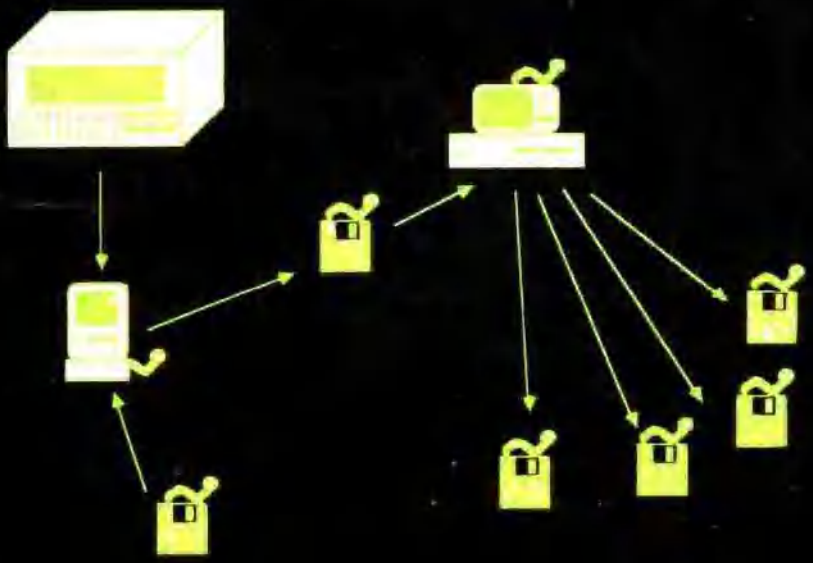
计算机病毒危机

THE COMPUTER VIRUS CRISIS



华北计算技术研究所情报室

计算机病毒危机

译者　王敬治　武彦生
校者　陈伯洲　尹祯祚
编辑　尹祯祚　李瑞珍

华北计算技术研究所情报室

译者的话

在我国，目前计算机病毒大有蔓延之势。为了适应当前我国计算机用户的急需，华北计算技术研究所情报室组织有关人员从速翻译了《计算机病毒危机》(The Computer Virus Crisis)一书。

《计算机病毒危机》是1989年美国最新出版的有关计算机病毒的基础读物。它以通俗易懂的语言阐述了计算机病毒的概念、传播、表现和种类。书中列举了大量事实。如 Monkey—on—Your—Back、Crabs、Scores、MacMag、PLO、Brain、SEX — EXE、nVIR、HyperCard 等典型病毒。同时，又从技术角度对病毒进行了详细的剖析，图文并茂，使读者对计算机病毒有一个形象生动的感性认识和理性认识。书中提出了避免病毒侵扰的 Safe—hex 方法及病毒疫苗技术，还简要地描述了侵扰计算机安全的“特洛伊木马术(Trojan horse)、意大利香肠(Salamis)”等12种方法，书后列出了有关病毒的技术术语解释，并附有大量有关病毒和抗毒软件的参考文献。

该书适于计算机用户的操作人员、技术人员及院校师生阅读。对广泛而深入研究计算机病毒的专家们也颇有裨益。

在翻译过程中，由于时间紧，完稿仓促，加之译者编者水平有限，书中译文错误、遗漏不妥之处在所难免，敬请读者批评指正。

译者

1990.5

目　录

前言

你为计算机病毒程序而烦脑吗？假如你使用个人计算机，特别是经常使用公告牌，你大概会有这种烦脑。本书所描述的详细内容有助于你了解病毒现象的全貌。核对用的清单有助于你去应付病毒问题，而病症清单有助于你对病毒进行诊断。书中还提供了参考用的附录，它有助于你排除病毒程序。附录中给出了抗病毒剂的简要评论，并有联系地址。假如你是专业工作者，你可找到有助于你深入技术细节的有关内容。

有一种集体游戏叫做打电话或传递消息。人们坐成圆圈，一个给其旁边的人说句耳语，这个人再把这句耳语传给其旁边的人，这样一个传一个，一直传一圈。最后一个人把他所听到的与最初他发出去的相比较。一般地说这个消息在传了一圈之后总是被走样和歪曲的。

前几个月中，一些有关计算机病毒程序的通讯报导就像上面所说的游戏一样。第一次报导理应适当地详细点，譬如像 Wall Street Journal 杂志中那样。（和一个安全专业工作者相比，报导者所述的内容，说明他并不真正了解情况，但他很会添枝加叶的描绘。）这情节传到专线发稿的各通讯社以后，为了适应各种报纸的需要，又对它们进行了不同的编辑（而这些编辑人员往往是完全没有专业知识的人。），当地报纸在印刷出这些内容时，与其原来的情况相比，几乎是面目皆非，很少有相似之处了。

