从小熟悉计算机并对计算机技术有浓厚兴趣的年青人，特别是象在美国这样计算机普及率很高的国家里，他们自持自己有高超的技术和过人的智慧，认为世界上没有做不成的事，他们凭借自己对计算机软件特别是操作系统的深入了解，编制了隐藏在计算机系统内部，能通过载体进行传播和复制，并在一定条件下激发和表现的程序，这就是计算机病毒。编制这些病毒程序的初衷，无非是要显示一下这些计算机神童的天才，并且从同伴计算机资源遭到损失当中寻求乐趣。一般讲这类病毒属于所谓的“良性”病毒，象小球病毒和 YANKEE 病毒，前者在一定条件下，从屏幕上显示一个跳动的小球；而后者则演奏一首著名的美国民歌，曾经轰动美国乃至世界的 internet 网络事件，就是 23 岁的美国青年莫里斯出于恶作剧制造的蠕虫病毒引起的。

（2）程序员的报复起源说

大家知道，计算机软件是一种知识密集的高科技产品，是软件工作者付出巨大脑力劳动的结晶。但软件资源的保护还没有适当的法律依据，许多商业软件被非法拷贝和非法复制，使软件程序员和软件制造商的利益受到严重损害。为了捍卫和保护自身的利益，也为了惩罚和教训那些不尊重软件程序员劳动成果的人，程序员和软件制造商在他们的软件产品中注入计算机病毒程序，并在一定条件下引发和破坏。支持这种说法的是 Pakistain Brain 病毒。这种病毒据说是巴基斯坦程序员阿尔维兄弟编写的，其目的是为了追踪对他们软件产品的非法拷贝者。这似乎也并无恶意，这种病毒最初只是修改磁盘的卷标，把卷标打上（C）Brain 的标记，后来被人修改过，其变种已具有巨大的破坏力。

（3）游戏程序起源说

据刊，大约十几年前，美国贝尔实验室的计算机程序员，在休息时为了消遣和娱乐，互相编制能够吃掉对方程序的程序，也许这种能吃掉程序的程序就是最早的人为破坏性程序，即：最早的计算机病毒。今天某些病毒程序的设计思想和技巧可能正源于当时的游戏程序。

另外，几年前曾有人提出一种叫“磁心战”（corewar）的游戏。先编写一个分配计算机内存空间的程序，和现在流行的微机一样，空间是由连续单元构成的，按模运算使得该存贮器

循环。游戏时，再分别由两个人各自编写一个汇编程序，这些程序装入内存后并被执行。执行的目的是企图破坏对方的程序，它按存贮器的循环周期每次一条指令的接近对方程序，看谁先把对方程序破坏。这种游戏程序也许离今天的病毒程序更为接近，因此游戏起源说也是有一定依据的。

关于计算机病毒的起源除了上面谈到的三种外，还有科幻小说起源说、特洛伊木马程序（Trojan horse program）起源说、蠕虫程序（Worm program）起源说等等。在上述计算机病毒种种起源学说的影响下，1983 年 11 月 3 日，弗雷德·科恩（Fred Cohen）博士研制出世界上第一个病毒程序，并于同年 11 月 10 日获准在运行 UNIX 操作系统的 VAX 11/750 机上进行病毒试验，在获得成功的五次演示实验中，使系统瘫痪所需的平均时间为半个小时，最短为 5 分钟。这个实验证实了，在对某特定计算机系统有透彻了解的条件下，可以编制某种病毒代码，这些代码一旦植入系统中，便可以繁殖，传染并破坏和控制整个系统，甚至于使之瘫痪。伦·艾德勒曼（Len Aclleman）把这种病毒代码命名为计算机病毒（Computer Viruses）。1983 年 11 月 3 日，也许这就是世界上最早的计算机病毒诞生日。今天我们很难指出计算机病毒的诞生到底基于何种起源说，但普遍认为计算机病毒的起源地是美国。这和美国计算机的高普及率无不相关；也和美国计算机软件、硬件高度发达，而计算机文明却得不到完善之间的矛盾无不相关。

