张建明　陈　婉　编著

微型计算机
实用反病毒技术指南

西安电子科技大学出版社

- 计算机反病毒实践的必备工具
- CPAV、SCAN、MSAV、KILL 和 KV200 用户的高级家教
- 反计算机病毒专家经验体会的真诚奉献

微型计算机
实用反病毒技术指南

张建明　陈　婉　编著

西安电子科技大学出版社

1996

(陕)新登字 010 号

[内容简介] 全书分为上、中、下 3 篇。上篇为基础篇，介绍计算机病毒及其防护方面的知识，其中包括：计算机病毒基本知识，计算机病毒检测、清除、免疫的一般理论和反病毒技术概论等内容。中篇为反病毒软件产品使用介绍，其中包括国内外目前比较流行，且编著者认为比较实用的 5 种反病毒软件产品最新版本的使用指南。涉及国外的反病毒实用软件有 CPAV 2.1、MS—DOS 6.0 版的 MSAV 和 SCAN 102，国产的反病毒软件有 KV 200 和 KILL 73.02 等，对于这些软件产品的介绍，编著者坚持用户观点并结合多年反病毒实践的体会，对它们作了比较详细和实用的说明指导。下篇主要介绍了传统工具在反病毒实践中的作用、使用方法以及反病毒方面的实例，内容涉及 PC 集成工具 PCTools、Norton Utility(NU)和动态调试工具 DEBUG 等。在附录中介绍了计算机反病毒的发展历史、计算机病毒的发作规律和时间，以及国内外常见的 1 561种病毒的主要特点。

本书编著者的用意在于向普通计算机用户，尤其是向非网络单位或个人计算机用户提供一种适合阅读，并对反病毒实践有实用价值的指导资料。因此在全书的系统结构设计中，有针对性的选择了反病毒技术及实践中的有关内容，体现了编著者的意图，具有一定的特色。可以十分肯定地说，《微型计算机实用反病毒技术指南》为广大计算机用户防护计算机病毒，排除计算机病毒的困扰，确保用户计算机系统的信息安全提供了一本难得的反病毒手册。完全可以预见，本书将成为普通计算机用户的良师益友，同时也不失为一本计算机反病毒的合适培训教材，并可作为大中专学生及计算机工作者有价值的参考资料。

实用反病毒技术指南

张建明 陈 婉 编著

责任编辑 徐德源

西安电子科技大学出版社出版发行

地址：西安市太白南路 2 号 邮编 710071

陕西省大荔县印刷厂印刷

各地新华书店经销

开本 787×1092 1/16 印张 16 4/16 字数 382 千字

1996 年 1 月第 1 版 1996 年 1 月第 1 次印刷 印数 1－8 000

ISBN 7－5606－0413－7/TP・0167 定价：16.50 元

前　言

随着电子计算机的迅猛发展，计算机的应用日趋深入和普及。计算机对人类社会发展的巨大贡献，使其在现代社会中居于战略地位，与此同时，计算机应用的社会化带来了一系列新的问题，信息化社会面临着计算机犯罪等一系列问题的严重威胁。

在一些发达国家，计算机犯罪是从60年代末期开始出现的，70年代至今发案率迅速上升，目前已构成发达国家和发展中国家面临的日趋严重的社会问题。

80年代中期计算机病毒的出现和全球性蔓延，使计算机系统安全面临着更加严重的威胁，计算机病毒是计算机犯罪的一种重要形式，计算机病毒的传播又加速了计算机犯罪活动的泛滥，这些问题充分暴露出当今计算机系统的脆弱性。

1988年11月2日，美国发生了6千多台计算机被病毒感染，造成美国历史上最大的计算机网络INTERNET不能正常运行的严重事件。这次攻击计算机网络的病毒程序设计者是Robert T. Morris，他设计的病毒程序约6 000字节，可以在UNIX环境下窃取口令，然后冒充合法用户将病毒程序复制到远程计算机中，病毒程序利用了Berkeley Unix 4.3中"SENDMALL"程序的缺陷，以3种途径入侵系统。这次事件中遭受计算机病毒攻击的INTERNET网包括5个计算机中心和12个地区节点，3个计算机网络（美国国防部高级研究计划局网络APPANET、军用网络MILNET、国家科学基金会网络NSFNET）。这个事件告诫人们，计算机病毒已成为当今大型信息系统和计算机网络安全的严重威胁。