作者们编纂本书的实际目的，在于为读者当好计算机安全和合法事务方面的顾问与参谋。一个偶然的机会，有一天午饭时，由于我们有两人正为那些被歪曲了的报告面伤心，所以打算讨论如何帮助

读者更好地对付计算机病毒程序。我们听说过 Macintosh 上的 MacMag 病毒，它在 1988 年 3 月 2 日使用户们大吃一惊。病毒在过去并不是个大问题，但突然广泛流传，我们就认为它要成为一个很大问题了。

根据那次讨论的一个观点，我们当中的一人就说："我们为何不写一本书。"本书就是这样出来的。

我们把有用的信息都编辑在书中，使用的语言对于没有很深技术经历的人也是通俗易懂的。有些人不太懂技术而只是简单地抄录，因此在他们的文章中常常出现一些不确切的地方。从技术角度出发，我们在本书中已经把这种不确切性去掉了。

《The Computer Virus Crisis》一书将有助于那些不管是正在或将要同病毒作斗争的人们。虽然技术性不是很强，但我们已写入了足够的技术材料以帮助有一些技术经历的人了解：病毒感染是怎么回事，如何识别病毒，如何对付病毒。如果你需要更多的资料，可参阅附录，它给出一系列的抗病毒产品。除了有关如何使用所提供的工具之外，有些软件包还包括了详细的技术线索。我们建议你查看一下疫苗和其它的保护软件。

在 Through the Looking Glass and What Alice Found There 一书中，Lewis Carroll 说："当我用一个词的时候，其意义应当很确切，不能有或多或少的含混不清。"因为在计算机安全性这个领域中所用的很多词都相当地含混不清（即使在有些专业人员中也是这样），所以我们在书中加入了一个"术语汇编"。用定义的方式向你介绍有关术语词汇。当每个人都用相同的字来表示相同的事的时候，再来谈论这些事就显得有些多余了。

本书举出的计算机病毒程序并不就是最后的了。很多破坏者正在积极制造病毒，而很多专业工作者正在设计防护的方法和产品。事物的变化非常快，比一本书能反映的快得多。以本书作为基础，你会知道如何才能跟上并了解杂志和期刊中不断出现的新材料。

在本书中的很多地方，我们给出了插图以便解释，计算机病毒是如何完成它要做的事情的。当我们在举出这些例子时，我们有个难处：假如我们把例子讲得非常完全和功能化，那我们就等于给出了一本"病毒谱"(cookbook)，它可能被破坏者利用来生产病毒。这不是我们的愿望与目的。我们不需要促进病毒蔓延。因此，所举的例子的完整性与详细程度只是为了足以说明病毒的要点，但不足以去产生病毒。我们要做的是为了帮助中等水平的计算机用户能了解：计算机病毒究竟是什么，如何保护自己不受其侵害。当你了解这些正在发生的情况时，你对计算机的使用不会有什么不安全感。

专业人员和编程人员阅读此书，会感到内容还不够充实，因为他们已有这种技术背景知识—它是我们专业的工作工具的一部分。

在编辑成书的过程中，我们得到了很多人的支持。一些软件开发者的产品列入了附录，他们不但提供了其产品的拷贝，而且提供了他们从事研究所集聚的资料与成果。Mr. Ian Fraser，他是 micro computer and Graphic Image Consultants 公司的老板，他提供了第五章中的很多技术细节和附录中有关的 DOS 抗病毒程序。Dr. H. Highland 是 Computer and Security 的主编，其工作有很高的技术水平，提供了有关数字资料及有关其工作小组发现的某些报告。Dianne Littwin 和 Maud Keisman (Van Nostrand Reinhold)为了保质按期地完成本书的出版，与我们进行了密切合作。Ms. Harriet Serenkin 为书稿提供了宝贵的修订意见。

我们从 Bowlder Colorado，Sopho 的副总裁 Michael Cervansky 那里听到关于"Safe hex"这个短语。它是公认的，也是计算机用户能接受的，我们选用它是为了使人们对于保护措施有个深刻的印象，即这些措施能使你与病毒打交道而产生麻烦的机会减到最小。

除了一个广告再版外，本书全部采用计算机编排印制。其草稿用 Galbraith Law Offices 的激光打印机印出。排版用同样的 PostScript 文件(University of Alberta Printing Services)。

希望你在阅读此书后会感觉到，病毒并不是神乎其神的。可惜能生产和扩散病毒的人太多。还希望你从本书中可以知道更多的问题。一旦了解了，你被攻击，被感染的机会就会极少。我们希望你采用“安全妙术法”(Safe hex)。最后，我们提请您：我们认为把病毒引入别人的计算机系统是不道德的，非法的，违反行业道德的。

