现代计算机最新反病毒技术

现代计算机
最新反病毒技术

刘丽华　编著

上海科学技术出版社

现代计算机最新反病毒技术

上海科
版社

现代计算机最新反病毒技术

刘丽华　编著

上海科学技术出版社

内 容 简 介

本书从实际应用的角度出发，详细地论述了当今计算机病毒的现象、诊治、解毒及预防方法；系统地剖析了当今国内最为流行的“小球病毒”、“大麻病毒”、“Brain 病毒”、“黑色星期五病毒”、“无名引导型病毒”；并针对实际应用中用户遇到的有关这几类病毒常见的问题进行解答。通过分析源程序代码，讨论了计算机病毒的基本构造、传播机理、解剖技术、相关的 DOS 技术知识。书中详细地介绍了 SOS 解毒软件的功能及操作使用，并讨论了“病毒克星”软件诊治 DOS 上的主引导扇区寄生型、引导扇区寄生型、中断服务程序寄生型的病毒以及诊断一切可执行文件寄生型病毒。

现代计算机最新反病毒技术
刘丽华 编著
上海科学技术出版社出版、发行
（上海瑞金二路450号）
新华书店上海发行所经销 常熟第七印刷厂印刷
开本787×1092 1/16 印张11.75 字数268,000
1993年9月第1版 1993年9月第1次印刷
印数 1—7,000
ISBN7-5323-3129-6/TP·32
定价：6.90元

（沪）新登字108号

前　言

自从1989年计算机病毒大量流入我国，引起各方面忧虑和重视。对计算机病毒防范的研究已成为重大课题。由于计算机病毒在世界许多国家和地区的大肆干扰，而且仍在迅速蔓延，种类不断增加。目前国内最为流行的计算机病毒有“小球病毒”、“大麻病毒”、“Brain病毒”、“黑色星期五病毒”以及最新流行的“无名引导型病毒”等。随着当今计算机应用的推广和普及，各种版本DOS和应用软件的广泛交流，非法复制软盘的现象日益严重，加之机器管理缺乏严格的制度，致使计算机病毒迅速蔓延。由于计算机病毒的存在，轻则使计算机降低运行速度，滋扰正常运转，重则破坏数据，毁损存储的信息资源。若任其滋生、蔓延，严重后果自不待言。

目前计算机用户急需了解病毒解除的方法以及如何免除病毒再次攻击，从根本上控制已知的、未来新产生的和再变种的各种病毒的传播和危害，为此编写了《现代计算机最新反病毒技术》一书。本书从内容上既注重理论分析，又着眼于实际问题的解决以及提高检测、监测、排除、预防病毒的能力和操作方法，也因此而具有较强的实用性。全书共分八章：第一章计算机病毒概述，介绍有关计算机病毒分类、特征、寄生方式、一般工作机理，最后落实到计算机病毒常用判别方法和处理的一般操作步骤；第二章计算机病毒的原理与诊治，详细地介绍了病毒的产生、感染、破坏及防治过程；第三章计算机病毒解析技术基础，由计算机的物理结构及各种与病毒有关的中断介绍病毒的侵入过程；第四章计算机典型病毒的分析及相关技术，分析了当今流行最广的几种计算机病毒及防治方法；第五章SOS反病毒软件的应用，介绍了最新SOS反病毒软件的使用及操作方法；第六章计算机病毒诊治软件SCAN及解毒软件KILL的应用，详细地介绍了诊治和解毒软件的使用及消毒免疫技巧；第七章计算机“病毒克星”使用说明与应用，主要介绍当今流行的各种病毒的防治软件的使用、预防及免疫；第八章实际应用中用户常遇到的有关病毒问题解答，主要针对当今流行的典型病毒常遇到的各种问题进行解答，有很强的实用性。

本书可供各类计算机软件编译及维护人员参考，亦可作为各类计算机专业人员的参考书。

本书在编写过程中，由于时间紧迫和水平所限，难免有一些失误和不妥之处，敬请批评指教。

刘丽华

1992年9月

目　录

第一章　计算机病毒概述

第一节　计算机病毒简介

一、计算机病毒的定义

我们可以从不同角度给出计算机病毒的定义。一种定义是通过磁盘、磁带和网络等作为媒介传播扩散，能"传染"其他程序的程序。另一种是能够实现自身复制且借助一定的载体存在的具有潜伏性、传染性和破坏性的程序。还有的定义是一种人为制造的程序，它通过不同的途径潜伏或寄生在存储媒体(如磁盘、内存)或程序里。当某种条件或时机成熟时，它会自生复制并传播，使计算机资源受到不同程序的破坏等等。这些说法在某种意义上借用了生物学病毒的概念，计算机病毒同生物病毒所相似之处是能够侵入计算机系统和网络，危害正常工作的"病原体"。它能够对计算机系统进行各种破坏，同时能够自我复制，具有传染性。所以，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，当达到某种条件时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。

