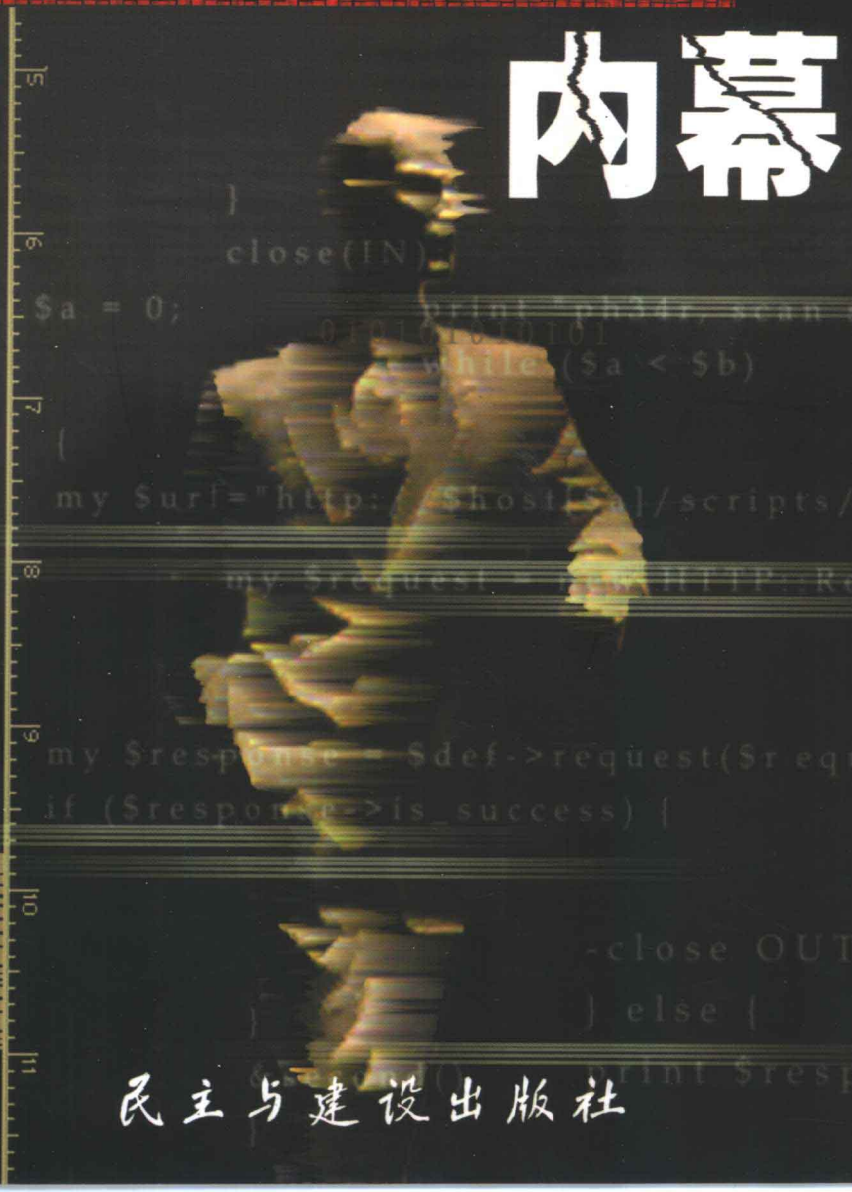
斑马多媒 体总策划

中国黑客

CHINESE HACKER

内幕



HACKER

民主与建设出版社

CHINESE HARKER: UNMASKING

中国黑客内幕

陈细木 主编

陈细木
朱云凯 编著
熊 杰

民主与建设出版社

图书在版编目(CIP)数据

中国黑客内幕/陈细木等编著.
-北京,民主与建设出版,2001
ISNB7-80112-435-9

Ⅰ.中… Ⅱ.陈… Ⅲ.中国当代
Ⅳ.125

中国版本图书馆 CIP 数据核字(2001)第 045671 号

责任编辑	闵 建
封面设计	黄 茬
出版发行	民主与建设出版社
电 话	(010)65523123 65523819
地 址	北京市朝外大街吉祥里 208 号
邮 编	100020
经 销	新华书店
印 刷	北京机工印刷厂印刷
开 本	880×1230 1/32
印 张	14
字 数	300 千字
版 次	2001 年 7 月第 1 版 2001 年 7 月第 1 次印刷
书 号	ISNB7-80112-435-9/G·179
定 价	25.00 元 (加 CD)

