ZHI ZHE WU WEI ZHI ZHE WU WEI ZHI ZHE WU WEI ZHI ZHE WU WEI

知者无畏

一个真实的病毒世界

朱传靖 著

金城出版社

知者无畏

一个真实的病毒世界

朱传靖著

金城出版社

图书在版编目(CIP)数据

知者无畏：一个真实的病毒世界 / 朱传靖著. - 北京：金城出版社，2002.1
ISBN 7-80084-364-5

Ⅰ.知... Ⅱ.朱... Ⅲ.计算机病毒 - 基本知识
Ⅳ.TP309.5

中国版本图书馆CIP数据核字(2001)第079593号

金城出版社出版发行
（北京朝阳区和平街11区37号楼 100013）
北京鑫洪源印刷厂印刷
850×1168毫米 1/32 8.75印张 180千字
2002年1月第1版 2002年1月第1次印刷
印数：1-5000册
ISBN 7-80084-364-5/TP·14
定价：29.80元

序

2001年9月11日，纽约世界贸易中心的两栋摩天大楼在巨大的爆炸声中轰然倒地。这是恐怖分子在现实世界制造的血腥惨案。引起世人的极大震惊。无独有偶，2001年9月18日，“数字空间的恐怖分子”继“红色代码”和“蓝色代码”之后，又以“尼姆达”病毒为武器，向网络世界频频发难，短短三天时间，就在全球至少造成了5亿美元的损失！

这是在现实世界和虚拟世界同时发生的两场恐怖事件和灾难，后者虽不流血，但其突发性和破坏力同样触目惊心和防不胜防。它再一次向人们昭示：在信息技术迅猛发展的时代，在电脑病毒愈演愈烈的今天，人们不能不拿起知识的武器向挑战文明的邪恶作战。而对于普通用户，电脑病毒始终还是一个神秘的存在，电视和报纸天天都有关于病毒的新闻，但是很少有人能够真正了解电脑病毒是什么，杀毒软件能做什么？不能做什么？

正如书名所说：“知者无畏”，这是对“无知者无畏”的嘲讽，对“愚者善畏”的认同。人心中最大的恐惧就是对未知的恐惧，恐怖片之所以恐怖，是因为你不知道下面将要发生什么。作者要做的，就是消除读者因为对病毒的无知所造成的恐惧，用翔实的资料和深入浅出的叙述告诉读者一个真实的病毒世界。

本书的作者很年轻，但是在反病毒战线已经历了十年的风风雨雨，是国内老牌杀毒软件VRV、VRV2000和最新的安全之星1+e、安全之星XP的主要研发人员和项目负责人。如今，把丰富的资料和深刻的见解融为一体，汇成专著。作为关于电脑病毒的专业技术著作，一般容易给人枯燥和深涩的感觉，但是这本书恰恰在这一点上做了可喜的突破，在坚持严肃性和权威

性的同时，语言生动、内容有趣，披露了很多真实的病毒故事，包括病毒制造者、病毒收集者鲜为人知的一面，一些杀毒软件技术的演化故事等等，内容易懂又不失严谨，做到了知识性和趣味性的统一。

作者还第一次为我们描述了一张完整的病毒编年史，从最早电脑病毒的萌芽和诞生，到最新的尼姆达病毒，对国际和国内重大的病毒事件进行了详细和深入的叙述，对于国内外著名的反病毒软件公司的成立、发展和演化都进行了详细的描述，在书中，你可以看到江民、瑞星、信源和创源以及金山的风雨历程。

中华民族的发展，需要经济的发展，更需要综合国力的增强，提高国民的整体素质是增强国力的一个重要内容，在七八十年代，很多老一辈的科学家写了很多科普的作品，引导了一代又一代的青少年走向了科技强国之路。在二十一世纪的今天，作者作为一个商品经济下的公司主要负责人之一，能够主动以普及病毒知识为己任，从整个行业乃至整个国家的信息安全高度来考虑，将自己多年的实践经验无私奉献给社会，为提高国民的反病毒意识和捍卫国家信息安全能力献技献策，非常难能可贵。

我想，作者已经很好地实现了他在书中所提出的目标，这是一本：

“在你遇到困难时候必备的参考书
可以经受时间考验的关于病毒的权威论述
在闲暇时阅读的数字空间的传奇故事。”

除此之外，本书还带给我们一些更深的思考：电脑病毒已经和国家的信息安全、甚至国家的军事力量息息相关，事实上，电脑病毒已经成为现代战争的进攻性武器，美新任国防部

长拉姆斯菲尔德执意坚持打造数码部队，加强信息战。军事专家相信，21世纪的战争将以信息战为最大特色。电脑病毒作为攻击性信息武器有其无可替代的优点：廉价、高效、杀伤力极强。虽然不使对方流血，但却让你失能，达到不战而屈人之兵的目的。

