计算机病毒手册

梁建瑞　编译　梅多伦　审校

科学技术文献出版社

计算机病毒手册

梁建瑞　编译
梅多伦　审校

科学技术文献出版社

(京)新登字130号

内 容 简 介

本书综述了近年来计算机病毒的研究成果，其内容涉及计算机病毒的各个方面：病毒的定义、分类和传染机制等基础理论；计算机病毒的预防和处理手段；反病毒软件的评估和测试方法；病毒防卫的概念基础和数学模型。

本书特别给出了有关各种计算机病毒的详细材料，深入剖析了20余种典型病毒的程序结构和作用原理，重点介绍了近年来证明是行之有效的病毒预防管理措施。本书实用性强，适用于计算机维护人员、微机使用人员、技术管理人员及行政管理人员参考使用。

图书在版编目(CIP)数据

计算机病毒手册／梁建瑞编译.-北京：科学技术文献出版社，1994.10

ISBN 7-5023-2224-8

Ⅰ.计… Ⅱ.梁… Ⅲ.计算机病毒-手册 Ⅳ.TP309-62

科学技术文献出版社出版
(北京复兴路15号 邮政编码100038)
北京市燕山联营印刷厂印刷 新华书店北京发行所发行
1994年10月第1版 1994年10月第1次印刷
850×1168毫米 32开本 7.625印张 200千字
科技新书目：320—098 印数：1—4400册
定价：8.40元

编译者序

计算机病毒自1987年开始在世界各地广泛传播，几乎同一时期迅速传入我国。各国政府和研究部门对此都比较重视，开展了大量的研究和防治工作，取得了不同程度的进展。我们综合了国内外这方面的研究成果，并参考了美国H.J.哈兰德教授著的《计算机病毒手册》，编译了这本可供计算机维护人员、微机操作人员、技术管理人员和行政领导干部参考使用的工具书。

本书专业性较强，考虑到非专业读者阅读的需要，我们专门在附录中为非专业读者准备了了解病毒必备的基础知识，并在章节组织上进行了特别的安排，非专业读者也可以跳过某些章节而有选择地阅读本书。另外，考虑到专业读者进一步研究的需要，我们还在附录中特地精选了几篇"经典"技术论文。

中国科学院计算所刘昌平博士和曾一平同志参加了本书附录二和第六章的编译工作。

本书在编译过程中，受到中国科学院计算所梅多伦研究员和胡永刚、朱叙国等同志的大力支持和帮助，在此表示衷心的感谢。由于时间仓促及作者水平有限，书中难免有不妥之处，希望读者给予批评指正。

目　录

第一章 导 论

关于计算机病毒，近年来国内外报刊、新闻媒介报道得很多。我国的《人民日报》就报道过多次。对“计算机病毒”一词，大家肯定已不再陌生。但计算机病毒究竟是什么？相信很多人至今也不甚明了，各种各样的误解在所难免。

一、计算机病毒实质上是程序

在计算机病毒尚未被人们认识之前，当计算机上出现一些奇怪现象时，如屏幕上忽然出现一个跳动的亮光点，或硬盘上的数据莫名其妙地丢失了，或原本完好的系统盘一下子启动不了系统了，人们直观的感觉就好像是计算机出了故障——“病了”。后经计算机专家研究“诊断”，发现它是由一些计算机程序造成的，并不是计算机部件坏了，也不是线路逻辑发生问题；而且不同的现象有时是由不同的程序造成的。当然，我们现在都知道它可能是染上了计算机病毒。这些导致计算机异常的程序就是计算机病毒。计算机出现病毒，正是计算机不自觉地运行了病毒程序的结果。

计算机病毒是人为设计的程序(一般是干坏事的程序)。设计者为了避免被人们发现，常将其设计成具有依附于其它正常程序之中的能力。该被依附的程序，被称为病毒的宿主程序。当病毒的宿主程序被计算机调用运行时，病毒程序也随之被运行。病毒程序一般都复制自己(繁殖)，并试求再依附于其它程序上，此即为传染。此时，病毒程序一般都不马上发生作用(干坏事)，以避免被人们立即发现，而是潜伏着，当某些条件适合时才触发破坏。我们知道，在传染病学中生物病毒正是这样的，它能传染疾病，但很小、很难发

