计算机病毒与安全及解计算机病毒的方法实例专辑

中国科学院成都计算机应用研究所情报室

前　言

自从美国首先发现计算机病毒以来，世界上许多国家（包括我国）和地区均发现了计算机病毒的侵扰。计算机病毒对于计算机的致命攻击，在于它的破坏性和传染性，但只要了解病毒的原理、分析其病毒产生的原因、病毒的防止和解毒也是不难的。为了防止计算机病毒的侵扰，促进计算机的应用和技术交流，我们广泛搜集了近期的最新资料，编制成《计算机病毒与安全及解计算机病毒的方法实例专辑》供广大计算机用户参考。该书内容丰富、新颖、具有较高的实用价值，是广大计算机应用工作者研究和防止及消除病毒的不可少的工具，也是一本难得的内部参考性的情报资料。

全书内容有：计算机安全、数据保护、计算机病毒的概念、原理、产生病毒原因，病毒的类型、病毒的分析、测试、防止和解计算机病毒的方法实例及程序等。

在资料的汇集中，得到了广大作者的热烈支持。有个别作者因地址不详未征求到意见，敬请原谅，有不妥的地方请批评指正。对全体作者积极支持此工作，表示衷心感谢。

由于水平有限及时间关系，搜集的资料还不很完全，错误难免，敬请读者指正。

该书在编辑的过程中受到了罗淳、孟晓玲、单永涛、敬奇等同志的支持，在此表示感谢。

该书由杨明芳、周永培统编

编者

990年4月16日

计算机病毒与安全及解计算机病毒的方法实例专辑

目　录

计算机病毒原理与预防

计算机病毒的分析及检测

解计算机病毒的方法及实例

计 算 机 安 全

数 据 保 护 与 恢 复

计算机病毒工作机理及防范技术探讨

侍永新 （中国矿业大学）

编者按：计算机病毒在世界上蔓延以来，目前人们发现的达44种之多。病毒已经受到了计算机界同仁的广泛重视。在国内，继小球病毒出现以来，又出现了一种新的传染范围较广的“大麻”病毒（或称Stone病毒）。本报虽然在去年先后发表过一些有关计算机病毒的消息和文章，但涉及大麻病毒的很少。为帮助我国用户早日排除大麻病毒造成的困扰，我们再次编辑了这期计算机病毒的专辑。以后我们还将陆续介绍“黑色星期五”、“数据犯罪”等有关病毒的解决方法。（编者：计算机世界报编辑部）

无论是对计算机专业人员还是非专业人员来说，计算机病毒已是一个十分热门而又非常令人头痛的问题了。计算机病毒危害性极大，在二十一世纪国际恐怖活动采取的五种新武器中，计算机病毒名列第二，所以计算机病毒越来越引起人们的关注。本文旨在系统地探讨计算机病毒的工作机理及防范技术。

计算机病毒的概念、特点及分类

计算机病毒是借用了生物病毒的概念。计算机病毒同生物病毒一样，也是能够侵入计算机系统和网络、危害其正常工作的“病原体”。它能对计算机进行各种破坏，同时还能够自我复制，同生物病毒一样，也有可能具有传染性。那么，到底什么是计算机病毒呢？到目前为止，还没有一个公认的概念。目前使用较多的是科恩(Frcd Cohen)下的定义，即计算机病毒是一个能够通过修改程序，并把自身的复制品包括在内去“传染”其它程序的程序。

笔者认为，科恩的定义并不完善，因为它没有完全揭示出计算机病毒的本质。那么，计算机病毒的根本性质是什么呢？这就是潜伏性和破坏性。计算机病毒可能在你不知不觉中侵入你的计算机系统潜伏起来，过一段时间再发作，进行破坏。《计算机犯罪》这本书记有这样一件事：某个银行职工在计算机管理程序中插入一小段程序，检查它的名字是否还在档案中，如果不在，则破坏系统，结果在他被炒了鱿鱼之后，银行数据也遭到了破坏。笔者认为这也属于计算机病毒的范畴，因为它具有某些生物病毒类似的性质，同时对计算机资源起到了破坏作用。综上所述，给出计算机病毒的概念：所谓计算机病毒就是能够通过某种途径潜伏在计算机存储介质（或程序）里，达到某种条件即被激活的具有对计算机资源进行破坏作用的一组程序或指令集合。

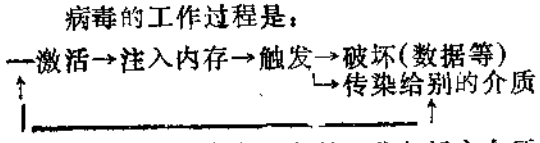
计算机病毒一般具有下面几个特点：①破坏性。从理论上讲，破坏性是无法衡量的。因为凡是由软件手段能触及到计算机资源的地方均可能受到计算机病毒的破坏。具体地讲体现在三个方面，a.占用CPU时间和内存开销，从而造成进程堵塞；b.对数据或文件进行破坏；c.打乱屏幕的显示。

②隐蔽性。病毒程序大多夹在正常程序之中，很难被发现。③潜伏性。病毒侵入后，一般不立即活动，需要等一段时间，条件成熟后才作用。④传染性。对于绝大多数计算机病毒来讲，传染是它的一个重要特性，它通过修改别的程序，并把自身的拷贝包括进去，从而达到扩散目的。

