计算机病毒的诊治与免疫

高　忠
高水英　编
莫日华

中山大学出版社

计算机病毒的诊治与免疫

高　忠　高水英　莫日华　编

中山大学出版社
1990

计算机病毒的诊治与免疫

高 忠 高水英 莫日华 编

*

中山大学出版社出版发行
（邮政编码：510275）
广东省新华书店经销
南方软件有限公司电脑排版
广州红旗印刷厂印刷

*

787×1092毫米 32开本 7印张 字数15.3万字
1990年4月第1版 1990年4月第1次印刷
印数：1～20000册

ISBN 7—306—00319—4

O·24 定价：4.00元

前　言

1989年上半年计算机病毒开始了对我国计算机界的入侵，并且很快成了威协我国计算机应用的一个严重问题。为了消除人们对计算机病毒的恐惧心里，宣传消毒、防毒的方法，我们立即对计算机病毒的有关机制和消除方法，进行了仔细的研究，并于1989年 8 月起在广州中山大学计算中心举办的数期计算机病毒防治学习班上，结合病毒防治的实际进行了广泛的探讨。在此基础上我们将讲稿整理修改，成为此书，现奉献给读者，供参考研究。

本书对现已在我国流行的几种计算机病毒的表现、危害、检测、消除和预防的方法，作了较详细的介绍。与本书相配合，我们在办班期间研制出了各种计算机病毒防治和免疫软件，并免费帮助用户对电脑和软件进行了大量的消毒工作，效果良好。

本书在形成过程中得到学员和软件用户的广泛支持，他们提出了许多宝贵的建议，在此一并表示感谢。

由于计算机病毒防治是新出现的课题，加上此书成书仓促，作者水平有限，不妥之处在所难免，敬请读者批评指正。

编　者

1989年12月

内 容 提 要

本书从实用的角度出发，深入分析了计算机病毒的特点和危害，详尽介绍了检测计算机病毒的途径和解毒免疫方法。

全书共分八章，主要内容包括：计算机病毒的基本概念，诊治病毒的常用工具的使用方法，病毒赖以藏身的磁盘的数据组织特点，DOS 系统结构原理和中断系统，目前流行的计算机病毒的剖析，诊断治疗计算机病毒的方法，以及相应的防治和免疫措施。书中提供了检测、清毒、治疗和免疫的程序实例，提出了象人类和平利用核能一样无害利用计算机病毒的设想。

本书是广大计算机用户和计算机安全工作者了解和防治计算机病毒的实用工具书，也可作为病毒防治学习班的教材。

目　录

第一章 概 述

目前全世界约发现 140 多种计算机病毒，计算机病毒已成为社会的新“公害”。

1.1 什么是计算机病毒

计算机病毒是指可以制造故障的一段计算机程序或一组计算机指令。它被计算机软件制造者有意无意地放进一个标准化的计算机程序或计算机操作系统中。尔后，该病毒会依照指令不断地进行自我复制，也就是进行繁殖和传播。有些病毒能控制计算机的磁盘系统，再去感染其它系统或程序，以及通过磁盘交换使用或计算机联网通讯把病毒传染给别的计算机。病毒依照其程序指令，可以干扰计算机的正常工作，甚至毁坏数据，使磁盘、磁盘文件不能使用或者产生一些其它形式的严重错误。

现在已发现的计算机病毒有 140 多种。不同病毒有不同特征。小的病毒只有 20 条指令，不到 50 个字节；而大的病毒像一个操作系统，由上万条指令组成。有些病毒传播很快，一旦侵入系统就马上摧毁系统；而另一些病毒则有较长潜伏期，机器在感染后二、三年才开始发病。有些病毒感染系统的所有程序和数据；而另一些病毒只对某些特定的程序或数据感兴趣。多数病毒一开始并不摧毁整个计算机系统，它们只在数据库或其它数据文件里将小数点向左或向右移一移，

增加或抹掉一、二个“0”。有些病毒甚至除了不断复制自己外，什么也不干，但它会占满整个磁盘空间，使计算机系统陷入瘫痪。

在网络系统中，由于病毒的载体是计算机网络，所以在几分钟内，病毒将传染网络中的所有计算机。病毒不仅在 IBM PC 及其兼容机之间传播，而且，许多事实证明小型计算机也已经成为计算机病毒攻击的牺牲者。

1989 年计算机病毒开始在我国各地相继出现。1989 年 7、8 月全国统计系统流行一种计算机小球病毒，不到两个月大多数省（区）统计局计算机站和部份地（市）县计算机站的微机都感染上这种病毒。近几个月来计算机病毒在我国各地区、各部门都有蔓延的趋势，我国计算机系统的安全面临严重的挑战。