请别这样干！

第一章 概述

今天是做案的时候吗？我知道，假如到了做案的时候，我就要干些重要事。不，星期五(13号)还没到呢。假如今天还不到做案的时候，我要把自己复制一遍。让我看看系统文件，我知道每台计算机都有系统文件。查看一下，该系统文件中是否有我？假如没有，我就把自己拷贝下来。假如我已在其中，让我看一下这台计算机的程序文件，至少有一个文件其中还没有我。对了，确实有一个，我试了48次之后才发现它。啊！它是个只读文件。那好了，我只要改变这个只读标志，这样我就能修改这个文件了。行了，我正在把自己拷贝到那个程序文件中去；拷贝后，我只对那个程序作了一点点儿手脚的修改：这儿加个"转移"那儿加个"返回"。我得记住做手脚的地方，要把修改过的文件恢复到只读标志。现在，我已掩盖好了自己留下的痕迹吗？经过检查，所有的属性都同我进来时一模一样；因为我找到了一些空地址来拷贝自己，所以长度未变。我还得记住，做手脚的日期要恢复到和我进来时一样的日期。是否不能让人很容易地发现我在什么地方，我已做完了吗？不，我还要在软盘驱动器上重复上述同样的过程。假如有网络的话，还要查一下我是否也可以通过它进行做手脚。现在我已做完了吗？是的，做完了。以上那些就是我考虑要在星期五(13)要做的事！我不知道FORMATC是什么意思？嘿，我要在把自己拷贝了50次之后再去做这件事。啊，我已是第49次了。下次……

以上所介绍的是当病毒在进行工作时，如果它能思改的话，它可能在思改些什么。很多病毒正是按这种方式工作的。直到发生错误你才会知道，在你的系统中已有了病毒。你不但要排除看得见的损害，还要找到病毒已把它自己复制到了哪些地方。

当然，你可能是很安全的。你从委托厂商那里购置计算机，编写你自己的全部程序，从不用别人的程序，也不和其他的计算机通信。如果你委托的厂商确实绝对小心。你才可能不受病毒的传染。病毒正以人类史中前所未有的方式改变着我们的世界，人们决不愿意购置一台很好的计算机而又让它染上病毒。

还有其他的保护方法，其中很多都有很好的效果。本书的目的在于向你介绍关于计算机病毒的真相，并帮助你在当今的信息革命中不受病毒的损害。

内容简介

本书包括四种信息：中等深度的技术信息；关于一般安全性和具体的病毒的参考资料；附录中的抗病毒产品及术语汇编中的各种定义；以及有关计算机病毒现象的一般信息。

假如你遇到了计算机病毒，可立即在附录中找出一种疫苗开发剂来解决所遇到的问题。假如你需要新疫苗，可参阅第 8 第 9 两章；其中包含如何去做的一些暗示。在一切问题解决后，可在第 4 第 7 章中得到如何防止以后中毒的建议。

假如你要概貌性地了解病毒，可从头到尾阅读。假如你已经有所了解了，可阅读第 5 章，它提供技术性更深的材料。

假如你有兴趣要制造和传播病毒，可阅读第 10 第 11 两章；需知那是违法的。第 6 章描述了犯罪者制造传播计算机病源的某些恶果。可别这样做！否则，对你自己比对别人会更不利。

病毒怎样侵袭你

在最近几个月里，已公布了很多关于计算机病毒的报告。1988年3月的MacMag"Peace"病毒所产生的冲击的确是一个大的突破[1]。其中有些报导是有所扩大与歪曲，比如关于西雅图的每台计算机都有病毒的报导。实际上，计算机病毒并不像感冒一样地传播。它没有智能，也不恨你，要避免病毒的暴发也不太难。

在一些计算机中已发现了相当险恶的病毒。过去几年中的某些开发工作已增加了人们对病毒的揭示。假如与其他的计算机通信，特别是从公开的软件库中调取程序，危险性就大了。假如从不认识的人那里获取软件的非法拷贝，那危险性就更大了。

另一方面，假如从微缩包装或电子邮件体制中获取程序，那么，危险性并不太大。

要问问自己，"有谁不喜欢我吗？"假如你是一个特别的目标，就要警惕了。假如你仅仅只是个John用户(或Jane用户)而且只应用某些常用知识，那么问题并不大。

问题在哪儿？

大约十年前，人们要求尽可能低价地在分时系统上运行作业。作业要在等待其他优先权更高的和更高付费的作业之后，才能得到一般运行的时间。那是星期五的下午。创建了一个小文件来检查，这个作业是否已运行过：假如它已运行过，文件中的命令将执行适当的输出并清除有关条件；假如它还没被运行过，它将再次到作业排队中登记。这样，作业运行费用最低，而其作者则不需整个星期五晚上都等在计算机旁。