近年来，计算机病毒大范围传播，欧洲、日本流行计算机病毒，香港和台湾地区计算机病毒入侵计算机系统的事件不断发生。自1989年春季我国大陆地区首次发现计算机病毒入侵以来，至今已发现100多种计算机病毒及其变体，而且值得注意的是，有些国外刚刚流行的计算机病毒，在相当短的时间内就在国内传播开来。实际情况表明，计算机病毒的传播是一种国际现象，受到国际环境的制约和影响，而且情况仍在继续发展中。据1991年10月有关部门抽样调查，我国大陆地区有近100万台微型计算机遭受病毒感染；而截至1994年10月的统计结果表明，全国大约有240万台微型计算机，其中33%的计算机遭受计算机病毒入侵，有的地方和单位计算机遭受病毒入侵率为100%。情况表明，计算机病毒对于我国计算机系统安全和计算机推广应用已经造成了严重的危害，有些

部门计算机系统感染病毒后，破坏了历史上一直保持下来的重要信息资源；有的影响中外合资企业的开工生产；有的金融系统遭受病毒破坏，导致20至30天不能对外营业；同样，病毒也威胁着要害单位和军事部门的计算机系统安全。

据美国Fridrik Skulason 1994年底的统计，已经发现计算机病毒及其变体3 955种，而Dataquest公司1992年初的调查结果是，1991年计算机病毒为2 500多种，而1990年只有756种。在接受调查者中，遇到病毒的比例也由1990年的26%上升至1991年的61%，增加了一倍多。

从感染病毒的途径来看，大多数病毒来自软盘，其比例高达67%，而其中49%又是从家用软盘带来的。其它感染途径分别为：不明来源29%，销售部门演示软盘6%，电子公告牌6%，非家用与销售部门演示软盘5%，修理服务人员4%，紧包装应用软件包3%，下行电子邮件线路2%。

从受病毒侵害造成的不同危害来看，其比例分别为：丧失工作能力62%，屏幕信息受干扰与阻塞41%，文件被毁38%，数据丢失30%，应用软件运行故障24%，系统失效23%。

事实告诉我们：防治计算机病毒是保障计算机信息系统安全的重要内容。与此同时，也应该看到参与对计算机病毒技术的讨论和技术研究工作，是防治计算机病毒技术研究的另一个主要方面。

目前流行的计算机病毒从各个方面暴露了当今计算机系统(包括各类微型计算机，小型、中型、大型和巨型计算机系统)安全方面存在的问题及其脆弱性，防范非授权使用计算机系统和非法入侵计算机系统已成为当务之急。

计算机病毒像幽灵一样在世界范围内游荡，构成了对现代社会的一种威胁。人们对计算机病毒认识的深化和逐步解决，对计算机科学和技术发展将会产生巨大的推动作用和影响，其意义远比GOTO语句的争论大得多。如果说从软件的形成和建立，使人们认识到知识的价值并进而建立起知识产业，那么计算机病毒的出现和蔓延将迫使人们认识正确运用知识和保护知识产权的重要性，并应该采取相应的积极措施。

事实上，计算机病毒是计算机科学技术和以计算机为核心的社会信息化进程发展到一定程度的必然产物。为了微型计算机的普及应用，要求操作系统简单明了、内部结构透彻清楚、软硬件产品透明度高，若缺乏安全措施，其缺点和受攻击之处易被人掌握。同时，由于社会上存在随意拷贝软件、侵犯知识产权、计算机法律不健全等因素，刺激了计算机病毒的产生和发展，诱发了某些有不良动机的人的犯罪意识和犯罪活动，使计算机病毒产生了较强的社会影响。

