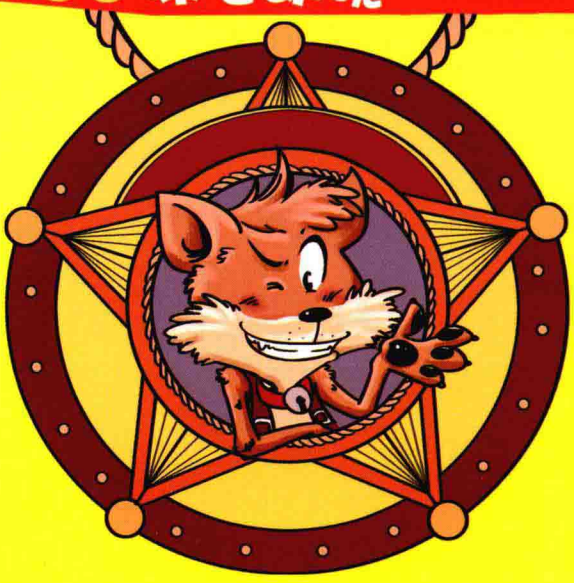
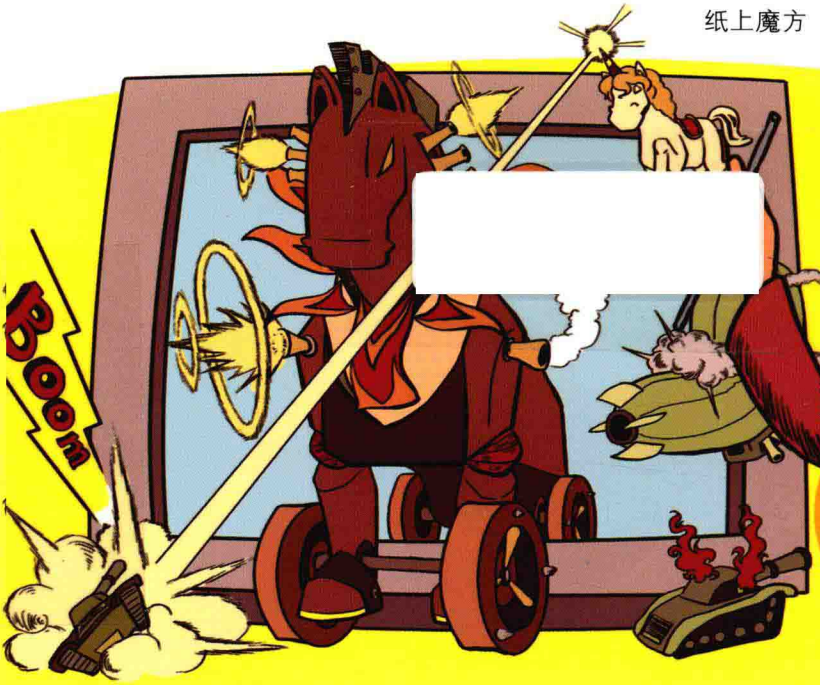
科学如此惊心动魄 · IT小精英



追踪网络病毒

纸上魔方 著



中国科学院院士 北京大学化学教授 黄春辉

北京大学数学教授 百家讲坛讲师 张顺燕

倾情力荐

吉林出版集团有限责任公司 | 全国百佳图书出版单位

科学如此惊心动魄·IT小精英

追踪网络病毒

纸上魔方 著

吉林出版集团有限责任公司 | 全国百佳图书出版单位

图书在版编目（CIP）数据

追踪网络病毒 / 纸上魔方著. — 长春：吉林出版集团有限责任公司，2015.6
（科学如此惊心动魄 · IT小精英）
ISBN 978-7-5534-7749-7

Ⅰ. ①追… Ⅱ. ①纸… Ⅲ. ①计算机网络—计算机病毒—少儿读物 Ⅳ. ①TP393.08-49

中国版本图书馆CIP数据核字(2015)第128299号

科学如此惊心动魄 · IT小精英
追踪网络病毒 ZHUIZONG WANGLUO BINGDU

出版策划：孙　昶
项目统筹：孔庆梅
项目策划：于姝姝
责任编辑：王　妍　姜婷婷
制　　作：纸上魔方（电话：13521294990）
出　　版：吉林出版集团有限责任公司（www. jlpg. cn/yiwen）
（长春市人民大街4646号，邮政编码：130021）
发　　行：吉林出版集团译文图书经营有限公司
（http: //shop34896900. taobao. com）
电　　话：总编办 0431-85656961　　营销部 0431-85671728
印　　刷：长春人民印业有限公司（电话：0431-84654188）
开　　本：720mm × 1000mm　1/16
印　　张：8
字　　数：80千字
印　　数：1-6 000册
版　　次：2015年8月第1版
印　　次：2015年8月第1次印刷
书　　号：ISBN 978-7-5534-7749-7
定　　价：23. 80元

