纽金真 王开恩 编译

计算机病毒危机

中国劳动
出版社

计算机病毒危机

P·菲特斯
〔美〕 P·约翰斯顿 著
M·克拉茨

钮金真 王开恩 编译

中国劳动出版社

计算机病毒危机

钮金真　王开恩　编译

责任编辑　凌　弘

中国劳动出版社出版发行
（北京地安门西大街教场胡同4号）
大兴包头营印刷厂印刷
新华书店北京发行所经销
787×1092毫米　32开本　7印张　160千字
1991年4月第1版　1991年4月第1次印刷
印数1—4950册

ISBN7—5045—0784—9/D·105　定价：4.00元

内 容 提 要

本书介绍了计算机病毒的种类、危害及其传染方式，阐述了计算机病毒的本质，着重介绍了预防和防止病毒传染的措施、恢复病毒所破坏的资源的方法及抗病毒软件。特别地，还涉及了一个新的领域——计算机犯罪的法律责任和道德义务，并附有词汇表和参考文献。

本书行文简明、生动、形象，既通俗易懂，只要具有初步的计算机常识，就可了解本书的大多数章节；又不乏精深的专业知识。可供计算机的一般用户、法律专业的部分师生、科研人员以及其他希望了解计算机病毒现象的一般读者参考。

译 者 序

计算机病毒正在世界各国的商业系统、政府部门、军事系统、教育系统及其他的计算机网络系统中蔓延，它吞噬着计算机用户宝贵的资源，摧毁着价格昂贵的计算机及其网络系统，不但给计算机用户带来了不可估量的损失，也给人类社会文明的发展罩上了一层阴影。

从最近的新闻媒介的宣传报道中，我们不难发现，计算机病毒对我国计算机行业的危害愈演愈烈，因此介绍有关的知识是十分必要的。本书可以说是普及这方面知识的最佳读本。

本书介绍了计算机病毒作用于IBMDOS和Macintosh系统的各种症状、种类、危害及其传染方式，阐述了计算机病毒的本质。怎样预防和阻止病毒的扩散则是本书的重点。若用户的计算机已染上病毒，本书则指导用户怎样清除病毒，怎样恢复病毒所造成的破坏。本书还涉及了一个新的领域——计算机犯罪的法律责任和道德义务。同时本书在附录中还介绍了对付病毒的各种软件及联系地址，并附有一个给每个术语以精确定义的词汇表和进一步自修用的参考文献。

本书写得生动、形象，既通俗易懂，又不乏精深的专业知识，是广大计算机用户防止病毒、检测病毒、同病毒进行战斗的有效武器。

本书在编译过程中得到了梁业伟教授、李志琴编审、干

海莲同志、钮春同志的热情支持和帮助，在此一并表示感谢。由于时间仓促，加上我们的水平有限，错误在所难免。我们恳切期望广大读者批评指正。

译者　　1990年8月24日

目　录

第一章 导 论

今天是那一天吗？我知道如果今天是那一天的话，我有些重要的事要做。不，今天还不是13号星期五。现在让我们来看一看：如果今天不是13号星期五，我就得复制自己，我们来考察一下系统文件；我知道会有一个系统文件，每一台计算机都有一个系统文件。这个就是：我已经在里面了吗？如果没有，我就会拷贝自己。不，我已经在那个程序中了；我们来检查一下这台计算机的程序文件。显然，至少有一个文件我还没有到里面去。对，就是这一个，我仅做了48次运行之后就找到了它。噢，它具有只读标志；太棒了，我只要修改这一标志就能改变这个文件，真是舒服极了；我不停地把自己拷贝到那一程序中；拷贝之后，我只对这程序做了一点修改，在这一段做了一小点转移操作，到那段则进行返回运行，我记得我好象改变了什么——噢，对了，得把文件变回到只读。现在，我已覆盖了磁道了吗？让我们来瞧一瞧，所有的属性和我来的时候一样；因为我找到一些空白空间把自己拷贝进去，所以文件长度没有发生变化。我还得记住把文件建立日期变回到我来时的日期。要找到我在哪儿决非轻而易举之事。我的事干完了吗？没有；若有

软盘存在的话，我需要在软盘进行同样的过程；并且我还需要看一下是否能作用于网络。现在我已经完成了吗？完了——噢，那就是13号星期五我将要做的事情！我想知道FORMAT C：是什么意思？嘿，如果我拷贝自己五十次之后，那就是我所要做的，现在我已经复制了四十九次了。下一次……

我们已经向你介绍了计算机病毒从事其工作时所想的一切(若它能思维的话)。有许多病毒的确是按这种方式工作。直到你的系统出现毛病你才知道病毒已在其中。于是你不仅得整修有形的损坏，而且得找出病毒复制件的藏身之处。

