计算机病毒危机

杨杰超 武斐霍宏奚红宇

北京大学出版社

计算机病毒危机

杨杰超　武　斐
霍　宏　奚红宇　编译

北京大学出版社

新登字:(京)159 号

计算机病毒危机

杨杰超　武　斐　霍　宏　奚红宇　编译

责任编辑:郭佑民

*

北京大学出版社出版

(北京大学校内)印刷

新华书店北京发行所发行　各地新华书店经售

*

850×1168 毫米　32 开本6.875印张　180 千字

1992 年 2 月第一版　1992 年 2 月第一次印刷

印数:00001—11,000 册

ISBN-301-01841-X/TP・146

定价:4.25 元

内 容 提 要

本书全面系统地介绍了计算机病毒的原理、症状及其危害，并结合病毒的产生及其传播方式，介绍了各种预防和消除病毒感染的保安方法，这主要包括：不非法拷贝软件、使用疫苗程序、做备份，以及采用法律和道德等手段。

本书融科学性、知识性和趣味性于一体，既是计算机病毒方面的专著，又可作为科普读物以及法律和道德方面的教科书。全书文字深入浅出，对于病毒现象的说明多采用图解的方法，每章的开头都有病毒的一段“自白”，形象地说明了病毒现象的特征。

本书可作为广大程序员、计算机科研人员、管理人员以及大专院校师生的参考资料或教材。

序

你担心计算机病毒程序吗?如果你使用个人计算机,尤其是当你频繁使用布告板时,你也许就会担心的。这本书就是给你提供准确的信息,以帮助你了解计算机病毒现象到底是怎样一回事。你将会发现本书列举的检查手段有助于你对付病毒;列举的症状将有助于你确诊你的问题,是否是病毒问题。首先,我们实用的警告会帮助你避免病毒问题的出现;另外,在附录中列举了迄今为止发现的一些病毒(包括其性质和现象),以及一些反病毒产品,并附有简短的评述和联系地址。如果你是一个专业人员,你会发现书中列举的参考文献将有助于你深入钻研技术细节。

有一个集体玩的游戏名叫打电话或传话。一群人围坐成一个圆圈,然后由其中的一个对他旁边的另一个人耳语一个消息,接着那个人又对下一个人耳语这一消息,如此下去,直到轮完一圈为止。最后那个听众很可能发现:他得到的消息与第一个人所讲的相比,已面目全非了。

引起对这种集体游戏联想的是过去关于计算机病毒程序的一些一般性新闻报道。例如,出现在《华尔街杂志》("Wall Street Journal")上的第一个报道,的确算是详实的(尽管在一个专业安全人员看来,消息报道者并不真正懂得所发生的事情,但毕竟记载详细,文笔颇佳)。这篇报道刊登出来后,经过为适应其他报纸需要而进行的编辑加工(通常由没有技术知识的人来做),等到地方报纸再次刊登出这则消息时,就和原来的报道大相径庭了。

我们在为失实的新闻报道感到惊愕的同时,感到有必要使广大的计算机用户了解并进而能够有效地对付计算机病毒程序。在

过去，病毒并非是什么严重问题，但随着突如其来的报道，我们倒希望它成为一个大问题来引起大家的重视。这本书就是循于这样的想法而编写的。

这本书主要是根据美国 VAN NOSTRAND REINHOLD 出版社，1989 年出版的“The Computer Virus Crisis”（作者 Philip Fites，Peter Johnston 和 Martin Kratz）一书及其他一些国内外有关资料编辑而成，同时还融入了奚红宇等在该领域里的部分工作。“The Computer Virus Crisis”一书的作者是从事计算机安全和法律事务方面咨询工作的，而奚红宇等则在软件方面做出了卓有成效的工作。一方面，我们使用能让没有较深技术背景的人可以明白的语言，将有用的信息寓于一书；另一方面，由于我们懂得有关的技术问题，从而能够避免出现技术方面的一些不准确性。

《计算机病毒危机》这本书将给那些正在或希望与计算机病毒打交道的人提供帮助。尽管这本书的水平相对而言是非专业类型的，但我们编辑了足够的技术细节来帮助那些具有一定技术背景的人弄明白：一些“漏洞”意味着什么？感染上病毒时，应怎样识别？如果需要清除病毒，他们该怎样做？附录还提供了一些关于病毒现象的描述和病毒产品的评价（有些软件包附带详细的技术提示和怎样使用所提供工具的用户手册。在使用一些反病毒软件之前，建议你最好对这些软件本身进行适当的检验），这也许能满足你进一步的需要。

