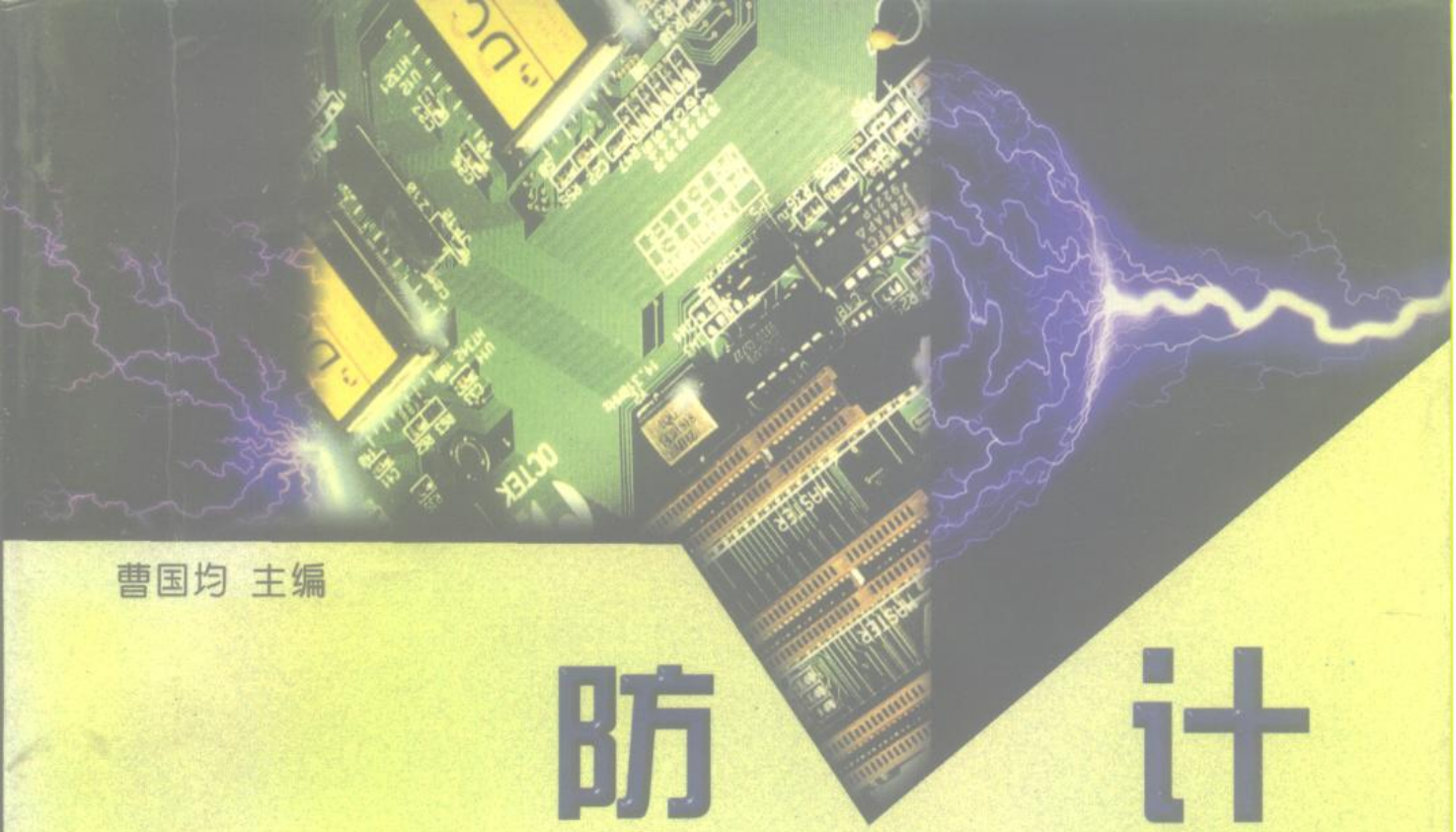

曹国均 主编

计算机病毒防治·检测与清除

电子科技大学出版社

计算机病毒防治、检测与清除

曹国钧　主编

王健　曹旺　田啸　李珊珊　编著

电子科技大学出版社

内 容 提 要

计算机病毒虽然可怕，但是只要掌握了防治、检测与清除病毒的方法，就可以在发现病毒时，使用手工、自动或清毒软件将其清除的。

本书从用户角度出发，首先介绍了计算机病毒（包括网络病毒）的特点、防治、检测的简单方法，然后介绍了使用DEBUG工具、PCTOOLS工具、常用消毒软件（如KV300、F—PROT 2.2.4、MSAV、求真杀毒卡及其软件、KILL等）、编程清除病毒的技术，在本书最后一章中还介绍了病毒带来的典型故障，并给出处理方法。

