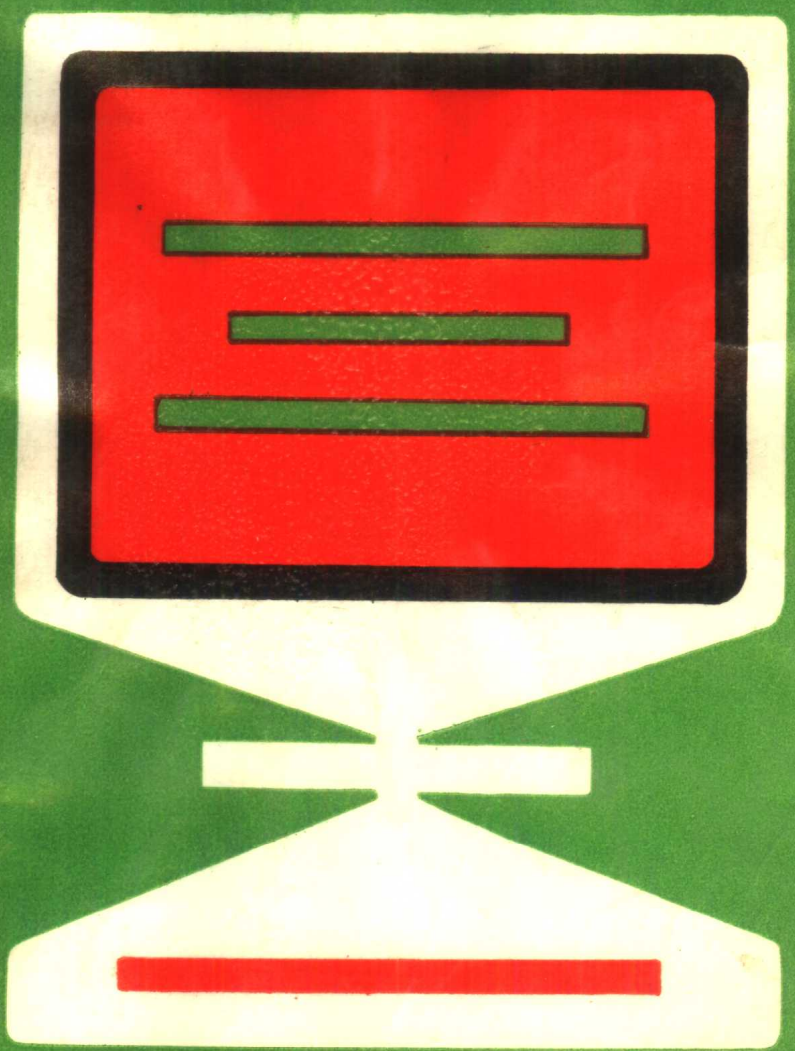
计算机病毒及其对策

方滨兴　褚滨生　顾棣　编著

黑龙江科学技术出版社



计算机病毒及其对策

方滨兴　褚滨生　顾棣　编著

黑龙江科学技术出版社

(黑)新登字第2号

责 任 编 辑：张丽生
封 面 设 计：张秉顺

计算机病毒及其对策

方滨兴 褚满生 顾 铮 编著

黑龙江科学技术出版社出版
（哈尔滨市南岗区建设街65号）
绥化市印刷厂印刷
黑龙江省新华书店发行

787×1092毫米16开本 16.75 印张 335 千字
1992年 9 月第 1 版 · 1992年 9 月第 1 次印刷
印数 1—5,000 册 定价：7.90
ISBN 7-5388-1958-4/TD·41

前　言

1989年以来，人们经常听到一个陌生却又容易接受的新名词：计算机病毒。计算机工作者无不关注计算机病毒；受害的计算机用户忙于收拾残局；计算机应用领域的专家学者在忙于寻找对策。由于“病毒”的肆虐，弄得人们一时不知所措，有的错把计算机硬件或软计的故障也怪罪成病毒。