当然，你也可以非常安全，你可从可信赖的制造商那里购买计算机，自己编写所有的程序，从不使用别人的程序，并且从不与其他计算机进行通信。只要你所信赖的制造商真的十分小心，你就不会有遭到病毒传染的危险。只要你拥有一台十分有用的计算机，你就可以以人类历史上从未可能有过的方式从事于改变世界的工作。

还有别的方式你可以保护你自己；有些甚至能提供很好的保护。本书的目的是向你介绍计算机病毒程序的本来面目，并帮助你在信息革命中成功地保护自己、防止病毒。

如何使用本书

本书包含四方面的信息：适度的技术信息；关于安全性的一般记述文献，尤其是病毒方面的其它参考文献；附录中抗病毒产品的评价和词汇表中词汇的定义；关于整个计算机

病毒现象的一般信息。

若你觉得你的计算机已染上了病毒，请马上求助于附录，并同疫苗开发者之一进行联系，解决你的问题。在你等待新的疫苗的同时，可参看第九章和第十章：这两章将提示你该做些什么。当清除一切病毒之后，可参看第五章和第八章，从中能得到一些怎样避免再度感染的建议。

若你只是想了解病毒，接着读下去。若你已经有了一定基础，可参看第六章，此章含有大部分技术性的内容。

若你觉得编制病毒和传播病毒非常有趣的话，阅读第十一章和第十二章，你将了解到这是违法行为。然后阅读第七章，本章描述了传播病毒的道德败坏者对其他人所造成的极坏的影响。别这样干！你不仅使你自己的事情变得更坏，而且也使我们其他人的事情变得更糟。

病毒怎样影响你

在过去的几个月中，出版界大量出版了关于计算机病毒的报道。这一突然爆发或许是由MacMag“和平”病毒于1988年3月的激发所推动①。不幸的是，有些材料则是耸人听闻或者被歪曲窜改，例如有一篇报道说西亚图的每一台计算机都有病毒。实际上，计算机病毒决不象普通的感冒那样传染。它们并没有智力；它们不嫉恨你；甚至避免大部分病毒的传染并非难事。

但是过去有，现在还有一些非常讨厌的病毒在计算机周围游荡。过去几年的一些进展增加了传染的机会。如果你同

注①：参见［和平病毒 1988］，［O'conner 1988］1988年2月左右第一次报道这种病毒，它被称为MacMag病毒或和平病毒。我们本着负起应负的责任的态度，使用了恶作剧者的名字。

其他计算机进行通信交流，尤其是如果你从公共公告牌（BBS）上装载程序，你就处于危险的境地。如果你从你不认识的人那里接收非法复制的软件（或者即使你确实知道你的复制件的来源，但却不知道他人的复制件的来源），你就处于非常危险的境地。

另一方面，如果你拥有热紧缩封套包装的买来的程序，或者是电子邮件配置，你就没有太大的危险。

你得问问自己，“任何人都那么讨厌我吗？”如果你成了特殊的目标，你就得留神注意。如果你仅是一个一般的用户，如果你只是应用一些常识，你或许永远也不会出问题。

到底是什么问题？

十年以前，我们中间的一个人需要在一个分时系统上尽可能便宜地运行一个作业。这个作业需要等一会儿才运行并且等待其他具有更高优先权、更昂贵的作业。那是在一个星期五的傍晚。为了检验看这一作业是否已经运行，他建立了一个很小的文件：如果作业已经运行，文件中的命令就适当地直接输出，并做清除处理；如果作业还没有运行，就把作业再提交到作业队列中。以这种方式，作业肯定以最低的速度运行，作者可以回家而不需在星期五晚上久等。

不幸的是命令文件并没有被十分仔细地检测。它缠绕着，重复地提交自己。事实上，一旦作业真的运行，命令文件就失去控制。星期天，在系统起动之后十分钟，作者就从系统管理员那里收到了一个有礼貌的并且十分直接了当的命令，要求他从作业队列中删除掉4096份同一作业的复制件，

以便其他人能够进入系统（图1.1）。这个局面的形成并非有意，但是其效果是制造了准病毒，并把它送进了系统。（十分令人窘迫地，花了大约十五分钟和用了几个除掉所有这些作业的实用程序才使得整个局面发生了改变）。