计算机病毒的分类方法很多。根据其表现性质可分为良性的和恶性的。良性的危害性比较小，可能是在屏幕上进行一些无意义的显示如国内出现的小球病毒就是良性的；恶性病毒可能会毁坏数据或文件，也可能使计算机停止工作。按激活时间可分为定时的和随机的。定时病毒仅在某一特定时间才发作，而随机病毒一般不是由时钟来激活的。按工作机理分为初始化病毒，程序入侵病毒和操作系统级病毒。按是否有传染性可分为不可传染性和传染性病毒。不可传染性病毒有可能比传染性的更具有危害性和难以预防，这种病毒的编制者往往就是计算机系统的程序设计者或维护者，且大多数带有报复性质。由于绝大多数病毒具有传染性，所以下面仅讨论这种病毒。

计算机病毒工作机理

病毒的工作过程是：



可以看到，病毒的完整工作包括六个环节：传染源或本体、传染媒介、激活、触发、表现、传染对象。传染源和传染对象可能是一致的，也可能不一致，但它们都依附于某些存储介质，从广义上看，网络中的计算机也属于此列。传播媒介可能是计算机网，也可能是可移动的存储介质如磁盘。激活指将病毒装入内存，并设置触发条件，一旦触发条件成熟，病毒就开始作用——自我复制到传染对象中，进行各种破坏活动等。激活和触发也可能是同一过程，即计算机病毒，且被激活，立刻就发生作用，激活的条件可能是某个程序的一次执行或系统的初始化。触发的条件则是多样化的，可以是内部时钟、系统的日期、用户标识符，也可能是系统的一次通讯等等。表现是病毒的主要目的之一，有时是屏幕上一句"善意的问题"，有时则能破坏系统的全部数据，如前所述，凡是软件技术能够触及到的地方，都在其表现范围。目前大部分恶性病毒的表现是毁掉硬盘的数据或使系统执行崩溃。病毒的传染是"病毒性能"的一个重要标志。在传染环节中，病毒复制一个自身副本到传染对象中去，同时修改之，以便于病毒能被激活。

结合上述环节，下面谈谈病毒的几种工作机理。

1. 病毒植入磁盘引导扇区中

任何操作系统都有个自举过程，例如DOS在启动时，首先由系统读入引导扇记录并执行之，将DOS读入内存。病毒程序就是利用了这一点，自身占据了引导扇而将原来的引导扇内容及病毒其它部分放到另外的磁盘空间，并给这些扇区标志为坏。这样，系统的一次初始化，病毒就被激活了。它首先将自身拷贝到内存高端并占据该范围，然后置触发条件如INT13H中断（磁盘读写中断）向量的修改，置内部时钟的某一值为条件等。最后引入正常的操作系统。这时一旦触发条件成熟，如一个磁盘读或写的请求，病毒就被触发。如果有磁盘没被感染（通过标志识别）则进行传染，方法如本节开始所述，然后就进入表现部分。

2. 病毒寄生在可执行程序中

这种病毒寄生在正常的可执行程序中，一旦程序执行，病毒就被激活，于是病毒程序首先被执行，它将自身常驻内存，然后置触发条件，也可能立即进行传染，但一般不作表现。做完这些工作以后，开始执行正常的程序，病毒程序也可能在执行正常程序之

后再置触发条件等工作。病毒可以寄存在原程序的首部也可以寄存在尾部，但都要修改源程序的长度和一些控制信息（如重定位信息），以保证病毒能成为原程序的一部分，并在执行时首先执行它。这种病毒传染性比较强，它也可能对网络上其它用户进行传染。这包括两方面，一方面是其它用户用该程序而被传染，另一方面病毒也可能会主动出击去传染其它用户，当然这需要更高的技术和手段。

3. 操作系统级病毒

笔者认为这种病毒是可能出现的。这种病毒修改操作系统本身，使病毒成为操作系统的一部分，只要机器工作，病毒就处在随时可能被触发的状态。现代操作系统的开放性和不绝对完善性给这种病毒出现的可能性提供了基础。它在传染方面也可能利用操作系统提供的性能，进行网络上大量的复制工作。去年使ARPA网陷入瘫痪的那种病毒和该方式有点类似，它的传播就是抓住了Berkeley Unix 4.3的三个漏洞，可以以三种方式侵入系统，通过Sendmail中的程序故障使调试位置呈通态；在finger程序的一部分使缓冲器过载，使之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。该病毒切断了系统的安全功能，把一段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 这样不断扩散最终使用户网络瘫痪。不过，到目前为止还未出现与操作系统融为一体的计算机病毒，一旦出现，将是场可怕的灾难。

计算机病毒的防范

人们对于各种各样的病毒，不得不设法防范。所谓防范不外乎包括三个方面：①预防，②检查病毒的存在，③病毒的根除。

病毒的预防就是保护传染对象不受病毒的传染，将之拒之门外。从理论上来说，计算机病毒在技术上是不可预防的，因为计算机病毒实际上就是一个程序，这样凡是由软件手段能触及到的，病毒也应能触及到，而且，任何系统的保护措施只能用软件方法保护，否则就会影响系统的性能。不过，对传播对象进行一些有限的保护还是可能的。针对第二种机理，我们可以给执行程序加密，病毒程序使侵入，经解码也会面目非，无法发挥作用。