前 言

四有：有妙赏，有哲思，有洞见，有超越。

妙赏：就是“赏妙”。妙就是事物的本质。

哲思：关注基本的、重大的、普遍的真理。关注演变，关注思想的更新。

洞见：要窥见事物内部的境界。

超越：就是让认识更上一层楼。

关于家长及孩子们最关心的问题：“如何学科学，怎么学？”我只谈几个重要方面，而非全面论述。

1. 致广大而尽精微。

柏拉图说：“我认为，只有当所有这些研究提高到彼此互相结合、互相关联的程度，并且能够对它们的相互关系得到一个总括的、成熟的看法时，我们的研究才算是有意义的，否则便是白费力气，毫无价值。”水泥和砖不是宏伟的建筑。在学习中，力争做到既有分析又有综合。在微观上重析理，明其幽微；在宏观上看结构，通其大义。

2. 循序渐进法。

按部就班地学习，它可以给你扎实的基础，这是做出创造性工作的开始。由浅入深，循序渐进，对基本概念、基本原理牢固掌握并熟练运用。切忌好高骛远、囫囵吞枣。

3. 以简驭繁。

笛卡尔是近代思想的开山祖师。他的方法大致可归结为两步：第一步是化繁为简，第二步是以简驭繁。化繁为简通常有两种方法：一是将复杂问题分解为简单问题，二是将一般问题特殊化。化繁为简这一步做得好，由简回归到繁，就容易了。

4. 验证与总结。

笛卡尔说："如果我在科学上发现了什么新的真理，我总可以说它们是建立在五六个已成功解决的问题上。"回顾一下你所做过的一切，看看困难的实质是什么，哪一步最关键，什么地方你还可以改进，这样久而久之，举一反三的本领就练出来了。

5. 刻苦努力。

不受一番冰霜苦，哪有梅花放清香？要记住，刻苦用功是读书有成的最基本的条件。古今中外，概莫能外。马克思说："在科学上是没有平坦的大道可走的，只有那些在崎岖的攀登上不畏劳苦的人，才有希望到达光辉的顶点。"

北京大学数学教授/百家讲坛讲师

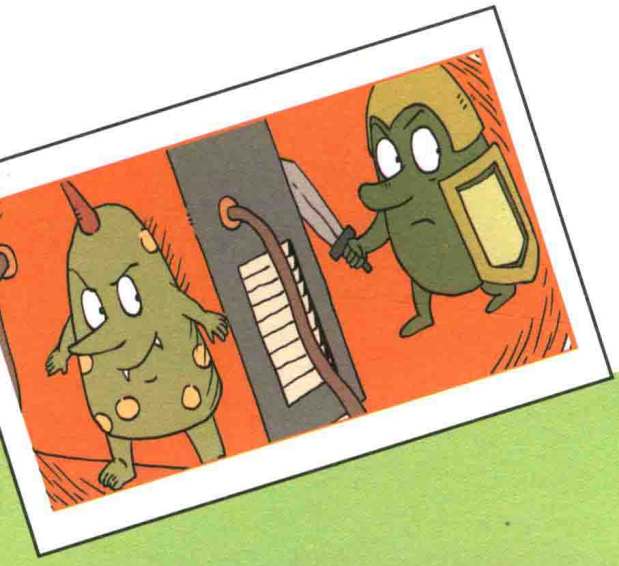
张收益

写给家长及孩子们的话

孩子是这个世界的未来，在这个科技飞速发展、全球文化经济共融的时代，家长转变教育理念并开拓孩子的视野是重中之重的事情。“科学如此惊心动魄”系列丛书，是一套涉及领域广阔的趣味科普故事书，囊括自然科学、人文、生物、天文、数学、地理、历史等学科知识，都是孩子们最感兴趣的主题，让孩子们在行动中不断开阔眼界，在不知不觉中掌握科学知识！