在“Through the Looking Glass and What Alice Found There”一书中，Lewis Carroll 有句格言：“当我使用一个词时，它的含义只是我选择用来表达的意思——不多也不少”。由于在计算机安全领域中许多词汇的使用相当混乱（即使在一些专业人员中间也是如此），因此本书的最后给出了一个词汇表。其中的定义将有助于你阅读本书和其他有关书籍。当每个人都使用相同的词语来表达相同的意思时，讨论问题就会更加富有成效。

这本书并非是计算机病毒程序的最终定论。很多破坏者还在疯狂地制造病毒，许多专业人员也在为设计防护方法和产品而煞费苦心。事物的变化极其迅速，远比一本书所能反映的要快。以本书为基础，你便能从报纸和杂志中了解到更多的材料，从而跟上当前的形势。

在本书中的很多地方，我们都采用图解的方式来讲明，一个计算机病毒是怎样能干它要干的事情的。设计这些例子是一件棘手的事情：如果给出的例子是十分完备且具有实际功能，那么我们实际上是提供了一个“菜谱”，很容易被破坏者利用来制造病毒。这是我们所不希望的。因为我们并不想加速病毒的传播，所以这些例子只对说明要点而言是充分详细和完善的，而对制造病毒而言则是不够的。已经具备了这方面的背景知识的专业人员和程序员在阅读本书时，会容易地看出所遗漏的信息。我们的目的是希望帮助计算机的普通用户了解计算机病毒程序是什么，以及怎样防治病毒。只有明白正在发生的事情，使用计算机才比较安全。

希望读完本书的读者能认识到：病毒并非是神秘或虚构的东西；然而不幸的是，能够制造和传播病毒的人太多。希望这本书能使你进一步意识到这个问题。一旦意识到这一点，你暴露给病毒或暴露后被感染的机会就比较少。

“保安方法(safe hex)”这一术语已广泛被计算机专业用户理解和采用。人们选用这一术语来表述一组用以最大限度地减少你被病毒感染机会的防护措施。我们建议你实施保安方法。

最后一点，我们希望你明白：把一个病毒引入到他人的计算机系统是一种不道德、不符合职业规范和非法的行为。千万不要这样做！

在编写本书的过程中，北京大学力学系一般力学教研室老师们给予我们许多支持与帮助，北京大学出版社的郭佑民同志对本书进行了认真仔细的审阅，并提出了很多宝贵意见，于此我们表示

衷心的感谢！

由于作者水平所限，书中一定存在一些缺点和错误，诚恳地希望读者不吝赐教。

编译者

一九九一年十月于燕园

目　录

第一章 引 言

今天是那一天吗？我知道如果时间合适的话，必须做一些重要的事情。不，今天还不是 13 号星期五。现在让我们看一看：如果今天不是那一天，我不得不自我复制。让我们查看一下系统文件。我知道有一个，每台计算机都应该有一个。找到了一个！我是否已把自己复制到它上面了呢？如果还没有，我就可以把自己复制上去。不，我已经把自己复制到它上面去了，再让我们查看一下这台计算机上的程序文件。至少还有一个文件我还没有把自己复制上去。是的，有一个，且我只尝试了 48 次就找到了它。噢，它被标记为“只读”文件。没问题，我只要改变其标记就可以改变这个文件。很好，我要把自己复制到这程序中。现在复制完了，我要对程序作一点小小的修改：在这里作一个小的跳转，在那里返回。我记得改变过某些东西——噢，是的，我应该把文件改回为只读文件。注意：我的足迹掩盖好了吗？让我们看看，所有的属性跟我刚进来时是完全一样的，文件长度也没有改变，因为我是找到一些空余的空间把自己复制进去的。我还必须记得把文件的产生日期改为我刚进入时文件的原有日期。没有明显的迹象可以看出我在那里，我已经做完了吗？没有，如果有软盘驱动器，我要在其上进行同样的处理，并看是否可以进入某个网络。现在我可以结束了吗？是的——噢，那就是我在 13 号星期五那天应该做的事情！我不知道“格式化 C:”是什么意思？嘿，如果我已经复制了 50 次我就该做这件事情了，现在我已经复制 49 次了，下一次……。