在实际中，人们提出一些限制传播途径的预防手段如“四模型”理论即基本的限制、分割模型、流模型、限制解释。这种理论实质就是限制控制权限和相对地隔离用户。理论和实践都证明，要根本地防止病毒就要求系统绝对地隔离才行，即完全切断传播途径，绝对的隔离要求用户不使用任何软件，因为你无法证明你所使用的软件没有病毒，这是不可能的，即使在现有系统情况下，也不能不和外界进行软件交流。不过我们可以采取有限的隔离措施来预防病毒的侵入。事实证明这是有效的，基于隔离的措施主要有两方面：管理上的和技术上的。管理上要求不使用来历不明的软件、不使用公告板上的程序以及加强系统的维护（如备份）等其它措施。从技术上主要限制用户的权限、限制数据在网络上流经的结点个数等。

尽管单用户比网络用户传染的机会要少，但在我国，软件的版权概念淡漠、软件相互拷贝随意进行，所以这种情况下病毒传染的危险性并不亚于网络，希望同行们重视这件事。

由于计算机病毒难以预防，所以我们不得不设法找出系统中的病毒并根除之。事实上，根除一种病毒并不是件非常困难的事，难的是如何发现它—尤其是在它发作前。由于大部分病毒并不是一侵入就开始作用的，所以在潜伏期内将它检查出来是可行的。一种理论认为，这个问题是不可判别的，因为判别程序也有可能被感染。但由于病毒很少

破坏它所寄生的程序(除非是一次性毁坏)，因此在实际中还是可行的。已有不少人研制出反病毒程序，不过大多只能对付一种已经出现了的病毒。日本的小一正香研制的反病毒程序据称可以对付好几种病毒。

检查的技术可分为静态检查和动态检查。静态检查试图在潜伏期内搜查出病毒的存在。静态检查一般限于备份和比较或程序长度的检查。静态检查难以测试程序的代码，因为病毒的代码和正常程序的代码并没有什么本质的不同。动态检查的目的是测试是否有病毒程序正在运行，主要检查用户是否超越权限、口令是否被截取或其它一些异常情况。动态检查也有其缺点：占用CPU时间、容易判断失常，不能完全检查出病毒来等。在“通用性”检查程序方面，目前还是个空白，有待于广大计算机工作者去填补。

针对我国的情况，笔者建议用下列简单有效的方法作为预防和检测手段。第一，选定一种操作系统，将引导扇内容作为数据保存起来，每次开机后检查启动盘引导扇和原引导扇内容是否相同，如不同则报告用户。由于不同厂商提供的同一版本的操作系统引导扇往往也不同。所以要求用户使用同一启动盘（可选用硬盘）。这种就杜绝了第一种病毒侵入的可能性。第二，经常检查一些常用可执行程序的长度（可通过程序方法来检查），以检测到第二种病毒的存在性。第三，对可执行程序采取一些简单的加密，防止程序被感染。根除病毒是针对某一具体的病毒进行的，方法有二，一是彻底清除之，使之消失，二是对它进行修改，使之无法被激活。

最后，笔者想引用某一权威人士的话作为本文的结尾：“计算机病毒如同爱滋病一般，唯一有效的预防方法就是洁身自好！”

文献出处：《计算机世界》1990年2月7日

计算机病毒浅谈

汪亚男 （电子科技大学）

摘要：本文由计算机病毒的含义谈起，结合国内外动态，系统地论述了计算机病毒的有关主要问题。论文共包含六个中心内容：从病毒特性、分类，乃至病毒的消除及予防。文章联系实际，予以详细论述。旨在使读者能对计算机病毒建立完整的概念和科学的态度。

关键词：计算机病毒 磁盘操作系统（简写：DOS） 扇区 介质 软盘 数据网络

正当计算机科学日新月异地飞速发展，利用计算机为人类源源造福时，一个新的研究课题严峻地摆在我们面前，这就是计算机病毒。

从七十年代开始，世界上一些计算机技术较为发达的国家，首先发现计算机病毒。在八十年代，我们国内也相继出现计算机病毒。从而，它成为计算机领域内的热门话题。尤其在近一、两年来，探讨和研究者日渐增多。

89年10月24日，成都晚报刊载一篇短文中叙述，自从新华社报导《“电脑病毒”在欧洲引起恐慌》的消息后，使一些人产生了疑虑，国外电脑有那么多带有病毒，我国已经生产和引进了许多电脑，且不少家庭有带电脑的彩电、冰箱等，那末，会不会传染上

电脑病毒呢？

从这则消息反映出，在我们周围的环境中，有一部分同志对计算机病毒还不够了解，比较陌生，因而，思想上产生了一些误解和疑虑。究竟什么是计算机病毒？请看本文介绍。

一、名称的由来

计算机“病毒”并非真正是医学上所指的、日常生活中存在的某种生物病毒，它之所以如此称谓，是因为它具有病毒的特性。众所周知，生物病毒能够侵入人体及其它生物体内，能感染健康的肌体并大量繁殖、衍生后代，最后导致生物死亡。

计算机“病毒”指的是进入计算机数据处理系统的错误信息。它是有意安放在计算机软件上的一段程序或者是一组指令；它具有再生能力，在计算机运行中秘密传播，是一个可以通过修改别的程序把自身复制在内去传染其它程序的程序。由此干扰其它程序的运行，破坏计算机的正常运转，所以称它为计算机“病毒”，也叫“软件病毒”