计算机病毒引起的一系列问题，最终将导致计算机发展史上的一次革命性变化。对此，我们应该密切关注并予以足够的重视。

但是作为普通的计算机用户，大家首先关心的是如何有效地预防计算机病

毒的侵入和传播，怎样清除侵入到计算机系统及文件上的计算机病毒，这是广大计算机用户迫切需要解决的问题。

本书集中了作者多年来对各种计算机病毒分析、研究的成果和反病毒实践的体会，并参考大量国内外计算机反病毒方面的书刊编撰而成。本书对目前国内普遍认同的5种反病毒实用软件产品的使用方法进行了详细的介绍，并对传统PC工具在反病毒实践中的地位、作用、使用方法作了进一步介绍，同时列举了一些典型的利用传统PC工具进行反病毒的实例。使得读者不但能够有效地使用实用的反病毒软件产品，还可以自己动手利用传统的PC工具检测和清除反病毒软件产品所无能为力的新病毒及其变体。

在全书的编写过程中，作者始终坚持用户观点，力求集理论性与实用性于一体，既为想了解计算机病毒的计算机工作者提供有价值的参考资料，更为正受计算机病毒危害的广大计算机用户提供一种实用的反病毒手册。

本书的部分内容曾在《中国电子报》连续登载，可作为计算机反病毒的培训教材，是一本难得的计算机反病毒手册，也可以作为大中专学生及科技工作者的自学参考书。

本书由张建明、陈婉同志合作编写。在编写过程中，得到了陈涛、权翠侠、张秦尉及陈树治同志的热情帮助，在此表示衷心感谢。徐德源及西安电子科技大学出版社的同志们为本书的迅速出版作出了辛勤的努力，在此也表示感谢。此外，曾雁、陈波同志完成了部分文稿的录入工作，在此一并表示感谢。

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反病毒方面的书刊资料，在此不一一列举。谨向有关资料的作者表示谢意。谨向在反病毒实践中作出贡献的国内外专家表示敬意！

虽然作者用意良苦，但毕竟水平有限，加之资料收集不很全面，书中难免有遗漏和错误之处，敬请读者和计算机同行朋友们不吝赐教。

编著者

1995年9月于瑶台

目　录

上　篇　计算机病毒及其防护

中　篇　最新实用反病毒软件使用指南

下 篇 手工反病毒

上　篇
计算机病毒及其防护

计算机病毒的出现不但影响到计算机应用事业的发展，同时也严重阻碍了计算机技术的进步。作为一般的计算机用户，要能正确认识计算机病毒及其危害，有效地防护由计算机病毒带来的对计算机信息系统安全的威胁，必须在正确认识计算机病毒的基础上，了解其一般表象及症状，并树立健康的反病毒思想。

第一章　计算机病毒的基本知识

当今的计算机系统本质上是一种程序控制的装置，用户可以共享系统的程序和数据资源，可以自己编写程序，也可以调用系统提供的程序，将若干不同功能的程序模块联机，装配成一个整体，用户可以命名进行授权使用。总之，程序体在系统内是可以传输、调用和复制的。

在相当一段时间，人们强调计算机系统向用户提供实用窗口和友好界面，而忽略了潜在的不安全因素。当一个具有破坏性的程序，在计算机之间进行传输并自己进行复制时，它给计算机系统带来的严重后果，使人们感到震惊。

人们对本来十分熟悉的东西突然感到迷惑不解，感到新奇和陌生，不能不说带有一定的戏剧性。事实上，人们对合法使用程序和系统资源是习惯的和熟悉的，对于非授权程序体的入侵和复制却了解得实在太少，甚至在一段时间里停留在很原始的水平上。

1.1　计算机病毒的基本概念

1.1.1　计算机病毒的定义及特征

1. 计算机病毒的定义

计算机病毒是隐藏在计算机系统的数据资源中、利用系统资源进行繁殖并生存，能够影响计算机系统正常运行并通过系统数据资源共享的途径进行传染的程序。这种计算机病毒程序一般要在计算机系统内，经历反复地自我繁殖和扩散，使计算机系统出现异常，最终导致计算机系统发生故障，甚至瘫痪。由于这种程序的特性和所经历的过程与生物病毒极为相似，所以人们称它为“计算机病毒”。