为了照顾不同层次的用户，本书在介绍预防、检测与清除病毒的方法时，给出了多种技术，这样，不同的用户可根据自己的需要选择合适的方法。

计算机病毒防治、检测与清除

曹国钧 主编

王健 曹旺 田啸 李珊珊 编著

*

电子科技大学出版社出版

（中国成都建设北路二段四号 邮编 610054）

电子科技大学出版社印刷厂印刷

新华书店经销

*

开本 787×1092 1/16 印张 15.75 字数 383 千字

版次 1997 年 8 月第一版 印次 1997 年 8 月第一次印刷

印数 1—5000 册

中国标准书号 ISBN 7—81043—770—4/TP·320

定价：18.00 元

前　言

作者第一次接触计算机病毒是在1989年8月。有一天上机时，屏幕上出现一个圆点并到处游动。当遇到字符时，就将该字符清除掉。当时，作者还未留意该现象，以为是一种游戏（那时作者的计算机知识还比较贫乏，只是一个十足的初学者！）。后来才知道这就是中国第一例计算机病毒“圆点病毒”。圆点病毒虽然是良性病毒，却给计算机屏幕的显示带来了不便。以后不断出现病毒，如大麻、6.4病毒……计算机病毒从第一代过渡到第二代，甚至第三代……人们为了使计算机不受病毒的侵害，研制了各种杀毒软件。最典型的是KILL、SCAN、CPAV及后来的KV200/KV300等。作者在检查病毒、清除病毒的过程中学到了许多知识，如病毒的机理、加密、解密、反跟踪技术等，本书就是这些技术的经验与总结。

本书共分为十二章。可以分为四个部分：第一部分为预防、检测、清除病毒的基本手段。第二部分为病毒预防技术。第三部分为使用DEBUG、PCTOOLS等进行手工清毒。第四部分为自动清毒（包括清毒软件与编程等）。本书中列举了许多典型例子，读者阅读了这些例子，可做到举一反三，提高自身的反病毒水平。

在写作过程中，作者得到了国家医药管理局重庆医药设计院有关同志的关心与支持，在此表示衷心感谢。

由于作者水平有限，书中难免出现不足之处，望读者批评指正。

目　录

第一章　计算机病毒的特点、防范与检测

1.1　计算机病毒的特点

1.1.1　计算机病毒分类

计算机病毒是一些能够自我复制的代码段，它能附着在应用程序或系统的其他可执行部分。在宿主程序执行的某些阶段，它能够获得执行控制权。病毒不仅能够附着在系统启动扇区、操作系统的某些模块、设备驱动程序上，而且可以附在任何应用程序如字处理程序、电子数据表格程序和数据库系统等等。病毒大致分为启动感染、系统感染和应用程序感染病毒三类。

大多数病毒在感染后不留下它们存在的外部特征。被感染的程序保持原功能不变，有时可以没有任何感染特征地运行数月，甚至数年。在这段时间内，病毒只是静静地把自身复制到系统内的其他程序上，并且能够感染插入该系统的软盘。经过无法预测的复制周期，病毒激活。这将引起各种明显的系统混乱，有时出现一些无害的提示信息或一些不正常的图形，有时则会导致系统部分或全部存储数据的破坏。这种特殊现象产生的原因是病毒激活通常基于一内部算法。

1.1.2　计算机病毒的传播

计算机病毒可以通过局部区域网络传播，也可以通过一些公开发布的程序，或者是通过远程计算机——计算机通信网传播。在个人计算机方面磁盘是主要传播媒介。如启动感染病毒只能通过磁盘这个媒介，在系统间传播。系统感染病毒通过系统插入被感染的系统传播。病毒或者附在一段已经存在的代码中，或者完全替换一段代码，把自身附着在其他程序上。启动感染病毒用自身替换整个启动扇区，充当启动程序。然而大多数病毒是把自己附在已经存在的程序中，因为这种方法使病毒不必重新编写被替代程序的代码。

一个病毒程序或者是把自己在外部与程序连接起来，或者是插入被感染程序内部。如果是外部连接，则程序大小会改变。这样的病毒可以通过列目录或其他外部观察方法测试出来。如果病毒选择把自身插入宿主程序的方法，它必须在宿主程序内找到足够的自由空间来装下病毒。大多数程序没有足够的自由空间，因此病毒只能找到有限的接收程序，这样病毒传播速度会降低。

一些证据表明病毒设计者充分考虑了上面几点，并且更乐于选择外部附着的方法。这些病毒一般是替换宿主程序的初始指令，用新的指令转移到病毒程序的主体。病毒代码一般附加在宿主程序的尾部。当病毒程序执行完毕，原来的程序会被恢复并把控制交给该宿主程序。

1.2 计算机病毒的防治

1.2.1 第一代病毒的防治

现在已经有许多方法来减少病毒感染。减少感染机会的方法有两类：一是抗病毒工具，一是用户安全操作措施。

1. 抗病毒工具

各类病毒进行感染，激活的机制一般来说各不相同，进行破坏计算机软硬件及数据资源的方式也不一样。如果我们只是粗略地查看一下各种病毒，似乎觉得现有技术无法捕捉到所有已经存在的病毒，更不用说那些还未发现的。然而这种假设是错误的。