二、“病毒”特性

通过让计算机“病毒”运行，打印汇编语言程序清单，可以观察到“病毒”的特性。

- 可传播性：不同的计算机“病毒”，其传播介质也不尽相同。例如，在计算机网络系统中，“病毒”传染的渠道，可能是通过数据网络的实体或者互连网络进行扩散；而在未联网的单用户微机系统中，则主要传播介质为磁盘。在带有“病毒”的计算机上，对无“病毒”软盘执行列程序清单指令，该软盘立即被感染；反之，只要使用带有“病毒”的软盘启动系统时，无“病毒”硬盘也立即染上“病毒”。总之，有的传染软盘（如“Brain”病毒），有的传染硬盘（如“硬盘”病毒，攻击对象为硬盘）根据传染性，每个受感染的程序又可能成为一个新“病毒”，继续再传染，呈连锁反应。
- 自我复制：“病毒”有自动进入相关程序中进行自我复制的能力。例如，自我复制到用户软件或操作系统中去。

三、“病毒”种类及危害

计算机“病毒”种类很多，按其性质可分为恶性、良性两大类。不同“病毒”，表现症状不同：有的可在计算机屏幕上直观；有的是使计算机系统内部产生异常现象；有的则潜伏一段时间后方才发作，等等。

- 恶性：带有蓄意破坏之目的，有意利用计算机病毒报复。例如，有一起病毒事例，起因是1名程序员因被公司解职，大为不满，企图报复，于是秘密输入一个病毒程序至计算机，此程序在五年后才发生作用，但其后果相当严重，造成整个计算机作业系统混乱，后来费了很大力气，才找出这个病毒程序。
- 良性：这是出于另一种目的，人为制造的一类病毒。例如，“Brain”病毒是在美国一大学发现，它是由一名程序员编写的。其本意是用“Brain”（汉语：“大脑”）来跟踪对他编制的软件进行非法复制者。所以，他有意使得其它任何软件盘的标题上标有“Brain”字样。
- 二元性：这类病毒性质介于上述二者之间。它由两部分组成，其每一部分，皆是无害的，但是若二者同时用在同一系统中，并结合起来之后，则变为有毒的了。

近年来，国内发现一种计算机病毒，名叫“小球”病毒。它所攻击的对象是单用户微机，如IBM-PC系列及其兼容机。据分析，此“病毒”属于良性，但不论是否处于激活状态，传染性都很强，其表现形式是在计算机屏幕上出现做弹跳运动的小球字符，运动轨迹很象台球桌上的台球运动方式，遇到碰撞发生弹跳或翻转。

综合上述，无论属何性质的“病毒”，总是有害的。如“Brain”，虽为良性，但也具有很大破坏性。当该“病毒”未被激活时，可以保留在软盘上，暂时无恙；一旦被激活之后，就会破坏磁盘上的文件分配表，后者是用来向操作系统提供磁盘上文件位置的信息，因而，当文件分配表受损后，磁盘文件也会遭到破坏。

“Brain”和小球”这类良性”病毒”，危害性主要是破坏屏幕显示，例如在屏幕上显示台球运动或显示一条消息，或者是杂乱无章的信息及图象等。此外，使磁盘操作速度变得很慢，占用CPU资源，或产生伪操作、假报警等。

至于恶性“病毒”所带来的影响，更是无法估量的，因为目前许多重要信息资源皆集中存贮在计算机中。在此，不作赘述。

四、“病毒”传染原理与过程

“小球”病毒是通过磁盘相互传染的。它能传染使用PC DOS或MS-DOS的IBM-PC/XT/AT及其系列机。感染的含义一是传染给别的程序，一是自身繁殖。例如，通过列文件清单、系统执行读盘操作皆可能引起感染，当带“病毒”的软盘插入计算机系统时，“病毒”程序首先自动将自己复制到主机内存的最高地址空间，占用2K字节。该“病毒”程序将磁盘上的原DOS系统引导程序（即0扇区内容）替换成自身的“病毒”程序，随后并插在磁盘操作服务程序或用户程序之前。

下面以“Brain”病毒为例，介绍它的传染过程。

“Brain”病毒程序共有4100字节，实际使用仅为一半，故是2K字节。

DOS操作系统在正常启动时，是将磁盘引导扇（即引导程序所占扇区）读入内存中0：7C00H处，并执行引导程序，使系统工作。而“病毒”程序在此之前，先初始化入口及所需参数。从磁盘文件分配表中找到一个空闲簇，并将对应的簇号记于“病毒”程序的特定单元。然后把原DOS引导程序从引导扇中转移到访空闲簇的簇号及内存最后两个簇所对应的扇区（共6个扇区）中，“病毒”将这些扇区列为“坏”扇区，而将“病毒”程序的初始入口及参数写到原DOS引导程序所占的扇区。也就是说，“病毒”程序占据磁盘中原DOS引导程序所占的扇区，而原DOS引导程序被移至别处。这样，原来无“病毒”软盘就被感染。此时，当被感染的磁盘操作系统运行时，则先将“病毒”程序读入内存，而后才去读原来的DOS引导程序。读入的“病毒”程序，存放于内存的最后2K字节，这就完成了一次感染。当进行读操作时，就有可能干扰本机或向外传播。

实验证明：若使用DOS-2.0，“病毒”程序将修改中断向量INT08H；若使用DOS-2.1，“病毒”程序将修改INT13H；若使用DOS-3.1，则修改引导程序。