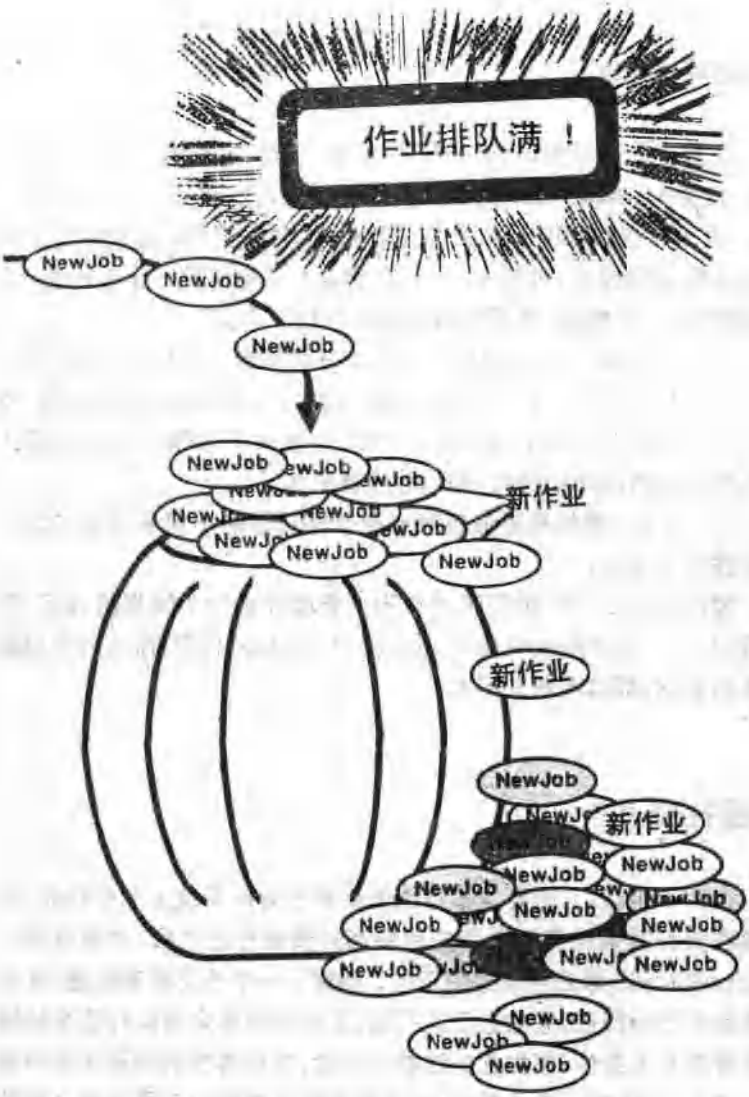


图 1.1　过多的作业

可惜，命令文件没有经过很仔细的测试。它在其反复传递过程中已遭损伤。事实上，只要作业一运行，命令文件的使用是很厉害的，可说是无限制的。系统在星期天被起动后 10 分钟，作者向系统管理程序人员提出了一个客气然而又坚决的请求，要求从作业排队中删除 4096 份相同作业拷贝，以便好让其他作业进入。情况并不是有意识的。但其效果是产生一种准病毒，并将它投入系统。（费了很大的劲，花了 15 分钟，采用几个实用程序清除了那些作业，才修复）。

Fred Cohen 在 1954 年时还没提出“病毒”[2]这个词，但那个命令文件与他后来的描述相符合。不管现在人们如何描绘病毒，但它并不是什么玄妙莫测的新东西。

病毒的概念并不新颖，滋生病毒也并不困难，为什么突然有问题了呢？计算机和通信的兼容性使病毒比过去传播得更远，更快，更容易；还因为现在有愈来愈多的人，成千上万的人使用计算机。（参阅第 2 章的“连接性”部分）。能滋生病毒的人必须具有计算机方面的技能，特别是编程的能力；访问你的计算机的本领；传播病毒的办法。看来，很多人都有滋生病毒的技能，有目的地或偶然性地滋生病毒。任何一个计算机科学系的学生和很多熟悉计算机的青年都有这种技能。

当然，专业人员是能滋生病毒的。但他们总想从其劳动中获得更多效益。他们做任何事都要想一想：“是否还有什么另外的容易的方法可以达到我的目的呢？”由于专业人员若想破坏计算机或程序，他会有更容易的方法，所以由专业人员传播病毒的并不多。

恐怖分子，间谍，以至合法专业人员也具有滋生病毒的技能与训练。但现在他们用破坏电力系统和贿赂银行出纳员的方法能得到更好的结果。

还有一种人，我们称之为文明破坏者 Vandals，其动机是要投石于釜以观热闹，他们破坏计算机系统只不过是为了表现他们的脑袋是如何高超与聪明（自认为的聪明）。他们通常并不想有高的收益，他