电脑快速入门丛书

DIANNAOKUAISURUMENCONGSHU

电脑病毒的检测治疗和预防

姜玉璋　编著

简明、准确、实用
简明、准确、实用

给初学者的书
给自学者的书

青岛出版社

电脑快速入门丛书

电脑病毒的检测治疗和预防

姜玉璋　编著

青岛出版社

鲁新登字 08 号

责任编辑　樊建修
封面设计　李伯书

电脑病毒的检测治疗和预防
姜玉璋　编著
*
青岛出版社出版
（青岛市徐州路 77 号）
邮政编码：266071
新华书店北京发行所发行
胶州市装潢印刷厂印刷
*
1995 年 8 月第 1 版　1995 年 10 月第 1 次印刷
32 开（850×1168 毫米）　6.5 印张　155 千字
印数 1—10110
ISBN 7—5436—1370—0/TP・112
定价：8.50 元

编者的话

当前，在人类社会生产和生活的方方面面，几乎无处不见电脑的存在，人类对电脑的依赖性越来越高，可以毫不夸张地说，人类已进入了一刻也离不开电脑的时代！如何保证电脑安全、可靠地工作一直是人们所非常关心的问题。近年来出现的电脑病毒给电脑系统安全造成巨大的危害，它是人们深恶痛绝的一大公害，由于它无孔不入，传染力极强，令人防不胜防，经常使电脑系统无法正常工作乃至瘫痪。尤其是现在的一些病毒制作技术更加巧妙，隐蔽性更强，破坏性也就更大了。

我们不想重复已有的有关病毒的论述，但有必要向广大电脑用户包括非电脑专业人员，揭开电脑病毒的神秘面纱，澄清一些错误认识，使更多的人对电脑病毒有一较全面的认识和科学的态度，提倡公众参与意识，把病毒制造者置于公众监督之下。

另一个更重要的目的，就是通过对病毒的分析，找出病毒的一般规律和病毒的致命的弱点，以便开发诊治、广谱预防和免疫的软件，提供方便好用的解毒手段。广大用户掌握了有关病毒的系统性知识和实用技术，公开病毒机理，即使遇到新的病毒，也能举一反三，排除故障，减少损失。

就象环境保护与工业防污染一样，工业技术发展的同时，就应考虑环境保护；在计算机推广应用的同时，也应考虑电脑安全与病毒防治同时起步，而且越早越好。

本书在编写过程中得到青岛市公安局计算机安全监察处、以及李坚之同志的支持和帮助，在此谨表示诚挚的感谢。

目　录

第一章　电脑病毒的奥秘

第一节　揭开电脑病毒神秘的面纱

自从1988年11月3日震惊世界的Internet网病毒事件，已有七、八年的历史了。时至今日，人们一谈起病毒仍然是心有余悸，谈毒色变。由于非电脑专业人员对电脑病毒知识缺少了解，往往造成误会，甚至害怕电脑病毒传染给他们的操作电脑的孩子，他们不相信在这样一个先进的设备中会产生病毒；又由于新闻界的介入，提前播发了可能发生病毒攻击电脑的消息，如某月15日又恰逢星期五，“黑色星期五”病毒果然发作，这势必给人们——特别是从事电脑而又知之不深的人们，造成恐惧心理，社会各界也普遍引起关注，这无疑给电脑病毒增添不少“威慑力”。许多人，其中不乏电脑专业人员都不禁要问：什么是电脑病毒？为什么会如此迅速地蔓延到整个世界的电脑领域？为什么传染IBM PC及其兼容机的病毒如此众多？

一、什么是电脑病毒

其实，电脑病毒就是人为编制的一组编码(程序)，只不过这组编码不是以合法程序的形式存在，而是寄生在某种合法程序(宿主程序)之上，它能够实现自身复制(繁殖)且使用合法的手段隐藏在电脑的存储介质中(潜伏)，当满足某些预定条件时，随着宿主程序的执行，则激活病毒程序代码，使其开始活动。通常这

种活动包括病毒代码有害地复制到其它系统或程序中(传染)，驻留内存，对宿主程序或操作系统进行修改，争夺第一控制权，销毁数据、损坏文件或长时间地占用系统资源，造成难以挽回的损失(破坏)。

不同的病毒具有不同的特征，小的病毒只有几十条指令，而大的病毒就象一个操作系统，由上万条指令组成。有些病毒传播很快，并且一旦侵入系统就马上摧毁系统；而另一些病毒具有较长的潜伏期，感染后仍需要一段时间才开始发作。多数病毒并不摧毁整个系统，而是感染文件，破坏数据等。