五、“病毒”检测

为了检测磁盘是否受到感染，可用CHKDSK命令或PCTOOL工具来进行。

若磁盘已被感染，可有下列迹象：

- 屏幕上出现小球字符（设为“小球”病毒）或杂乱无章信息；
- 磁盘上的0扇区内容被替换。这可从比较无病毒磁盘与有病毒磁盘的0扇

区，则能发现该病毒将磁盘上的原DOS引导程序替换成“病毒”程序。

- 磁盘上有一簇（此为磁盘分配单位，在软盘中，一簇为两个扇区）被标记为“坏”扇区，恰占1K字节。此时可发现，磁盘容量刚好减少1K字节。若磁盘未被感染，则该盘的输入/输出参数必须为：1个扇区长512字节，每簇则应由两个扇区组成。
- 通常，欲对磁盘传染的“Brain”病毒，将要搜索被标为“坏”的三个连续的簇。若盘上没有空闲簇，病毒程序将不传染给磁盘；若有一个空闲簇，并且不是最后两个簇，则“病毒”将选择这个空闲簇连同随后两个簇一起重写，并将这三个簇（6个扇区）标为“坏”扇区。被重写部分，若是指令，则将不再被执行；若是数据，则不再被读出。利用这种方法也可判断磁盘是否已被感染。

六、病毒的消除及预防

计算机系统资源共享与病毒防护，二者是有抵触的，由于资源共享，增加了病毒传染的危险性。

由经验得知，病毒的传染，必须要执行读盘操作。若现行操作盘有“写保护”，或者磁盘剩余空间不足1K字节，或者读写盘出错，都将抵制病毒传染。

此外，某些类型的软盘，天然具有免疫能力。例如，那些格式化成盘空间分配量是以一个扇区为一簇的软盘，它们都能抵抗感染。

对于非系统软盘，因为不能用来直接启动系统，即使染上病毒，隐藏在引导记录模块中的病毒程序没有机会执行，因此，传染病毒的危险性较小。

（一）消除病毒的途径

- 恢复DOS引导扇：既然病毒程序修改了原操作系统DOS引导扇，当然只要恢复原来的DOS引导扇，就可消除病毒。

从病毒程序读取原DOS引到程序所在簇号，读取该簇内容，并写回到DOS引导扇，这样就恢复了DOS引导扇。然后在磁盘文件分配表中找到该簇号对应的内容，将其清零，从而释放“病毒”程序所占的磁盘空间。

- 利用DEBUG程序恢复DOS引导扇

设对A驱动器中的软盘操作，所用的计算机应是未受感染的，机型为0520型或IBM-PC系列。首先读入A盘0扇区内容，取病毒程序所在扇区号；读入病毒程序及原DOS引导程序；给原DOS引导程序加上免疫标志；恢复磁盘上原DOS系统引导程序。

- 研制出能够正确测定正常程序起始位置的软件工具，以便消除病毒。
- 对于良性病毒还可以采用：使用无病毒系统软盘，重新引导启动系统。或者关机后再启动，皆可以恢复正常工作。

（二）予防病毒的措施

对于计算机病毒应该积极予防。措施如下：

- 研制“疫苗”软件

所谓“疫苗”软件，就是加入计算机系统的自动处理软件。当系统启动后，首先执行“疫苗”软件，用来检查磁盘是否已被感染，若已感染，则运行解毒程序。这样，未等到传播就把病毒消除。

- 贴“写保护”

贴“写保护”是个好办法。若没有染上病毒的系统盘，贴有写保护，则该盘不会被感染。

- 使用固定盘做启动盘，把暂时不要写

入的软盘，贴上“写保护”。

- 不要随意拷贝或运行任何未经正式许可的软件。
- 不要随意拷贝游戏盘。因为游戏程序为了防止他人拷贝，制作者很可能在盘中夹有病毒程序。例如，MACINTOSH计算机游戏程序盘酿成的病毒灾害，就是一个先例。
- 将文件加密存贮。对可能坏的扇区要加以保护，并将程序加密。运行前再进行解密。
- 使用MS-DOS（或PC-DOS）3.31以上的软盘，这些操作系统已具有自动免疫能力。
- 新软件在使用前，要通过带有隔离的双驱动器的机器中检查，以控制病毒传染。

以上所述表明，当前计算机病毒的出现已对计算机信息系统的安全带来威胁。因此，研究和解决计算机病毒问题并非杞人忧天，而是形势的需要。同时，还应该看到：随着计算机软件功能日渐复杂和软件应用日益广泛，计算机病毒程序本身的设计技巧也会愈加精湛和多样化，这给解毒和抗毒增加了难度，更难找到能治百病的“万灵药方”。特别是，当计算机走向网络化时，计算机病毒，尤其是隐含在网络中的病毒更具有危险性。

九十年代的第一个新春即将到来，回顾我国科技领域取得的巨大成就，展望我国科技发展的未来远景，我们精神振奋，正满怀信心地跟踪世界科技发展动向，近接计算机领域的这一世界性挑战！

参考文献（略）

文献出处：《计算机应用》1990年，第1期43—46页

一种传染性极强的计算机病毒

王祖林　（北京航空航天大学电子工程系）

计算机病毒已侵入我国，这并非耸人听闻。笔者所在单位，有相当数量的IBM PC系列及其兼容机已遭某病毒感染，如不采取措施，剩下的机器受感染也只是时间问题。该病毒传染性极强，对我国用户危害特别大。