为了正确认识和对付计算机病毒，为计算机更广泛应用扫清道路，笔者通过几年来的研究，并在同仁的协作下，编著了这本《计算机病毒及其对策》。本书基于“从方法上与病毒抗争”的思想，对计算机病毒乃至攻击性程序进行了分析，给出了防治方法，并断定，不同计算机病毒防范方法是唯一的。就是说，由于目前流行的计算机病毒均在本书所述某类计算机病毒之中，因而对所列各类计算机病毒有了妥善的防御方法之后，对尚未出现的病毒也可以预先防范。

本书概述了计算机病毒的特点与形成（第一、二两章）；着重探讨了计算机病毒的分类，并指出分类的目的和依据；（第三章）；介绍了出现在PC机上的计算机病毒机制（第四章）和相应的检查方法（第五章）；基于消除病毒乃是计算机维护的重要侧面，在介绍消除计算机病毒的同时，介绍了一些计算机系统维护的经验与技巧（第六章）；作者在研究计算机病毒时，采用汇编语言编制了一套计算机病毒检测、消除工具包。书中将把编程思想介绍给读者（第七章），并讨论了部分工具（第八章）。

在本书编著过程中，得到黑龙江省公安厅刘德钦，哈尔滨工业大学葛维翰、杨发、黄仲伟、刘军，国防科技大学计算机系以及公安部计算机监察局、电子部15所、中科院计算所、国家科委八六三计划智能机办公室、航空航天工业部办公厅等单位一些计算同仁的大力协助，在此一并致谢。

受学知水平和资料所限，本书不足和缺失之处望同仁及广大读者批评指正。

编者

1991年10月于哈工大

目　　录

第一章　概述

第二章　计算机病毒的特点与形成

第三章　计算机病毒的分类

第四章　PC机病毒机制

第七章 自制检测、消除病毒软件工具

第八章 计算机病毒的防疫

第九章 结束语

第一章 概 述

计算机病毒基本上是在1989年初出现的，到1990年初开始大蔓延，至今已通过各种手段逐渐平息下去。但是，作为一种反思，分析一下计算机病毒产生的基础和由此产生的社会问题，防止病毒的再发生，仍然是必要的。

§1.1 计算机病毒产生的基础

计算机病毒之所以能够大量产生，并广为蔓延，是由于计算机系统的全开放性技术基础和使用者管理的不健全性所致。计算机作为20世纪人类科学技术发展的重要成果为人类带来的方便是无法估计的。它已深入到我们生活的各个领域，科学计算、文字处理、档案管理、过程控制等等都离不开它。

1.1.1 计算机病毒产生的技术基础

讨论计算机病毒产生的技术基础，应首先了解计算机的系统结构。计算机系统是由硬件和软件两部分构成。硬件是CPU、总线、内存和外设等一些硬设备，软件是控制、驱动这些硬件设备的程序。软件包括操作系统、编译程序和应用程序。程序员编制程序通常是操作系统所提供的一个虚拟机上进行的，操作系统掩盖了驱动设备的具体细节，给用户提供了一些方便，简短的原语用于驱动设备。一个操作系统，用户使用时所需了解的细节越少，则系统的安全性就越高，但同时系统开放性越低，用户编程的灵活性也就越差。反之，若安全性降低，开放性升高，用户编程的灵活性也就提高。而计算机系统的实现，往往是系统安全性和开放度的一种折衷，不同的系统取舍各有不同。一般的大型系统，如UNIX、VMS等，通常开放度较低，对用户权限限制较为严格，相应的安全性较好。而个人计算机，如IBM PC，由于为个人所有，强调使用的方便和灵活，系统是完全开放的。用户通过查阅技术手册即可了解系统的所有细节。如IBM PC机由查阅技术手册，可了解操作系统DOS的引导过程，读取磁盘的某面某道某扇区，并将其搬到内存运行之，而且亦可使用BIOS中的INT13功能对其进行读写而不受任何限制。另外，DOS允许用户占用系统中断，并可读写执行文件（.COM和.EXE文件）。这样一些技术细节的开发，为病毒制造者提供了理想的条件，事实上，目前国内发现的PC机病毒都是利用这些方便条件设计的。