如果说人为设计的计算机病毒程序为源病毒的话，则有一类相对应的病毒应该称为计算机病毒变体(Computer Virus－Variance)。

所谓计算机病毒变体，是指在计算机系统运行过程中，计算机病毒可以将自身程序有修改地拷贝到其它程序体内，其病毒再生体是来源于同一种病毒而表现形式不同的计算机病毒系列。

2. 计算机病毒特征

计算机病毒一般有下列特点：

1) 病毒是人为编制的程序

病毒程序的设计者往往对计算机内部结构比较熟悉，程序设计短小精悍、技巧性强，这样就使得病毒程序不易被人察觉和发现。

2) 隐蔽性

计算机病毒的源程序可以是一个独立的程序体，源病毒经过扩散生成的再生病毒往往采用附加或插入的方式隐藏在可执行程序或数据文件中，采取分散或多处隐藏的方式；而当有病毒程序潜伏的程序体被合法调用时，病毒程序也"合法"进入，并可将分散的程序部分在所非法占用的存储空间进行重新装配，构成一个完整的病毒体投入运行。

3) 传染性

病毒程序一旦进入计算机系统就开始寻找其能够感染的对象并通过自我复制迅速地传播到整个系统。例如微型计算机的计算机病毒，可以在运行过程中根据病毒程序的中断请求随机读写，不断进行病毒体的扩散。病毒程序一旦加到当前运行的程序的程序体上面，就开始搜索能进行感染的其它程序，从而使病毒很快扩散到磁盘存储器和整个计算机系统。

4) 潜伏性

病毒感染计算机系统后，往往并不立即发作，它可以在几天、几周甚至几个月、几年内悄悄地繁殖和扩散而不被发觉，并使得许多数据资源成为病毒的"携带者"而迅速向外传播。

5) 表现性(破坏性)

病毒设计者的目的在于影响计算机系统，因此它势必要表现自己的存在，对计算机系统实施攻击：占用系统资源、破坏系统数据、干扰系统的正常运行，甚至于摧毁系统。

计算机病毒的这些特征是与其构成、传染以及表现(破坏)机制密切相关的。

1.1.2 计算机病毒的作用机制

本节介绍计算机病毒的作用机制及其相关问题，先介绍计算机病毒的一般构成，然后逐个分析计算机病毒的3大作用机制：引导机制、传染机制和破坏机制。目的在于更加深入地认识计算机病毒，为有效地进行计算机病毒的防治，掌握计算机病毒防范的技术方法作一些准备。

1. 计算机病毒的一般构成

计算机病毒代码的结构一般来说包括3大功能模块，即引导模块，传染模块和破坏/表现模块。其中，后两个模块各包含一段触发条件即检查代码，它们分别检查是否满足传染触发的条件和是否满足表现触发的条件，只有在相应的条件满足时，病毒才会进行传染或表现/破坏。必须指出的是，不是任何病毒都必须包括这3个模块。例如，维也纳(Vienna)病毒就没有引导模块，巴基斯坦(Pakistani Brain)病毒则没有破坏模块。

