计算机反病毒技术实用指南

李向宇 郭 薇 编著

国防工业出版社

计算机反病毒技术实用指南

李向宇　郭　薇　编著

国防工业出版社

(京)新登字 106 号

内 容 简 介

本书是一部关于计算机病毒防治实践的总结，具体地介绍了计算机病毒的发展历史，讨论了有关计算机病毒的基本技术概念；从 DOS 的基本知识入手，介绍了计算机病毒的预防、检测和消除的基本常识；深入地讨论了传染计算机系统的引导区和文件的病毒的检测及消除技术；系统地介绍了计算机病毒的预防技术、方法，以及病毒预防、检测和消除软件的技术实现及其评价方法。本书对国内出现的具体计算机病毒给出了具体的检测步骤和消除方法，对世界上常见的近 300 种病毒的表现症状和基本检测方法作了简明的介绍，同时还介绍了国内使用较多的几种反病毒产品的使用方法。

本书适于计算机操作人员，研制、开发、应用人员和大中专院校的师生阅读参考。

计算机反病毒技术实用指南

李向宇　郭　薇　编著

责任编辑　王祖珮　马征宇

国防工业出版社出版发行

（北京市海淀区紫竹院南路 23 号）

（邮政编码 100044）

新华书店经售

北京钓鱼台印刷厂印刷

787×1092 毫米　16 开本　印张 30¼　695 千字

1992 年 11 月第一版　1992 年 11 月第一次印刷　印数：00001—10000 册

ISBN 7-118-01073-1/TP・138　定价：25.50 元

前　言

从80年代初期开始，计算机科学技术的发展突飞猛进，计算机的应用范围愈加广泛。80年代后期，计算机病毒广泛蔓延，它对计算机应用的威胁越来越受到计算机界人士的重视，并引起了各行业计算机用户的普遍关注。

随着计算机在我国的普及推广，计算机病毒的滋扰也愈加频繁。由于病毒本身所具有的特性，决定了它的危害性极大，而又难以对付。现在，如何判别和防治计算机病毒，这已成为我国广大计算机研制和应用人员所面临的一个重大难题。

1990年我应约为国际数据集团爱奇高技术(北京)有限公司编写了一本约40万字的《计算机病毒概论》。当时，该公司以内部资料的形式印出后，售出了数万册，受到了读者青睐。自该资料问世之时起，我便成了有关读者的朋友。近几年内，我除了利用业余时间给读者寄出大量回信外，还尽我所能为不少单位解决有关计算机病毒的问题。由于本人的精力和能力有限，有的读者来信未能函复，有的单位的约请未能应许，至今，我常感内疚。借此机会，一并致歉。好在这次又应国防工业出版社之约，有机会将我多年的些微努力总结成书奉献于社会，倘若我的读者朋友们读后有所裨益，我就感到快慰了。

本书针对社会需要从实用的角度出发，介绍了近300种目前国内外常见的计算机病毒，并对国内广泛蔓延的计算机病毒给出了相应的检测与消除的实用方法。书中所提供的每个检测与消除程序，均已在AST 286、386，COMPAQ 386，IBM PC/XT、AT等微机上调试通过，无须做任何修改即可用来解决实际问题。同时，书中还介绍了一些目前国内外流行的反病毒产品，可供苦于无力处理病毒问题的计算机用户选用。

本书共10章：第一章，计算机病毒产生的历史背景；第二章，计算机病毒的基本概念；第三章，DOS内存管理技术与内存中计算机病毒的检测；第四章，传染引导区与文件的计算机病毒的检测与消除；第五章，国内出现的计算机病毒的检测与消除实用技术；第六章，常见病毒300种；第七章，计算机病毒的预防；第八章，计算机反病毒软件的功能及其评价；第九章，反病毒产品介绍；第十章，计算机文化与文明。

本书之所以称为实用指南，是因为它着重对病毒的症状、种类、特征、检测及其消除技术进行了详尽的讨论，所介绍的计算机病毒种类之多、内容之全面，足以作为一般计算机用户随时参阅的手册。而对于具备计算机体系结构、操作系统等方面知识，熟练掌握汇编语言的读者来说，它又为深入研究病毒防治技术提供了必要的理论基础。本书力图能为广大计算机用户排忧解难。