该病毒不论是否处于活跃状态均具有传染性。当其处于活跃状态时，屏幕上出现一遵循反射定律的动态小球字符（ASCII码为07），很象台球桌上台球的运动方式。对西文DOS的用户，影响不是很大，但对中文DOS用户则产生很大影响。若用户使用的是汉卡，即使显示内容不动，也将会被该病毒显示的小球字符弄得面目全非。若用户使用的是显示11行汉字的CCDOS，整个显示内容将由于小球字符的显示而上窜下跳，根本无法正常运行用户程序。该病毒的另一危害是使磁盘操作速度变慢，有时达到令人难以忍受的地步。

鉴于问题的严重性，笔者已研究出消除该病毒以及给磁盘加上免疫能力的方法。

可以用PCTOOLS来检查磁盘是否受到感染。若磁盘已被感染，你能发现磁盘上有一簇（磁盘分配单位）被标记为坏。对软盘而言，一簇是两个扇区。另外，磁盘上0扇区内容被替换，这个可以通过比较一下健康的磁盘与被感染后的磁盘两者的0扇区内容来确定。不过，如果你的计算机上已发现屏

幕上偶尔出现一乱窜的小球字符，就几乎可以断定你所使用的操作系统已被感染。

该病毒将磁盘上的原操作系统引导程序（即0扇区内容）替换成它自己的程序。它在一开机时，就修改主机内存大小，将最高端2千字节据为己有，随后在操作系统磁盘操作服务程序前插入一段程序。这样，用户所有的磁盘操作都置于它的监视之下，一旦它发现了还未被感染的磁盘，它便将自身复制到那个磁盘上去，完成一次传染。当被感染的操作系统运行时，该病毒时刻在寻找苏醒的机会。在计算机运行中，每隔半小时就有约一秒的危险期。在危险期中，若用户执行磁盘读操作，该病毒便开始苏醒。它将一段显示程序插于系统时钟中断服务程序之前。这样，屏幕上将以每秒18次的速率显示小球字符。

下面给出消除该病毒以及给磁盘加上免疫能力的方法。假设是对A驱动器中的软盘进行操作。下面的〈CR〉是回车键。

该方法目前已经在如下环境下使用过：GW-DOS2.0/2.1,MS-DOS2.0/2.1,3.1，机型为长城0520CH及原装IBM PC/XT。

消毒方法如下：

```
A>C: DEBUG〈CR〉
-L 100 0 0 1〈CR〉          ；读入A盘0扇区内容
-D2F9 2FA〈CR〉             ；取病毒程序所在逻辑扇区号，其值随磁盘不同而不同
6711:02F9 94 02
-L 100 0 0294 2〈CR〉       ；读入病毒程序及原系统引导程序，共二扇区
-E 4FC 57 13〈CR〉          ；给原系统引导程序加免疫标志
-W 300 0 0 1〈CR〉          ；恢复磁盘上原系统引导程序
-Q〈CR〉                    ；完成消毒工作，返回DOS
A>
```

注意：以上操作要在未受感染的计算机操作系统下进行。另外，被病毒程序侵占的一簇空间也可以收回，方法简单，这儿不再多述。

文献出处：《微计算机应用》1989年5期61—62页

计算机“病毒”的消除及预防

季宗水　裴杰

5月24日，《计算机世界》报第一版刊登了题为《我国相继发现计算机“病毒”程序》的文章，文中提到西南铝加工厂计算中心发现了一种计算机“病毒”，它能感染使用MS-DOS（PC-DOS）的IMB-PC及各种兼容机，且流行极快。就在机电行业内部也发现类似情况，有多台微机受“病毒”侵袭，工作无法正常进展。

通过对被“病毒”感染的计算机磁盘的仔细分析研究，我们目前已完全掌握了此类“病毒”的生成原因和传播途径，并且已研制成功反“病毒”程序，能够严格抑制“病毒”的传播，并能从根本上消除“病毒”。

为了使已受感染的计算机早日恢复正常

工作，给国家和企业减少损失，同时也为了使尚未受到“病毒”侵害的用户能对此类“病毒”有所警惕，减少计算机“病毒”的传染机会，特将我们的研究成果告知广大计算机用户，希望能对大家有所帮助和启发。

一、计算机„病毒”的原理

计算机“病毒”是在计算机内部运行的一种干扰程序，它的运行可引起计算机工作的异常，消耗机器资源，降低处理速度，甚至破坏各种文件及数据，造成机器的瘫痪，给计算机系统带来难以挽回的损失。这种干扰程序，人们之所以称之为“病毒”，原因在于它同一般生物病毒一样，具有多样性和传染性。

计算机“病毒”的多样性在于：不同的“病毒”在发作时，呈现不同的症状，有些可直观察觉，有些则无表面异常，而在系统内部造成异常；还有些“病毒”在不同条件下呈现不同的症状；更有甚者，一些“病毒”在感染时并无异常，而在隐伏一段时间以后才发作。如此种种，计算机“病毒”给人以扑朔迷离的感觉，同时，不同种类的计算机“病毒”的传播介质也不尽相同，这些都体现了计算机“病毒”的多样性。另一方面，计算机“病毒”的传染性是更危险的特性。在计算机网络系统中，它可能通过网络通迅机制广为扩散，而在单机操作中，主要的传播介质则是软盘。由于软盘便于携带，所以“病毒”的传播很易突破地区和部门的限制。

