

少年科学大讲堂

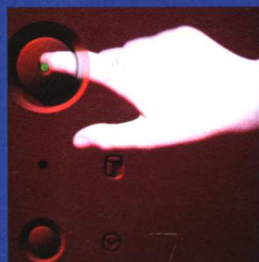


WANGLUO CHUANRANBING

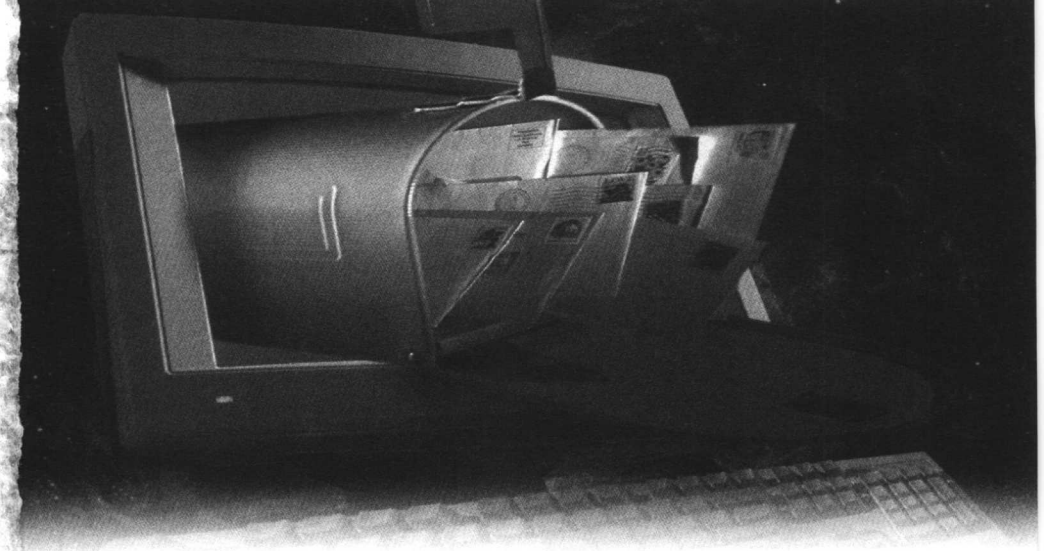
网络传染病



□ 郭静雯 编著



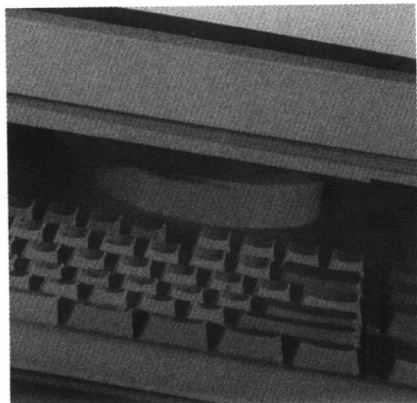
少年儿童出版社



网络传染病

郭静雯 编著

少年儿童出版社



一任天真

我们倡导天性、率真的阅读与成长

ISBN 978-7-5324-7296-3 / N·804

图书在版编目(C I P)数据

网络流行病/郭静雯编著. —上海: 少年儿童出版社,
2007.8

(少年科学大讲堂)