病毒的一般模块构成可用图 1－1 表示。

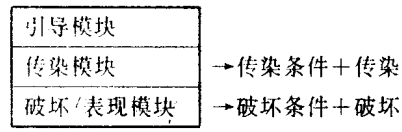


图　1－1

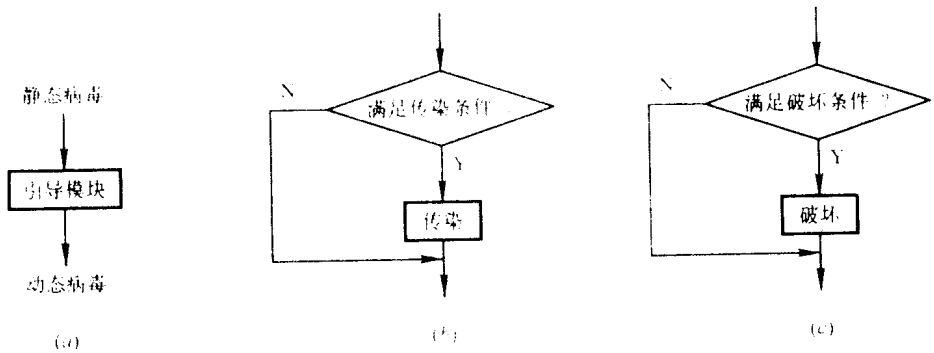
3 个模块各自的作用是这样的，引导模块将病毒由外存引入内存，使后两个模块处于活动状态。传染模块显然用来将病毒传染到其它对象上去。破坏/表现模块实施病毒的破坏作用，如删除文件，格式化磁盘等，由于有些病毒的该模块并没有明显的恶意破坏作用，而只是进行一些视屏或发声方面的自我表现作用，故该模块有时又称表现模块。本节之后的内容中将根据具体病毒将该模块称为破坏模块或表现模块。

2. 计算机病毒的状态

计算机病毒有两种状态，即静态病毒和动态病毒。静态病毒是指存储介质(例如软盘，硬盘，磁带等)上的计算机病毒。静态病毒没有处于加载状态，不能执行病毒的传染或破坏作用。病毒的传染和破坏主要是由动态病毒进行的。动态病毒是指已进入内存，正处于运行状态的计算机病毒。内存中处于活动状态的病毒时刻监视系统的运行，一旦传染条件或破坏条件被触发，即调用其传染代码段或破坏代码段，使病毒得以扩散，系统蒙受损失。动态病毒在 RAM 中存在的时间称为动态病毒的生命期。动态病毒的生命期可长可短，有些病毒的动态病毒只在运行宿主程序的瞬间存在，运行完即退出内存。但是，大多数病毒则是自第一次被运行后即保留在内存中了，它的生命期较长，会一直延续到下一次重新启动或关机。

3. 计算机病毒的一般工作流程

了解了计算机病毒的一般构成和它的两种状态，我们就可以来考察计算机病毒的一般工作流程了。首先，通过第一次非授权的加载，计算机病毒的模块被执行，病毒由静态转为动态。尔后，动态的病毒通过某种触发手段(多为中断)不断地检查是否满足传染条件或破坏条件，一旦满足，则执行相应的传染功能。简单的流程如图 1－2 所示。



(a)　(b)　(c)

图　1－2

图 1－2 中，我们没有把 3 个流程连在一起，是因为它们各自的运行在时间上不一定是连续的。执行完病毒引导模块后，可能就直接退出病毒代码，以后两个模块要到触发了某一机制时才执行，例如通过 DOS 的 INT 13H(磁盘操作中断)或 INT 21H 的 DOS 功能调用等。

1.1.3　计算机病毒的工作原理

前面提到，计算机病毒的引导模块主要是将静态病毒激活成为动态病毒。这一过程是

如何实现的呢？引导模块还有没有其它功能呢？下面详细分析这两个问题。

病毒程序将自身一段程序代码保留在内存中有两种手段，一种是通过程序驻留；另一种方法是将病毒代码移到内存最高端，然后把内存大小指示单元减少几千字节，以欺骗DOS使之不会再使用最高端的病毒代码所占用的空间。这两种情况下，内存病毒均通过某些修改了的中断调用而取得执行权，这样获得执行权的一般是传染模块和破坏模块。

因此，我们说病毒的引导模块除了把病毒程序代码引入内存外，还有另外两个功能：其一，对内存的病毒代码采取保护措施，使之不会被覆盖；其二，要对内存中的病毒代码设定某种激活方式，使之在适当的时候能取得执行权。病毒的引导模块既可能与其它两模块一起运行，也可能与另两个模块中的一个一起运行，甚至于独自先运行。

上一节已提到过，并非所有病毒都包括引导模块，如果动态病毒是瞬时的，也就是说，病毒代码运行完以后就全部退出内存，那么这种病毒是不含引导模块的，DOS本身的加载机制使病毒取得瞬间动态，而这一瞬间，动态病毒执行了传染和破坏两个模块。显然，这种病毒的隐蔽性更强，因为内存中的病毒停留时间是如此之短，使你几乎无法察觉。