为了有效地抑制病毒，我们首先必须看到病毒的一些基本弱点，而且我们需要把这些共同特征抽取出来，作为我们制服病毒的出发点。病毒的第一个弱点，也是最重要的弱点——它们的宿主目标必须是计算机系统的可执行片段。就是说它们只能感染系统启动程序、操作系统单元，或应用程序。它们无法有效地感染数据文件、表格信息，或其他系统原始数据。病毒的第二个弱点是任何感染总是以某种方式改变被感染的系统片段。病毒要么是完全替代系统的一段代码，或者是修改已经存在的代码。如果它附加在一个已存在的程序上，它会改变程序的开头、结尾或程序中间的某些部分；如果它藏在盘的空白区，那么这些区域会被病毒覆盖；如果病毒是把原来的启动扇区移到不显眼的位置，这种移动会改变系统。总之任何感染总会残留一些痕迹。

病毒的第三个弱点是：如果病毒要存活、繁衍，那么它的程序代码必须能够被执行，即病毒至少在初次感染后把自己放在能够获得控制权的地方，否则病毒永远不能复制或激活。这表明病毒不能随意把自身附着在宿主程序上。它必须知道宿主程序的大致结构，这样才能在宿主程序执行时，病毒程序得以执行。病毒必须把自身或一部分定位于宿主程序的特殊位置，这一局限可被抗病毒工具充分利用。现在有多种方法开发各种抗病毒软件。归结起来抗病毒程序可以分成感染预防、感染检测和感染识别三大不同类别。

感染预防程序常驻内存，监视其他程序的存取要求和程序进出内存情况，并核查所有的系统设备请求，监视系统表和系统控制结构，即系统活动的每一方面都被监视和核查。一旦病毒向系统渗透，即向系统内的某段可执行代码有存取要求，抗病毒程序就会中止系统并给出告警信息，然后消除病毒。然而怎样判断对一段程序的存取是病毒的侵扰，还是正常的访问呢？在正常的情况下一个字处理程序或数据库程序或一个图形包很少试图写到另一个程序中。这种存取一般只发生在所讨论的程序被新版本取代，或程序被初次装入系统中。当然，实际上有些正常的系统功能调用会被抗病毒程序误认为是病毒侵扰而错误地报警。抗病毒程序质量的一个尺度是错误报警的频率。设计很差的程序可能会因为错误报警过频而变得毫无用处。有时预防程序会被采用防检测手段的病毒欺骗。这些病毒用难以被检测和预防的存取手段，如直接写向可控制存储设备的硬件，或用I/O调用以避免检测。启动感染病毒在加电或重启时感染系统，此时预防程序还没被装

入，所以，不能被预防程序克服。

感染检测程序是基于这样的原理：感染病毒后，通过查找踪迹可检测出病毒的存在。这些踪迹是在病毒感染过程中修改的系统信息。这类程序一般比预防程序可靠，并适用于各类不同的病毒。感染检测程序一般是通过接种疫苗法和“快照”技术实现的。接种疫苗法是通过修改程序使每个程序具有检验或其他算法判断程序指令序列是否被改变的测试机制。每次程序运行都执行检测，若与上次运行有任何区别则认为病毒出现。不过，此法也有缺陷，首先许多关键程序如启动程序几乎无法“接种”(启动感染病毒完合替代启动程序，这样接种过的启动程序永远没有机会执行)。第二个问题是感染了接种程序的病毒永远在自测机制执行前获得控制权。

可能现在最有效的检测感染程序是使用“快照”技术。“快照”程序在系统初始安装时登记系统的所有关键信息。随后，检测例程周期性地运行，如果当前系统状态与原来“快照”的区别——感染的痕迹被检测到，被感染的区域即可被识别出来。由于“快照”程序拥有在同一时刻检测、比较系统所有部分的优势，所以能检测出三大类病毒。并且“快照”文件和比较程序可脱机保存，因而自身不会被病毒感染。

“快照”技术在识别病毒感染上很成功，但也可能存在一定缺点：用某种查证技术查遍整个系统是相当费时的（有些程序使用“分支地址图”法检查可执行程序，可将检验时间减至几秒)。应该注意，在检测程序进行检测之前，病毒有可能（当然，这种可能性很小）激活并进行破坏。

当系统已明显被感染时，就需用感染识别程序。它们在系统的每个角落寻找一段具体病毒代码或病毒标签及版权标志或特定的文件名或在特定磁盘地址的关键数据等病毒特征，如发现，就追踪并消除之。这类程序的缺陷是在设计前需要一个病毒实例，在识别、分离、抽取特征后才能着手开发消毒程序。这样的软件开发周期一般较长。然而对于消除大量的感染磁盘或系统，用这样的程序比用手工方法要快速、有效得多。