总而言之，计算机病毒已经产生并实实在在地危害着我们，我们的任务是清除病毒带来的损害同时，恢复计算机的巨大声誉。今天计算机病毒的广泛传播和巨大危害，使怎样预防和消除计算机病毒成为首要问题，至于追踪它的起源就留给计算机发展史的作者吧。

1.2 计算机病毒的概念和特性

计算机病毒在很短的时间里席卷全国甚至于全世界，但什么是计算机病毒，它有什么危害，怎样防治它？这是许多人，其中也包括一部分计算机专业人员要求解答的问题。

美国对计算机病毒采用狭义定义，即：自我繁殖和向无毒计算机扩散的加密性指令集。日本对计算机病毒采用广义定义，即：不断滋长且危及越来越多计算机工作的程序或指令集。

尽管对计算机病毒人们尚无统一确切的定义，我们认为，计算机病毒（COMPUTER VIRUS）是隐藏在计算机系统内的一种破坏性程序。它能够利用系统数据资源进行繁殖并生存，并通过系统数据共享进行传染。它和生物学病毒具有相似的特性，例如：传染性、流行性、繁殖性、表现性等等。但它们的本质区别是明显的：前者是一种程序，而后者是一种微生物。计算机科学借用了生物学的术语，用“计算机病毒”表示具有上述特性的程序。

计算机病毒的特性：

（1）传染性：对其它健康磁盘或者健康程序进行传染，使其同母本程序一样成为新的传染源，这是计算机病毒最重要的特点之一。传染性使得计算机病毒的分布以几何级数增长。以扬基病毒为例，1989 年 9 月 30 日在维也那联合国办事处首次发现，半年以后，我国很多地区和城市就发现该种病毒，可见其传染力是何等之强。

（2）潜伏性：病毒发作之前，把自己隐蔽在合法文件之中，偷偷地传播，以扩大其传染和破坏的范围。更有甚者，当年投放传染的病毒在本年度只传染不发作，首次潜伏期长达一

年甚至更长。潜伏期过后，病毒发作时再想控制病毒的传染为时已晚，其传染面已扩大到无法控制的局面。例如：Sunday 病毒，1989 年它潜伏一年，这期间它只悄悄的传染，直到 1990 年才开始发作并破坏计算机系统。所以尽管其问世不长，但染毒数量却很多，传染面很广。

（3）隐蔽性：病毒的隐蔽性有二层含意：一是其存在的隐蔽性。它把自身依附于某种载体，不发作则不易发现。二是其攻击的隐蔽性。计算机病毒进入系统是隐蔽的，它的传染过程、破坏数据一般也是隐蔽的，不易为用户查觉。

（4）破坏性：病毒侵入系统的目的在于破坏系统，根据破坏系统的程度不同，我们把它分为良性病毒和恶性病毒。前者只占有计算机系统的资源，使系统运行速度变慢浪费机时，浪费内存，让机器无谓的消耗。而后者在发作时，则毁坏程序和数据，甚至变成死机，造成不可挽回的损失。这里的良性和恶性只是相对而言，本质上都是一种破坏性程序。属于良性病毒种类的有小球、扬基等；属于恶性病毒种类的有黑色星期五、Sunday、大麻等。

破坏性是计算机病毒的最重要特性，而其它特性都是为实现破坏性而服务的，但没有隐蔽性、潜伏性和传染性，计算机病毒是达不到破坏性这一根本目的的。它们相辅相成，互相依托，才体现了计算机病毒的全部特性。从目前发现的各种计算机病毒来看，几乎毫无例外的具有上述特性。另外：计算机病毒还有所谓“静态”和“动态”之分。计算机病毒一般依附于磁盘进行传染，依附在磁盘上的病毒没有经过引导，我们说它处于“静态”，处于静态的病毒只能通过拷贝进行传染。如果病毒程序通过引导进入系统内存，并驻留那里，便处于“动态”了，在满足一定的触发条件下其传染部分和表现部分纷纷活动，因此“动态”病毒构成对于系统直接威胁。而静态病毒构成对系统的潜在威胁。而从病毒的防治观点看，无论静态，还是动态，都属于清除之列。