不论对普通公民，还是对于肩负国防重任的现代战士，信息时代最大的力量是知识的力量，最好的武装是知识的武装，我赞赏本书的书名："知者无畏"，也期望此书能够有飨读者。

2001.10.20

戴浩民

目录

第三章

第四章

第五章

第六章

第七章

第八章

第九章

第十章

前言

知识就是力量

“知识就是力量”，当我拿起笔准备写这本书的时候，立刻就想起了这句话。很久以前，我还很小的时候，有一本最喜欢的杂志就叫这个名字，好长时间没有机会看到这本杂志了，也不知道现在这份杂志是不是还存在。只是记得在当时，这份杂志告诉我一个全新的世界，从飞往外太空的迭达罗斯飞船到如何从海洋中找到稀有金属，书中所描述的世界对一个充满了好奇心的孩子是如此的奇妙，它告诉我好多好多以前根本没有梦想过的事情。从杂志和书本中得到的这些远远超过同龄小伙伴的知识以及随之而来的对更多知识的渴望，也是支持我直到今天还能在这个狂飙一样的行业继续生存的力量之所在。

顺便说一句，记得我小时候看的书是《知识就是力量》、《少年科学画报》、《少年科学》等等，现在的小孩子好像不看这些东西了，他们整天面对的都是电视里的日本动画片，还有相关的连环画，我不知道那种打来打去的东西对小孩子能起什么作用。也许是杞人忧天吧，在这种没有任何内涵的快餐文化熏陶下长大的一代，今后还能有对知识的渴望吗？当他们长大以后，严酷的竞争再来告诉他们知识就是力量的时候，他们又能以什么样的心态和行动去面对呢？

谈起电脑病毒，广大的读者恐怕都有谈虎色变的感觉，不知道这东西到底躲在什么地方，也不知道它们会对自己做些什么。不知道有谁说过这样一句话“无知者无畏”，我觉得真实

情况恰恰相反，真正无畏的人只能是拥有了足够知识的人。人心中最大的恐惧就是对未知的恐惧，恐怖片之所以恐怖，是因为你不知道下面将要发生什么；电脑病毒之所以恐怖，也正是因为你不知道它们是什么，它们能做什么。而在电脑病毒这样一个迫切需要知识的领域，真正专业性的书籍很少，而仅有的一些书，不是从哗众取宠的目的出发，拼凑一些骇人听闻的病毒和黑客的故事，就是非常简单和粗浅，对80年代的病毒进行教科书般的描述，缺少具有专业性和权威性的著作，对于一些新的病毒和反病毒技术，像VBScript病毒、因特网蠕虫等，更是缺少足够的论述。

在病毒和反病毒行业中，掌握了最多病毒和反病毒知识无疑不是学校的老师，而是整天和病毒打交道的厂商，这些从杀毒软件上获取了大量利润的厂商出于种种目的（广大电脑用户的无知也许就是他们最大的机会和利润所在吧），将一些很简单的问题，很简单的答案隐藏在广告和宣传的迷雾中，有意无意的夸大病毒的危害，误导用户对所面临的问题作出不正确的判断，把不是病毒的现象当成病毒，把杀毒软件无法解决的问题归结为系统本身的缺陷。

我相信，如果本书的读者掌握了足够的知识，就能够不再为媒体的宣传所左右，不会有那种被夸大的或者被误导的恐惧存在。因此，写这样一本书的初衷，就是用通俗易懂的语言，把复杂的问题简单化，告诉读者一些似是而非的概念的真实含义，让读者能够客观的了解到我们所面临的威胁真的有多大，一旦这些危险降临的时候，如何能够理智的面对，如何尽可能的把损失减小到最低程度。从而消除那种被夸大的恐惧，真正切实的保护自己的电脑和数据的安全。

在中国，对下一代的重视远远超过世界上任何其他国家，大量经济并不非常宽裕的家庭为了孩子，把很大一笔积蓄都投

资到一台电脑上面。由于没有全部购买正版软件，不可避免的会经常遇到一些怀疑是病毒造成的现象；由于缺乏足够的知识，只能去询问朋友或者病急乱投医，根据广告和媒体宣传在自己心目中形成的第一印象购买一些杀毒软件。杀毒软件厂商也利用媒体所造成的对计算机病毒的恐惧，制造一些病毒事件、夸大甚至制造一种恐慌情绪，从而成功的达到最终目的，让用户花钱购买杀毒软件，以及不断的对杀毒软件进行版本升级，从中获取高额的利润。

我希望读者阅读本书之后，能够掌握一些病毒和反病毒的知识，拥有足够的判断力对自己的电脑所面临的问题、现象进行诊断、知道自己所面对的是硬件故障，病毒还是其他什么原因所造成的现象，从而作出恰当的决定，保护自己的电脑和电脑上更加重要的数据。

知识就是力量，谨把这句话送给本书的所有读者。

关于本书

为什么要写这本书?