你刚才已被引入一个被激活的计算机病毒着手工作时，可能

进行的思维中(如果它能够思维的话)。已经有病毒精确地按这种方式工作。有时在系统的某部分发生故障之前,你甚至不知道病毒已在你的系统中。然后你不但要修复可见的损失,而且还要找出任何病毒已自我复制进去的地方。

当然,你也可以非常安全。你只要从可信任的制造商那里买来机器,编写你自己的所有程序,永远不使用他人的程序,永远不与其他的计算机联网。只要你信任的制造商确实做到非常小心,你就不会有暴露给病毒的危险。可是这样你的计算机的用途就要受到限制,而且你不能从事以人类社会历史前所未有的方式改变我们世界的活动。

还存在其他的方法你可以用来保护你自己,其中一些甚至可以给你提供很好的保护。本书的目的就是向你介绍计算机病毒程序方面的事情,这将帮助你保护自己,防治病毒,使你加入到信息革命的洪流中。

1.1 如何使用本书

本书包括四种类型的信息:适中的技术信息;安全方面一般性的参考文献以及病毒方面的专业性参考文献;附录 A 中反病毒产品的评论和词汇表中术语的定义;计算机病毒现象的一般信息。

如果你认为你已经感染上了计算机病毒,请立即翻阅附录 A,并与某一疫苗的开发者联系,以着手解决你的问题。在你等待你的新疫苗时,请看看第八章和第九章,那里包括了很多关于你该做什么的提示。在你清除完病毒后,看看第四章和第七章,可以得到如何避免以后问题的建议。

如果你仅仅是想了解病毒,请连续地读下去。如果你已经知道了一些,请看第五章,那里有更多的技术材料。

如果你认为制造和扩散病毒也许是件很好玩的事情，请阅读第十章和第十一章，那里你将看到这样做是违法的。

然后，读一下第六章，那里叙述了一些由不道德者向他人扩散计算机病毒所造成的不良影响。千万不要这样做，否则，你损害自己的同时也损害了他人。

1.2 病毒是怎样感染你的

在过去几个月里，报界发表了很多关于计算机病毒的报道。1988 年 3 月 MacMag“和平”病毒触发[①]，在它的推动下，病毒真正开始泛滥。

不幸的是，其中某些材料是耸人听闻和失实的。例如有一篇报道说：西雅图市的每一台计算机都感染上了病毒。实际上，计算机病毒并不像平常的流感那样传播。它们并不是智能化的，它们并不会恨你，避免绝大多数的漏洞并非一件很困难的事情。

不过的确曾经有过，而且现在仍然有一些非常讨厌的病毒在计算机里为所欲为。过去几年的发展已经增加了人们暴露给病毒的机会。如果你跟其他的计算机通话，特别是当你从公共的布告板上取下程序时，你的危险就很大。如果你从不认识的人那里接受非法拷贝来的软件(或，即使你知道你的拷贝的来源，但你不知道他人拷贝的来源)，你的危险同样是很大的。

然而，如果你的程序是以压缩包装的方式购买进来的，那么你的危险就不会很大。

你需要问问自己：“难道有人如此讨厌我?”如果你是一个特殊目标，你必须小心。如果你仅仅是个一般的用户，你只要简单地应用一些常识，就很可能永远不会遇到问题。

1.3 问题是什么

大约 10 年前，我们中的一个希望在一个分时系统上，尽可能廉价地运行一个作业。作业需要一些时间来运行，且必须等待别的具有较高优先权的作业。那天是星期五下午接近傍晚的时候，我们编写了一个小文件，用来检查作业是否已经运行。如果作业已经运行，文件中的命令就及时地将作业清除掉。如果作业还未运行，就把它再次提交到作业队列中。按这种方式，作业运行肯定费用最低，并且运行作业者可以回家而不必一直等到星期五晚上。

不幸，没有对命令文件进行足够细心的测试。它不停地往作业队列中提交作业。事实上，一开始运行，命令文件就失控了。星期天，在系统启动 10 分钟后，作者接到系统管理员打来的有礼貌而又相当尖刻的电话，他希望把同一作业的 4 096 份相同的拷贝从作业队列中删除掉，以便别人能进来(图 1.1)。事情并非是故意造成的，但结果却是产生了一个准病毒，且把其放进了系统里(最后用了大约 15 分钟及几个实用程序，花了很大的力气才把所有的那些作业清除掉)。

Fred Cohen 当时还没有创造“病毒”这一术语[2]，但那命令文件却符合了他后来的描述。本书内容的要点是：尽管你今天才有机会阅读本书，但病毒并不是什么新的、不可思议的，或者是不可知的东西。