2. 用户安全操作措施

实施适当的安全措施与使用抗病毒工具同样重要。计算机用户采取以下简单措施可大大减少病毒感染的机会。

(1) 首先而且是最重要的是，只使用最初发布的软件包中的写保护启动原盘来启动系统，而不用其他任何盘。大多数启动感染病毒只能通过用感染软盘启动才可感染系统。使用来历不明的启动盘大大增加系统感染的可能。

(2) 在只有软盘驱动器的 PC 系统，启动盘标签必须与原系统盘一致。

(3) 如果系统拥有硬盘，不要用软盘启动（唯一例外是在清除病毒感染时)。

(4) 慎重对待共享的软件。若可能，只在设有硬盘的系统上使用。若一定要在硬盘上使用，把它们置于子目录下。因为有些病毒只在当前目录下活动，这样可以减少感染范围。

(5) 在格式化时建立有意义的盘标签，并观察标签是否变化（如在 Dir 时)。

(6) 观察各类系统活动是否有变化。如程序装入是否比平时长?·磁盘存取是否过多?是否在系统设备空闲时过多的指示灯亮？是否可用系统存储量减少？是否程序或文件突

然消失？是否可用盘空间减少？所有这些都是病毒感染的征兆。

（7）如果你在一个合作环境下工作，应尽量减少直接交换可执行代码。如果要使用他人的PC资源（如激光打印机），把必要数据拷入盘中，不可含任何可执行程序，也不要用可启动盘和包含系统文件的盘。

（8）若在网络环境下工作，不要把共享软件放在可被任意其他PC用户存取的公共服务器目录下。

（9）若在网络环境下工作，不要把文件服务器结点作为工作站，只准系统管理员使用文件服务器结点。

（10）若用3270仿真器连在主机系统上，应把所有3270仿真软件集中在一分离子目录下，不要在该目录下加进任何非仿真工具集内的可执行代码，若可能，应删除盘上其他所有软件。3270仿真器是病毒从PC机跳入主机系统的主要途径。

1.2.2 第二代计算机病毒及其防治

目前，又有一些新的计算机病毒在悄悄蔓延。这些病毒与以往的引导型病毒、文件型病毒和混合型病毒不同，它们既不占用任何内存，也不盗用或修改任何系统数据及其他资源。从各个方面看，它们与普通的程序没有任何不同，因此把它们称为第二代病毒。由于目前很少有防计算机病毒软件、硬件能检测到它们，所以非常有必要了解这些计算机病毒的特点，以便防治这些病毒。

1. 第二代计算机病毒的特征

首先我们简单介绍两个第二代病毒的例子。

“Fired love（12017）”，中文名称“燃烧的爱”。该病毒由Turbo C语言写成，全长12017B。“Fired Love（12017）”不驻留内存，仅感染.EXE文件，由于没有改写.EXE文件的标题，所以在很多情况下是会造成死机或不能被MS-DOS认可启动运行的。事实上用高级语言书写的病毒也可以对.EXE文件标题进行正确定位，尽管在实现上有一定难度。这个病毒的代码被插入到.EXE文件标题与原正文之间，因没有改写原程序内容，所以清除它还是不太困难的。

“FOOL”，中文名称“傻瓜”。该病毒因病毒体内有一字符串“FOOL”而得名，显然是用汇编语言写成，长度不确定，依被感染文件的内容不同而变化，大概在2197±8B左右。这个病毒身兼数职，既感染可执行文件.COM及.EXE，又感染隐扇区，具有很强的感染力。文件型病毒能感染属性为只读和隐含的文件，除了足够小的.COM文件外，几乎能感染尺寸充分大的文件，但本身不具破坏性，其病毒标志亦较特别，并不在文件本身之内，本部不驻留内存，不改写任何中断，检测极难。引导型病毒感染引导扇区时，几乎不能觉察到代码的变化，病毒标志很隐蔽。本部驻留内存，但在MS-DOS下根本不能用通常的方法检查到内存量的减少，而一般的工具软件如PCTOOLS更是无法检查到。与文件型病毒不同，引导具有危害性，当引导次数达到100（64H）时，如果有写盘操作，则小数点的位置会被移动一次且仅一次。

从以上病毒简介使我们可以看出，以前有关病毒的特征消失了，其识别方法可能失

效了。唯一可行的办法是从文件长度的变化去观察。然而，病毒也可以在这个问题上蒙蔽用户。以上两种病毒虽然没有，但谁能保证其他病毒不会这样做呢?