1. 计算机病毒的传染机制

计算机病毒最重要的特点就是具有传染性，是否具有传染性是区分一段程序代码是否为计算机病毒的主要特征。那么计算机病毒是怎样进行传染的呢？

1）计算机病毒的传染过程

计算机病毒总是借助于一定载体而存在的。计算机病毒的传染就是指计算机病毒从一个载体侵入另一个载体的过程。根据研究的范围不同，传染的含义也不同。对于网络系统而言，计算机病毒的传染是指计算机病毒由一个计算机系统进入另一个计算机系统的过程，这里的载体指的是单一的计算机系统。对于非联网的微机用户，计算机病毒的传染仍有两个层次，高层传染是指计算机病毒从一个存储介质侵入另一个存储介质，这些存储介质通常是软盘、硬盘或磁带等。低层传染是计算机病毒从一个文件侵入另一个文件。传染过程可以用图1－3表示。

其中载体可分为3个层次，如图1－4所示。

图　1－3

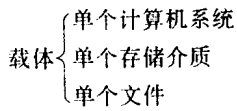


图　1－4

计算机病毒传染的过程是这样的：网络上的传染利用网络间通信实现。存储介质或文件间的传染一般利用RAM作中间媒体，即先由带毒介质或文件进入RAM，再由RAM侵入一无毒介质或文件，如图1－5所示。

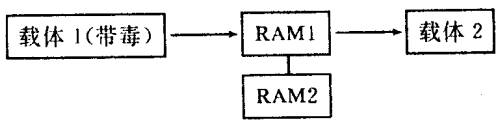


图　1－5

从带毒载体进入内存，一般利用了操作系统的加载机制或引导机制。当系统运行一个带毒文件或用一带毒系统盘启动时，病毒就进入内存。而从RAM侵入无毒介质则利用了操作系统的读写磁盘中断或加载机制。内存中的病毒时刻监视着操作系统的每一个操作，一

且该操作满足病毒设定的传染条件(通常为访问一无毒盘或加载一无毒文件等)，病毒程序便将自身代码拷贝到受攻击目标上去，使之受传染。

以上病毒传染都是利用其自身的传染机制实现的，是病毒的主动攻击；通常见到的还有另一种传染，例如，把一个带毒的文件拷贝到一新盘上去或对一个带毒盘作全盘拷贝都会使新盘受到传染，这种传染是一种被动传染，这期间病毒的传染机制并没起作用。主动传染和被动传染在效果上是等效的，但后者的成功取决于用户对病毒的存在不知不觉。

2) 计算机病毒的传染途径

计算机病毒传染的途径有两种，一种是利用磁性存储介质(如磁盘或磁带)等传染载体进行传染。病毒最先隐藏在磁介质中，当一台计算机使用该介质时，病毒进入系统。目前使用得最多得是软盘；另一种是以网络作为传染载体。计算机网络是在一定的通信协议及网络操作系统支持下而实现的一种数据共享环境。它包括主机、工作站、节点机及终端设备等设施。各设施之间的通信或数据共享为计算机病毒的传染提供了机会。由于我国计算机网络化的程度还不高，目前计算机病毒的传染主要是通过前一途径进行的，下面我们着重介绍前者的实现。

利用存储介质的传染，是以操作系统的加载机制和存储机制为基础的。不经过文件的存取，介质上的病毒就不会进入 RAM；而没加载运行则不会有文件的存取。文件型病毒与操作系统型病毒传染的实现有一些不同。

我们先看一个操作系统型病毒传染的实例。假定用硬盘启动，且该硬盘已染上了小球病毒(Bouncing Ball)，那么加电自举以后，小球病毒的引导模块就把全部病毒代码 1 024 字节保存到了内存的 97C0:7C00H 处(即 RAM 最高段)。然后修改 INT 13H 的中断向量，使之指向病毒的传染块。以后，一旦通过 INT 13H 进行读写磁盘的操作，计算机病毒的传染块便取得控制权，它就进行如下操作：