与生物病毒不同的是，几乎所有的计算机病毒都是人为地故意制造出来的，有时一旦扩散出来后连编者自己也无法控制。它已经不是一个简单的纯计算机学术问题，而是一个严重的社会问题了。

二、计算机病毒出现的条件

计算机病毒的产生是计算机技术和以计算机为核心的社会信息化进程发展到一定阶段的必然产物。它产生的背景是：

1．计算机病毒是计算机犯罪的一种新的衍化形式

计算机病毒是高技术犯罪，是某些人恶作剧和报复心态在计算机应用领域的表现。具有瞬时性、动态性和随机性，不易取证，风险小破坏大，从而刺激了犯罪意识和犯罪活动的特点。

2．计算机软硬件产品的脆弱性是根本的技术原因

计算机是电子产品，数据从输入、存储、处理、输出等环节，易误入、篡改、丢失、作假和破坏；程序易被删除、改写；计算机软件设计的手工方式，效率低，生产周期长，人们至今没有办法事先了解一个程序有没有错误，只能在运行中发现，修改错误，并不知道还有多少错误和缺陷隐藏在其中，这就为病毒的侵入提供了方便。

3．微型计算机的普及应用是计算机病毒产生的必要环境

1983 年 11 月 3 日美国计算机专家首次提出了计算机病毒的概念并进行了验证。几年前计算机病毒就迅速蔓延，到我国才是近年来的事，而这几年正是我国微机普及应用热潮，微机的广泛普及，操作系统简单明了，软、硬件透明度高，基本上没有什么安全措施，能够透彻了解它内部结构的用户日益增多，对其存在的缺点和易攻击处也了解得越来越清楚，不同的目的可以做出截然不同的选择。目前，在 IBM-PC 系列及其兼容机上广泛流行着各

种病毒就很说明这个问题。

三、计算机病毒的来源

计算机病毒有以下 4 种来源：

① 搞计算机的人员和业余爱好者的恶作剧寻开心制造出的病毒，例如象圆点一类的良性病毒。

② 软件公司及用户为保护自己的软件被非法复制而采取的报复性惩罚措施。因为他们发现对软件上锁，不如在其中藏有病毒对非法拷贝的打击大，这更加大了各种病毒的传播。

③ 旨在攻击和摧毁计算机信息系统和计算机系统而制造的病毒。例如 1987 年底出现在以色列耶路撒冷西伯莱大学的犹太人病毒，就是雇员在工作中受挫或被辞退时故意制造的，它针对性强，破坏性大，产生于内部，防不胜防。

④ 用于研究或有目的而设计的程序，由于某种原因失去控制或产生了意想不到的效果。

四、计算机病毒的分类

在计算机病毒分类中，可根据危害性、激活的时间、入侵方式、传染方式等对其进行分类。按危害性可分为良性和恶性病毒；良性的危害性小，不破坏系统和数据，但大量占用系统开销，将使机器无法正常工作，而陷于瘫痪，如国内出现的圆点病毒就是良性的。恶性病毒可能会毁坏数据文件，也可能使计算机停止工作。若按激活的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。若按其入侵方式可分操作系统型病毒，圆点病毒和大麻病毒是典型的操作系统病毒，这种病毒具有很强的破坏力（用它自己的程序意图加入或取代部分操作系统进行工作），可以导致整个系统的瘫痪；源码病毒，在程序被编译之前插入到 FORTRAN、C或 PASCAL 等语言编制的源程序，完成这一工作的病毒程序一般是在语言处理程序或连接程序中；外壳病毒，常附在主程序的首尾，对源程序不作修改，这种病毒较常见，易于编写，也易于发现，一般测试可执行文件的大小即可知；入侵病毒，侵入到主程序之中，并替代主程序中部分不常用到的功能模块或堆栈区，这种病毒一般是针对某些特定程序而编写的。若按其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险性和难以预防。若按传染方式可分磁盘引导区传染的计算机病毒、操作系统传染的计算机病毒和一般应用程序传染的计算机病毒。若按其病毒攻击的机种可分为攻击微机的，攻击小型机的，攻击工作站的，其中以攻击微型计算机的病毒为多，世界上出现的病毒几乎 90% 是攻击 IBM-PC 机及其兼容机。