电脑病毒实际上是借助生物学病毒的概念，它同生物病毒所相似之处是能够侵入电脑系统和网络，危害正常工作的电脑系统。与生物病毒不同的是几乎所有的电脑病毒都是人为地故意制造出来的，有时一旦扩散出去后连病毒制造者自己也无法控制。它已经不是一个简单的纯学术问题，而且一个严重的社会问题了，所以，有必要向广大电脑用户包括非电脑专业人员，揭开电脑病毒的神秘面纱，澄清一些错误认识，使更多的人对电脑病毒有一较全面的认识和科学的态度，提倡公众参与意识，把病毒制造者置于公众监督之下。

二、电脑病毒产生的历史背景

当电脑病毒以这种无生命的可执行代码，以有生命的生物病毒的特征在电脑系统之间进行传染、蔓延、大量地吞噬用户数据时，当由于电脑病毒的突然出现而引起电脑用户相当程度的恐慌时，当新闻媒介大肆渲染时，电脑病毒的起源问题引起了人们的广泛探讨。

(1) 病毒起源说种种

电脑病毒出现在80年代末期，源于美国，这是公认的事实。但它起源于谁家，究竟谁是制造电脑病毒的罪魁祸首？却众说纷

纭，莫衷一是。计有：

① 科学幻想起源说。1977 年夏，Thomas. J. Ryan 出版了一本幻想小说《The Adolescence of p－1》，书中作者幻想出世界上第一个电脑病毒，这种病毒能从一台电脑到另一台电脑传染流行，能控制 7000 台电脑的操作系统。

这种说法的根据是：人类社会的许多现行科学技术，都是先有幻想之后才成为现实的，如由“嫦娥奔月”到阿波罗登月，由“千里眼”到电视，由“顺风耳”到电话等。也许该书问世之后，有些人才顿开茅塞，借助于他们对电脑硬件系统，尤其是对软件系统的深入了解，发现并设计出病毒。

1983 年美国电脑安全专家 Fred Cohen 通过在运行 UNIX 操作系统的 VAX Ⅱ/750 机上进行了病毒实验，证明了电脑病毒实现的现实性，至此电脑病毒有了由幻想变成现实的理论依据。

② 恶作剧起源说。据资料介绍，电脑病毒起源于搞恶作剧的人。他们有的是想要炫耀一下自己的才华，有的是为发泄私愤而采取恶意地报复。

引起世界计算机界震动的 Internet 网络事件就是一个典型的恶作剧事例，病毒制造者是一个年仅 23 岁的 Cornell 大学的学生 Robert Morris，他在 1988 年 11 月 2 日晚把他编写的程序输入到 Internet 网后，心安理得地回去睡大觉，满有把握地以为他的杰作会顺利通过各级网络口令而永存到政府及研究机构的电脑系统中，谁知他的程序竟然以闪电般的速度不断地自我复制起来，并向整个网络迅速蔓延开来，网络中的约 6200 台基于 Unix 的 VAX 系列小型机及 Sun 工作站都染上了病毒，损失惨重，他也因此而被送上法庭。

Morris 的恶作剧是没有恶意的，但大多的恶作剧是出于某种报复目的的。如某银行职员在计算机管理程序中插入一小段程序，检查他的名字是否还在该银行系统的档案里，如果不在则破坏系

统。结果在他被解雇后，该程序便对银行数据进行了破坏，从而达到它个人报复的目的。

③ 游戏程序起源说。几十年前，当时 AT&T Bell 实验室的技术人员为了娱乐，在自己实验室的机器上编制了可以吃掉对方程序的程序，它们被装到任意的一些非覆盖区中并被执行，通过使用自动重定位，每个程序按存储器循环周期每次一条指令地逐渐接近其它程序，结果，若被对手修改而不能执行某条指令者为失败。所以有人认为，这是第一个电脑病毒的雏形。

④ 软件保护起源说。电脑软件是一种技术密集型的高科技产品，但对软件资源的保护至今尚无一个切实可行的办法，这样使得许多软件被非法拷贝，从而使软件制造商的利益受到侵害。所以有人认为电脑病毒的出现是软件制造商为了惩罚那些非法复制者而在软件产品中加入病毒程序，由一定条件触发传染并具一定的破坏作用，给非法拷贝者以严厉的惩罚。

后来人们猜测，可能是这种软件开发者为保护它们的利益从事的恶作剧工作，逐渐演化成了电脑病毒。这方面典型例子就是巴基斯坦智囊病毒，它是由巴基斯坦的阿尔维兄弟为了追踪非法复制其软件产品的用户而编制的。