本书适用于计算机研制、开发和应用人员，也可供大专院校计算机专业师生参考。

本书所给出的反病毒实用程序均由作者李向宇、郭薇编制并调试。

在本书的编写过程中，得到了许多同行专家的指导和帮助，在此谨致谢忱。由于作者水平有限，加之编写时间仓促，书中错误之处在所难免，恳请广大专家、学者及同行给予批评指正。

李向宇　1992年9月

目　录

第一章　计算机病毒产生的历史背景

1.0　引　　言

著名的数学家，计算机的创始人 John Von Neumann(冯·诺依曼)早在 40 多年前在其 Theory and Organization of Complicated Automata(《复杂自动机器的理论与结构》)一文中指出，一部实际上足够复杂的机器具有复制自身的能力。当时这种理论并没有受到人们的普遍重视。直到今天，计算机病毒出现之后，人们才认识到了这一理论的重要性。于是一些计算机安全专家，从理论上探讨、研究了计算机病毒产生的深层原因，并研究了 Von Neumann 体系结构与计算机病毒之间的关系。其中 Herschberg 和 Paans 曾指出：可以判定，计算机病毒将长期存在于计算机应用领域中。Ghamman 也指出：病毒利用了 Von Neumann 计算机体系结构，这种体系结构被应用于我们今天几乎所有的办公用计算机中；这种体系结构，把存储的程序当作数据处理，并可以动态地对其进行修改，以满足变化的需要。操作系统程序和用户程序都被如此看待。当今计算机病毒正是利用了系统可执行程序能被动态修改的特性，达到了传染的目的。当今计算机病毒以传染 IBM PC、AT、286、386、486 等兼容计算机的病毒居多。其原因有二：(1)IBM 微型机及其兼容机的应用普及率最高(这是最主要的原因)；(2)IBM 微型机及其兼容机的软件支撑环境——IBM PC－DOS(MS－DOS)存在着自身的脆弱性。众所周知，DOS 操作系统是安全性与易操作性的一种折中。从用户的友好角度看，DOS 是一个相当友好的系统，它赋于用户极大的自主权力——用户可以修改 DOS 操作系统，从而便于用户扩展系统功能。DOS 的 FAT 表、文件目录、中断向量表等对用户是透明的，DOS 为用户提供了一些便于用户编程的中断服务程序，用户可以编写程序使之常驻内存，甚至用户可以修改 ROM 中断功能；用户可以编写 SHELL 程序代替 DOS 的命令解释程序——COMMAND. COM 程序，如果用户具有更高的技术层次，甚至可以修改 IBMDOS. COM 和 IBMBIO. COM。也就是说，从安全性的角度来看，DOS 结构的各个层次都可以受到攻击，DOS 不是一个很好的安全操作系统。所以，DOS 操作系统本身存在着其固有的脆弱性，这也成了当今计算机病毒攻击 DOS 环境的一个原因。

在计算机病毒产生的历史演化过程中，1988 年 11 月 2 日 Internet 网络事件是一个重要的转折点。

Internet 网络是美国最大的计算机网络，它包括 5 个计算中心，12 个地区节点，连接着政府、大学、研究所和拥有政府合同的约 25 万台计算机系统。Internet 有三个基本网络：美国国防高级研究计划局网络——ARPANET(Advanced Research Projects Agency Network)、军用网络——MILNET(Military Network)和美国国家科学基金会网络——NSF Net(National Science Foundation Network)。1988 年 11 月 2 日，美国 Cornell 大学年仅 23 岁的研究

生 Robert T. Morris 编写的 Morris 蠕虫(Worm)程序攻击了这一美国最大的计算机网络。一夜之间,Internet 网络上的 6200 多台计算机不能正常运行,从而,轰动了整个世界的计算机领域。对于这一事件,人们无不感到震惊。在此之后,计算机病毒在计算机领域内广泛蔓延开来,于是人们产生了种种猜测,也引起了一定的恐慌。时至今日,面对如此众多的计算机病毒,人们会问,计算机病毒究竟是怎样产生的?为何如此迅速地蔓延到整个世界的计算机领域?为何传染 IBM PC 及其兼容机的病毒如此众多?实际上,任何事情都有其发生、发展和演化的过程,计算机病毒也不例外。了解病毒演化的历史,对于更好地消除人们思想中的计算机病毒恐惧症是有益的。