但是，既然病毒不是一个新的概念，而且制造病毒并非是一件困难的事情，甚至认为病毒是偶然出现的，那么病毒现象为什么又突然成为一个严重问题了呢？这一方面是由于计算机的兼容性和通信能力的不断增强，使病毒可以比过去更广、更快及更容易地扩散出去。另一方面是现在有大量的人，事实上有无数的人，在使用计算机(看第二章的联网问题)。

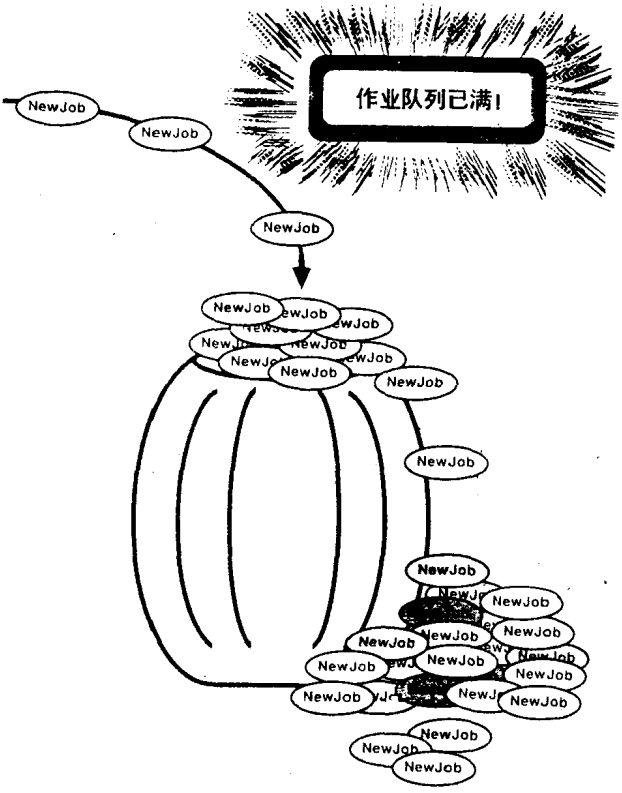

图 1.1 作业太多

New Job:新作业

现在让我们来瞧瞧那种会制造病毒的人吧!在计算机方面,他们必须具有一定的技能,特别是编程的能力。他们必须对某台计算机,特别是对你的计算机,进行某种形式的接触。他们必须有扩散病毒的某种理由。大概有成千上万的人具有制造病毒的能力,不管是有意的还是偶然的。任意一个计算机科学系的学生和大批专长于计算机的年轻人都有这种能力。

当然，专业人员也能够编制病毒程序，但他们考虑其努力所得到的回报。他们做某件事情之前总要问问："是否有更容易、更安全的办法以达到我的目的？"没有多少计算机病毒是通过专业人员扩散的，其简单的原因是：那些想毁坏或损坏程序的专业人员有比这更简易的方法可以达到其目的。

一些具有专业技能，且经过专门训练的人，希望扰乱计算机系统。恐怖分子、间谍以及正规的专业人员拥有达到这一目的所必须的技能。到目前为止，他们通过袭击供电系统及贿赂银行出纳员已取得了可观的成绩。大概当前的病毒泛滥不是专业人员为了达到某一目的而特意制造并扩散的。

还有另一类人，我们称之为破坏者。他们的动机是希望破坏工作环境，以达到看热闹的目的，或通过毁坏计算机系统来显示他们非凡的智商（他们自己是这样认为的）。他们通常不是为了寻求利益，他们并不关心其所得到的可能会比危险或所付出的代价要小。他们就是那种在博物馆毁坏油画、向别人窗户扔石头的人，且通常是人类社会中相当卑鄙的可怜虫。如果这种人拥有专业技能，他们可能会制造计算机病毒。

1.4 计算机病毒是什么

计算机病毒可以被定义为：能够自我复制的恶意的软件[3]。就我们的目的说来，这个定义有点偏见：一个病毒不必是恶意的。计算机病毒的特征是：它能够自我复制，并且还能在产生其自身之外的系统上进行自我复制，并以某种方式把自己附着在其他程序上（看词汇表和第二章）。先前提到命令文件的例子，几乎就是一个病毒：它不断复制，且不允许对系统进行存取（尽管不是有意而为，但其结果却是恶意的）。如果它被拷贝到公司所维护的其他计算机系统上，它会做同样的事情，但它不感染其他任何程序。