(1) 读入目标盘的自举扇区(BOOT 扇区)；

(2) 判断是否满足传染条件；

(3) 如果满足传染条件(即目标盘 BOOT 区的 01FCH 偏移位置为 5713H 标志)，则将病毒代码的前 512 字节写入 BOOT 引导程序，将其后 512 字节写入某一空簇，随后将该簇标以坏簇标志，以保护该簇不被重写；

(4) 跳转到原 INT 13H 的入口，执行正常的系统操作。

这样，小球病毒就完成了对一磁盘的传染过程。

我们再来看看一个文件型病毒的传染过程。假如 VVV.COM(或 .EXE)文件已染有耶路撒冷(Jerusalem)病毒，那么运行该文件后，耶路撒冷的引导模块就会修改 INT 21H 的中断向量，使之指向病毒传染模块，并将病毒代码驻留内存，之后退回操作系统。这样，以后再有任何加载执行文件的操作，病毒的传染模块将通过 INT 21H 的调用获得控制权，进行以下操作：

(1) 读出该文件特定部分；

(2) 判断是否满足传染条件；

(3) 如果满足条件，则用某种方式将病毒代码与该可执行文件链接，链接后把文件重新写入磁盘；

(4) 转原 INT 21H 入口，对该执行文件进行正常加载。

这样，耶路撒冷病毒就完成了一次传染过程。染上文件型病毒的文件，这种病毒在磁盘上存储的方式对于 .COM 执行文件和 .EXE 执行文件是有所区别的。

病毒在 .COM 文件上的链接存储方式如下所述。

病毒侵入一个 .COM 文件后，一般要保证运行时先运行病毒块，再运行原文件。在存储上，病毒既可放在原文件前面，也可放在后面，因而其链接方式有两种。

方式一的处理过程是先将原文件读到病毒代码的后面，然后两部分一起存盘。

方式二是将原文件前 3 字节保存到病毒代码中去，然后将磁盘上原文件的前 3 字节改为一个 JMP 指令，使之转移到文件尾，最后在文件尾增加病毒代码。

图 1－6 为两种方式分别链接出的带毒文件。

病毒对 .EXE 文件的链接存储方式如下所述。

对于 .EXE 文件感染的病毒，其链接手段与 .COM 文件基本是一致的，即通过把病毒写入原文件的后面，然后修改文件头格中的寄存器初始化控制信息，使病毒段先被运行，在病毒段退出前再根据病毒代码中保存的原寄存器初值控制信息转原文件执行。图 1－7 为 .EXE文件受病毒感染后的结果。

图 1－6　　图 1－7

病毒链接时的处理一般都保证了执行带毒文件时，先运行病毒代码，再运行原正常文件。对于病毒代码在前的链接存储方式，这样运行是很自然的事，对于病毒代码在后的链接存储方式，要达到这一目标，有两种链接方式。对于 .COM 文件，多利用将文件最前面若干字节(如 3 个字节)存到病毒代码里去，然后在最前面放一 JMP 指令，使之跳到病毒代码执行，等病毒代码执行完后，再恢复文件前几字节，转去执行。对于 .EXE 文件，则可利用修改 .EXE 文件头格中的控制信息，使加载定位后的运行体从病毒代码段开始运行。

无论文件型病毒还是操作系统型病毒，其传染过程总的来说是相似的，可归纳如下：

(1) 驻入内存。病毒停留在内存中，监视系统的运行，选择机会进行传染。这一步通常由引导模块实现，如没引导模块，则这一步也不会有。

(2) 判断传染条件。传染模块被激活后，会马上对攻击目标进行判断，以决定是否传染之。

(3) 传染。通过适当的方式把病毒写入磁盘，同时保证被攻击的对象(引导记录、原执行文件)仍可正常运行，即进行的是传染而非破坏，因为病毒要以一个特洛伊木马(Trojan horse)的形式寄生。

文件型病毒与操作系统型病毒在传染上的主要区别是其传染模块激活的方式不同，操作系统型多用 INT 13H，文件型多用 INT 21H。当然，如我们前面已强调的，计算机病毒可以在第一次运行时就执行传染模块，而无需驻留内存后再用中断去激活。例如，操作系统型病毒的大麻病毒(对磁盘传染部分)和文件型病毒的维也纳病毒即如此。