现。它使用生物体细胞并依附于细胞中，生长繁殖，从而随着细胞的繁殖而发展。最后，在某些情况下被诱发，发生作用，致使生物机体产生病变而发病。由于病毒程序与医学病毒在这许多特征方面的类似性，以及传染病学的思想和手段对预防和处理计算机病毒方面的借鉴作用(参见第二章中“计算机病毒与传染病学”一节)，人们才使用了“计算机病毒”一词来称谓上述计算机程序。

二、计算机决不会自己生出病毒

尽管现在关于计算机病毒的文章和报道已经很多，但那些不太熟悉计算机技术的人仍暗自怀疑：计算机病毒会不会是由于计算机系统在现在这个时代夜以继日地运行，因而“年久失修”，逻辑紊乱所造成？会不会是由于各种大量的计算机程序相互作用“互相倾轧”所造成？会不会至少有一部分计算机病毒是由于这样所造成？因为在这个时代，什么怪现象都可能发生，既然人类社会能生出艾滋病病毒，那么难道计算机世界就不会生出它自己的什么东西？再者，现在世界各国都在研究“人工智能”，计算机系统会不会是由于拥有了“人工智能”而制造了计算机病毒？

我们回答是：都不会的！计算机病毒是人为编制的程序，它最初必须是由人来装入(输入)计算机的。它随后的复制、传染、发作，虽然不再需用人工干预，但它正是由于人们在程序中已经预先设定的结果；它也正是计算机病毒与偶然的程序错误或某一次的操作失误所不同的地方。它的特征(功能)是能够巧妙地隐藏、繁衍从而存在、传播下去。

我们即使在计算机上胡乱地击键(学生初次上机时常有这种情况发生)，计算机也决不会就生出病毒来，最多是出现死机，或者是由于含有错误操作而丢失数据等。我们将键盘设想成一个由许多方块所组成的平台，并设想上面有一头(愚蠢的)驴子胡乱地用蹄子蹬踏(击键)，那么可以想象，无论驴子蹬踏多久，也永远不可能生出

所谓计算机病毒来!

计算机病毒与计算机故障也不同。计算机故障虽然也会造成计算机异常，但它不具有计算机病毒的特征，比如它不会传染。在计算机发展的早期，曾经发生过一个计算机故障，后来被发现是由于一个蛾子造成的；它因为被继电器挤扁而充当了绝缘体（据说这个蛾子至今仍被保存在美国的航海历史博物馆里）。这种故障，显然与计算机病毒毫不相干。

至于"人工智能"，与计算机病毒也扯不到一起。因为大部分计算机并不具有"人工智能"，人们并没有主动地赋予它们。自然，"人工智能"必须是人工的产物。

三、数字游戏

这是一个大家最常提出的问题。对于杀病毒软件，人们最常提出的问题也是："到底能杀死多少种病毒?"。在书刊文章中，常见有人宣称已发现了56种病毒，而另有人则宣称已收集了560种病毒。就好像能列举的病毒种类越多，就越是这方面的权威似的。事实上，病毒具有多变性，例如Brain病毒(或称巴基斯坦病毒)，其主要表现是在被它感染的磁盘上写"Brain"作为卷标。如果发现另有病毒写"Ha-Ha"作为磁盘卷标，而其各方面均和Brain病毒相同，那么，能把它称为一个"新"病毒吗？因为，除了五个ASCII字符不同外，两个程序的其它各方面均是相同的。

对病毒的多变性问题，我们有一个简单的方法，就是：只要病毒程序的关键码未改变，我们就称其为变种或变体。不过，确有其他人使用更简单方法的：只要有变化，无论变化大小，均作为一个新病毒。这样，有些病毒，比如小球病毒，因为其有十几种变体，因此就被视为了十几种病毒。当然，我们的做法也遇到一些问题：