当然，按照计算机病毒的特点及特性，计算机病毒的分类方法还有其他的方法，例如按攻击的机种分，按寄生方式分等等。因此，同一种病毒可以有不同的分法。

五、计算机病毒的特点

计算机病毒一般具有以下几个特点：

(1) 破坏性　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。其表现：占用 CPU 时间和内存开销，从而造成进程堵塞；对数据或文件进行破坏；打乱屏幕的显示等。

(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，从而达到扩散的目的。

六、微型计算机病毒寄生的主要载体

计算机病毒是一种可直接或间接执行的文件，是依附于系统特点的文件，是没有文件名的秘密的程序，但它的存在却不能以独立文件的形式存在，它必须是以现有的硬软件资源而存在的。

目前从微机系统的永久性存储设备即外存储器容量角度来讲，硬盘容量是一般软盘容量的几十至几百倍，并且硬盘容量越来越大，软盘分一般密度320KB或360KB，中等密度720KB和高密度1.2MB 3种。微机系统所使用的文件存放于磁盘之中，所以微机的病毒是以磁盘为主要载体的。

七、计算机病毒的寄生方式

计算机病毒一般寄生在以下几个地方：

(1) 寄生在磁盘引导扇区中　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区记录并执行它，将DOS读入内存。病毒程序就是利用了这一点，自身占据了引导扇区而将原来的引导扇区内容及其病毒的其他部分放到磁盘的其他空间，并给这些扇区标志为坏簇。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的高端并占据该范围，然后置触发条件如INT 13H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。如果磁盘没有被感染(通过识别标志)则进行传染。

(2) 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。病毒可以寄生在原程序的首部也可以寄生在尾部，但都要修改源程序的长度和一些控制信息，以保证病毒成为源程序的一部分，并在执行时首先执行它。这种病毒传染性比较强。

(3) 寄生在硬盘的主引导扇区中　例如大麻病毒感染硬盘的主引导扇区，该扇区与DOS无关。

八、计算机病毒在磁盘中存储位置

从目录发现的计算机病毒来分析，病毒在磁盘中的存储位置有两种：

① 存储于磁盘的引导扇区，对软盘来说只有一个引导扇区，而对硬盘来说有些病毒则可能存储在主引导扇区，例如大麻病毒。

② 存储于磁盘的用户空间中，例如黑色星期五病毒，专门感染COM和EXE可执行文件，将自身作为正常程序的一部分和正常程序连接在一起驻留在磁盘用户空间中。

九、计算机病毒的破坏作用

不管是良性病毒还是恶性病毒，对用户都会造成一定的破坏性。目前侵入我国的计算机病毒的破坏情况，主要表现在以下几方面：

① 破坏文件分配表FAT，使用户在磁盘上的信息丢失。例如在长城0520CH机上打印时多次发现CLLB24字库文件存在，而当运行3070打印机的驱动程序3.COM时，屏幕

总提示“无字库文件”，将存在硬盘上的 CLLB24 文件删除，用 RESTORE 命令再将该字库文件还原到 C 盘上，再运行 3.COM 还是提示无字库文件，其原因就是大麻病毒破坏了硬盘 DOS 文件分配表，虽然文件还存在但文件名与文件数据失去了联系。

② 删除软盘上或者硬盘上的可执行文件或数据文件。如果删除的文件是系统文件，则会导致这片盘不能引导系统。例如黑色星期五病毒当某月 13 日又为星期五时，运行.COM 或 EXE 文件将会删除该文件。1990 年 4 月 15 日是北京晚报报道我国有些地方的计算机在 4 月13日激发了感染上的“13日星期五”病毒，计算机工作效率或程序受到不同程度的破坏。

③ 修改或破坏文件中的数据。

④ 改变磁盘分配，造成数据写入错误。

⑤ 影响内存常驻程序的正常执行。

⑥ 在磁盘上产生坏的扇区，使磁盘可用空间减小。

⑦ 更改或重写磁盘的卷标。

⑧ 使内存可用的空间因病毒程序自身在系统中的多次复制而减小，使得正常的数据或文件不能存储。

⑨ 对整个磁盘或磁盘的特定磁道或扇区进行格式化。

⑩ 在系统中产生新文件。

⑪ 改变系统的正常运行过程。

十、计算机病毒的共性

从已经发现的计算机病毒来看，不管哪种病毒它们都具有一些共同的特性。主要表现在：

(1) 修改引导扇区或可执行文件　它是修改的方法一种替代，例如圆点病毒以有毒引导扇代替正常引导扇，一种是链接，要么病毒程序链接在文件首部，例如感染的黑色星期五病毒.COM文件，要么链接在文件尾部，例如被感染的.EXE 文件，要么链接在文件的中间。