1.2 计算机病毒的特点和种类

计算机病毒的特点：

(1) 小巧灵活：小程序可以隐藏，不易被发现。

(2) 可传播：病毒程序一旦加到当前运行的主程序上就传染很快，迅速扩散到整个系统。

(3) 可潜伏：被感染的程序几周、几个月不被发现，一旦发现则各方面均已受感染。

(4) 可激发：病毒程序设计要求可以在某一点激发或引爆。例如：在指定时刻，指定用户识别符，用户文件使用次数等激发或引爆。

关于计算机病毒的种类，按狭义的定义，只有能自我繁殖和扩展且危及计算机工作的，才称为“计算机病毒”。美国

主要采取这种狭义的定义。按广义的定义，除了上述“真正的病毒”外，还有三种能危及计算机工作的现象也称为“计算机病毒”。这就是：①逻辑炸弹；②陷阱入口；③特洛伊木马现象。日本主要使用这种广义的定义。

逻辑炸弹是由写程序的人有意设置的，是一种经过一定时间便会造成破坏数据恶果的定时炸弹；也有不是按经过的时间，而是以进行某特定事务处理的输入作为触发信号而起爆的炸弹。

陷阱入口也是由程序开发者有意安排的。当程序开发完毕放进计算机里实际运行后，只有他自己掌握操作的秘密，使程序完成某种事情，而别人则往往会进入子程序死循环或其他岐路。

特洛伊木马是借用古代特洛伊战争中，把士兵隐藏在木马中进入敌方城堡，出其不意而攻占城堡的故事，来表示某些有意骗人犯错误的程序。它由程序开发者开发一个外表上很有魅力而且显得可靠的程序，可是使用者使用一定时间或运行一定次数之后，便会发生巨大故障或各种问题。从功能上看，同逻辑炸弹有相同之处。

以上各种类型的程序，在某种意义上都是“古典的”计算机犯罪的手法，当它进入计算机时，就会破坏数据和程序。

也可根据病毒所寻找的宿主，将病毒分为以下四种：

(1) 源码病毒 (Source Code Viruses)：它可在程序被编译前插入到诸如 BASIC、Pascal 等编写的源程序之中。

(2) 入侵病毒 (Intrusive Viruses)：侵入到现有程序，插入主程序之中。

(3)操作系统病毒(Operating System Viruses)：根据 Digital

Dispatch 公司材料，操作系统病毒程序把大量的攻击逻辑隐藏在虚假地标明了是坏的磁盘扇区上，其它的装在常驻 RAM 的程序或设备的驱动器之中，以便秘密地从内存进行感染或攻击。这种病毒有很强的破坏力，可以导致整个系统瘫痪。

（4）外壳病毒（Shell Viruses）：它包围在主程序的周围，对原来的程序不作修改。

从病毒的破坏意图来看，病毒又可分为：

（1）良性病毒：此种病毒多为恶作剧，但也有一定的破坏性，或副作用。

（2）恶性病毒：是有目的的人为破坏。最常见的恶性病毒往往是消除数据，删除文件或对硬盘进行格式化。

1.3 计算机病毒的破坏作用

计算机病毒不论是恶性病毒还是良性病毒，其危害性都很大。最常见的恶性病毒往往是消除数据、删除文件，或对硬盘进行格式化。恶性病毒可以中断一个大型计算机中心的正常工作，可以使一个计算机网络陷于瘫痪，造成灾难性的后果。

良性病毒虽然是恶作剧，但由于它消耗系统资源，往往由此而造成计算机系统不能正常运行的恶性后果。

计算机病毒虽然大都是一些小程序，但其破坏能力不取决于病毒程序的大小，而是取决于计算机病毒的再生能力。计算机病毒像爱滋病一样，只要接触就传染。一个典型的 PC 系统下的病毒，能在几个星期内扩散到数百台未联网的计算机中，在已联网的系统中，传播的信息流能在几个小时内将病毒传遍数千台计算机。任何系统只要允许信息被分享、解释

并再传送，病毒就能扩散到整个系统。正是由于系统具有这些功能，计算机病毒才能得以按指数模式进行广泛传播。由于计算机病毒隐藏在合法用户的文件中，因而病毒程序的执行是“合法”的。有的病毒往往潜伏很深，一旦爆发，就可能摧毁整个系统。

近年来，利用计算机病毒侵扰计算机系统的事件层出不穷，比较著名的事件有：1989 年 10 月 13 日（星期五）1813（黑色星期五）病毒传遍了欧洲和美洲。

据报道，这一天，许多国家虽然都作了充分的防范准备，但是 1813 病毒仍然使荷兰有 10 万台电脑受到病毒感染。法国的雷诺汽车公司、巴黎银行和其他中小企业，都有电脑被感染。法国电脑安全联合会 10 月 13 日查出有 200 家公司被六种电脑病毒感染。一名中小企业的负责人眼见他的全部帐务资料从电脑记忆中消失。巴黎国家银行尼斯总处的电脑被病毒感染后，在客户资料档案消失前一刻，把该病毒找到并予以消除，才免遭大祸。美国 IBM 电脑公司的微电脑和两用电脑也受到病毒侵袭。据有关专家估计，黑色星期五全球至少有 1%的微电脑可能感染上电脑病毒。

1.4 制造计算机病毒是犯罪行为

今年 1 月 22 日美国联邦法院宣布在 1988 年 11 月初采用病毒程序造成美国各地 6000 台计算机工作紊乱的罗伯特·莫里斯有罪，并处以 5 年监禁和 25 万美元罚款。