●比如，一个病毒攻击除COMMAND.COM之外的所有.COM程序，又出现一个变种，连COMMAND.COM也攻击，尽管此病毒的

源码变化并不大，修改不困难，但该变种就不同了，因为病毒的动作已变化了。

●再比如，如果一个病毒只在5.25英寸软盘上，但同时又出现了只在硬盘上的，那么，我们认为它是一个新病毒吗？

我们认为，只要两个病毒具有相同的源码并且动作大致相同，则它们是同一源病毒的变体。但是，如果它们的动作已被改变，则它们就应被划为一个新种。许多讨论病毒的书中将 PC 机（IBM-PC及其兼容机）、Macintosh机及VAX机的病毒都列举在一起，甚至还将一些听说的、未得证实的事件也说成病毒，致使有关病毒种类的数字大相径庭，使广大读者陷于数字游戏之中。有鉴于此，本书暂且不谈这个问题，而是给读者呈现出更为实用的知识。考虑到Macintosh机在我们国家并不多见，而大中型计算机（由于其操作系统比较复杂且具有内部安全性）不易受到病毒攻击，本书将只给出二十余种DOS机病毒并详加剖析。这些病毒都有实在的程序拷贝，数据都是严格检查过的。读者对这些病毒弄懂掌握后，对其相应的变体，就容易了解得多了。

第二章　计算机病毒的基本概念

这章介绍一些基础知识，为大家理解计算机病毒及其工作原理做准备。在这章里，我们给出了几个当今有代表性的计算机病毒的定义和其它相关术语的解释，并对计算机病毒进行了粗略的分类。考虑到非专业读者阅读本书的需要，我们还特地在附录一中有选择地介绍了DOS软磁盘的内部结构知识，这对我们弄清计算机病毒在磁盘上自我复制和潜伏的机理十分重要。

一、基本定义

我们知道，针对一种现象和问题，科学研究常常要花大量的时间来寻求一个公认的定义。有些人认为这很不值得，岂不知许多成功研究都是从定义开始的。而且，研究某些定义，也能确保我们谈论的话题是同一个东西。

即使搞计算机病毒研究的人，也很难轻易区分一个病毒的众多副份，究竟怎样才能确保我们谈论的是同一个病毒？依据它们有相同的字节吗？如果病毒是ASCII码的，那么可以对它进行鉴别吗？这时，只有比较反汇编过来的代码，可以说别无它法。

1．计算机病毒

简单地把计算机病毒定义为“一个可传染的寄生程序，只在一种特有程序出现时复制”，或“唯一的一类不应该与其它恶意程序混淆的程序”，对计算机界来说，都是不可接受的。这些定义过分简化了计算机病毒的特性。让我们来看看下面的五个关于计算机病毒的定义：

（1）“病毒程序的传染，就是通过修改其它程序从而嵌入其自

身的复制品，当然，嵌入的也可能是一个变化了的版本，一个变种或另一个子代。病毒可以是其设计者想使用的任何代码。病毒可以通过系统和网络传播，从而随意修改程序和数据。”

(2) 病毒：(a)“特洛伊木马”(后面有解释)的一个变种。它正在繁衍（将自身附于文件、程序上），带有一个触发机制(事件、时间）和一种破坏功能（删除文件、发送数据)。(b) 为了恶意目的被引入磁盘操作系统的一组码。它可以在某个时刻触发一个过程，删除盘上的所有文件。病毒的恶果能够危害到许多用户，一个含有计算机病毒的盘装进计算机后，病毒就驻入到计算机内存。每当它检测到有新盘装入系统时，它就将自己写入那个盘里。

(3)“一个计算机病毒就是这样的程序码，它常常把自己附在一个程序文件的开头或末尾，并且包含两个部分：

● 一部分负责自身复制，即在某个时刻（通常是当一个已被传染的程序运行时，或一个要被传染的程序运行时）拷贝整个病毒码（或其修改了的版本）到程序文件（或磁盘的其它区域）从而达到繁衍的目的。

● 另一部分即是当某一事件发生时（如一个已被传染的程序对某一数据运行时，或病毒已经复制到多少次时）就执行某些操作（常常是些对文件或磁盘具有破坏作用的操作)。”

(4)“病毒就是一种可以自我繁衍的‘特洛伊木马’，它包含一个功能部，一个触发部和一个复制部。”