下面，我们比较第一代病毒的常见特征来感性地认识一下第二代病毒的一般表现形式。

(1) 软盘起动时硬盘灯亮了不止一次　现在，病毒可以在操作系统操作硬盘时再行感染硬盘，其余时候潜伏忍耐，所以在软盘起动时硬盘灯亮亦只一次。虽然其操作硬盘绝对超过一次，但由于硬盘读写速度高，靠外观感知显然是不行的。

(2) INT 13H 中断被修改　这种单纯的观察，很早以前就失效了。因为从 MS-DOS 自版本 3.0 起为了适应日益发展的存储介质，已对该中断做了扩充与完善，而且软驱数量的增多使各厂家也纷纷推出自己的设备驱动程序。

(3) 内存量被减小　INT 12H 可获取的内存量（在 0：413H 处，一字）被减小，而病毒就安置于因此占有的内存块处。

DOS 对内存容量的获取是一次性的，以后若直接对 0：413H 处进行任何操作，它都将置之不理，此举显然存在严重的缺陷。因为病毒可以很容易地判断系统是否已引入了 MS-DOS，若已引入，则将 0：413H 处的原内存量恢复，而 MS-DOS 却全然不觉，它不会将程序代码加载到自己早已获取的内存高端以外的位置。

(4) 工具软件可发现 MS-DOS 可用内存量与系统内存量的不一致性　有些用户，过分依赖于像 PC TOOLS 一类的工具软件查询系统配置，去了解病毒的存在。然而，PC-TOOLS 之类的工具软件只是简单地从系统数据区或某些特定的内存单元取析数据，因而它们的局限性也是不言而喻的。在第二代病毒出现以前，用 DEBUG 直接查看数据段偏移 2 处一字的内容是简单有效的办法，它从中不仅可知内存量的变化，还可直接知道病毒寄生的段域。

然而，第二代病毒可以让你根本无法用以上介绍的方法探知其存在。这个问题相当复杂，有兴趣的读者不妨研究 MS-DOS 关于 PSP 的运作机理，可知病毒要对内存量进行伪装也是完全可以做得到的。不过，这种技术较为复杂，搞不好容易造成死机。

(5) INT 21H 有了与平常不同的段值　第二代病毒将不再单纯以 INT21H 作为攻击目标，它们将转而攻击其他诸如 INT 25H、INT 26H、INT 27H 以及 INT 40H 等从前未被注意的几个中断。即使攻击 INT 21H，也可能只搜索其中的诸如 CALL [wreg]、CMP AH，breg 之类的指令，然后将其改向（发 INT 指令或段间调用、跳转指令），而不直接改写 INT 21H 中断及其向量。这种技术是目前已知的被病毒采用的最复杂的一种，其实现的难度最大。从前言部分可知，这种技术将被抛弃，那种全新的做法必会受到病毒设计者的青睐。

(6) 盘操作速度变慢　这种判断方法是幼稚的。殊不知，病毒完全可能使你的盘操作速度明显“加快”呢。其原因很简单，病毒只需放弃用户数据区内的盘操作或只操作其中一部分，即可达到加速的效果。

(7) 文件长度增加　早期的某些病毒，已能对文件长度增加这个缺陷作一些伪装，比如在查找匹配首文件及其他匹配文件时，病毒会将文件的原来长度给出，从而迷惑用户，但不能很彻底。第二代病毒的伪装将更完善，即使用指针移至文件末部及 FCB 方法查找匹配文件都将被病毒迷惑，用户已不能放心且方便地调用 MS-DOS 功能调用了。

（8）引导记录不正常　一般的资料都会提醒读者，观察引导记录的正常信息是否消失或被替换等等。现在，引导记录仍然被修改，但修改量很少，并且代码是正常的，不认真追踪不易察觉。第四种引导型在某些地方甚至根本不对原代码做任何修改。

（9）其余特征　第二代病毒最大的特点是不露痕迹。体现在传播上时，是读写盘或操作文件的速度没有直观上的变慢，体现在发作方式上，则不会有口号或即使有也不公开。它们一般不会给显示器一个明显的干扰，但可能会吞食或像“黑洞”那样，不知不觉地吞食一些显示字符。而在攻击串、并行口设备时，也不仅是简单地取消，更可能的是输出中有“疵点”，若表现在文件输出上，这样的破坏将更具危害性。假如在编制程序，由于病毒的作用（插入“疵点”），必须花数倍于平时的时间去调试代码，并且由于总不能解决问题，工作将不能继续进行，除非发现了病毒的存在并加以清除。在汉字操作系统下，各种输出可能屏蔽汉字，但我们往往会认为汉字系统出了问题，或者软件不适于在汉字系统下运行，也可能认为诸如打印机之类的外设出了故障。

2. 第二代计算机病毒的防治

自从病毒的蔓延及其危害被人们认识过来，防治病毒技术的发展也是很迅速的。然而，勿庸讳言，在像 Millennium AntiVirus 这样优秀的软件出现之前，反病毒技术在总体上是逊于病毒的，在这场长期的对抗中处于下风地位。滞后的扫描、消毒怎么可能与不断翻新花样的病毒一试锋芒呢？只要对病毒稍事修改，或仅修改病毒的标志，就能逃过消毒软件的检查，任何一个病毒，都可以产生几百种甚至几千种的变异。因此，这种反病毒功能虽然在一定的阶段、一定的程度上起了一些积极的作用，但其功能有限。