ISBN 978-7-5324-7296-3

I .网... II .郭... III .计算机病毒—少年读物 IV .TP309.5-
49

中国版本图书馆CIP数据核字 (2007) 第106830号



网络流行病

郭静雯 编著

费 嘉 装帧

责任编辑 岑建强 美术编辑 费 嘉

责任校对 沈丽蓉 责任监印 万友明

出版发行: 上海世纪出版股份有限公司 少年儿童出版社

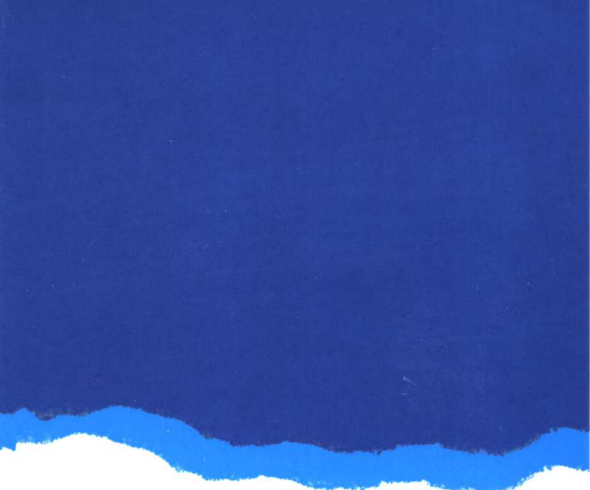
地址: 上海延安西路 1538 号 邮编: 200052

易文网: www.ewen.cc 少儿网: www.jcph.com

电子邮件: postmaster@jcph.com

版权所有 侵权必究

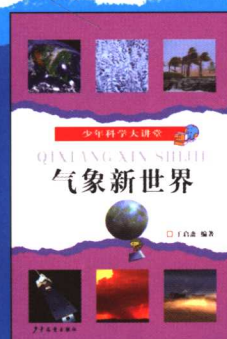
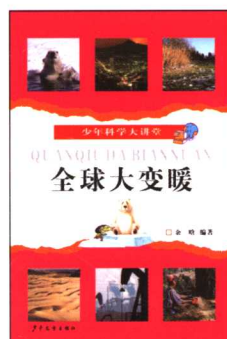
如发生质量问题, 读者可向工厂调换



作者简介

郭静雯，写手，喜欢安静文字、音乐和电影，擅长烹调、淘碟和品鉴美食。作为一个文学青年，认为写字和筛沙一样是体力活，想像力比形容词重要，现代一定比古代好。





编者的话

在一个落后时代的人看来,现代科学和魔法是没什么区别的。实际上,现代科学的发展早已远远超越了哈利·波特的想像。在魔法和神话里,从来没有出现过2000万吨级的聚变核弹,无论是宙斯的闪电还是孙悟空的金箍棒,在能量上和核弹根本不是一个级别;另外,神话和魔法的空间也显得过于狭窄,当魔幻故事还在月球轨道内进行的时候,人类的探测器快要飞出太阳系了。

科学的发展常常会超出人类的想像。19世纪时,有科学家通过流体力学原理得出结论:火车速度不可能超过每小时150千米,否则车内的空气就会被抽空;20世纪初,大多数物理学家都认为人类对于物质规律的认识已经完成,没有什么更多的事情要做了;20世纪60年代的大师冯·诺依曼说,全世界有一台巨型计算机就足够了,因为我们根本没那么多东西要算……

亲爱的小读者,这就是科学的美丽:充满力量,又在迅速变化;好像离你很远,却又在你身边。为了帮助你了解科学发展的

最新动态,我们编辑了《少年科学大讲堂》这套书。从作者到编辑,都努力用最浅显的语言,尽量让科学变得易读易懂。但是,这毕竟不是一套校园小说,你需要一点点耐心,才能享受到阅读和思考带来的乐趣。在阅读完成以后,你可以试着回答这样一个问题:科学能给我们带来什么呢?更强大的动力,更方便的沟通,更接近神话的世界,还是更惨重的灾难,更恐怖的损失?

这个问题没有标准答案,你可以在漫长的时间里,验证自己的回答。

目 录

前言	001
一、认识病毒	005
铁家伙也中毒? 什么是计算机病毒	007
计算机病毒的起源	013
计算机病毒怎样搞破坏	018
二、病毒档案大公开	027
计算机是怎么一回事	029
无孔不入:操作系统漏洞	037
暗藏的特务:木马病毒	042
网络上的暗礁:网页病毒	051
不要和陌生人说话:即时消息病毒	059
网络瘟疫:蠕虫病毒	064
强买强卖:流氓软件	071

三、绝地攻防:反病毒的战争	077
程序、计算机语言和机器语言	079
病毒的指纹:病毒码	086
弥天大网:扫描引擎	090
远程攻防:网络防火墙	094
虚拟演员:蜜罐技术	102
后记	111



前言

1999年4月26日,对于大部分计算机用户来说,是一个非常恐怖的日子。这一天,全世界有超过6000万台电脑用户刚刚开机,只看到屏幕一闪,随后整个系统就瘫痪了。许多电脑主板损坏,硬盘不能正常工作,里面保存的文件、材料和数据全部消失得一千二净。这次电脑灾难给人们日常生活带来了很大影响:政府不能正常办公,银行搞不清楚账户里的钱,机场只能手工检票,报社连报纸都印不出来。在俄罗斯,有120家大公司只能放假两天,修理电脑;在马来西亚,12家股票交易所电脑崩溃,经理人买不进,抛不出,着急得几乎发狂。据统计,这个叫做CIH的小小病毒,带来的经济损失超过10亿美元,比一场发生在中等城市的6级大地震还要严重得多。

CIH病毒并不是第一例大规模爆发的计算机病毒,但是,它拥有的高度破坏性却是从前的所有病毒都不能比拟的。从那以后,计算机安全问题成为计算机领域最受关注的问题之一。工程师们开始思索,怎么样让文件和数据不被窃取,怎么样修补操作系统的漏洞,怎么样让网络变得清洁通畅。当时,许多工程师认为,电脑科技的发展能最终解决计算机病毒问题,因为更强大的处理器和更先进的搜索技术,加上定期更新的病毒数据库,将让病毒无所遁形。