前面讨论了系统细节的开放，为病毒的产生提供了条件。实际上，在一些开放度较低，用户权限限制严格的系统中也发现了病毒（如UNIX），这是什么原因呢？这是病毒制造者利用了系统设计的缺陷。目前，许多系统在保安方面都有缺陷，造成这种缺陷的原因是多方面的。首先，是系统设计者忽略了安全问题，只考虑系统能否完成指定的功

能，而不考虑这些功能是否能被利用来做对系统有害的事；其次，是高技术产业中软件的落后生产方式——手工生产方式造成的。这种方式使产品缺乏标准，难以进行正确性测试与验证。这些就是系统设计缺陷产生的主要原因。这些缺陷不但给病毒的入侵提供了方便，而且给一些威胁计算机安全的犯罪行为，如计算机诈骗、国家及商业机密数据的窃取提供了方便条件。自80年代初期，随着计算机的普及，了解计算机系统结构的用户越来越多，计算机诈骗和机密失窃事件不断发生，这就引起了人们对计算机系统安全重要性的认识。许多科学家开始对现存系统弱点及相应安全技术的研究，希望这种研究成果能杜绝计算机病毒和计算机犯罪的发生，使计算机文明逐步走向成熟。

1.1.2 计算机病毒产生的社会基础

电子计算机自1945年诞生以来，以其计算的高速度、高精度，进入到人类生活的各个领域。随着硬件成本下降、体积缩小，已进入一般家庭。计算机高度的普及，使了解系统结构的用户越来越多，而相应的法律制约手段却不健全。这从某种程度上为计算机犯罪的发生提供了社会基础。

计算机病毒的起源至今没有确切的说法。但基本上分为两类：一是恶作剧。这种说法认为计算机病毒起源于搞恶作剧的人。这些人编制病毒程序往往是为了显示自己在计算机方面的超群知识或戏弄他人。缺乏必要的法律制约，使人们认识不到这种恶作剧所导致的后果。二是软件保护所引起。目前，计算机界存在着一种怪现象，软件是一种成本很高的高科技产品，而软件制造者的权益没有得到保护。软件的非法复制非常普遍，使得软件制造者的利益受到严重的损害。因此，软件制造商们用病毒软件来保护自己的版权，惩罚复制者，其副作用则导致病毒蔓延。不论这些说法是否正确，然而软件不受法律保护的情况作为病毒产生的社会原因，是不容忽视的。

§1.2 计算机病毒的危害性

计算机病毒（主要是PC机DOS环境）1989年初开始在我国出现，至1990年初，在短短的一年里，几乎所有的PC机都染上了病毒。在这段时间里，且不说由于数据丢失、程序破坏所造成的损失，仅用于清除病毒、研制反病毒软件所投入的人力、财力、时间就是一笔巨大的损失。仅黑龙江省就有工业大学、林业大学、公安厅等数家单位投入力量进行反病毒软件的研制。

1.2.1 INTERNET事件

1988年11月2日晚，美国最大的计算机网络INTERNET网受到了计算机病毒的攻击。INTERNET网络是以UNIX为主要操作系统的网络。至1988年11月3日，网络中基于UNIX的VAX系列的小型机和SUN工作站已有的6200台染上了病毒，造成的损失约9000多万美元。这次INTERNET网络中发现的是一种称为“蠕虫“的病毒，它利用了UNIX系统中电子邮件的缺陷侵入INTERNET网络，并在网络中不断地自我复制，一夜之间就给计算机用户造成了巨大的损失。通过这一事件UNIX的弱点暴露无遗，使得UNIX制造商AT&T公司和用户恐慌万分。