⑤ 美国软件俱乐部起源说。美国软件使用者俱乐部是由那些志同道合的电脑爱好者组成的一个团体。通过这一组织，利用电脑网络分享彼此的设计心得。也有人在公告板(BBS)上显示自己开发的程序并注明欢迎大家通过网络来选用，但在一定时间内必须邮寄使用费用。通常，这种公告板上的程序暗藏杀机，如果有人使用了这项程序却又不付费用的话，在特定的时间内，暗藏在程序中的病毒就象定时炸弹一样开始爆炸，借以警告那些“占便宜”的使用者。如果使用者乖乖地寄上费用的话，设计者会寄给解毒程序。如果不知内情的“盗用者”把这种带病毒的程序分享给其它朋友或亲友，于是一传十，十传百，电脑病毒就广泛地传播

开来。这样，美国软件俱乐部就成了电脑病毒的制造源了。

上述各种说法都有它的根据和道理，从不同的角度说明了电脑病毒的各种成因，但任何一个事物的产生和发展，都有其历史背景和社会原因。随着电脑的日益普及，应用技术的日益深入，电脑系统本身的脆弱性，明显地暴露出来，成为被攻击的对象，这是必然的。至于谁第一个制造出病毒的人，已经不重要。下面我们看看电脑病毒的发展历史就会更清楚了。

(2) 电脑病毒的历史

从历史的角度看，任何一种事物的产生和发展都有其原因和背景，这种原因和背景又都是可以考证的，电脑病毒也不例外。

① 电脑鼻祖 John Von Neumann(冯·诺依曼)的预言。1949年电脑鼻祖著名数学家 John Von Neumann(冯·诺依曼)发表了名为《Theory and Organization of Complicated Automata》(《复杂自动机器的理论与结构》)的论文，在世界上第一次描述了程序复制机制理论，即程序能在内存中进行繁殖。1957年他逝世后，耶鲁大学出版社(Yale University Press)出版了他的遗著《The Computer and Brian》(《计算机与人脑》)，又详细地讨论了复制程序的理论。当时人们并没有注意到这种超前于实践的理论，有人还怀疑这种理论，致使这种理论沉睡了许多年。电脑病毒的出现恰恰说明了他的理论的实践性。

② ANIMAL 游戏程序。美国人凯恩所著《计算机防护》一书中列举了这样一件事实：早在 UNIVAC1108 机时代，就在该系统上出现了一个叫做 ANIMAL 的游戏程序，该程序运行时，向人们提出 20 个问题，请游戏者猜动物，如果游戏者猜对了，则 ANIMAL 不对系统作任何操作，否则该程序则把动物复制到每一个文件中去。ANIMAL 在进行写操作时，首先检查被写的文件是否有 ANIMAL 的备份存在，如果存在，则再检查是否为新版本。并且 ANIMAL 还能对拷贝生成的日期建立一个非法时间，并

利用日期来判断文件的备份是不是当前版本所建。这一程序的一些机制和当前的电脑病毒的传染机制颇为相似。

③ John Conway 设计活的软件。60 年代，美国电脑专家 John Conway 确信能够创建一种具有电子复制机制的活的软件，他的努力使得人们对于电脑的利用由简单的逻辑处理向更高的水平提高了一步，但从另一个角度看，他的程序已向现代的电脑病毒进化了一步。在他的一个程序中，他以行和列的形式创建了各种图形，当程序运行时，各种图形根据环境的变化而变化，当元素都挤在一起时，有些元素会因缺乏空间而消失，而当它们分散得太广时，又会因彼此分离或与生存的支持系统分离而不能生存。图形在运动过程中不断变大，当变得太大时也会自行消失，同时一些元素可以自行寻找更合适的环境。实际上，从某种角度讲，Conway 的程序设计方法和屏幕的表现形式都有些象 20 年后的病毒。

④ Ken Thompson 的泄密。在 Conway 之前，美国一些研究中心尤其是 MIT(Massachusetts Institute of Technology)的一些研究人员，在 AT&T Bell 实验室及加州 Palo Alto 的 Xerox Corporation 的研究中心从事人工智能基础研究。当时 AT&T 及 Xerox 的编程人员，利用磁芯存储器中的数据和程序娱乐自身，他们通过改变存储器中的代码使得原来用以整理数据的程序也能销毁其它程序。他们把这种编程方法称之为 Core War。编制这种程序的 3 个年轻人 Douglas Mcilroy、Victor Vysottsky 和 Robert Morris(非 Internet 网事件中的 Morris)。他们利用磁芯战概念，设计出具有自我繁殖能力且在探查到敌方程序运行时能销毁敌方程序的程序。当时有人称这种程序为“生物体”。后来因这种“生物体”程序影响了 Xerox530 机的正常运行，于是磁芯战游戏被终止。当时这种程序设计方法只为少数人所了解，他们意识到这种具有自我复制能力的程序对电脑应用的潜在威胁，于是磁芯战的