(5)“真正的病毒就是一套指令，可以自己繁衍或通过计算机系统和网络繁衍，并有意做些对系统合法而对系统（或网）的所有者是不期望发生的事情。这个定义的关键就是，病毒的引进是故意所为，而不是技术差错，即在病毒后面隐含着人的主动意图。病毒造成的危害，可能不只是让计算机不按主人的意图运行，还可以造成数据和软件无可挽回的损失。病毒破坏的潜力还不能在量上表示，但它可以影响的范围却是无限的。”

在一个由纽约的 Deloitte, Haskins & Sells 研究所发起的，美

国信息系统安全协会参与筹办的“计算机病毒邀请讨论会”上，计算机病毒定义讨论组对上述定义做了引伸表述。这个小组在报告中指出：“一个定义不应该与电子数据处理界及一般公众所理解的概念相矛盾，但它仍应当意思清楚，应能将计算机病毒与其它滥用计算机的情况区别开来。”因此，他们提出这样几条：

●“隐含病毒的指令集可以有不同的形式，它们可能包括软件中的程序指令（通常的情况），硬连线指令，通讯口令控制符，参数或工作控制语句。这个定义不应当将任何可能传播病毒的特殊载体排除在外。”

●“病毒定义不应当对其繁衍成什么子代有新限制。病毒可以在许多软件系统中复制自己。但是，病毒生成的指令也可能在形式上和内容上都不同于先前的病毒。一句话，计算机病毒是可以演化的。”

●“一些计算机专家试图根据病毒所造成的危害的程度区分出良性病毒和恶性病毒。然而，即使被称为良性的病毒也占用存贮空间和机时，为操作人员所不愿。对一个现存病毒，程序设计人员增加一些具有高度破坏作用的程序码，此病毒即变成了某种意义上的‘变种’。增改一个现存病毒比设计一个新病毒可以少动不少脑筋。因此，良性病毒总是被修改，最终会变成所谓恶性病毒。”

●“应该把计算机病毒同程序差错区别开来，后者是不管愿意不愿意都可能发生的。根据定义，差错不是故意的，而计算机病毒则总是被人有意为之的。”

2.“蠕虫”

这个词因为1988年11月美国康纳（Cornell）大学一学生所制造的“Internet事件”而为人们所熟悉。在“计算机蠕虫——一份给康纳大学教务长的报告”中这样写着：“这个恶意程序既然复制了自己，而没有一定要将其附在宿主程序上来完成复制，因此，技术上它应被称为‘蠕虫’。严格地说，它不是一个网络蠕虫，而是一个主机蠕虫，只是通过网络传播罢了。这个网络本身在整个事件过程中

都一直在正常运行着。”

这里是美国弗雷德·柯亨博士所作的定义：

“蠕虫程序使用未被占用的处理程序来执行并行运算。有名的‘Xerox蠕虫’就是一个误码造成，致使蠕虫在网络做引导时仍拒不放弃处理程序，以致要克服蠕虫就必须重新启动整个网。”

下面的又一个定义出自报告——《计算机病毒及其对共享系统影响能力的研究》，该报告是1988年9月由美国宾夕法尼亚州众议会所属的预算与财政委员会作的。

“蠕虫：最初设计为采用小的时间段以充分利用空闲设备处理较长请求的程序。蠕虫程序在空闲外围设备间分配工作量，最后再将每件工作串在一起。这使得设备得以更有效的利用，减少了排队问题和机时延误，提高了总的效率。蠕虫程序最早的设计，是服从于需要使用蠕虫程序正使用着的设备的新的程序申请，然而，它以后又被修改成拒绝一切其它程序的申请，从而使蠕虫程序总是在使用一切可以利用的资源，这样，其它的任何操作都是不可能的了。”

朗利（Longley）和赛恩（Shain）在他们的《数据和计算机安全：标准、概念和术语词典》中，将蠕虫定义如下：

“在软件保护中，由软件出版商预设的、在发现未经许可使用时执行惩罚的程序。蠕虫好的情况是暂停被保护的程序，坏的情况则是在它每次运行时都造成一些“讹误”（Corruption），最后导致磁盘毁坏。蠕虫是危险的，因为它能够随时被激活，所以不奇怪，被这样保护的软件包自然不好卖。”