防病毒硬卡的产生正是为了弥补消极扫描软件的严重不足，在当前市场上也可谓百花齐放、各显神通。究竟硬卡反病毒有多大的作用？我们只需认真分析一下就不难得出结论。我们知道，市面上各种防毒卡都只是软件的固化形式，其中大部分纯粹是为了防止非法复制或迎合用户对硬件的迷信才硬化的，并不会比软件更安全、更有效；相反，病毒程序只需三五条指令就能置硬卡于死地，硬卡之脆弱不言而喻。况且，目前的硬卡都缺少智能，对用户操作干涉过多，增添麻烦不说，许多工作需要自动连贯地进行，在这里，只好“顾全大局”忍痛做出牺牲了。

最有希望彻底阻止引导型病毒的方法之一是完善 MS-DOS 本身。但新近推出的 MS-DOS6.0 虽新增了防病毒命令，结果却不尽人意。

防病毒技术的发展最终回归于依靠软件或软件与硬件的配合，已是大势所趋，也是防病毒技术逐渐走向成熟的开始。当前最优秀的一些软件已能在很大程度上自动识别许多第一代病毒，虽然它们尚不能预警第二代病毒，又可能被针对性的病毒击破，但比从前那种被动脆弱又不可靠的防病毒技术来说已是前进了一大步，不可同日而语。

在防病毒的过程中，有一些令人不安的因素至今还没有完全排除。某些有危害性的防病毒软件或硬卡也在市场上露面。

看来，防病毒技术的突破必须建立在对病毒机理的透彻认识、对 MS-DOS 的深刻了解以及具有丰富的实际经验之上，三者缺一不可。Millennium Software Central（以下简称 MSC）推出的 AntiVirus V3.0 是众多防病毒软件中的佼佼者，本文愿向读者慎重推荐之。

病毒的蔓延，其中重要的一个原因是非法复制软件的现象大量存在，许多实用软件为了防止及惩罚侵权行为，都可能在程序体内殖入病毒代码。所以，为了免遭病毒危害，应加强道德及法制观念，不非法复制、使用未经授权的软件，不要因小失大，也不要过分自信。因为殖于高级语言编译的可执行代码内的病毒很难被发现和检测。一般地，在购置软件时应注意是否有用户手册等必要的资料，最好要弄清该软件的出版者是否提供有售后服务及升级服务。

病毒防治软件 Millennium AntiVirus（以下简称 AntiVirus）是建立在对病毒的共性（不管是第一代的还是第二代，还是未来的病毒）和对 MS-DOS 及其许多重要数据的分析消化基础上。它设计得十分精巧，虽然没有那种华丽的外表，然而却极其有效。它对自身和 DOS 以及所有可能受病毒攻击的单元、数据都层层设防，病毒根本无法攻击受 AntiVirus 保护的系统。为了预防万一，MSC 又专门提供了 AntiVirus V3.0 的多种变异版本，这样，要攻破 AntiVirus 的防线概率为零。此外，MSC 已公开声明，在保证质量的同时，还将保证将来有升级服务与售后服务。因此，用户尽可放心使用 AntiVirus。

首先，AntiVirus 的安装十分简单方便，根本不需用户做过多的干预。用户只需用购得的 AntiVirus 原件启动电脑系统，除非发现你的电脑系统已经异常，否则 AntiVirus 立即与原有资源融于一体。今后，任何病毒都难逃脱 AntiVirus 的控制。

其次，AntiVirus 本身设计得十分安全可靠，不像市面上某些防病毒软件那样具有危险的副作用。AntiVirus 的策略是获取用户正当的资源并加以保护、利用，而不修改用户任何有用的数据、单元。

第三，AntiVirus 不但防病毒独具匠心，用于保护用户资源也是卓有成效，AntiVirus 的这种功能已超出了防病毒的范畴。受其保护的计算机系统，非授权用户无法对其进行操作、访问，甚至用 DOS 的 FDISK 破坏也不能奏效。

第四，任何引导型病毒的侵袭都可被立即清除，任何带有文件型病毒的程序都可照常运行，而不对系统构成威胁，换句话说用户可以安全带病毒运行而不用担忧运行效率会降低。

事实上，对 AntiVirus 研制长达 4 年，经历过包括第二代病毒在内的针对性测试，仍稳如泰山。由于它在某种程度上具有对未来的预见性，病毒设计者很难期望制造一种能躲过 AntiVirus 侦查、控制的新病毒，除非该病毒不是运行于 MS-DOS 之上。