(2) 通过驻留内存进行感染　传染是计算机病毒的一大特征。任何一种病毒都是通过驻留内存进行传染。当启动系统或执行被感染的软件时，病毒随之被读入内存，并常驻内存，监视系统的运行，随时攻击要攻击的目标，把病毒传播到无毒载体上，但前提条件是病毒驻留内存。

(3) 修改中断服务处理程序的入口地址　病毒程序被引导常驻内存的过程中，通常作法是修改系统的中断程序的入口地址，也叫系统的中断向量。例如 INT13H 磁盘读写操作或系统功能调用 INT21H。病毒为了进行传染，就必须不时的调用驻留内存的病毒代码，作为长城系列或 IBM-PC 系列机实现这种目的最方便的办法是修改中断程序的入口地址，让系统中断经常转向病毒的控制部分，这样一旦执行磁盘的读写请求或加载执行的程序，则首先进入病毒程序，让病毒自身繁殖传染给被读写的磁盘或被加载执行的程序，然后再转移到原中断程序入口地址完成正常的操作。

第二节　计算机病毒的感染方式

一、计算机病毒传染的先决条件

计算机病毒的传染是以计算机系统的运行及读写磁盘为基础的。没有这样的条件，计

算机病毒是不会传染的，因为计算机不启动不运行时，就谈不上对磁盘的读写操作或数据共享，没有磁盘的读写，病毒就传播不到磁盘上或网络里。所以只要计算机运行就会有磁盘读写动作，病毒传染的第一步是驻留内存，一旦进入内存之后，寻找传染机会，寻找可攻击的对象，判断条件是否满足，决定是否可传染，当条件满足时进行传染，将病毒写入磁盘系统。

二、计算机病毒传染通过的途径

计算机病毒之所以称之为病毒是因为其具有传染性的本质，传染渠道通常有以下几种：

(1) 通过软盘　通过使用外界被感染的软盘，例如，不同渠道来的系统盘，来历不明的软件、游戏盘等是最普遍的传染途径。由于使用带有病毒的软盘，使机器感染病毒发病，并传染给未被感染的"干净"的软盘。大量的软盘交换，合法或非法的程序拷贝，不加控制的随便在机器上使用各种软件造成了病毒感染，泛滥蔓延的温床。

(2) 通过硬盘　通过硬盘传染也是重要的渠道，由于带有病毒机器移到其他地方使用，维修等，将干净的软盘传染并再扩散。

(3) 通过网络　这种传染扩散极快，能在很短时间内传遍网络上的机器。

目前在我国现阶段，计算机普及程度低，还没有形成大的网络，基本上是单机运行，所以网络传染还没构成大的危害，因此主要传播途径是通过软盘。

三、计算机病毒对微型计算机系统的影响

计算机病毒对微机而言，它的影响表现在：

① 破坏硬盘的分区表，即硬盘的主引导扇区。

② 破坏或重写软盘或硬盘 DOS 系统 BOOT 区，即引导区。

③ 影响系统运行速度，使系统的运行明显变慢。

④ 破坏程序或覆盖文件。

⑤ 破坏数据文件。

⑥ 格式化或者删除所有或部分磁盘内容。

⑦ 直接或间接破坏文件连接。

⑧ 使被感染程序或覆盖文件的长度增大。

四、计算机病毒传染的一般过程

在系统运行时，病毒通过病毒载体即系统的内存储器进入系统的内存。该病毒在系统内存中监视系统的运行。当它发现有攻击的目标存在并满足条件时，便从内存中将自身存入被攻击的目标，从而将病毒进行传播，而病毒利用系统INT13H读写磁盘的中断又将其写入系统的外存储器软盘或硬盘，再感染其他系统。

五、可执行文件被计算机病毒传染后的情况

可执行文件.COM 或.EXE 感染上了病毒，例如黑色星期五病毒，它驻入内存的条件是执行被传染的文件。一旦进入内存，便开始监视系统的运行。当它发现被传染的目标时，进行如下操作：