“蠕虫”病毒的制造者罗伯特·莫里斯毕业于康内尔大学计算机专业，当时年仅23

岁。他编制该程序是一种恶作剧行为，之前并没有考虑到病毒会如此迅速地侵入网络使其瘫痪。INTERNET网络事件引起人们对UNIX系统安全问题的认识，AT&T公司加快了对UNIX安全手段的研究，并推出了安全软件MSL。但由此我们可想到其它操作系统是否也存在某些缺陷，UNIX系统是否还存在别的缺陷？总不能等到病毒攻击发生之后才来考虑防御的手段，明智的方法是防患于未然。

1.2.2 黑色星期五

1989年10月13日（星期五）是世界上IBM—PC机及其兼容机最为惊恐的一天，因为有人事前宣布，这一天有一种称为“13日星期五”的病毒将广泛攻击正在运行的PC机。这个消息使得人们纷纷对重要的数据和程序进行备份，有的干脆决定：该日停机1天。当然，后面发生的情况远没有所说的那么严重。因为除用户提前做了大量准备工作外，“13日星期五”这种病毒的触发条件是系统时钟为13日星期五，而大部分用户的系统时钟是不准确的。虽然13日星期五没有如预想的那样集中发作，造成巨大破坏，但它引起的恐慌，程序和数据的大量备份，因系统时钟不准而引起的陆续发作，清理系统所占用的时间等，均造成了巨大的损失。而且“13日星期五”病毒的潜在威胁并没有真正解除，只要该病毒存在，条件适合时必定触发。

1.2.3 计算机信任感的危机

计算机自诞生的那一天起，一直是以快速、准确取信于人的。但由于计算机病毒的频繁发作，动摇了人们对计算机的信任。人们开始怀疑计算机程序和数据的正确性，担心受到攻击。实际上，在计算机病毒未被彻底控制之前是无法消除这种心理上的怀疑的。目前市场上的反病毒软件通常只针对某几种特定的病毒，对于该病毒的变种或新病毒则无能为力。当一种新病毒侵入计算机系统时，人们是无法发现的，即使病毒已经发作，也必须是有经验的操作员才能发现。目前的这种状况，需要社会上各方面强有力的合作才能改变。

第二章　计算机病毒的特点与形成

§2.1　计算机病毒的特点

一种计算机病毒通常由两部分组成。一部分为传染部分，这部分完成将自身写入一个可执行文件（外壳型病毒）或嵌入操作系统的引导过程（操作系统型病毒）。另一部分为表现部分，这部分一般以一定的方式通知用户系统已被感染。如大麻病毒的“your pc is stoned”，小球病毒的屏幕上小球的不断跳跃等等，病毒完成破坏性功能部分亦属于表现部分。病毒程序的编写往往是短小精干，有些还采用反跟踪技术，如YANKEE，当它感染debug后，一但发觉debug程序加载了一个染有YANKEE病毒的可执行程序就将该程序的YANKEE病毒清除，防止该病毒被跟踪。

2.1.1　攻击性

无论是良性还是恶性病毒都具有攻击性。恶性病毒的表现部分通常是以时间因素触发时间炸弹或以一定的逻辑条件触发逻辑炸弹，一但条件成立，或删除程序，或破坏数据。在任何病毒程序中均有主动攻击即主动起破坏作用的程序段，如染有维也纳病毒的文件，在指定时期时运行即可能被废弃。有些染有病毒的系统当硬盘数据达到一定数量时，造成文件丢失或启动不了，而且染有病毒的系统速度减慢，这对于要求时间严格的应用本身也是一种攻击性。病毒入侵造成的系统时间和空间的浪费都是不容忽视的。

2.1.2　传染性

计算机病毒能够生存下来并造成破坏，主要是由于它能由一个系统传染到另一个系统，由一个文件传染到另一个文件，这是因为一个不具有传染性的病毒缺乏生命力，也就不称为病毒了。如不能传染，一但其表现部分发作，就可能被察觉并被清除。