综上所述，我们知道计算机病毒，实质就是一段由人为设计的计算机程序，这个程序能够修改其它程序而把自身拷贝到其它程序之内，从而完成对其它程序的传染。由于“病毒”程序是由人为设计的，所以，如果设计者怀有恶意，则他所设计的程序就可能对计算机系统造成严重威胁，甚至造成致命的损坏。

计算机病毒的出现和迅速蔓延，在相当大的程度上反映了当今计算机系统的脆弱性。计算机系统的各个组成部分、接口、界面和各个层次的相互转换都存在着不少漏洞和薄弱环节。硬件设计缺乏整体安全性考虑，尤其是软件方面，一个系统软件是由各自具有不同功能的程序所构成，是若干人年的产物，易于存在隐患和潜在威胁。计算机系统对不同层次、不同界面上局部程序的改动，缺乏有效的测试手段和敏感性，缺乏自动化的检测工具，更缺乏系统软件完整性的检验手段，软件的手工业的生产方法，难以防御程序体大大小小的修改或变动，使得计算机病毒的入侵很容易进行。

计算机病毒能够存在于大多数编译器中，所以每次调用编译程序就是一次潜在的计算机病毒攻击或侵入。计算机病毒难于侵入固化软件，但固化软件执行过程中却难于抵制病毒程序的侵入。

计算机病毒的破坏能力不取决于病毒程序的长短，而在相当大的程度上取决于计算机病毒的再生能力。计算机系统（特别是计算机网络）的资源共享，为计算机病毒的传染和破坏创造了条件。

1.3 计算机病毒的传播现状

计算机病毒在国际上大规模传染始于1987年，但当时新闻媒介对计算机病毒侵害的反应是冷淡的。而1988年11月3日在美国发生的Internet网络遭受计算机病毒攻击事件震惊了世界后，从此一个崭新的名词“计算机病毒”闯入了新闻报道领域，并且逐步由陌生到熟悉闯入了千万个计算机用户的大门。人们由恐慌到冷静，开始积极研究与之斗争的策略和办法。

有报道说，计算机病毒种类从1988年至今已有260余种。这还不包括形形色色的小批量病毒变种，从Internet网络至今，计算机病毒在短短的两三年就传遍了全球，引起了世界范围内的恐慌和警觉，可以说计算机所到之处也是其病毒所达之处，计算机应用面越是拓宽，计算机病毒的传播面也就越是扩大。许多国家和地区，如美国、西欧、日本、印度和中国等都曾发生过计算机病毒的恶性事件。

即使在苏联也发现了多种病毒，这些病毒包括：扬基、Aacsina、Microsoft88（543）、星期天、Pixel、Stone、磁盘杀手、乒乓、维也纳、耶路撒冷、黑色星期五、Brain等。随着病毒的流行和传播，苏联还发现了“土生土长”的国产病毒：Victor Virus（胜利者病毒）以及其它各种病毒的变种。

计算机病毒的攻击对象是有针对性的，不同种类的病毒攻击不同种类的计算机种。由于IBM PC及其兼容机占了计算机的主导潮流，则攻击它的计算机病毒也特别多，约占60%；其次以Machitosh（大苹果）计算机为攻击对象的病毒也为数不少；再次以攻击VAX机及unix操作系统的计算机病毒。总之越是流行机种，越是普及机型，其遭受病毒攻击的可能性越大。其危害范围也越广。

在我国，西南铝加工厂计算中心，于1989年3月首次发现计算机病毒程序，并把它命名为“001”号病毒程序，这就是今天大家熟知的小球病毒。随后《计算机世界》等一大批报刊和杂志相继发表了有关报道，从此拉开了我国计算机病毒热的帷幕，随着时间的推移，各种计算机病毒通过不同渠道传入我国，同时计算机界的有识之士开始研究剖析病毒程序，并提出了各种检测和诊治病毒的软件，为控制计算机病毒的蔓延，为减少病毒所造成的损失起到了巨大的作用。

在我国已经相继发现了小球、大麻、扬基、耶路撒冷、Sunday、Brain等多种国外流行的病毒，其中小球、大麻流传最广，危害最大，几乎遍布全国城乡各地。特别是二者的交叉传染，使常用的解毒软件无能为力。值得注意的是国内也发现了各样变种病毒，甚至于完全由国内制造的国产病毒，如：中国炸弹（Chinese Bomb）、美国佬坐轿等。