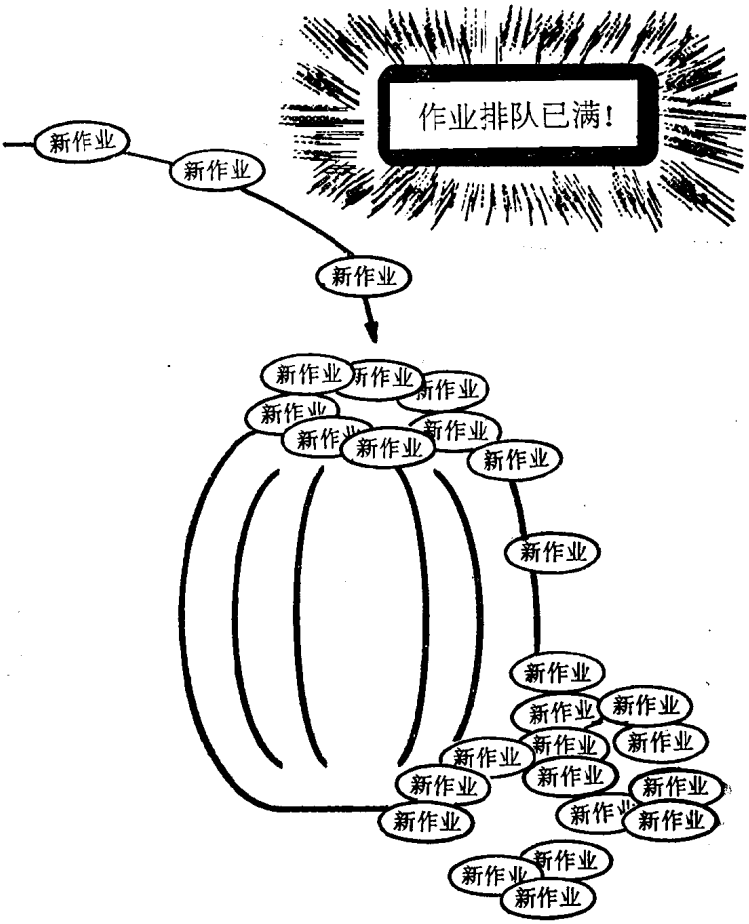

图1.1　太多的作业

弗雷德·科恩并没有制造“病毒”这个词②，但是这个命令文件却适合于其后来的描述。这个故事表明病毒不是新的、有魔力的东西或者是其他未知的东西，不管你现今对病毒怎样理解。

但是如果病毒的概念并不是真正的新东西，并且制造病毒并不十分困难，甚至偶然地就能制造病毒，为什么突然地就变成了一个问题了呢？部分原因是因为计算机兼容性的提高，交流通信的增多使得病毒有可能比过去传染得更远、更快、更容易。另一部分原因是因为现在有更多的人，事实上有数百万人在使用计算机。

让我们来看一下能制造病毒的这类人。他们得懂得计算机的一些技术，尤其是编程的技术。他们得了解通向计算机，特别是通向你的计算机的途径。他们得有传播病毒的理由。非常有可能，数百万人都拥有有意或无意地制造病毒的技术。任何计算机科学的学生和一大批在计算机方面有造就的年轻人都有这种技术。

当然，专业人员能编制病毒程序。但是他们要考虑其努力所得到的回报。在行事之前，他们问道：“达到我的目的有更为容易、更为安全的方式吗？”专业人员较少传播病毒，其简单原因是因为想毁坏或破坏程序或计算机的专业人员有更为容易的方式来达到其目的。

有许多拥有专业技术和训练有素的人想搅乱计算机系统。恐怖分子、间谍和合法的专业人员都具有这种所需的技术。如今，他们通过采用攻击电源供给及贿赂银行出纳员之

注②：〔Cohen 1984〕（参见第二章的“联络性”问题）

类的手段，已取得了更好的结果。当今大量涌现的病毒或许并不是由专业人员为达到某种目的而制造和传播的。

还有另一种类型的人，我们称他们为蓄意破坏者。他们的动机是破坏工艺品，并观看火星四溅或者通过损坏计算机系统来显示他们高超的才能（如他们自己断定的那样）。他们不总是以获利为目的，或许冒险的代价和花费比得到的回报要大，但他们并不在乎。他们是在博物馆中对绘画刻痕、朝窗户掷石头的那一种人，一般地说，他们非常讨厌，他们是令人可怜的一类人的典范。如果这一类人拥有技术性的技能，他们就会制造病毒。

什么是计算机病毒？

计算机病毒可以定义为能够自我复制的恶意的软件③，这一定义因为我们的某些目的而带有一点偏见：病毒不一定是恶意的。计算机病毒的关键是其自我复制，它只能在计算机系统中自我复制，它能以某种方式附加在其他程序上（参见词汇表和第二章）。上述提到的命令文件的例子就近乎是一种病毒，它能进行自我复制并阻塞对系统的访问（尽管这种方式并不是所期望的但却是恶意的），如果它已被复制了的话，它同样能对这家公司所支持的其他计算机系统产生作用。但是，它并不感染其他任何程序。

病毒只是一类程序的名称，它们能进行复制并传染其他程序。此外，它们还能做其他程序所能做的一切（参见第四

注③：参见〔Podell 1987〕具有同样的定义.