目前病毒一般通过软盘进行传染，它的藏身处为系统引导区，也即DOS的BOOT区；或附在执行文件上。但不管哪一种情况，病毒要进入软盘就必须往软盘上写内容，故将软盘贴上写保护口就可以防止病毒侵入。

2.1.3　隐蔽性

由于病毒程序都是利用DOS和BIOS的系统功能完成其功能，所以病毒程序一般都比较短小，容易附着在系统或可执行文件上而不容易察觉。另外一些病毒程序采用反跟踪技术和密码技术，则更难于发现。一个编制巧妙的计算机病毒程序，可以在几周甚至几年内隐蔽在合法文件之中，对其它系统进行传染，这就是计算机病毒生存下来的主要原因。计算机病毒的隐蔽性越好，在系统中存在的时间就越长，病毒的传染范围就越大。

计算机病毒进入系统并破坏程序和数据的过程是不容易查觉的。就计算机病毒本身其存留不定，可能隐蔽在备份盘或其它介质上。一种病毒可能在表面上被清除，但若干

年后，随机地或有目的地再次传染开来。病毒在一种载体上的寿命，如不人为清除，则与载体寿命一致。备份系统文件，目的是为防止病毒对文件的破坏而导致系统资源的损失，而实际上往往为病毒提供了安全场所，为病毒的再次触发激活创造了条件。

§2.2 计算机病毒的表现形式

计算机病毒具有传染性和隐蔽性的目的就是为了潜伏下来，等待条件成熟，激活表现部分，完成其预定的破坏功能。

2.2.1 发作形式

计算机病毒的发作形式根据设计者的目的而各不相同，可能是摧毁系统、破坏程序或数据，也可能是显示某些东西开个玩笑。如大麻病毒发作时显示“your pc is stoned”；小球病毒发作时屏幕上出现一个不断跳动的小亮点；13日星期五发作时删除可执行文件。发作的形式，是病毒设计者的目的所在。如美国某公司一职员，在设计管理程序时，将一段检查职员表中是否有设计者名字，如有则正常执行，否则删除所有数据的程序编入系统。当这个职员被解雇时，程序逻辑条件触发，所有数据均被删除。当然这种程序没有传染性，不属于计算机病毒类，但由此可联想到病毒表现部分的类似破坏性。

2.2.2 传染形式

计算机病毒之所以造成目前这样大的影响，是由于它的传染性。一个典型的PC系统病毒，能在几周内传染数百台未联网的计算机中。我国计算机病毒大约是出现在1989年初，当时只是良性的小球病毒，危害性不大。到1990年，计算机病毒几乎感染了所有的PC机，速度之快是相当惊人的。

计算机病毒由于种类的不同，其传染的方式和渠道也不尽相同。操作系统类病毒感染磁盘，通过改变系统引导过程来完成传染。当系统启动时，病毒程序首先获得控制权，完成自己的初始化工作之后，再继续系统的正常引导。DOS环境中，操作系统类病毒先于DOS进入内存，通常是改变磁盘中断INT13H来完成传染。如大麻病毒是占据DOS分区的引导记录，而将正常DOS分区引导记录保存到其它地方，大麻病毒完成初始化后，再将正常DOS分区读入内存，并将控制权交给DOS。而小球病毒是驻留在系统分区表中，当引导系统时，病毒首先进入内存修改INT8H和INT13H的地址，等待一定的条件发作。

可执行文件类病毒通常附在COM或EXE文件之上。驻留内存的病毒通常是占据DOS中断INT21H，以便加载一个程序就检查是否染有此病毒（也有不检查的），无则修改此程序头部的相关参数，将病毒加入程序。不驻留内存的病毒是一但触发条件成立就立即感染，然后马上退出内存，此类病毒极难发现。