最近在国内1575病毒，2708病毒以及其它国产病毒象深圳1号，深圳2号，6.4病毒，1901病毒等又呈流行蔓延之势。特别是1901病毒，由于其隐蔽性好，传染力强，目前还没有现成的检测软件和消毒软件供广大计算机用户使用，因此危害更为严重。由它传染的机器，以及与其交叉感染的机器数量正在增加；交叉感染后的系统很容易造成死机，或者不能引导系统。当人们找到消除这种病毒的方法后，这种病毒的传染将被逐渐控制住。但随后一种新的病毒可能又会出现。

病毒的种类和变种正不断呈上升趋势，而解毒软件和检测软件也在不断的完善；魔高一

尺，道高一丈，两军对垒正呈犬牙交错、交替上升之势。

和计算机病毒作斗争，将是长期的、艰巨的任务。

1.4 常用计算机病毒术语

（1）病毒（Virus）

指隐藏在合法程序中的一块程序段，这种程序段具有自我繁殖扩散的能力，能够将自身复制到别的合法程序或数据文件中去。

病毒因其寄宿在合法程序体内，自然就享有合法程序所拥有的运行优先级。一旦携病毒程序运行，病毒即随之激活，并伺机进行传染。

（2）病虫（Worm）

这是一种独立存在，且具有自我繁殖能力的程序。这种程序与宿主系统的关键部分相连接，只要系统在运行，它也就在运行，伺机进行繁殖，并制造破坏。

“Worm”出自“Tapeworm”一词，后者最早出现在1975年的一本科学幻想小说“The Shoskwave Rider”中，系指打入计算机资源中，能够自动进行传染的程序。

（3）炸弹（Bomb）

指被设置在合法程序中，通过事件或条件引发后，会破坏程序和数据的子程序段。

（4）特洛伊木马（Trojan horse）

有两种定义：

①指携带有炸弹、病毒或病虫的程序，即携病毒程序。

②能够进入操作系统或系统模块的程序。利用这种程序，可以打进到操作系统内核，完成某种事情。

例如，利用假冒的帐务挂号程序来应付用户的挂号操作，当骗取到用户的帐号和密码之后，再造出挂号失败的假象引开用户，背地里却转调用真的挂号过程，从而进入帐务系统中为所欲为。

（5）后门（Backdoor）

同特洛伊木马的定义②。

（6）陷阱入口（Trapdoor）

同特洛伊木马的定义②。

（7）起手（Hacker）

指潜心于剖析程序或系统的人。

带贬意时，系指那些偷偷摸摸打进到别人的系统，并有意进行破坏活动的家伙（在我国常称为恶作剧者）。

（8）免疫力及计算机病毒的免疫

免疫力本是医学上的专用名词，其含义是：人体对病原体的侵入是有防御能力的，这种防御疾病的抵抗力叫免疫力。有些人虽然有病原体进入体内，但没有得病，说明这个人是有免疫力的。

免疫力有两种：

①一般免疫力，每个人从生下来都有防御传染病的能力，叫“一般免疫力”，这种免疫力防御一般的病原体都有一定的效力，但它并不特别有效，一旦有大量病原体侵入，它是抵抗不住的。

②特殊免疫力，这种免疫力多是后天自己产生的，是由于人体感染过某种病原体或注射过某种预防接种，体内就产生了针对某种病原体的免疫力，此种免疫力叫“特殊免疫力”。

计算机病毒学借用了这个概念，是指计算机系统有防御某种或某些计算机病毒感染的能力。例如：对大麻病毒的免疫是指对计算机系统进行某些处理之后，该系统可以免于受到大麻病毒的攻击和传染。

第 2 章　计算机病毒的传播机制和预防措施

2.1　计算机病毒的结构

计算机病毒是一种程序，却又是一种特殊的程序，它是隐藏在计算机系统内的一种破坏性程序。具有隐藏性、传染性、潜伏性和破坏性等特点，它没有文件名，列目录看不到。但只要它存在，总可以把它找到，并分离出它的程序清单。从剖析多种病毒程序的清单中发现，病毒程序一般结构由以下几个部分组成。