最近一段时间，在各种报纸或者杂志甚至电视上，你经常可以看到类似下面的一些消息:

【路透社北京消息】本周二，中国公安部向全国发布紧急通知,警告红码II蠕虫病毒已侵入中国。本周四一位网络安全专家称,红码II蠕虫病毒正在大肆侵袭中国的计算机系统,但最终遭受破坏的机器数目却远远低于其他国家。另据国家计算机病毒应急处理中心统计，病毒侵袭的速度虽快，但截止到本周三晚的上报案例数还不到100。

红码II蠕虫病毒已重创了美国、欧洲和亚洲其他各国的计算机系统，其袭击对象仍是视窗 2000、视窗NT操作系统，及其网络信息服务器软件。七月份逞凶的第一代红码病毒感染了30万台计算机，它会在用户网页上显示“已被中国人入侵”(Hacked by Chinese) 红码II病毒虽然不再发出这种信息，但是它更可恶，它使被感染的计算机“后门”大开，方便了众多黑客们的自由出入。重启被感染的计算机即可摆脱第一代病毒，但是红码II病毒可以自行重启感染过的服务器并通过该服务器的IP地址历史记录进行快速传播。

另外值得注意的是，有些人虽然遭到病毒侵袭却不愿公开，因而病毒袭击我国计算机的真实数目可能远高于上述统计。

这则消息让我想起了三年以前，1998年和1999年CIH病毒在世界范围有两次大爆发，中央电视台在新闻联播中作了大量相关的报道，在新闻联播这样的媒体中反复出现对计算机病毒的报道，充分说明了计算机病毒已经成为一个社会现象，而一次计算机病毒感染可以演变成一次重大的新闻事件，也说明了计算机病毒所造成的影响和公众对计算机病毒的恐惧和关注。

CIH之后，是“梅丽莎”、“爱虫”、“女鬼”、“Fun Love”等等病毒，几乎每个月都会有新的病毒在各种媒体上招摇过市，粉墨登场。也许是用户更加理智的缘故吧，这些病毒虽然各具特色，也造成了一些宣传的热点，但一直没有掀起象CIH一样的波澜。

而短短几个月前，一个名叫“红色代码”的病毒成为所有媒体的关注焦点，报纸、电视不遗余力的宣传这种所谓“新世纪的新概念病毒”。而实际上，这种病毒只是针对视窗NT或者视窗2000上的因特网信息服务器(Internet Information Server，微软开发的一种主要用于服务器的软件，可以让你的机器成为一个因特网的站点)、普通家用计算机用户，基本上没有任何机会接触到这种“可怕的”病毒。但是在媒体一片“狼来了”的声音中，你，作为普普通通的个人电脑用户，基本上不可能具有足够的专业知识对这个病毒进行自己的分析，那么，你怎么能够知道事情的真相？又有谁来告诉你，该如何去做呢？

当然，在电脑病毒面前还有另外一种态度，“我不看报纸，不管宣传，这些和我有什么关系呢”，也许你会这么说。是的，你可以不理会这些宣传。你也许只是一个普通用户而已，每天和电脑打交道就是简单的上上网，打打字，也许你是一个计算机的发烧友，拆拆机器，装装软件，不去关心“红色代码”或者“蓝色代码”什么的。

但是，如果硬盘灯突然莫名其妙的疯狂闪烁，鼠标在屏幕上突然停顿，电脑经常莫名其妙的重新启动，你的第一个反应是什么，病毒？黑客？不要告诉我你不会遇到这种情况，在近十年和病毒打交道的历史中，有太多用户因为没有足够的警惕蒙受了惨重的损失，一些证券厂商因为病毒的破坏，损失了价值连城的交易数据，还有作家的书稿、程序员的程序等等，面对这样一个确确实实存在的威胁，采取鸵鸟政策也是于事无补的。

从事这一行业近十年的时间，我目睹了无数用户的热情、希望和失望，也经历了一次又一次的病毒流行所造成的恐惧，作为一个长期以来以电脑病毒为生的行业人士，感觉到有必要向大家讲述一些真实的病毒故事，在病毒和反病毒的世界里，已经充满了太多似是而非的概念，虚假的承诺，读者需要的是真实的材料、客观的描述和对病毒的全面、权威的分析。这也是我在写作这本书的过程中，一直提醒自己努力去做到的：尽可能抛开一个厂商的局限性，完全从病毒和反病毒的历史和技术出发，给读者提供一个可信的病毒知识来源。

电脑病毒真的存在吗？

电脑病毒已经成为一种社会现象，你可以不知道DOS，可以不知道视窗操作系统，但是你不可能不知道电脑病毒。电脑病毒本身和围绕电脑病毒的种种宣传、舆论，已经极大地影响了我们的生活。电脑机病毒像一种传染力极大的瘟疫一样，幽灵般在各种各样的电脑中出没。然而，电脑病毒作为一种特殊的软件，想要确实触摸到它的存在，对于普通用户是比较困难的。如何判断一个文件是不是被病毒感染？最简单的办法当然是比较没有被感染的文件和怀疑被感染的文件，但是有谁会在电脑中保存一份没有被感染的文件，谁又能保证这个文件本身没有被感染呢？