网络中的病毒是利用网络的通讯机制以存文件的形式传播到网络的各个结点，在目标结点上编译、连接、运行及继续传染

第三章　计算机病毒的分类

为了更好地防范病毒，必须对病毒有个整体的了解，将病毒加以归类。出于不同的出发点，病毒的分类方法也就不同。例如，可以从攻击对象来进行分类，这是针对应用人员，往往只对某一种机型非常熟悉的情况而言；也可以从攻击的环境来分类，这是针对单机环境或网络环境而言。总之，不同的分类往往仅标明了病毒的某一个侧面，各分类之间可以交叉，因而一个病毒可以通过多种分类来更多地被描述出其各种特征。

在众多的分类方法中，树状分类是一种比较好的方法，通过这种分类方法，可以将病毒的工作机理的各种方法孤立出来，从而对其进行防范。

§3.1　一般的计算机病毒分类方法

3.1.1　按照攻击对象分类

按照攻击对象分类是按病毒所依托的指令系统分类。这也是病毒编制者所要求的必要环境。显然，各类病毒是与相应种类的系统机在世界上的分布成正比的。研究人员也可以针对这种分类分别对病毒展开反攻。现在看来，大致可以分为三类。

1.攻击INTEL指令系统的依托机型

这里包括IBM PC机及其各种兼容机，包括我国的长城、浪潮、联想等各种国产兼容机。尤其是大麻这类来自主引导区（或称分区）的病毒，它们是与操作系统的种类无关的，因而无论采用什么样的操作系统均有可能被感染上。

由于IBM PC机及其兼容机在世界上的总量超过2000万台，仅我国就有数十万台，因而这类病毒的产生机会与传播途径都是防不胜防的。尤其是这类机器早已浸透到各国的政府、军事、教育、科研等环节中，因而具有很大的危险性。目前在我国盛行的并被公安部“通缉”的几种病毒均是IBM PC机及兼容机病毒。

2.攻击Motorala 6800系列指令系统的依托机型

6800系列指令系统的典型机器是AppleⅡ及大苹果——Macintosh。由于Apple公司在世界微机市场上占有很重要的地位，因而这类机器也不可避免地出现被病毒攻击的现象。如被称为Scores NVIR及Peace（Macmag）的病毒均属于攻击Macintosh的病毒。

据报导，我国已出现了Appla—Ⅱ机的病毒，Macintosh的病毒也很严重。尤其是这类系统的系统功能很强，采用软开关的控制方法，操作系统相对封闭，并且在国内流行时间不长，因而病毒导致死机常常使人束手无策。这类病毒需要有人下力进行研究。

3.攻击源语言的依托机型

这是指直接对病毒源文件进行链接而导致被攻击的情况。显然，这只能在网络环境

下进行，到目前为止，普遍受害的是SUN与VAX类型的系统。例如，举人听闻的Intelnet事件的受害机型就是这类机型。而我国正在运行的联机网络普遍挂接的是这两类机型，因此需要得到高度的重视。

3.1.2 按照依附方式分类

计算机病毒的表现形式也是一个程序，但由于病毒程序的非法性，必须借助合法的手段来启动。因而病毒必须附在操作系统或正常文件之上。根据病毒依附位置来分类，可以有效地掌握预防病毒的本质方法。一般说来病毒可以分为三类。

1.操作系统类病毒

操作系统类病毒是指病毒取代了操作系统的引导模块，而先于安装操作系统进入系统。这类病毒无视操作系统的类型，如DOS系统，XENIX系统等。这类病毒是通过占据操作系统引导区而被激活，同时还保存了引导区的副本以便保证系统能够被引导出来。如现在流行的大麻病毒、小球病毒、巴基斯坦智囊病毒、6.4病毒等均是此类。