总之，AntiVirus 的诞生，给反病毒技术输入了新鲜血液，带来了新的希望。也许，病毒与反病毒的对抗将因此进入一个新的时期。

1.3 检测病毒的简单有效方法

计算机病毒的变种及新的病毒不断地出现，而已有的消毒软件（如 Scan、Clean、Kill、Msav、CPAV、KV200/KV300 等）功能总是滞后并且有限，往往检测不到新出现的病毒。专业的计算机人员由于对病毒的运行机制了解较多，防护意识较强，对病毒的检测和排除可轻而易举地进行，病毒对他们一般不会造成多大的危害。但是对于大多数用户而言，由于不太了解病毒知识，只能依靠手头现有的消毒软件大概地了解一下机器中是否有病

毒存在，由于有些病毒无法及时检出，等到发现时往往已经造成较大的损失。

计算机病毒主要分为系统型和文件型两种。系统型病毒寄居在软盘、硬盘的BOOT区及主引导扇区中，通过启动系统被激活进行传染，这类病毒隐蔽性高，传染性强，不易为一般用户所觉察。文件型病毒主要寄居在可执行的.COM、.EXE型文件中，通过运行带毒文件而激活，一般而言其传染性较强但隐蔽性不如系统型病毒高，可轻易地被用户所发觉。上述病毒一旦被激活，大部分必须驻留内存才能伺机传染。病毒驻留内存后隐蔽地占用部分内存（如1KB、2KB、3KB等），并不向DOS说明占用情况，有些查毒软件（如RAMMMAP——内存病毒捕捉器）根据病毒的这一特点即可报告病毒激活情况以提请用户注意。

下面介绍几种简单有效的方法，可方便地预防、检测病毒的侵入，避免病毒带来的一些麻烦。

1. 使用PCTOOLS.EXE查看内存检测病毒

PCTOOLS.EXE（Deluxe R4.309）是流行的实用工具软件，到处可见。启动PCTOOLS后按F3键进入Disk and Special Function（磁盘和特殊功能）界面，再按I键进入System Information Service（系统信息服务）界面，如图1-1所示：

```
Advanced PC Tools 5.0

———————————— System Information Service ————————————

                                  Computer — IBM/PC AT
                  The BIOS programs are dated — 11/16/95
                                Operating system — DOS 7.00
                          Number of logical disk drives — 32
                                Logical drive letter range — A thru
                                              Serial Ports — 2
                                            Parallel Ports — 1
                                              CPU Type — 80386
                    Relative speed (orig PC=100%) —9540%
                          Math co—processor present — 80387
          User programs are loaded at HEX paragraph — 04F1
Memory used by DOS and resident programs — 20240 bytes
          Memory available for user programs — 635104 bytes
                        Total memory reported by DOS — 639K
          PC Tools has found the total memory to be — 640K
          Enhanced Graphics Adapter present (color) — 256K
          Expanded memory total — 23856K, in use — 736K
          Additional ROM BIOS found at HEX paragraph — C000K

                                                Press any key to return
```

图1-1

我们可以在该界面上看到如下两行（COMPAQ 机中第一行为 639K）：

Total memory reported by DOS—640K

PC Tools has found the total memory to be—640K

当病毒被激活驻留内存后，由于其不向 DOS 报告内存使用信息，故 DOS 所检测到的内存量将减少，据此可知病毒被激活，需要立即采取处理措施。下面的几例在用 KILL-77.00、SCAN229、MSAV 时均未发现病毒感染信息，但用 PCTOOLS 查看内存时发现了病毒的存在。

例 1 1996 年 4 月，我们在膝上型 COMPAQ 486 和 AST 386P/25 上使用 PCTOOLS 查看系统信息时发现由 DOS 报告的内存为 637KB 和 638KB，怀疑有病毒进入，经分析软、硬盘上均有系统型病毒，其中有病毒标志“Welcome to BUDP, Beijing, 1994”，由 NU.EXE 手工清除该病毒后重新启动机器（注意：PCTOOLS 不能查看和修改硬盘分区表的信息），再使用 PCTOOLS 查看时，DOS 报告的内存分别为 639KB（Compaq）和 640KB（AST 及其他兼容机），机器情况正常。

例 2 1996 年 9 月我们在 COMPAQ 386DP/33 和 AST 386P/25 上使用 PCTOOLS 查看系统信息时发现由 DOS 报告的内存为 637KB 和 638KB，经分析软、硬盘均有系统型病毒，其中有病毒标志“I am LiXiBin!”，清除该病毒后重新启动机器，再使用 PCTOOLS 查看时，DOS 报告的内存分别为 639KB（COMPAQ）和 640KB（AST 及其他兼容机），机器工作正常。

例 3 1996 年 10 月我们在 COMPAQ 386DP/33 和 AST 386P/25 上使用 PCTOOLS 查看系统信息时发现由 DOS 报告的内存为 637KB 和 638KB，经分析软、硬盘未发现系统型病毒，在比较 Command.com 时发现增加 1024 个字节，显然有外壳型病毒侵入，对感染后的 Command.com 分析发现有病毒标志“LNNBMG”，该病毒只一次性感染 COM 型文件，更新染病毒文件后重新启动机器，再用 PCTOOLS 查看时，DOS 报告的内存分别为 639KB（COMPAQ）和 640KB（AST 及其他兼容机），机器工作正常。