① 首先对运行的可执行文件特定地址的标识位信息进行判断是否已感染了病毒；

② 当条件满足，利用 INT13H 将病毒链接到可执行文件的首部或尾部或中间，并存入磁盘中；

③ 完成传染后，继续监视系统的运行，试图寻找新的攻击目标。

六、操作系统病毒的感染

正常的PCDOS启动过程是：

① 加电开机后进入系统的检测程序并执行该程序对系统的基本设备进行检测；

② 检测正常后从系统盘0面，0道，1扇区即逻辑0扇区读入BOOT引导程序到内存的0000:7C00处；

③ 转入BOOT执行之；

④ BOOT判断是否为系统盘，如果不是系统则提示：

non-system disk or disk error

Replace and strike any key when ready

否则，读入IBM BIO.COM和IBM DOS.COM两个隐含文件；

⑤ 执行IBM BIO.COM和IBM DOS.COM两个隐含文件，将COMMAND.COM装入内存；

⑥ 系统正常运行，DOS启动成功。

如果系统盘已感染了病毒，PCDOS的启动将是另一番景象，其过程为：

① 将BOOT区中病毒代码首先读入内存的0000:7C00处；

② 病毒将自身全部代码读入内存的某一安全地区，常驻内存，监视系统的运行；

③ 修改INT13H中断服务处理程序的入口地址，使之指向病毒控制模块并执行之。因为任何一种病毒要感染软盘或者硬盘，都离不开对磁盘的读写操作，修改INT13H中断服务程序的入口地址是一项少不了的操作；

④ 病毒程序全部被读入内存后，才读入正常的BOOT内容到内存的0000:7C00处，进行正常的启动过程；

⑤ 病毒程序伺机等待随时准备感染新的系统盘。

如果发现有可攻击的对象，病毒要进行下列的工作：

① 将目标盘的引导扇读入内存，对该盘进行判别是否传染了病毒；

② 当满足传染条件时，则将病毒的全部或者一部分写入BOOT区，把正常的磁盘的引导区程序写入磁盘特定位置；

③ 返回正常的INT13H中断服务处理程序，完成了对目标盘的传染。

七、计算机病毒的软、硬盘的感染

操作系统型病毒只有在系统引导时进入内存。如果一个软盘染有病毒，但并不从它上面引导系统，则病毒不会进入内存，也就不能活动。例如圆点病毒感染软盘、硬盘的引导扇区，只要用带病毒的盘启动系统后，病毒便驻留内存，对哪个盘进行操作就对哪个盘进行感染。

八、计算机病毒对非系统盘感染后的处理方法

因为操作系统型病毒只有在系统引导时才进入内存，开始活动，对非系统盘感染病毒后，不从它上面引导系统，则病毒不会进入内存。这时对已感染的非系统盘消毒最简的方法是将盘上有用的文件拷贝出来，然后将带毒盘重新格式化即可。

九、计算机病毒的主要症状

从目前发现的病毒来看，主要症状有：

① 由于病毒程序把自己或操作系统的一部分用坏簇隐蔽起来，磁盘坏簇莫名其妙地增

多。

② 由于病毒程序附加在可执行程序头尾或插在中间，使可执行程序容量增大。

③ 由于病毒程序把自己的某个特殊标志作为标签，使接触到的磁盘出现特别标签。

④ 由于病毒本身或其复制品不断侵占系统空间，使可用系统空间变小。

⑤ 由于病毒程序的异常活动，造成异常的磁盘访问。

⑥ 由于病毒程序附加或占用引导部分，使系统引导变慢。

⑦ 丢失数据和程序。

⑧ 中断向量发生变化。

⑨ 打印出现问题。

⑩ 死机现象增多。

⑪ 生成不可见的表格文件或特定文件。

⑫ 系统出现异常动作，例如：突然死机，又在无任何外界介入下，自行起动。

⑬ 出现一些无意义的画面问候等显示。

⑭ 程序运行出现异常现象或不合理的结果。

⑮ 磁盘的卷标名发生变化。

⑯ 系统不承认磁盘或硬盘不能引导系统等。

⑰ 在系统内装有汉字库正常的情况下不能调用汉字库或不能打印汉字。

⑱ 在使用写保护的软盘时屏幕上出现软盘写保护提示。

⑲ 异常要求用户输入口令。

十、计算机病毒的种类

迄今为止，全世界发现的计算机病毒有将近300种，其中的一部分已在世界各地蔓延。其传播之快，生命力之强，危害之广为计算机界所震惊。而且直至今日，病毒蔓延的势头有增无减，它所造成的计算机资源破坏以及对人类社会的各个领域带来的影响无法统计也难以预测。在我国，计算机病毒的入侵还仅仅是个开始。随着与国际技术交流的不断增加，计算机病毒的危害性将成为急待解决的一大社会和技术问题。