L.G.琼斯（Lauzie Ganong Jones）女士在她出席“1989年信息系统审查与控制大会”时，提出了下面的定义：

“蠕虫：一个通过通讯通道在其它系统上拷贝、并使拷贝激活的程序。也就是指这样一个程序，它不停地在内存区拷贝自己，而对操作系统不留下任何这些拷贝存在的记录，从而避开正常的系统控制。”

3. 其它概念

下面几个术语，在计算机病毒和蠕虫的讨论中经常会用到。我们给出这些术语的多个定义，正象上面的一样，还没有一个定义被人们普遍接受。

●“特洛伊木马是这样一种程序，执行其说明中未提到的服务。这些服务如果是违反安全法则的，那么它们就可能是特别危险的。”——弗雷德·柯亨。

●“特洛伊木马：(1) 这样的一种计算机程序，表面上具有实用功能，而又隐含盗用进程、有损计算机安全的非法功能。例如，为特洛伊木马的程序设计者盲目拷贝文件。(2) 看起来实用但包含‘暗门’(trapdoor) 的计算机程序。(3) 被插入在计算机程序中的程序，它执行未在程序说明中描述的功能。利用属于调用环境的权力，拷贝、滥用或销毁数据。例如，隐含在文本编辑软件中的特洛伊木马就可以把被编辑的文件中的机密信息拷贝到攻击者可访问的文件上。”——朗利和赛恩。

●“‘逻辑炸弹’是这样一种程序，当某些系统条件满足时，诸如一个特定时间或某些数据（一个名字或代码）存在或不存在时，就触发进行破坏。”——弗雷德·柯亨。

●“暗门就是一个进入系统的入口，一般只有设计者才知道，但有时也会被其他人发现。”——弗雷德·柯亨。

●“暗门：(1) 一种隐含的软件或硬件机构，可以超越系统保护机制。它可以某种难以觉察的方式被激活（如终端随机确定的击键顺序)。(2) 在自动数据处理系统中，为收集、交换或破坏数据的目的而有意留的‘缺口’。(3) 存在于系统软件或硬件中的条件，可能会被触发从而偷偷破坏软件或硬件的安全特征。这个条件可以从内部（如一个计数器、数据或时间值，或一种预设的环境）唤醒，也可以从外部（如由远距离终端或应用程序输入的命令）唤醒。”——朗利和赛恩。

●“暗门：一种隐含的软件或硬件机构，能够被触发并能越过

系统保护机制。它可以某种不易发现的方式被激活，如在终端按随机确定的顺序击键盘。软件开发者常常在他们开发的软件中引进暗门，以便他们能够重新进入系统执行某些功能。”——美国计算机安全中心。

二、病毒概述

在本书以后章节里将详细分析许多病毒的程序逻辑，在这节里我们仅谈三点。第一，总结一下已有的计算机病毒。第二，给出一种计算机病毒的伪码表示。第三，介绍一下早期由弗雷德·柯亨博士编制的最原始的病毒。

1. 典型的计算机病毒

虽然在前面给出的五个病毒定义之间存在语义上或其它方面的差别，但现有计算机病毒不外乎两类：

(a) 引导扇区传染病毒（或称Boot区传染病毒）。

(b) 可执行程序传染病毒。

引导扇区传染病毒可能是自包含的，也可能是溢出病种。自包含病毒整个隐藏在软盘的原始引导扇区中。溢出病种则需要另外的磁盘空间，这类病毒可能在它要传染一磁盘时先检查是否有足够的磁盘空间（簇），也可能就直接覆盖磁盘上的原有文件。磁盘引导扇区传染病毒，即是将其自身安装在磁盘上，它在磁盘上的位置，将依据所用的操作系统版本而定。

可执行程序传染的病毒，是将其自身附在.COM或.EXE程序上。附在COMMAND.COM上的仅仅是一种特殊的.COM病毒。这些病毒的绝大部分，都是将其自身的一部分附在程序的开头，然后跟有关的JMP指令，病毒码的剩余部分则将连接在被传染程序的末尾，从而完成对程序的传染。

2. 程序逻辑

这里给出的伪码病毒，既可攻击.COM程序，也可攻击.EXE