2.嵌入型文件类病毒

嵌入型病毒是指将病毒嵌入到正常的文件之中。这种病毒常常难以识别，难以剥离出来，但侵害范围小。

嵌入型病毒有两种来源，一种是来自源码病毒，即在网络上用高级语言编的病毒程序，提供给用户调用链接，其结果则将病毒侵入到程序中，其中C语言较为普遍。显然，要清除病毒则需要废除整个文件。另一种是针对某种特定文件而生成的病毒。因而只有特定的文件才能对文件的程序结构进行了解并改动。然后用这一变型程序来取代所有同名的程序。尽管这种病毒的影响范围小，但消除的方法只能是删除整个程序。

3.文件类外壳型病毒

这是一种最普遍的病毒，如流传甚广的扬基（Yankee Doodle）、瀑布（1701/1704）、维也纳（Vienna/648）、耶路撒冷（Jerusalem）等病毒均属此列。这类病毒使得文件加长，附在文件的前端或后端，第一条指令一定是指向病毒，或属于病毒体，使病毒能够在文件执行之前进入系统。

实际上，这些病毒还可以分成两类。第一种称为操作系统类病毒，后两种称为文件型病毒。这个分类方式非常有利于对病毒的进一步分析，这将在后续章节中提及。

3.1.3 按照环境进行分类

计算机病毒的显著特点在于其传染特性。不同的环境传染方式不同，所应采取的预防措施也就不同。一般来说可分为两类。

1.单机病毒

这是一种通过软件交流的方法进行传染的病毒。国内目前发现的主要是这类病毒。这种病毒往往出于对软件所有权保护而流传开的。其载体是磁盘，如果不使用来历不明的盘，或未经安全认可的文件，则可以有效地预防该类病毒。

2.计算机网络病毒

计算机网络的传播媒介不再是移动式媒体，而是网络通道，这种病毒的传染能力强，破坏力大，有效的防范措施是严格执行网络协议，对不明身份的信息包不预接收，以免受害。

3.1.4 按照操作系统类型进行分类

计算机病毒是利用了操作系统的漏洞而出现的破坏性程序，因而无论采用何种机型，相同的操作系统所面临的病毒则是带有共性特征的，因而根据这种分类，可以从操作系统的薄弱环节着手，来防范病毒，从而达到在其它种机型中举一反三的功效。目前所流行的有4种。

1.基本I/O系统病毒

这类病毒是利用驻留的ROM BIOS与磁盘操作系统的界面协议的开放性而炮制出来的。如IBM PC系列的ROM BIOS与磁盘操作系统的协议是在内存低端的中断向量表、ROM参数区及ROM通信区。ROM BIOS向磁盘操作系统交递控制权的唯一方式，是将当前盘的0头0道1扇区的内容读出，送至0：7c00处，然后转向该起始点。由此病毒占据了这个位置而截获了控制权，如OHIO、TYPO等病毒。

2.MS—DOS/PC—DOS类病毒

这是利用MS—DOS/PC—DOS创建进程的方法来进行传染。即修改操作系统创建进程的工作方式，将传染病毒的工作过程嵌入其中，从而每次创建一个进程，病毒即将自身复制到被创建的程序上。由于这类操作系统的进程创建采用的是INT 21的功能4B，因而这类病毒普遍修改这个控制向量。如Sunday、Payday、MIXL等。

3.Macintosh—DOS类病毒

这类病毒也是以传染应用程序为主。如按攻击对象分类的攻击6800类指令系统类的例子。

4.UNIX类病毒

这类病毒主要出现在网络环境中，病毒利用UNIX的漏洞来侵入系统，如Berkeley，UNIX4.3版本有着三个漏洞：a.通过Sendmail中的程序故障使调试位置呈通态。b.在fiagel程序的一部分中使缓冲器过载，使之对病毒程序的另一部分进行编译链接。c.通过获取口令进入系统。由此切断系统的安全功能，而达到使一般程序复制到另一网络用户。通过编译连接运行，吞食二进制文件，并不断地扩散。如IBM的圣诞树、FO—SHOI4、UNIX蠕虫等病毒。