计算机“病毒”的种类虽然很多，但仔细分析起来，其组成一般不外三大部分：即自举部分、传播部分和表现部分。其中，自举部分完成“病毒”程序自身的装入、联接，初始化参数和入口等工作；传播部分将“病毒”传染到健康的机器或介质上；表现部分则完成干扰本机、破坏系统的工作。下面就结合我们遇到的一种计算机“病毒”程序，对这三个组成部分逐一进行分析，并介绍消除的方法。这种“病毒”程序运行于IBM-PC及兼容机上（使用MS-DOS或PC-DOS），是一种单机“病毒”，传播介质是软盘。

1. “病毒”程序的自举部分

大家知道，DOS操作系统在开始启动时，是将磁盘引导扇读入内存中0：7C00H处，并执行引导程序，使系统开始工作，而“病毒”程序在这些工作之前，先要初始化其自身入口及需要的参数，并将全部“病毒”程序读入内存，以备执行，而后才去读原来的DOS引导程序，进行正常启动。图1给出了这一过程，其中虚线框起来的部分，是“病毒”程序增加的操作。

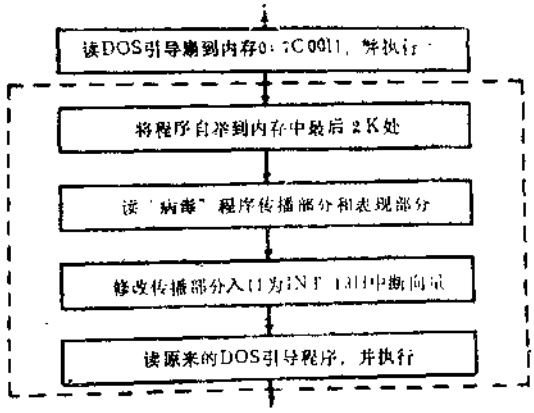


图1 “病毒”程序自举部分工作流程

仔细分析“病毒”程序的自举过程，可以看到：

第一，该程序的自举部分占据了磁盘中原DOS引导程序所占的扇区（软盘为逻辑0道0扇，硬盘视划分情况而定），原来的DOS引导程序被搬到磁盘其它位置。（详见本节第二部分），ROM BIOS只是“机械地”将该扇区的内容读到内存中0：7C00H处并执行，这样就进入了“病毒”程序。

第二，“病毒”程序首先将本身自举到内存中最后2K，留出0：7C00H处的内存

区域，以备而后读入真正的DOS引导程序。

第三，读入“病毒”程序传播和部分表现部分（也在内存最后2K处）。

第四，将传播部分的起始地址作为磁盘中断的中断向量，即修改0：0开始的中断向量表中第13H项（0：4CH）。

第五，读入原来的DOS引导程序并执行。到此，自举完成，“病毒”程序已全部装入内存并准备就绪。随时可能干扰本机及对外传播，但用户此时，也仅仅是感到DOS已“正常”启动，意识不到有丝毫异样。

那么，“病毒”又是怎样传播的呢？

2. “病毒”程序的传播部分

前面已经提到，“病毒”程序的传播部分作为INT 13H的中断处理程序，即每进行一次磁盘操作（调用INT 13H），都有可能引起传播部分的执行，它的工作过程如图2。

传播部分启动以后：

第一，判断此次磁盘操作是否读磁盘，仅当进行读操作时，才能干扰本机或对外传播，这使得“病毒”具有更危险的传染性，一条简单的DIR命令，就会使磁盘受到感染。如果要进行的是其它操作，直接去执行原INT 13H。

第二，在读盘操作时，一旦“病毒”程序认为时机成熟，就启动本机表现程序，使本机的工作无法正常进行，否则，不干扰本机。在用户看来，并不是每次读盘操作都带来干扰，而具有随机性，要想抑制“病毒”的干扰就更加困难。

第三，为了减少重复操作，确保传播完成，“病毒”程序检查此次所读的驱动器是否与上次所读的是同一驱动器，在相同情况下，延迟一段时间（大于换软盘时间）后再准备污染磁盘。对不同驱动器，则直接准备污染磁盘。这时，仅对健康磁盘做进一步的工作，这是通过读入该磁盘的引导扇确定的，即如引导扇中的是DOS引导程序，则视