目前传入我国的计算机病毒主要有以下几种，它们是：

(1) 小球 (Bouncingball) 病毒　别名：弹球病毒、乒乓、圆点病毒、001病毒、TYPE-A病毒。

(2) 大麻(Marijuana)病毒　别名：Stoned 病毒、Marijuana病毒和石头病毒。

(3) 黑色星期五病毒　别名：犹太人病毒，以色列病毒，耶路撒冷病毒，希伯莱病毒，长方块病毒，疯狂拷贝病毒。

(4) 维也纳病毒　别名：648病毒；

(5) 扬基病毒　别名：美国佬病毒、涂鸦病毒。

(6) 1701/1704病毒。

(7) 雨点病毒　别名：感冒病毒，落花病毒。

(8) 巴基斯坦智囊(Brain)病毒。

为了使读者对计算机病毒有更广泛的了解，下面对一些在我国尚未出现但在国外已有很高知名度的病毒作一简单介绍。

1. 以恶作剧形式出现的病毒

(1) “星期天病毒”(Sunday,在西雅图发现) 其每周星期天发作。在显示出“今天是星期天,何必这么辛苦呢?”之后,捣毁FAT表,使磁盘数据完全破坏。

(2) “荷兰女孩病毒” (Holland Girl, 在荷兰发现) 在其1332字节的病毒程序中提供了一个名为“Sylvia”的荷兰女孩的征婚广告。

(3) “Amstrad”病毒(在葡萄牙发现) 感染.COM文件,在增加的847字节的病毒程序中,携带了一份“Amstrad”计算机的假广告……。

像这些以恶作剧的形式出现的计算机病毒,形式各异,花样不断翻新,被这些病毒侵扰后,常常被搞得哭笑不得,而又无可奈何。

2. 专门对数据进行破坏或修改的病毒

(1) “魔鬼的舞蹈” (Devil's Dance 在墨西哥城发现) 感染.COM文件,增加941字节,并篡改传送到串行口和并行口上的数据。

(2) “发薪日”(Payday, 在荷兰发现) “黑色星期五”病毒的变种。它在每周星期五(13日除外)捣毁用户文件。

(3) “里斯本病毒”(Lisbon,在里斯本发现) 感染COM文件,增加648字节。被感染的文件有八分之一的程序头被修改为“@AIDS”。

(4) “DBASE病毒”(在纽约发现) 感染COM文件并专门捣毁DSF文件中的数据。

(5) “阿拉巴马病毒”(Alabama,在希伯莱大学发现) 感染.EXE文件,增加1560字节,在进入内存后操纵FAT表,使文件名互换造成文件逐渐遗失。

(6) “TYPO病毒”(打印错,在英国布莱顿发现) 感染.COM文件后,增加867字节并修改并行口上的数据,使打印机出错。

3. 攻击系统区造成系统瘫痪的病毒

(1) “艾滋病木马”病毒 (AIDS Information Trojan) 寄生DOS引导扇区,用被它感染的系统盘启动90次后,硬盘被密钥死锁。

(2) “勒海病毒” (Lehigh, 在美国宾州伯利恒勒海大学发现) 攻击Command.COM,使其增长20字节,它改变文件生成日期和时间,并在4次感染后摧毁所有系统数据。

(3) “林荫散步道病毒”(在美国加州奥克兰梅利特学院发现) 侵犯系统引导扇区,将原引导扇区存放磁盘上第一空闲簇,它类似于“小球病毒”,但原引导扇区不加保护,用户程序覆盖后导致不能启动。

(4) “秘密复仇者”病毒(Dark Avenger) 攻击的对象很多,包括.COM文件,感染后增加1800字节,获得控制后具有反监控和反跟踪能力,对文件和FAT表定时破坏。

4. 偏爱沉默型病毒

(1) “幽灵病毒”(Ghost virus,在冰岛大学发现) 同时以BOOT区和.COM文件为对象,感染后无丝毫症状。

(2) “什么都不做病毒”(Do—Nothing,在以色列发现) 除感染.COM文件增加608字节外,对文件和系统区均不造成危害。

(3) “数据犯罪”病毒(Datacrime,在荷兰发现) 寄生在.COM文件和EXE文件上(1514字节)。

这种类型病毒,病毒程序使用了密文技术,不使用特殊技术,这种病毒程序很难发现。

5. “小球病毒”变异型病毒