2.1.1　初始化引导部分

引导部分的功能是完成病毒程序的初始化，如：工作单元和参数设置，修改某些中断矢量，并保存原有中断矢量。把病毒程序的一部分，或者全部移到内存地址的高端。对于某些传染文件的病毒还要恢复原文件头，为执行用户原文件做准备。简言之，初始化引导程序是完成一切准备工作，让病毒按预定设想去执行任务。也就是常说的使病毒由“静态”变为“动态”。

2.1.2　传染部分

病毒程序根据种类的不同有不同的传染方式：对于替换 Boot 区的操作系统类病毒，主要是通过修改中断向量 INT 13H 进行传染。被病毒控制的 INT 13H 中断服务程序，在用户进行磁盘读写操作时偷偷的进行传染。而磁盘读写操作是计算机用户最常使用的操作之一，象 DIR、COPY、REN 等 DOS 命令都有这种操作，因此它传染的机会相当多。象大麻、小球、巴基斯坦智囊病毒属于这一类。

另一大类病毒是通过文件进行传染且传染文件的计算机外壳型病毒 (Shell Virus)。这一类病毒主要通过修改 INT 21H 中断矢量，重写其中的 4B00 功能，即 EXEC DOS 加载功能，而实现传染的。当 DOS 加载一个有毒文件时，则病毒被引导并驻留到内存。当 DOS 再加载另一个健康文件时，则由病毒控制的加载功能，即 INT 21H 4B00 功能中断服务程序，先判断文件是否有病毒标志，若没有，则进行传染。这一类病毒是专门传染可执行文件的，把病毒自身链接到被传染的文件上，以增大文件的长度。由于编制可执行文件的目的，就是要执行的，哪怕只执行一次，也将传染。

传染机制是病毒的重要机制，这部分程序是精心设计，精心编制的。从病毒程序的长度看，这部分占相当大的比重。

2.1.3　触发和表现部分（破坏）

触发部分又叫监视部分，一般通过修改 INT 8H 或 INT 1CH 等和时钟有关的中断，随时对小时、分钟、秒等参数进行监视或者通过 DOS 的功能调用，查看系统年、月、日、星期几等日期参数，一旦条件满足即启动表现部分或者破坏部分。

表现部分通常是显示一串字符，如：大麻病毒显示“Your PC is now stoned!”；Sunday 病毒显示“today is sunday…”等等；或者显示一些怪影、怪像；例如：小球病毒发作时显示一

个运动的乒乓球在屏幕上到处跳动；而黑色星期五病毒则在屏幕上开一个窗口(Wondown)，窗口内的字符有规律的向上跳动，翻滚；1575 病毒发作时，则在屏幕上显示一条色彩斑烂的“毛毛虫”，虫子一边蠕动，一边吞吃屏幕上的字符；还有的病毒表现时，发出某些音响，甚至于演奏歌曲。

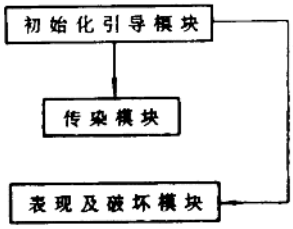

图 2·1-1 病毒程序模块图

表现部分主要通过怪音，怪像，来干扰用户，破坏计算机用户的正常工作，如果仅是这样，它属于良性病毒范畴。但许多计算机病毒在表现部分中，加入一些破坏性指令，如：删去正在运行的文件；破坏系统的引导扇，包括硬盘主引导记录和软盘引导扇；往磁盘的 FAT 表中及文件目录区中非法存入其它数据，造成用户程序和文件的彻底破坏。更为恶毒的是某些病毒在发作时，对磁盘进行格式化，甚至对硬盘进行低层格式化，这样全部数据和程序则荡然无存了。恶性病毒程序的模块结构，可以用图 2.1-1 表示。