中国科学院院士/北京大学化学教授

黄春辉



目录

第一章　揭开网络病毒的真面目 1

让计算机生病的计算机病毒 2

小病毒的超强威力 6

第二章　探寻计算机病毒的“特长”和“家族谱” 11

计算机病毒的普遍特性 12

庞大的计算机病毒种族分类 19

第三章　追踪计算机病毒“发家史” 23

网络病毒的始祖 24

计算机病毒的“更新换代” 27

越变越厉害的计算机病毒 32

第四章　计算机病毒的常见手段和表现 37

计算机病毒的常见攻击手段：毁坏存储数据 38

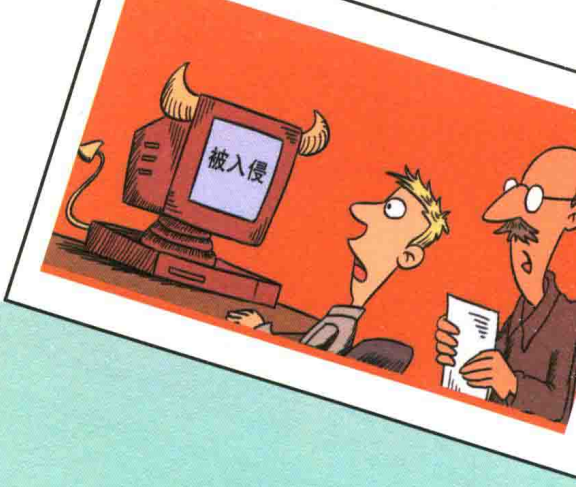
计算机病毒入侵的常见表现：计算机突然“变慢”了 42

第五章　文件型病毒的可恶之处 47

文件型病毒的发展 48

可怕的CIH病毒 52

目录



第六章　善于伪装的木马病毒　57

一点儿都不可爱的“木马”　58

知己知彼，网络世界中的“后门木马”　62

第七章　与众不同的蠕虫病毒　67

网络中的“蠕虫”是怎么来的　68

蠕虫病毒和普通网络病毒的区别　74

第八章　伺机而动的网页病毒　81

什么是网页病毒　82

“网页挂马”怎么办　86

脚本病毒的运作原理和预防　89

第九章　来者不善的即时消息病毒　93

神秘的“即时消息”很可怕　94

学会拦截即时消息病毒　98

第十章　雷霆扫毒，计算机反病毒大战　103

病毒码：计算机病毒的“通缉令”　104

“防火墙”：抵御计算机病毒的“堡垒”　109

杀毒软件：计算机病毒的“杀手”　114

第一章

揭开网络病毒的真面目

让计算机生病的计算机病毒

1949年，一个叫冯·诺依曼的骨灰级电脑“大神”在自己的论文中发表了一个“天马行空”的想法：将来，我们的电脑一定会出问题的。什么问题呢？那就是恶意程序。这些程序技能高超，能自己“繁殖”，自己传播，就像细菌一样，侵害我们的电脑。

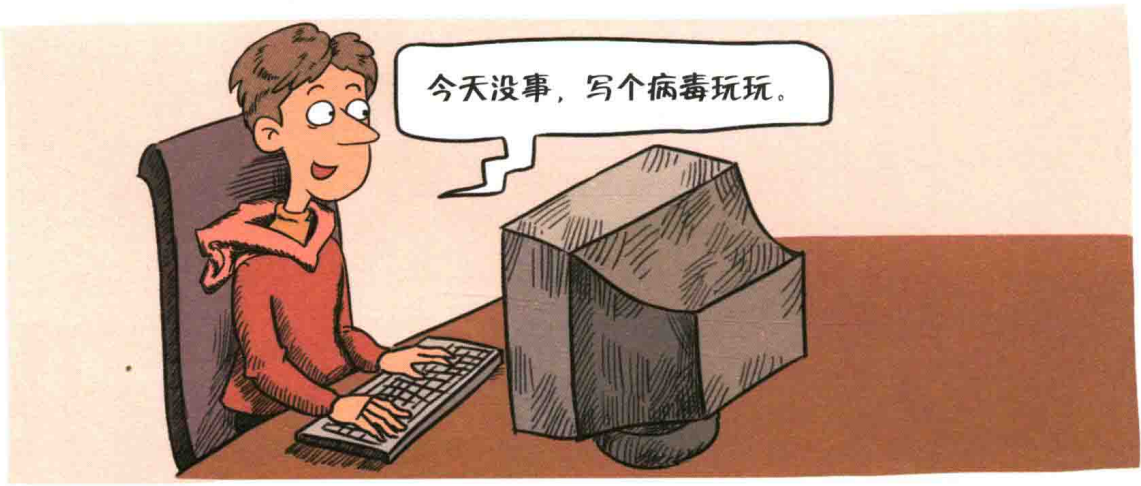
这个想法在现在看是十分正确的，但是在当时，人们根本不敢想象会有这么厉害的程序，所以也没人理会冯·诺依曼的话。直到19世纪90年代，真正的电脑病毒出现了，人们才明白真的是“不听冯·诺依曼的话，吃亏在眼前”啊。

其实，电脑病毒和影响我们身体健康的病毒一样，是一种侵害电脑“健康”的病毒源。

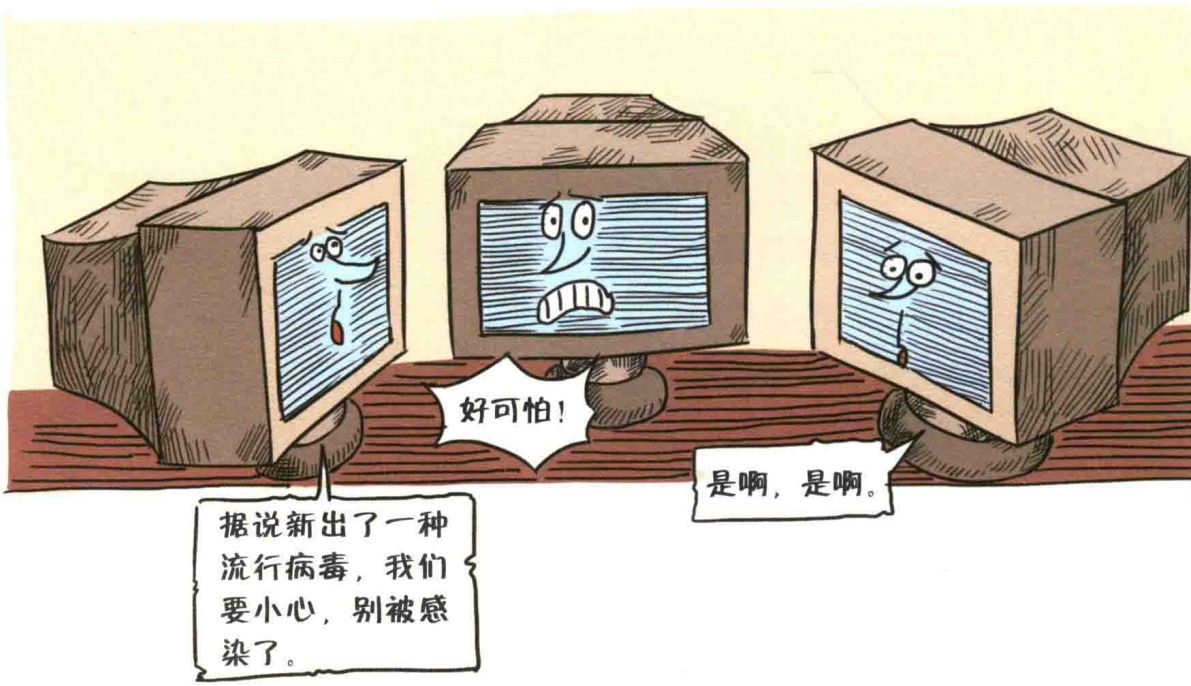
世界上对于电脑病毒的标准叫法是“计算机病毒”，主要是指为达到某种目的而制造、传播具有一定破坏性，会影响电脑正常使用的有害程序。“电脑病毒”是我们对这些恶意程序的俗称。

就像我们人体接触到感冒病毒，很可能会引起咳嗽、发热等症状一样，如果我们的电脑接触到这些电脑病毒也会出现相应的病毒感染现象。它们首先会寄生在电脑中等待时机，一旦时机成熟，它们就会被激活，并不断自我复制，一

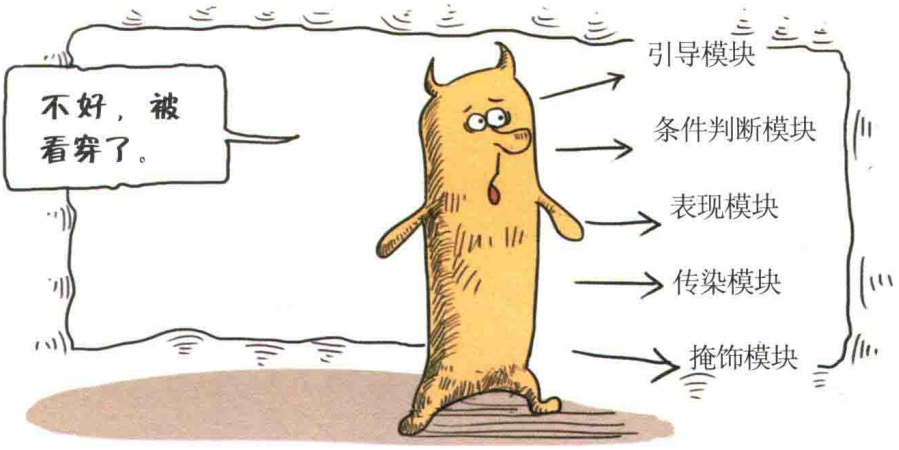
变二、二变四。当这些病毒“繁殖”到一定数量之后，电脑就会“发病”了。有的病症是“电脑变得很慢”，有的病症是“电脑中储存的文件不见了”……



所以说，人们将这些人为制造的，专门用来影响电脑“健康”，损坏电脑数据的一切程序和指令，广义地归纳到电脑病毒的行列，以防患于未然。



为了更好地将电脑病毒“揪”出来，人们对电脑病毒的“结构”进行分析。通过分析，人们发现，虽然电脑病毒千变万化，种类繁多，但是它们基本上都有类似的“结构”，分别是引导模块、条件判断模块、表现模块、传染模块和掩饰模块。



随着五大模块的设置不同，不同病毒的爆发力和影响力各有所不同。在计算机病毒发展史上，CIH病毒、特洛伊木马病毒、逻辑炸弹病毒以及蠕虫病毒就是计算机病毒中的“佼佼者”。

你知道吗

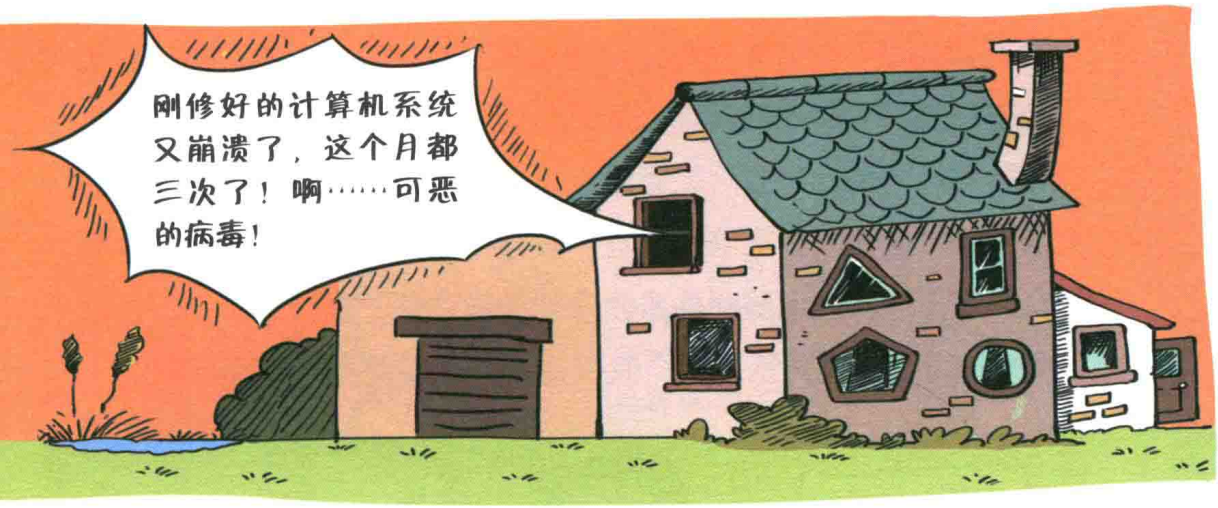
我们生活中俗称的“电脑”，也就是个人计算机，是由计算机硬件和软件两大部分组成的。计算机硬件包括中央处理器、存储器和外部设备等，也就是CPU、主板、内存等设备；而软件则包括计算机运行程序和相应的文档，如网页浏览器、文档处理器、图像影音播放器等。

小病毒的超强威力

人们对于生物病毒的了解是从无到有，从浅到深的，对于电脑病毒的认识也一样。

现在，人们的生活几乎都离不开电脑，我们可以试想一下，如果今天辛苦做的作业存在电脑里，可偏偏碰上电脑病毒，整个作业文档不见了……这不是噩耗嘛！

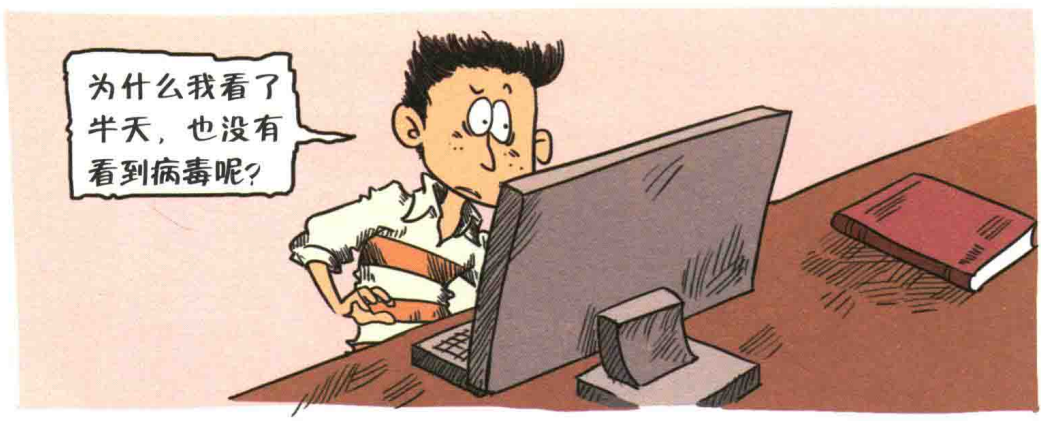
当然，你可能会说：“怕什么呀，我们有杀毒软件。”是的，现在确实有杀毒软件，可是杀毒软件是近年来才兴起的。在有杀毒软件的情况下，电脑病毒尚且让人这么着急，大家可以想象一下，在以前没有杀毒软件的年代，电脑病毒到底是何等“嚣张”啊！



为什么电脑病毒具有如此强大的威力呢？这主要和电脑病毒的特性有关。

说到世界上首屈一指的“间谍”，电脑病毒绝对榜上有名！因为，善于伪装、乐于潜伏、精于繁殖就是电脑病毒最大的特性。

在入侵电脑的过程中，电脑病毒首先会伪装自己，为自己“整整容”，让自己看起来像一个正常的程序。一旦你错信了伪装后的它，把电脑病毒储存到电脑，它就会潜伏在你的电脑中。刚开始，它不会有大动作，可是潜伏的过程中，它会不断地“繁殖”，复制出多个和自己一模一样的“兄弟姐妹”。当“兄弟姐妹”已经“济济一堂”，数量充足的时候，它们就会发动“人海战术”，全面入侵电脑的硬盘、软盘、内存……由于病毒人多势众，寡不敌众的电脑硬件或软件就会被“杀”个措手不及，被迫受感染，而出现速度变慢、数据丢失，甚至完全瘫痪的病症。



而且，随着互联网的兴起，电脑病毒又多了一条网络传播的途径。

不错，网络传播这个途径对于电脑病毒来讲，简直是一个新天地。

“帮助”电脑病毒发现这个新天地的，是一个叫罗伯特·莫里斯的年轻人，他当年只有24岁，是美国康奈尔大学的研究员。他编制出一种叫“蠕虫”的网络电脑病毒，并上传到互联网。结果，导致十几万台计算机和1200多个连接设备进入休克状态，美国九成网络需要紧急关闭超过16小时，军用网络更是关机长达40小时，造成超过1亿美元的经济损失。

至此，人们才意识到：互联网搭配电脑病毒可是大事件呀！

你知道吗

计算机病毒武器，是指将计算机病毒应用到军事上，将病毒输入敌方军用计算机系统，对系统文件、战术程序进行干扰和破坏，使敌方计算机系统功能削弱，甚至瘫痪的一种非致命性武器。据国外电子战专家估计，目前计算机病毒武器研制已经进入实用阶段。