例 4 1996 年 11 月，我们拷贝到染毒后的 KILL.EXE（公安部 77.01 版，当时未觉察到，并且 KILL 也未检查出），在 AST 386P/25 上使用后用 PCTOOLS 查看系统信息时发现由 DOS 报告的内存为 638KB，经分析软盘、硬盘均未发现系统型病毒，查看文件长度时发现某些 EXE 和 COM 文件增加了 1110 到 1115 字节，可见有外壳型病毒的侵入，对感染后的文件分析发现有病毒标志“VVGn”。该病毒在使用 DIR 命令或执行文件时进行传染，且可与“LNNBMG”病毒一起对 COM 文件进行交叉感染，之后每次使用 DIR 命令，均使当前目录中的第一个 COM 文件增长了 2KB 左右。

2. 预防、减少病毒危害的简单方法

当前各种软件系统越来越庞大，像 VC++ 1.0（20 张高密盘）、Borland C++ 3.1（18 张高密盘）等，安装后占用几十兆字节的硬盘空间。当系统被病毒感染瘫痪后，重新安装系统费时费力、十分麻烦；特别是对那些手头没有备份的软件系统，一旦感染病毒使系统陷于瘫痪时，更使用户恼怒不已。一般而言，病毒的检测以及对系统型病毒的清除（NU、PCTOOLS、DEBUG 进行手工消毒）十分简单，但是文件型病毒（外壳型和入侵

型）危害严重，不易清除，常使染毒文件无法再用。那些多人使用的公共计算机，染毒的机会又特别大，因此，需要一种尽量将病毒带来的麻烦减少的简单方法。我们在下面将为读者介绍几种常见方法。

（1）绝大多数的文件型病毒为外壳型病毒，通过检查可执行文件的长度变化很容易地检查被感染的文件，这种方法特别适用于那些不驻留内存病毒的检测。为了以后比较文件长度，故应保留原始干净文件的长度，但是把许多文件长度打印出来加以保留并不方便。我们的做法是利用DOS的输出重定向功能，在各个子目录文件安装之后立即键入：

DIR *.* /S > files.len

则将各个子目录中的原始文件的长度、生成时间等信息保留在files. len文件中。使用时可通过PCTOOLS或Type命令方便地查看files.len中的内容。

（2）用户若有CPAV.EXE查毒软件，则不必使用（1）中的方法。因为CPAV将在各个子目录中自动生成Smarkchk.cps文件，其中记录了该目录下所有文件的长度、生成日期、时间及属性。这些内容变化后，若再次运行CPAV时将自动向用户报告变化的情况。使用CPAV时不可任意删除Smartchk.sys文件，否则将起不到自动监视文件信息变化的作用。

（3）由于病毒一般只感染可执行文件，而所有可执行文件的总的存储量相对于应用系统来说比较少，因此对于较大的应用系统，安装之后应立即备份其中的所有可执行文件，对于以后更新被病毒破坏的文件以维护整个系统将带来很大的方便。例如，我们办公室使用WPS 6.0F，安装之后需要占用20MB的硬盘空间。由于使用的人多，经常受到病毒侵扰而不能正常运行，常常需要重新安装。由于WPS 6.0F中的.com、.EXE、.ovl文件总量约为1.3MB，故可使用1.44MB的小盘保存，也可使用ARJ.EXE压缩到一张360KB软盘中，以后只要使用该盘更新系统的可执行文件，感到十分方便。

当要保留的可执行文件较多时，可先进行压缩。例如，我们曾将Borland C++ 3.1的9.7MB的可执行文件压缩为4.6MB予以保留（因无系统原盘，故出此计），而后来确为系统维护起到了一定的作用。

（4）当某应用系统暂时不使用时，将所有可执行文件的后缀改名，如将.COM、.EXE、.OVL分别改为.CON、.EXF、.OVM等，或者用用户自己了解的名字，也可较好地预防病毒的感染。另外，这种方法也可有效地防止别人执行某些敏感的文件。当需要重新使用系统时，只需将后缀改回即可。例如，

```
c: \>ren *.con *.com
c: \>ren *.exf *.exe
c: \>ren *.ovm *.ovl
```

3. 使用PCTOOLS检测染毒文件

PCTOOLS提供了许多功能，如二进制文件的编辑（E命令）、在磁盘或文件中寻找特定字符串（F命令）、磁盘和文件内容比较（O命令）、系统信息显示（I命令）等，这些命令对于病毒的简单检测是非常实用的。下面是查找、清除外壳型病毒的一般步骤。

（1）使用PCTOOLS查找未知文件病毒时，可先用已有的长度较短的.COM和.EXE