2.2 计算机病毒的分类与概览

按着计算机病毒的传染机制及特性，有几种分类病毒的方法，简要介绍如下：

2.2.1 按攻击机种分类

(1) 攻击 IBM—PC 及其兼容机的病毒

世界上，现已有 2500 万台以上 PC 及其兼容机，因此攻击它的病毒种类最多，版本更新也最快。同时以基本病毒程序为主干，少许改动若干指令，使表现和破坏部分发生变化的病毒变种也最多。目前，在我国发现的各种计算机病毒绝大部分都是属于攻击 IBM—PC 及其兼容机的病毒。

(2) 攻击 Macintosh 系列计算机病毒

Macintosh 系列微机是美国 APPLE 公司继 APPLE—II 之后推出的新一代产品；采用 68000 或者 68020 做 CPU，由于性能/价格比较高，逐步成为新一代的主流机器。它于 1988 年获微机销售总额第一；是国外流行的机种之一，国内也正逐渐的推开。

攻击 Macintosh 的病毒也有若干种，例如 score 病毒、nVIR 病毒、Macmag 病毒、猴子病毒，Crade 病毒及 Hypercard 病毒等。

(3) 攻击 Unix 操作系统的病毒

Unix 操作系统是应用最广的操作系统之一。它是用 C 语言编制的，有广泛的可移植性，被称为操作系统的工业标准。许多机种都采用 Unix 操作系统，并且许多大网均采用 Unix 为其主操作系统。攻击 Unix 操作系统的病毒危害则显得特别严重。象 1988 年 11 月 3 日莫里斯制造的蠕虫病毒就是专门传染 Unix 操作系统支持下的 Sun—3 工作站和 VAX 系列机的，该病毒利用了几种 Unix 操作系统标准软件设计的一些缺陷。使 INTERNET 网几乎陷于瘫解，造成了巨大的经济损失。

2.2.2 按链接或寄生方式分类

(1) 源码病毒 (Source Code Virus)

这种病毒专门攻击高级语言编写的程序，其特点是在源程序被编译之前，将自身插入到源程序之中，变为源程序的合法成分。例如：攻击 BASIC 语言、C 语言、DBASE 语言和 FORTRAN 语言等等。

（2）操作系统病毒（Operation System Virus）

用病毒程序模块取代操作系统中的引导模块或其它部分。病毒随着计算机系统的引导操作而被驻入内存，并获得控制权，从而进行传染和破坏。因此有人称操作系统病毒为系统引导型病毒。目前国内所见到的许多病毒属于这种类型。例如：大麻病毒、小球病毒和巴基斯坦智囊病毒等。

（3）外壳形病毒（Shell Virus）

将病毒程序自身链接到主程序的四周。或链接到主程序的头部，当主程序加载时，首先执行病毒程序；或者链接到主程序的尾部，同时修改文件头，并把程序指针指向文件尾部，同样使病毒程序首先获得控制权。这类病毒种类较多，象国内流行的黑色星期五、Yankee 和 Sunday 病毒以及中国炸弹等都属于外壳型病毒。一般可通过检查文件长度是否改变而判断病毒的存在，也可以通过删除文件清除病毒。

（4）入侵病毒（Intrusive Virus）

入侵病毒将自身插入到主程序中间，和主程序以插入的方式链接，这种病毒较难编写，技巧也高，使中毒文件消除病毒也很困难，目前国内还没有发现这种病毒。

2.2.3 按感染和隐藏病毒代码方式分类

（1）BOOT 型病毒

它藏在磁盘的 BOOT 区内，包括硬盘的主引导记录和分区表，其感染时极难发现。它在系统引导时驻留，又习惯称之为引导型病毒。

（2）文件型病毒

是专门传染可执行文件的病毒，它包括 COM 文件、EXE 文件和其它由 EXEC 功能加载并执行的可覆盖文件。

（3）命令型病毒

命令型病毒通常是修改某个 DOS 命令。例如 COPY 或 DIR 只要使用这些命令就会传染。

（4）编码型病毒

若病毒程序代码是固定的，就容易让扫毒软件找到，所以某些病毒会对自身代码进行编码，使得每次得到的病毒码皆不相同，这样可以躲过许多解毒、扫毒程序。

从国内发现的多种病毒来看，它们基本上属于两大类。一类是替代磁盘 Boot 扇区的操作系统型病毒，另一类是专门以链接方式传染文件的外壳型病毒。即引导型病毒和文件型病毒。