1.1 计算机病毒的历史

当计算机病毒这种无生命的计算机可执行代码,以有生命的生物病毒的特性在计算机用户的计算机系统之间进行广泛传染、蔓延、大量地吞噬用户数据时,当由于计算机病毒的"突然"降临而引起计算机用户对计算机病毒产生相当程度的恐惶感,各种新闻媒介大肆渲染时,计算机病毒的起源问题引起了人们的广泛探讨。似乎所有的计算机厂商、计算机专家、计算机用户,都以不同程度或站在不同立场上对计算机病毒的产生进行了分析、判断和猜测,于是产生了多种计算机病毒的起源说,如:科学幻想起源说、恶作剧者起源说、AT&T 贝尔实验室游戏程序起源说、软件俱乐部起源说等等。但是,纵观历史,这些说法都没有从历史长河的角度全面地概括计算机病毒的真正起源、发展及演化的全过程。这里,我们的目的不是去单纯地断言计算机病毒的确切起源,进而使之成为一种新的计算机病毒起源说,而是从历史的角度进行分析、讨论,以求能在计算机技术发展的历史长河中,从相关技术出现的时间先后上追溯计算机病毒产生的可能性或原因。可以肯定,计算机病毒的产生是一个历史的问题,计算机病毒的发展与蔓延是计算机科学技术高度发展以及计算机文化与文明迟迟得不到完善的必然结果。但在计算机病毒蔓延之初,产生的这些起源说实际上都是病毒产生、发展过程中的一个片面的小插曲。

1.1.1 人们的猜测——计算机病毒的种种起源说

当计算机病毒在美国学术界逐渐蔓延,尤其是自 1988 年 11 月 2 日 Internet 受到 Morris 蠕虫(Worm)程序攻击而引起世界轰动以来,对于计算机病毒,人们经历了一个由不可理解——恐慌——逐渐了解并认识的发展过程。现在对于计算机病毒,人们已经从技术上逐渐地完善了自己的认识。但是,由于计算机病毒传染之初人们对于计算机病毒不尽了解,以及病毒给计算机用户造成的巨大损失,人们在不同的程度上对计算机病毒产生了一种前所未有的恐慌感和神秘感。在这种情况下,人们对于计算机病毒的出现产生了种种推测和猜想,从而诞生了数种计算机病毒的起源说,如:

1. 科学幻想起源说

这种起源说认为,计算机病毒起源于科学幻想小说。1975 年美国科普作家 Thomas Brunner 出版了一本名为 Shock Wave Rider(《震荡波骑士》)的幻想小说,该书以 Worm 和 Virus(计算机病毒)为主,第一次描述了信息化社会中计算机作为正义和邪恶双方斗争的重要工具的故事,使计算机间产生了第一次"幻想"中的相互攻击。在此之后,1977 年夏

天，Thomas J. Ryan 也出版了一本幻想小说，名为 The Adolescence of P—1(《P—1 的青春》)，在该书中，T. J. Ryan 幻想出现了世界上第一个计算机“病毒”，该“病毒”从一台计算机到另一台计算机间传染流行，一时间感染并控制了 7000 多台计算机的操作系统。1983 年，美国的科幻电影 War Games 在美国上映，该影片赞美了一个孤独的少年在自己的卧室中通过一台 PC 机从事军事活动的故事。War Games 上映之后，在一定程度上激发了计算机恶作剧者的活动。1984 年，William Gibson 出版了小说 Neuromaner，书中首次出现了计算机流氓(Cyberpunk)的概念。这一概念和 Fred Cohen 对计算机病毒的定义几乎是同时出现的，从此，科学幻想中的计算机病毒在作家的笔下和计算机的现实世界中得到了发挥和实现。有资料认为，MIT(麻省理工学院)的恶作剧者从这些科学幻想中得到启发，并在该学院电气工程系 Smith 博士的科学幻想小说的鼓励下，编制了 Space War(太空大战)游戏程序。为此，有人认为，可能是这些科幻小说启发一些人发明了计算机病毒。

2. 恶作剧者起源说

1984 年，Hacker 一书的作者 Steven Levy 认为，计算机恶作剧者是对计算机的存取信息具有浓厚兴趣，且认为自己可对计算机系统无所不能的人。恶作剧者认为自己才华出众，为了显示自己在计算机方面的天资，设计、开发出具有自我复制能力的“活的”程序——计算机病毒，并造成了在社会上的流传。