莫里斯今年 24 岁，是康奈尔大学的研究生。前年 11 月，他编制的病毒程序通过 UNIX 操作系统的漏洞进入联结一些美国军事单位和研究机构的 Internet 计算机机构网络，造成

了轰动一时的计算机病毒感染事件。

联邦法庭陪审团在合议 6 个小时后，宣布莫里斯有罪。在此之前，他的辨护律师说，莫里斯从未打算妨碍官方计算机系统的工作，那个事件是一个学生犯的程序错误。但是，起诉人说莫里斯病毒程序“并不是幼稚的恶作剧”。

自从 1986 年美国公布计算机欺诈和滥用条例以来，莫里斯是第一个据此条例被送上法庭的人。

在我国虽然未有发生如此重大的病毒感染事件，但许多计算机管理单位和用户都身受其害，许多微机都不同程度地受到了“病毒”的感染，这些现象正引起国家有关部门的密切注意。鉴于有一些人仍热衷于制造和传播“病毒”，一些计算机管理单位和部门，以及广大计算机用户呼吁有关部门迅速采取行动，制止病毒流行，并建议国家有关部门立法，给制造计算机病毒者以严惩。

1.5 计算机病毒预防

要预防病毒，首先要了解病毒，提高用户的安全意识。如果用户意识到可能受到计算机病毒的严重威胁，他就会自觉地对计算机病毒进行预防。如果用户对病毒一无所知，病毒就有可能猖狂肆虐。

预防计算机病毒，最主要的是要堵塞病毒传播的途径：

(1) 严禁工作人员把外单位的程序带入系统运行。磁盘只准流出，不能随便流入。流入软件必须经过检疫。软件流出也必须检查消毒。

(2) 严禁工作人员玩各种计算机游戏，游戏软件是病毒传播的主要载体。

(3) 对新搬进的机器要“消毒”后再使用。

(4) 限制网上可执行代码的交换。

(5) 写保护所有系统盘和文件。

(6) 除非是原始盘，绝不用软盘去引导硬盘。

(7) 绝不执行不知来源的程序。

(8) 绝不把用户数据或程序写到系统盘上。

(9) 复制备份文件，并检查消毒保存。

由于堵塞病毒的传播比较困难，所以我们要一面预防，一面经常检查病毒，以便及早发现，及时防治。如果你的计算机系统出现了以下几种不正常现象，应当考虑病毒是否已侵入你的计算机系统。

(1) 磁盘引导扇区被修改。

(2) 根目录区被修改。

(3) COMMAND. COM 系统文件被修改。

(4) AUTOEXEC. BAT、CONFIG. SYS 被修改。

(5) 磁盘出现固定的坏扇区。

(6) 屏幕显示特殊的信息和图像。

(7) 系统运行中经常无故死机。

(8) 系统的配置出现错误。

(9) 磁盘上出现异常文件。

(10) 磁盘文件内容被修改。

(11) 磁盘文件的长度无故增加。

(12) 磁盘文件无故消失。

(13) 程序装入时间比平常长。

(14) 磁盘访问时间比平时长。

(15) 用户并没有访问的设备出现“忙”信号。

(16) 可用存储空间突然变小。

（17）可执行文件的长度发生变化。

（18）文件的日期发生变化。

（19）OFFICE 运行时，突然死机。

系统被病毒感染后的治疗，除了上述的“诊断”过程之外，还有一个过程叫修复。修复因病毒的种类和感染的程度而异。最简单的修复可以是将系统电源关开一次并用健康的原始盘导引，然后抹掉硬盘上的病毒，当然同时还要对所有被感染的软盘进行“消毒”。当有数据或程序丢失或被篡改时，则要恢复这些数据和程序。联在网上的机器被感染后的修复要复杂得多，只要不是同时将网上每一台机器里的病毒排除，便很有可能马上又都被感染，因此这种修复要花费大量的人力和物力。

为了防止计算机病毒的扩散，消除计算机病毒，恢复被病毒破坏的磁道和数据，现在已有专门防治计算机病毒的软件问世。这种软件有两大类：一类用于病毒检测；另一类用于病毒防治和免疫。

用于病毒检测的软件，如我们汉化的病毒检测软件，可以对 39 种计算机病毒进行检测。它可以对磁盘上每一个文件进行检测，一旦发现病毒，立即在屏幕上告知你是何种病毒侵入了哪个文件之中。它可以对病毒进行诊断，但它还不能对病毒进行防治。

另一种是计算机病毒防治软件。这种软件一般是针对具体病毒进行防治，消除病毒和“接种免疫”。我们现已开发的有小球病毒防治软件，巴基斯坦智囊病毒防治软件，STONE 石头病毒防治软件，1813 黑色星期五病毒防治软件，等等。这种软件随着病毒的不断发现而增多。这些软件当然也不是万能的，它只能对症下药，一种药方一般只能防治一种病毒。由

于软件开发环境的不同，这类软件也不是在任何环境下都能适用的。