概念从此消声匿迹了，但在1983年，这种“沉睡”了20年的程序自我复制机制的秘密，被Ken Thompson(曾组织Unix操作系统开发、研制并获奖)在给计算机器协会成员的一次演说中泄露出去。1984年Scientific American(《科学美国人》)出版，详细地探讨了磁芯战，同时包括有编写可自我复制程序的信息。这样，有关电脑病毒实现的可能性、原理及设计方法基本公开。

⑤ 学术界的升温及美国大学的早期病毒。当Ken Thompson泄露了程序自我复制机制实践活动，并由一些学术刊物刊载了有关内容以后，学术界发生了极大的兴趣，很快抓住了这一机会并深入地研究了这种现象，于是美国几所大学的学生及从事科研、教学的工作人员开始尝试编制病毒程序，美国大学校园里出现了早期病毒的踪迹。如1985年美国几所大学受到早期病毒Cookie Mouster的传染，病毒在屏幕上频繁地显示：“I want a cookie”(我要吃甜饼)或者“Cookie Mouster is Here”，用户必须回答“Cookie”，程序才能继续往下运行。

⑥ 科学幻想小说的出版。这一时期，科学幻想也很活跃，1975年Thomas Brunner出版了《Shock Wave Rider》(《震荡波骑士》)科幻小说，该书以Worm(蠕虫)和Virus(病毒)为主，第一次描述了信息化社会中电脑作为正义和邪恶双方斗争的重要工具的故事，使电脑间产生第一次“幻想”中的相互攻击。此后，1977年夏，Thomas J·Ryan也出版了《The Adolescence of P—1》(《P—1的青春》)，在该书中，T·J·Ryan幻想出世界上第一个电脑病毒，该病毒从一台电脑到另一台电脑间传染流行，并控制7000多台电脑的操作系统。1983年科幻电影War Games在美国上映，该片赞美了一个孤独的少年在自己的卧室中通过一台电脑从事军事活动的故事，该片上映后，在一定程度上激发了恶作剧者的活动。

⑦ Fred Cohen的工作。Fred Cohen在1983年作博士论文

时，着手研究电脑病毒传染性实现的可能性及病毒防御的研究工作，并于1984年在全美计算机安全会议上做了病毒传染的实验，并正式定名为计算机病毒。其实验结果及过程发表在1987年Computer & Security(计算机与安全)杂志上，题目为："Computer Virus:Theory and experiments"。Fred Cohen的实验是纯学术性质的，他只是验证了病毒存在的可能性。

⑧ 恶作剧者的尝试。从另一方面讲，病毒的产生与恶作剧者有一定的关系。恶作剧者(Hacker)的名字是早在1956年就定了名的，当初Hacker是指那些实践新的计算技术，特别是采用新技术编制自己程序的酷爱者，如1966年两个美国研究生创建了能拷贝自身的程序。80年代初，Hacker开始活跃起来，并成立了许多俱乐部，他们探讨电脑领域中的问题，认为自己对于电脑技术无所不能。当程序自我复制的秘密泄露之后不久，这些年轻的Hacker开始加紧探索编制具有自我繁殖能力的程序。1985年7月IBM PC机上出现了一个恶意的特洛依木马(Trojan Horse)程序EGABTR，这个程序可以在一般的PC机上提供比IBM EGA图象还漂亮的图象效果。EGABTR在其首次运行时就删除磁盘上每一个文件，终止系统运行并显示："Arf,Arf! Gotcha!"。此后，出现了几个类似的程序：NUKELA、FILER，用BASIC编制的用于告知用户盘上还有多少可利用空间的SEE FREE、DOSKNOWS以及能删除盘上所有文件并在屏幕上显示"SURPRISE"的SURPRISE程序等。

综上所述，实际上，在1988年11月Internet网事件之前，电脑病毒已经出现，只不过没有造成多大的影响而已。据资料称：

1970年出现了CREEPER(及REAPER疫苗)；

1974年出现了RABBIT病毒；

1980年美国远景规划计算机网络上出现了DEDUX病毒；

1981－1982年出现了在APPLE II上的ELK CLONER病