3. AT&T 游戏程序起源说

几十年前，当计算机刚刚在社会上得以逐渐应用的时候，贝尔实验室(Bell Laboratories)的技术人员为了娱乐，在自己实验室的计算机上编制了可以吃掉对方程序的程序——Core War(核心战)程序。有人认为这是第一个计算机病毒的雏形。

4. 软件设计者软件自我保护起源说

由于软件产品不能得到适当的法律保护，软件制造商设计、开发的软件产品被大量地非法拷贝，其利益受到损失。为了防止自己开发的软件被非法拷贝，他们在自己的软件系统中加入惩罚非法拷贝软件者的、可以传染的具有一定破坏作用的计算机程序。后来人们猜测，可能是这种软件开发者为保护自己的利益而从事的恶作剧性的工作，逐渐演化成了危及社会的计算机病毒。究其原因，这种起源说可能来自巴基斯坦智囊病毒(Pakistani Brain)。

5. 美国计算机软件俱乐部起源说

美国计算机软件使用者俱乐部是由一些志同道合的计算机技术爱好者组成的一个团体。这些计算机爱好者通过这样的组织，利用计算机网络分享对计算机开发、研究的心得体会。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免费选用，还有人将自己的程序公开在 BBS 上，并欢迎大家选用，但必须在一定时间内邮寄使用费用。通常后者显示在 BBS 上的程序“暗藏杀机”，如果有人使用了这些程序却不付费用，则在特定的时间内，暗藏在合法程序中的破坏性计算机程序机制就会像定时炸弹一样爆发，借以警告那些“占便宜”的使用者。有人认为，这样的程序逐渐演成了当今的计算机病毒。

6. 美国中学生起源说

随着计算机应用的普及，尤其在美国，计算机的家庭占有率较高。许多年轻的大学生、中学生甚至小学生很容易接触计算机，他们对计算机语言和操作系统(尤其是 IBM PC/

AT、XT 机使用的 MS—DOS 及 IBM PC—DOS)都有相当的了解。有资料说,计算机病毒是美国一些十几岁到二十来岁的计算机爱好者想出来并付之于实践的。这些被人们认为是计算机"神童"的娃娃,一开始只是想编写一些程序同自己的伙伴开个玩笑,其目的,一是要显示一下自己的知识实力,二是要从朋友的机器资源损失中求得乐趣。不幸的是,这种玩笑开得越来越大,范围也越来越广,并被恶意攻击者所利用,从而成了今天蔓延全世界的计算机病毒。

7. Fred Cohen(弗里德·科恩)计算机病毒实验起源说

1983 年美国加利福尼亚州的计算机研究人员 Fred Cohen 博士开始研究计算机病毒对系统攻击的可能性,并于 1984 年在美国计算机安全会议上演示计算机病毒。有人认为,这是世界上首例计算机病毒,可能是计算机病毒广泛蔓延的一种征兆。

对于计算机病毒的起源至今人们众说不一,上面这七种起源说只是其中的代表。这些起源说似乎都有道理,都可能在计算机病毒的产生中起过一定的作用。但是,如果不纵观历史而单纯地研究这些起源说,计算机病毒的真正源泉就难以考证了。如前所述,任何一种事物的产生都有其产生、发展的历史背景,计算机本身正像许多事物一样有其自身的优点,也有自身的缺点(安全方面的漏洞),计算机的这些缺点对于病毒而言,主要在于计算机系统自身的脆弱性。而计算机系统尤其是操作系统本身的一些功能、特性等也在人们不断地开发、研制中,许多人都在不同的角度上发现着计算机系统尤其是操作系统的不完善的一面,进而使之完善。实际上,完善的过程也就是一种从发现弱点到克服弱点的过程。从相反的角度讲,这种完善的过程在一定程度上也是人们发现计算机程序复制机制,进而一些恶作剧者"埋头苦干"编制计算机病毒的过程。从计算机技术尤其是软件技术发展历史的角度来研究,就计算机病毒而言,我们也许能发现些什么。