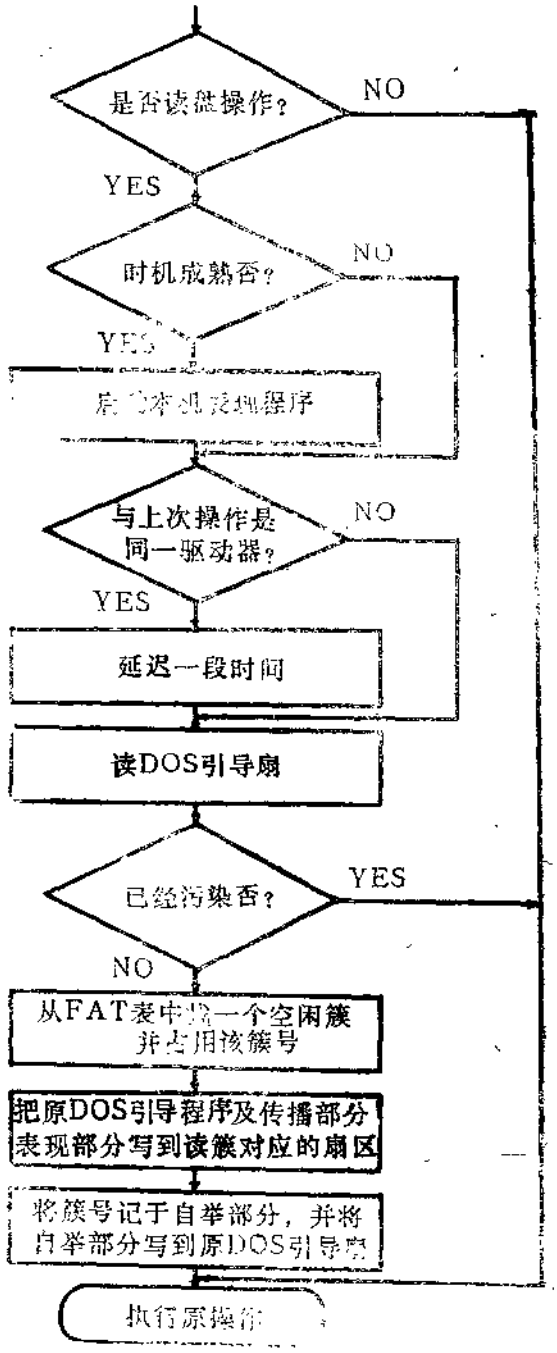


图2 “病毒”程序传播部分工作流程

其为健康，否则认为已染有“病毒”。

第四，具体的传播工作是，从磁盘FAT（文件分配表）中找到一个空闲簇，并将对应簇号记于“病毒”程序自举部分中的特定单元，然后把原DOS引导程序从引导扇中转

移到该空闲簇对应的扇区中，将“病毒”程序的传播部分和表现部分也写到这些扇区中，最后将“病毒”程序的自举部分写到原DOS引导程序所占的扇区（即引导扇）中。这时，健康的磁盘已被污染，并具有了可怕的传染性。

当然，下一步还应进行读盘操作，这使用户看起来毫无破绽。（这里用到计算磁盘簇号的知识，见本文第二部分。）

3．表现部分

这部分程序的目的，在于给本机的工作带来干扰，使其不能正常工作。根据“病毒”的性质，干扰也可分为良性和恶性两种。前者不会破坏机器内的程序和数据，可能的表现形式有破坏屏幕显示内容（如本文开始引用的文章所述），降低机器处理速度，产生伪操作使运算结果出现异常或无故报警等等。

总之，这类“病毒”发作时，只要用正常的系统盘重新引导系统或关机，待彻底消除“病毒”后，还可照常工作。

恶性“病毒”的干扰就不同了。它可能将磁盘上的数据和程序破坏掉。使长期辛苦工作成果毁于一旦，给工作带来难以弥补损失。如这类“病毒”扩散开来，将给受害者带来难以估量的损失。

“病毒”程序的表现方式千姿百态，程序实现也各不相同。如图2中提到的“时机成熟”时启动表现程序，即是利用了时钟中断。

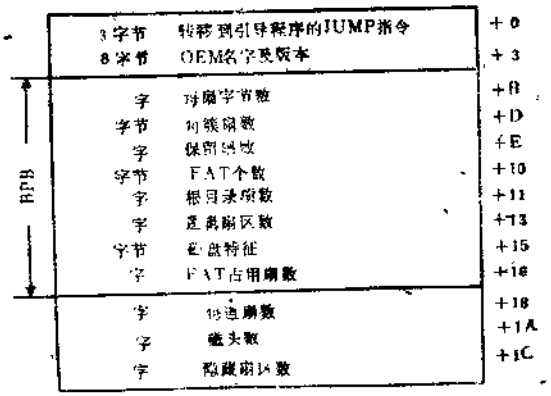
二、“病毒”的消除

了解了“病毒”生成及传播的原理，就不难从根本上消除它了。由于此种“病毒”是通过磁盘传播的，因此在编写反“病毒”程序之前，必须对磁盘结构及分配情况有一个深入的了解。

1．预备知识

介绍“病毒”程序原理时，曾提到“病毒”程序占用磁盘的第一个空闲簇，存放原DOS引导程序等，因此必须了解闲簇，存放原DOS引导程序等，因此必须了解闲簇号的计算方法。

每个DOS格式的磁盘，其最初部分是引导扇，其中包括一张称为BIOS参数块（Bios Parameter Block简称BPB）的表格，表中的参数与引导扇中其它数据一道，描绘了整个磁盘的使用情况，如图3。从DOS用户角度出发，磁盘空间可分为两部分：系统占用部分和文件正文存贮部分，如图4。系统占用部分包括隐藏扇区、保留扇区、FAT占用扇和目录占用扇。隐藏扇区和保留扇区可由引导扇中查得，后两项则可由公式计算求得。



* 磁盘上非DOS占用的扇区

图3 引导扇格式

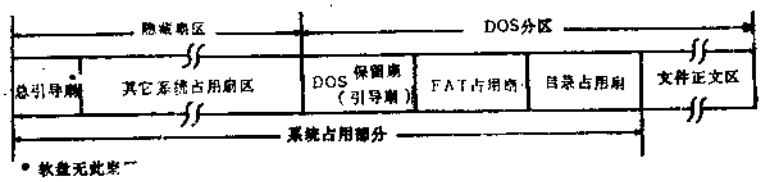


图4 磁盘存贮示意图