3.1.5 按传染方式分类

计算机病毒的传染过程有其特定的途径。这种途径是病毒起作用的关键环节，掌握这一环节则可有效地扼制病毒的扩散。一般来说，可以分为三类。

1.引导区类病毒

这类病毒是藏在磁盘系统的引导区中，利用ROM BIOS所提供的控制权转变协议来截获控制权，从而可以进行驻留，当执行磁盘操作时即可传染。如Alameds、磁盘杀手、幻影病毒等。

2.文件类驻留型病毒

这种方法是将病毒链在文件前或后，通过执行附有病毒的程序即可将病毒激活，使病毒得以驻留内存，以便以后可创建一个进程，均将被创建程序传染上病毒。如哥伦布日、荷兰、Flips等病毒。

3.文件类不驻留型

这种方法是将病毒链在文件的首部或尾部，通过执行附有病毒的程序，即可将病毒激活，使其发作。这类病毒是针对防止内存驻留不明程序的抗病毒系统而编制的。其特点在于运行一次只传染一个文件。如Amstrad、Do—Nothing、Lisbon、Vienna等病毒。

3.1.6 按破坏情况分类

计算机病毒分为传染部分与发作部分。传染部分是各病毒的共性，而发作部分则各有所不同。这往往是依赖编程者的动机。因而可分为良性病毒、中性病毒和恶性病毒三类。

1.良性病毒

良性病毒是指那种对系统没有危害的病毒。这类病毒往往是出于编制者的展示其高超技巧的心态，一般只在屏幕上给予一些提示，或给出一些特定的画面，但对系统自身是无影响的。如小球病毒，只是定时出现一些球状正弦曲线的图案，并不破坏系统。再如苹果病毒，每当发作时就显示“我要吃苹果”，只要键入“苹果请”，即可继续运行。

2.中性病毒

所谓中性病毒只指处于良性病毒与恶性病毒之间的病毒。这种病毒从主观上没有破坏系统的恶意，但在客观上却由于其占用系统资源而影响系统的正常运行。如Yankee Doodle病毒的发作过程仅是奏Yankee Doodle音乐，但这个病毒的存在，则影响2.13汉字系统的正常启动运行，同时也影响LISP语言的读、写盘的操作。再如大麻病毒，本来是出现在硬盘分区中的病毒，其额外占用的是硬盘中的保留扇区，不影响系统。但由于对INT13的修改，无法正常运行格式化软件。而其对软盘高密盘的破坏也是由于软盘中无保留扇区，因而征用双密盘的目录区的最后一个扇区。但所对应的物理头、道、扇区恰好是高密盘的目录区的第三个扇区，因而当高密盘的文件超过32个则被破坏。这应该说是一种巧合。

3.恶性计算机病毒

恶性计算机病毒以破坏系统为目的，因而常常使计算机系统被破坏得无法恢复。这个现象从几个方面表现出来。

①破坏数据区，即病毒在发作后随机向磁盘数据区执行写操作，使得数据被破坏。

②破坏重要参数区，即将磁盘的重要参数区，如目录区、文件分配表等进行破坏。

③破坏引导区，使系统无法引导。即向引导区写随机信息，使得系统无法引导。

④破坏网络的正常工作，大量地向网络发送信息，使得网络阻塞而无法正常运行。

⑤破坏磁盘介质，反复向某一道读写信息，使得该道被超常使用而损坏。

⑥破坏硬设备，如磁盘驱动器、喇叭、屏幕等，即反复采取极限做法使得硬设备超负荷使用而失效。

流行于我国的典型恶性计算机病毒，是号称为磁盘杀手的PC机操作系统类病毒。这种病毒寄存在引导区，并将其余部分隐藏在分区的后半部。该病毒在破坏计算机前没有任何症状，从而使得用户得不到警告而毫无查觉，在发作时，屏幕上将出现这样的显示：

Disk Killer—Version 1.00 by COMPUTER OGRE 04/Q1/1989