从计算机病毒的发展趋势看，计算机病毒的种类很难说会一成不变；新的种类，新的变种会不断出现，因此我们无法断言未来计算机病毒的种类究竟会有多少。

目前发现的 IBM PC 微机病毒，其感染的对象一般有：硬盘分区表，系统 Boot 区，可执行文件（包括 EXE，COM，BIN，SYS，PIF 以及覆盖文件，如 OVL，OVG，OV1，OV2，OVR 文件）以及 COMMAND. COM 文件等。通过总结目前发现的大多数计算机病毒的感染情况，编制成表格，形成计算机病毒概览表，供用户方便的查询。

IBM—PC 及其兼容机已知计算机病毒概览表

病毒英文名	中译名	类型	感染对象 使驻系 PP 覆软硬主 用留统 CE 盖引引引 密内文 OX 文导导导 文存件 ME 件区区区	感染对象增加的字节数	危害性
AIDS Trojan	艾滋病木马	B	X X X	Overwrite	B, O
Avenue	林荫散步道	B	. X . . . . X X .	Overwrite	B, O
Ghost Boot Version	幽灵 BOOT	B	. X . . . . X X .	Overwrite	B, O
Ashar	*	B	. X . . . . X . .	Overwrite	B
Disd Killer	磁盘杀手	B	. X . . . . X X .	Overwrite	B, O, P, D, F
Ohio	俄亥俄	B	. X . . . . X . .	Overwrite	B
Typo (Boot Virus)	打印错	B	. X . . . X X .	Overwrite	B, O
Swap/Israeli Boot	以色列	B	. X . . . . X . .	Overwrite	B
Pentagon	五角大楼	B	. . . . . X . .	Overwrite	B
Stoned/Marijuana	大麻	B	. X . . . . X . X	Overwrite	O, B, L
PingPong—B	乒乓 B 型	B	. X . . . . X . X	Overwrite	O, B
DenZuk	*	B	. X . . . . X . .	Overwrite	O, B
Yale/ Alameda	耶鲁	B	. X . . . . X . .	Overwrite	B
Pakistani Brain	巴基斯坦智囊	B	. X . . . . X . .	Overwrite	B
Devli' s Dance	魔鬼的舞蹈	F	. X . X	941	P, L
Amstrad	*	F	. . . X	847	P
Payday	发薪日	F	. X . X X X . . .	1808	P
Datacrime I —B	数据犯罪 I —B 型	F	X . X X X	1917	P, F
Sylvia/ Holland	荷兰女孩	F	. X . X	1332	P

病毒英文名	中译名	类型	感染对象 使驻系 PP 覆软硬主 用留统 CE 盖引引引 密内文 OX 文导导导 文存件 ME 件区区区	感染对象增加的字节数	危害性
Do—Nonthing	什么都不做	F	. . . X	608	P
Sunday	星期天	F	. X . X X X . . .	1636	O, P
Lisbon	里斯本	F	. . . X . . .	648	P
Typo/Fumble	低能儿	F	. X . X	867	O, P
Dbase	*	F	. X . X	1864	D, O, P
GhostCOM Version	幽灵 COM 版	F	. . . X	2351	B, P
New Jerusalem	新耶路撒冷	F	. X . X X X . . .	1808	O, P
Alabama	阿拉巴马	F	. X . . X	1560	O, P, L
Yankee Doodle	扬基	F	. X . X X	2885	O, P
2930	2930	F	. X . X X	2930	P
AIDS	艾滋病	F	. . . X	Overwrite	P
1536/Zero Bug	臭虫	F	. X . X	1536	O, P
MIXI	迷幻	F	. X . . X	1618	O, P
Dard Avenger	秘密复仇者	F	. X X X X X . . .	1800	O, P, L
3551/Syslock	系统死锁	F	X . . X X	3551	P, D
VACSIMA	*	F	. X . X X X	1206	O, P
1514/ Datacrime I	数据犯罪 I 型	F	X . . X X . . .	1514	P, F
Icelandic I	冰岛 I 型	F	. X . . X	661	O, P
3066/ Traceback	寻根	F	X . X X	3066	P