1.1.2 计算机病毒的历史

如前所述,从历史的角度来讲,任何一种事件都有其产生的原因和历史背景,并且这种原因和历史背景又都是可以考证的,计算机病毒也不例外。从 1945 年诞生世界上第一台 ENIAC 计算机之后,在电子计算机领域内人们作了许多工作。计算机系统从初期的庞然大物到今天的具有强大功能的、小巧玲珑的计算机系统,计算机的硬件、软件技术有了巨大的发展。今天当我们回过头来追溯计算机病毒的历史成因时,也不能忽略计算机技术发展过程这一点。从历史的角度讲,与计算机病毒的形成有关的技术和事件有:

1. 计算机的鼻祖 John Von Neumann 的发现

1949 年计算机的创始人著名数学家 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的理论,即程序能够在内存中进行繁殖。1957 年 Von Neumann 逝世后,耶鲁大学出版社(Yale University Press)出版了他的遗著 The Computer and Brain(《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,甚至有人还怀疑这种理论的实践性,致使这一理论在这位伟大的科学家逝世之后沉睡了许多年。直这种理论被后来的人应用起来,并出现了程序自毁的概念。

2. ANIMAL 游戏程序

美国人凯恩所著的《计算机防护》一书中列举了这样一件事情：早在 UNIVAC 1108 机时代，就在该系统上出现了一个称为 ANIMAL 的游戏程序（该程序有几个不同的版本），该程序运行时，向人们提出 20 个基本问题，请游戏者猜动物，如果游戏者记住了每个动物，则 ANIMAL 程序对于系统不做任何额外操作，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，首先检测要写的文件是否有 ANIMAL 的备份存在，如果存在，则再检测已存在的备份是否为新版本。并且 ANIMAL 还能对拷贝生成的日期建立一个非法时间，并利用日期来判定文件上的 ANIMAL 程序的备份是否为当前运行的 ANIMAL 版本所建立。可以说这一程序的一些机制和当前的计算机病毒的传染机制有些类似之处。

3. John Conway 设计的活的软件

在 60 年代，美国计算机专家 John Conway（康微）确信能够创建一种具有电子复制机制的“活的软件”（Living Software，这种软件能在计算机中活动），并且作了初步的工作。Conway 的努力使得人们对于计算机的利用由对数据的简单的逻辑处理向更高的水平提高了一步，这可以说是计算机发展史上尤其是软件发展史上的一大成就；但从另一个角度讲，Conway 的程序又向现代的计算机病毒进化了一步。Game of Life 程序就是一例，在这一程序中，无论是屏幕的显示还是编程的艺术性都很好，屏幕上的图形在寻找生存的环境时，可以变化、移动，当结构不稳定时，有些图形可以自行消失。在 Conway 的又一个程序中，Conway 以单元的行和列的形式创建了各种图形，单元的行和列属于一个放大的表，构成处理表的操作符及其他项是一种类型的元素，各种规则是图形中的每个元素将怎样活动的集合。当程序运行时，各种图形根据环境的变化而变化，当元素都挤在一个地方时，有的元素会由于缺乏空间而消失，而当它们分散得太广时，又会由于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适合的环境。实际上，从某种角度上讲，Conway 的程序设计方法及其屏幕的表现形式都有些像 20 年后的病毒，但 Conway 的程序并不能说就是计算机病毒。

4. AT&T Bell 实验室研究人员的工作

在 Conway 之前，即 Von Neumann 提出程序复制机制理论之后 10 年（1959 年），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 贝尔实验室及加利福尼亚 Palo Alto 的 Xerox Corporation 的研究中心从事人工智能的基础研究。当时 AT&T 及 Xerox 的编程人员，利用公司机器的核心存储器中的数据和程序娱乐自身，他们通过改变核心存储器中的代码使得原来用以整理数据的程序也能消毁其他程序。程序的编制者将这种编程的方法称之为 Core War。编制这种程序的是 AT&T Bell 的三个年轻人 Douglas Mcilroy（道格拉斯·麦基尔罗伊）、Victor Vysottsky（维克特·维索特斯）及 Robert Morris（罗伯特·莫里斯，与编制蠕虫程序的 Morris 不是一人）。他们利用核心战的概念，设计出具有自我繁殖能力且在探查到敌方程序运行时能消毁敌方程序的程序，用此进行比赛。当时也有人根据这种程序自我繁殖的特性称这样的程序为“生物体”。这种程序采用的设计技术逐渐地更加成熟。这种“生物体”程序以后影响了 Xerox 530 机的正常运行，于是 Core War 游戏被终止。当时这种程序设计的方法只为少数人了解，自身的知