3) 计算机病毒的传染方式

计算机病毒的传染方式，大体可归为以下方式：

(1) 病毒程序的直接传染方式(图 1－8)。源病毒 CV 将病毒传播给程序对象 P1，P2，…，Pn，程序 Pi($1 \leqslant i \leqslant n$)中的 CV 是源病毒的再生病毒。

(2) 病毒程序的间接传染方式(图 1－9)。源病毒程序将病毒传染给程序对象 P1，P1 再将病毒传染给 P2，以此继续传播下去。

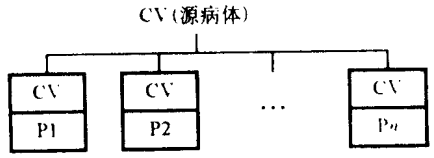


图　1－8

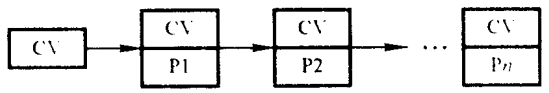


图　1－9

4) 计算机病毒的交叉传染方式

计算机病毒的传染已经成为一个世界性的问题。在目前世界上已出现的多种病毒中，有相当一部分是攻击 IBM PC 及其兼容机的。这就不可避免地出现了一个计算机系统同时染上几种病毒的所谓交叉感染的现象。

病毒的交叉传染使得病毒传染、破坏的行为变得更为复杂，从而对病毒的免疫和解毒增加了困难。为了解决这些困难，本小节分析一下计算机病毒交叉感染的细节。

计算机病毒的交叉感染分为两类，一类是同类型计算机病毒的交叉感染。例如同是操作系统型的小球病毒和大麻病毒的交叉感染，或同是文件型的耶路撒冷和扬基都德病毒的交叉感染。另一类是不同型的计算机病毒的交叉感染，如操作系统型的小球病毒和文件型的耶路撒冷病毒同时侵入系统。后一类交叉感染病毒之间较少相互影响，一般不会使病毒作用的行为发生改变。而前一类交叉感染使得病毒的藏身位置，传染方式有一定改变，给病毒免疫和解毒带来了困难。我们着重分析前一种情况的交叉感染。

首先，我们指出一点，病毒的交叉感染所指的对象不是固定的，例如，同为操作系统型病毒的交叉感染的对象一般是指同一张盘，而同为文件型病毒的交叉感染的对象一般是指单个文件。

同类病毒交叉感染可能使病毒之间互相影响，它们争夺静态藏身位置，争夺传染控制权，造成了病毒作用复杂化。若有一带有两种同类病毒的传染源，通过某种加载，两种病毒均进入 RAM，那么遇到第一个传染目标后，哪种病毒会先攻击呢？它取决于什么呢？我们就两种不同病毒作一分析。

如果一张存有系统文件的软盘，同时带有操作系统型的小球病毒和大麻病毒，当用该盘启动时，两种病毒都会进入内存，以后两种病毒传染的先后与进入内存的先后有关。假定这张软盘先感染了小球病毒，以后又感染了大麻病毒。显然，刚感染小球病毒时，BOOT 区放的是小球病毒的一部分代码，而正常引导程序被移到某一空簇上去了；再染上大麻病毒后，BOOT 区里的小球病毒又被移走，新占据的是大麻病毒。因此，用这张软盘启动时，BOOT 区大麻病毒先运行而进入内存，然后大麻病毒把小球病毒当作原 BOOT 区的引导程序加载运行，使得小球病毒进入内存，最后由小球病毒加载真正的引导程序。可见后染的病毒先被运行而进入内存。传染模块是通过 INT 13H 的入口被修改指向大麻病毒传染块，小球病毒再进入，INT 13H 先触发小球病毒，由其判断是否传染，然后由大麻病毒判断是否传染。如果两个传染条件都满足，那么传染顺序肯定是先传染小球病毒，再传染大麻病毒这么一个先后顺序。当然，如果传染目标只满足两病毒中的一种的传染条件，那么传染