随着电脑技术和网络技术的飞速发展,只不过7

年以后,我们不但拥有了10倍以上的CPU时钟频率,20倍以上的内存和硬盘容量以及50倍以上的上网速度,同时也拥有了成千上万种形形色色的病毒。病毒非但没有被消灭,反而实力更强大,种类更庞杂。从最红火的病毒“熊猫烧香”,到千奇百怪的网页病毒、后门木马,病毒的功能和传播方式都有了飞跃式的发展,和“熊猫烧香”相比,CIH病毒简直又呆又笨,好像病毒里的弱智一样。

为了绞杀病毒,软件厂商们投入巨额经费,动用最精锐的研究人员,使用最尖端的电脑科技。但是,无论如何努力,计算机病毒仍然根本没办法消灭。每天,光是旧病毒产生的新变种都让技术人员疲于奔命,更别说新制造出来的、威力更加强大的病毒了。经过将近10年的斗争,最大的反病毒软件厂商诺顿表示,在可以预见的将来,有计算机的地方都将有病毒。每一个电脑用户,都要习惯和那些已知或者未知的计算机病毒打交道。杀毒,恢复数据,保护资料安全,将成为烧饭,洗衣服,或者交通规则一样的最基本的生活常识。这也是本书要告诉你的内容:什么是病毒,病毒怎样搞破坏,如何在病毒的重重包围下上网,中毒以后怎么样让一切恢复正常。

一、认识病毒

和生物界的病毒一样，电脑病毒传播迅速又很难察觉，危害巨大又难以清除。任何电脑病毒都是一段程序，它在被创造者出于各种目的写出来以前，根本就不存在。从最早的“磁芯大战”到“震荡波”，电脑病毒从在实验室里诞生到席卷全球，只用了不到 50 年时间。

铁家伙也生病？什么是计算机病毒

病毒是什么呢？病毒是最小最小的生命体，小到连细胞结构都没有。大多数病毒体中只包含一种核酸（就是我们所说的DNA或者RNA）和一点蛋白质。病毒是这么的小，以至于它只能寄生在别的生物体内才能存活。于是，根据寄生的地方不同，我们把病毒分成动物病毒、植物病毒、细菌病毒等等。也许你要问，病毒是那么的渺小，那么的微弱，它能做什么呢？答案会让你大吃一惊：它能改变历史！

还记得2004年的“非典”夏天吗？街上的行人都戴着口罩，一个人感染，一个居民小区就被封闭，所有的公共场所都冷冷清清，人们连上街都觉得害怕。还有大家熟悉的“疯牛病”，它由一种叫朊病毒的奇怪病毒引起，能通过食品途径从牛传染给人。为了控制疫情，光是在1996年，英国就屠杀了1100万头牛，造成的经济损失超过300亿美元。

再朝前看，从1918年到1919年两年时间里，新型流感病毒传遍世界，一半以上的人口受到袭击，因此而死亡的人口数量甚至多于第一次世界大战。古罗马、印加帝国、玛雅文明，这些曾经辉煌一时的文明最后消失，也都和小小的病毒有分不开的关系。即使

到了现在,地球上每天因为病毒感染而打喷嚏、流鼻涕、发高烧的人也难计其数。从人类社会变迁、民族兴衰、战争胜败到人口迁徙,病毒并不是历史的推动力,但它确实实实在在地改变着历史。

现在,你知道病毒的可怕了吧?它渺小却力量强大,微弱却传播迅速,一旦蔓延开来,后果不堪设想。虽然和中世纪相比,人类在医学和科学上取得了空前的进展,但是,细说起来,人类到现在为止彻底消灭的病毒只有一种——天花。而伴随着更多变种病毒、新型病毒出现的,还有另一种中世纪人完全想像不到的新病毒:电脑病毒。

电脑病毒和生物病毒有着完全一样的特征:传播迅速又很难察觉,危害巨大又难以清除。和生物病毒不一样的是,电脑病毒是人类自己制造出来的,从本质上说,任何电脑病毒都是一段程序,它在被创造者出于各种目的写出来以前,根本就不存在。1994年,我们国家正式颁布了《计算机信息系统安全保护条例》,一群大专家坐下来讨论了好几个月,给计算机病毒下了这样的定义:计算机病毒,是指编制或者在计算机程序中插入的破坏计算机功能或者毁坏数据,影响计算机使用,并能自我复制的一组计算机指令或者程序代码。

电脑病毒可以隐藏在看起来是正常的程序里: