电脑王国里的故事丛书

形影难离

——电脑黑客与电脑病毒的故事

王会 武爱民 著

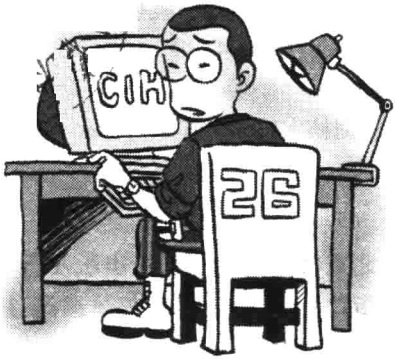
北京师范大学出版社

电脑王国里的故事丛书

形影难离

——电脑黑客与电脑病毒的故事

王会 武爱民 著



北京师范大学出版社

图书在版编目(CIP)数据

形影难离：电脑黑客与电脑病毒的故事／王会，武爱民主编．
北京：北京师范大学出版社，2000.6
（电脑王国里的故事丛书）
ISBN 7-303-05434-0

Ⅰ.形… Ⅱ.①王…②武… Ⅲ.计算机病毒－普及读物②计算机网络－安全技术－普及读物 Ⅳ.TP393.4-49

中国版本图书馆 CIP 数据核字(2000)第 31513 号

北京师范大学出版社出版发行
（北京新街口外大街 19 号 邮政编码：100875）
出版人：常汝吉
北京师范大学印刷厂印刷 全国新华书店经销
开本：890mm×1 240mm 1/32 印张：7 字数：101 千字
2000 年 7 月第 1 版 2000 年 7 月第 1 次印刷
印数：1～5 000 定价：10.00 元

前言

半个世纪前，世界第一台计算机（电脑）出现时，它只是孤独地落户在实验室里，围着它的不过是几个科学家而已。人类并没有意识到就是这个被人冷落的笨重的庞然大物将会给世界带来多么深远的影响。

几十年来，人类勤奋地创造着历史。在我们这个星球上，惟独人类有如此巨大的力量。时间走到21世纪，电脑一下子离人们的生活近了，电脑的使用范围小到使人足不出户就可购物、治病、取款、炒股、工作、学习……大到航天登月遨游宇宙，电脑几乎遍布到这个世界的任何一个地方。人们这才意识到，电脑与人类已经密不可分了。的确，电脑就像人类忠实的朋友，默默地为人类工作。几十年

来，人类勤奋地创造着历史，在我们这个星球上，惟独人类有力量改变世界。然而，科学是一把锋利的双刃剑。当一台叫“深蓝”的电脑第一次战胜了世界象棋大师，人们吃惊地发现，电脑的智能在人类的创造下正呈几何系数升级，在悄悄地向人类自身发出一个严峻的信息：电脑终究有一天会向人类彻底宣战。人类不禁扪心自问，在不久的将来，电脑能否战胜人脑？当全世界为捉拿“千年虫”如履薄冰地度过2000年零点并为之无端耗资几千亿美元而唏嘘慨叹时，美国雅虎、有线新闻等世界五大网站同时遭到神秘黑客猛烈的袭击，举世震惊。当人们尚未从惊慌中醒来时，微软等三家网站又受到黑客更猛烈地袭击……据统计，在中国，20世纪最后一年，约有64%的上网公司受到过黑客袭击。如今的每一天，世界各地的数以万计的黑客伺机行动，侵入网页非法掠财，传播病毒，攻击银行、股市，造成几百亿上千亿美元的损失。人类不禁发出这样的忧虑：在电脑已经统治着人类的今天，一旦希特勒式的电脑黑客进入核武库，按动核按纽，人类将如何面对？

难道人类真的最终毁灭于自己手中？假如这个推论正确的话，无疑，电脑就是人类的第一号杀手。

电脑，真是一个神奇的发明。没有人类的操纵，它几乎没有生命，几岁的孩子可以随心所欲地使用它。然而，一旦人类开启了它，它就会展示出超跃

人类的非凡智慧。一个科普作家在他的小说中这样描写电脑化了的世界：当人类进入到2030年，地球上所有的东西都电脑化了，就连人类的大脑中也被植入了一个米粒大小的智能芯片。有了这个智能芯片，人类可以随心所欲地掌握任何知识。过去从小学到博士所学习的知识仅需几分钟时间便可以全部掌握。一部《战争与和平》，每个人仅用几秒钟就可以一字不错地全文背诵……“学习”“读书”这些词语在人类的字典中已经消失，人类欣喜若狂。然而，一场宇宙辐射忽然降临，击毁了人类头脑中的芯片，网络中的地球瘫痪了，地球上出现了几十亿痴呆人。这位科普作家大声疾呼：是电脑毁灭了人类。

如今，新千年带着人类已经昂首走进了神秘的电脑世界，每个人类成员都不可能远离电脑。基于此，这套《电脑王国里的故事丛书》便应运而生。编写这套丛书的目的很显见，那就是让人们尽可能多地了解电脑王国的秘密。我们摒弃了过去那种因过于追求专业化语言而使图书变得枯燥无味少有读者的尴尬，在写作中尽量注意读者的阅读兴趣，每篇文章都设置曲折引人的故事，辅以流畅的文学语言，使读者在轻松的阅读享受中掌握了解电脑知识。

未来的世界必定是电脑的世界。愿我们这套《电脑王国里的故事丛书》能给广大读者带来愉快和知识。

目录

美丽杀手不美丽

1999年3月28日，警报在因特网上响起:一种名为“美丽杀手”（Melissa，又译作“梅利莎”）的病毒正在通过因特网快速进行传播!美国国家设施保护中心正式发出警告: 所有微

软Office用户不要打开任何来路不明的邮件!

可是已经晚了。

警告发出的第二天,就有数以百万计的计算机被感染上该病毒。包括微软、英特尔、摩托罗拉、朗讯等大公司在内的上百家公司成了“美丽杀手”的牺牲品,美国政府、企业及军方的站点都遭到它的攻击,几十所大学的站点被迫宣布关机。而且可怕的是,“美丽杀手”没有停止它张狂的步伐,还在以极罕见的速度在因特网上蔓延着。

著名反病毒公司NAI的所罗门博士提取了这种病毒,他和几个专家解码后发现:这是一种专门针对微软的电子邮件服务器MS Exchange的Word宏病毒。

由于“美丽杀手”可以自动地进行自我复制,因此也可以说它属于蠕虫类病毒。大概正是因为它的多面性,其作者竟得意洋洋地在病毒代码中写道:“蠕虫类?宏病毒?Word97病毒?还是Word2000病毒?你们自己看着办吧!”

如果某个用户的电子信箱被感染了“美丽杀手”病毒,那么,在他的信箱里就会看到一封题为“来自XX的重要信息”的邮件,其中XX是发件人的名字,打开后,正文中写着:

“这是你索要的文件……不要给其他人看。”用户正在云里雾里地琢磨自己何时向××索要过文件时，病毒已经开始通过他的MS Exchange和Outlook的通讯录，给前50个通讯地址发出了带有“美丽杀手”病毒的电子邮件，于是，灾难又降临到另外50个用户头上，只要打开邮件，每个用户又会传染50个用户，就这样反复传递，“美丽杀手”以几何级的速度向外传播，直至“淹没”网站的电子邮件服务器，使其瘫痪。

据计算，如果“美丽杀手“能够按理论上的速度进行传播，那它只需繁殖5次就可以让全世界所有的网络用户都收到一份!

这还不是最可怕的。

更让所罗门博士吃惊的是，“美丽杀手”在发送带毒邮件的同时，还可以把用户重要的核心机密扩散出去，用户甚至连这些文件被扩散到哪儿都不知道。

“美丽杀手”并不美丽!

当计算机专家们终于研究出阻止“美丽杀手”传播的方法时，它竟然发生变异了!

变异的“美丽杀手”可以躲开针对它的反病毒软件，并在复制和发送过程中附带上更多的“致命”文件。

看来“美丽杀手”的编制者也没有闲着。

受国防部资助的美国“电脑紧急反应小组”在各种媒体上都发出了紧急公告：呼吁所有用户采取一切措施，严防“美丽杀手”。这是它成立10年来第二次认为某种病毒重要到需要发布公告的时候。第一次是在1994年，那次是为了提醒用户注意一种可以让黑客提取口令的病毒。

就在这时，另一种名为“爸爸”（PAPA，又译“怕怕”）的病毒又出现了！

真是个多事之秋。

“爸爸”与“美丽杀手”同样可以迅速扩散，如果说有什么不同的话，就是它把发送有毒邮件的数目增为60个，而且不仅仅是干扰邮件服务器，它可以使整个网络瘫痪！

“爸爸”与“美丽杀手”的作者是否是同一个人？不得而知。但不管怎样，美国联邦调查局得加紧调查的步伐了。

两位软件工程师首先在病毒中提取了与“美国在线”（AOL）的一个用户及网站有关的情报，情报显示，“美丽杀手”的编制者在美国在线上用的名字叫Sky Roket。

联邦特工一调查，却发现这个Sky Roket不过是病毒制造者从别的用户那里窃取的一个

名字。

饱受“美丽杀手”摧残之苦的美国在线决定全力配合联邦调查局的行动，经过数日的跟踪调查，他们发现“美丽杀手”最初来自新泽西州。

在联邦政府专家的协助下，联邦特工用了三天的时间分析了“美丽杀手”出生地的电话号码，终于找到并抓获了机主戴维·L·史密斯——一个30岁的英俊青年。

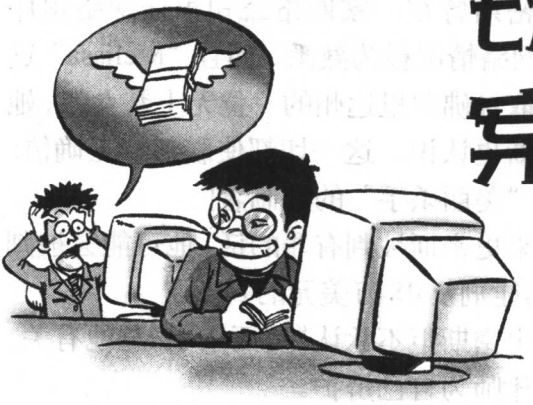
史密斯曾在一家网络公司担任网络程序员，对网络情况极为熟悉，而且“Melissa”这个名字取自佛罗里达州的一位无上装女郎，她和史密斯也认识。这一切都使联邦特工确信：他就是“美丽杀手”的编制者！

如果史密斯被判有罪的话，他可能会被判处40年徒刑及48万美元的罚款。

但史密斯拒不承认“美丽杀手”与他有关，并请了律师为自己辩护。

究竟史密斯是否是“美丽杀人”的始作俑者？现在还是个谜。

84万元股票失窃案



35岁的李振民可以算得上股市中的幸运儿了，自打3年前开始炒股，他就福星高照，财源广进，逐渐成为股民们的风向标。

如今，李振民堂而皇之地在大户室里占据着一席之地，每天坐在电脑前，观察大盘的走

势，比起那些拥挤在大厅里的股民，的确是一个天上，一个地下。

除了股票交易中用到电脑外，李振民和这个玩意儿没有其他任何缘份，所以，当听到病毒、黑客之类的名词时，他就像听一个遥远的传说，一笑置之。

大户室的电脑都像一个个加上双重保险的保险柜，要想在这里偷取股票或转移现金的话，罪犯必须持有证券公司送给操作员的密钥和他自己设定的口令。

在国外，对黑客来说也许这是小菜一碟，但在国内，尤其是这个相对落后的内陆城市，李振民好像还没有发现有这样的奇才。

所以，在1999年5月21日，当李振民从面前的电脑里怎么也找不到自己价值84万元的股票时，还以为是电脑出了故障，或是证券公司营业部误操作造成的。

当营业部经理严肃地告诉他：他的股票被人盗窃了的时候，李振民愣了足足有2分钟不知道该说些什么。

“贼怎么能把我的股票划到他的帐户上呢？”李振民问，他的脑海里忽然涌出了自己听过的有关黑客的传说，于是又加了一句：“难道他是黑客？”

“从他的行为方式来说，应该算是个黑客，但只能算是一个低层次的黑客。”经理说。

什么？把别人加密保存到电脑里的巨额股票轻易地划到自己的名下，还“只能算是个低层次的黑客？”那要是高层次的黑客呢？是不是可以把瑞士国家银行都归到自己名下呢？

李振民一下子对黑客有了一个清晰的认识，不过，他没有时间在这个问题上较真儿，84万元股票转天就没影了，他还有闲心考虑别的事儿吗？

报案吧。

公安局接到报案后，详细地询问了他所了解的情况，又到现场进行了戡查，认为犯罪嫌疑人不是从网络侵入大户室的电脑的，而是直接利用大户室的电脑调走了李振民的股票。

这下搜索范围一下子就缩小了，能出入大户室的也就那么十来个人，罪犯很可能就在他们中间。

另外，能够调阅别人的帐户，说明他具有破译密码的能力和时间。

会是谁呢？

老张？不可能，除了会输入交易的几个命令外，他对电脑可以算得上是个完完全全的门

外汉。

小刘？也不可能，虽然他是响当当的研究生，又精通电脑，不过，他的帐户上有价值近千万的股票，犯不着为自己的这点钱动心思。

李振民琢磨了半天，也想不到这笔钱是谁“贪污”了，不过，通过公安人员的讲解，他对黑客又有了具体的认识，原来电脑只要连上网络，就可能被任何一个地方的黑客攻击。

公安局的人可不像他这样只会琢磨，他们成立了好几个小组，对营业部、银行等单位连夜进行明查暗访，排查嫌疑人，最后终于发现了狐狸的尾巴：大户室的崔某大学毕业，精通电脑操作，会编程，此君炒股5年，赔得多赚得少，两天前忽然推说老家有事，把股票全部赔本卖掉了。

而且，据银行的营业员反映，前天上午有一个孕妇分4次提取了12万元现金，想到崔某的妻子正在妊娠期间，公安人员认为这次股票盗窃案极有可能是崔某所为，于是果断地将崔某夫妇二人传唤，在强大的攻势下，崔某终于承认：84万元股票是他盗窃的。

因为运气不佳，股越炒越赔，所以崔某萌生了利用电脑盗窃别人股票的想法，他学过电脑技术，知道只要将用户的密码破解了，就可