注:如有印、装质量问题,请与出版社联系。

序

《电脑报》常务副社长、天极网CEO：李志高

2001年5月1日前后，“黑客”、“红客”、“中国黑客”、“美国黑客”等词汇在媒体上频繁出现。一时间，翻看报纸，打开网页，大大小小的攻击事件、态度各异的黑客宣言、众说纷纭的评论随处可见。

黑客是赛伯(cyber)空间的游侠：以发现系统漏洞为乐趣，促进技术提高为己任。事实上，包括天极网(www.yesky.com)在内的著名商业网站都得到过黑客暗中的帮助。但是，有的黑客似乎背弃了鼻祖们定下的行为准则。例如给美国计算机系统带来5,000万美元损失的鲍勃·莫利斯(1988年)、通过互联网窃取美国富豪上千万美元的艾布都拉(2000年)。因此从某种意义来讲，黑客也可能成为网络自由空间的江洋大盗：他们为了满足好奇心，甚至为了其他的目的在互联网上为非作歹。但是，最近又有不少媒体认为“五一中美黑客大战”中的中国黑客可以被称为“红客”，因为中国黑客试图通过自己的方式维护民族尊严。到底什么是中国黑客？

看过《中国黑客内幕》，我有一个很强烈的感受：外国黑客也好，中国黑客也罢，都是互联网时代的必然产物。从E-mail 、网上聊天 、网页浏览、IP电话到逐步完善的电子商务，高速发展的互联网技术的确正在改变我们工作、生活的方式。与此同时，相对应的后台技术却也给一个特定的人群留下了一片“乐土”。他们凭借自己对底层技术的了解，可以通过网络随意进入在常人看来神秘莫测的计算机系统。这个人群就是黑客。就像习武之人有正有邪一样，黑客也有不同的类型，他们有自己不同的价值观和行为准则。换言之，我们很难用简单的好人或坏人，侠客或大盗来给中国黑客下个定义。

《中国黑客内幕》一书中，作者始终没有直接的告诉读者什么是中国黑客。他们把事件背后的人物搬到前台，让黑客事件的受害者、黑客

以及网络反“黑”专家来诠释“中国黑客”，把黑客的本来面目展现在读者面前。不愧为披露中国黑客内幕第一书。

此外，《中国黑客内幕》一书作者还从技术的层面分析了黑客常用的攻击手段，并为读者提供了一个比较全面的网络安全解决方案。为提高普及网民网络安全意识起到了积极作用。

前言

《电脑报》记者、本书主编
陈细木

市面上讲黑客的书并不鲜见，但一直没有一本讲中国黑客的书。一开始，我们还以为发现了块“处女地”。后来慢慢发现，不是同行们不愿意写一本专门讲中国黑客的书，而是要写一本讲中国黑客的书的确很难。

首先，黑客的概念就是一个问题——在中国，什么人是黑客？是深藏不露的系统漏洞“猎手”？是在实验室里悄悄研究黑客软件的技术顽童？是整天没事就上网摆弄“傻瓜式”黑客软件的调皮青年？还是在互连网上玩玩邮件炸弹、骗骗新手QQ密码的无聊之辈？

这个问题，我们倒是有自己的观点：黑客是信息时代的副产物。信息系统的技术漏洞以及相对新生事物的滞后的法律是黑客产生的主要因素。不同时期的黑客有不同的特点。比如，诞生于上个世纪50年代的第一代黑客就是典型的系统漏洞“猎手。他们以发现计算机系统漏洞并提出相应的补丁为荣，以破坏系统数据为耻。而到了几十年后的今天，我们只能用“形形色色”来形容黑客，他们采用的手段不同，但目的都是非法进入别人的计算机。有的黑客至今还恪守“通往电脑的路不止一条、所有的信息都应当是免费的、打破电脑极权、在电脑上创造艺术和美、计算机将使生活更美好”等等黑客原则（史蒂夫·利维在其著名的《黑客电脑史》提出）。有的黑客被称为网上哗众取宠者（Cyberbunk），他们类似于西方的“嬉皮士。”这些人往往玩世不恭，标新立异，把人生当游戏。他们以在网上能够给人带来烦恼为目的。而有的黑客，已经完全违背了早期黑客的传统，他们把个人利益放在第一位，他们利用自己的电脑技术在网络上从事着非法活动，这类黑客往往被称为网络骇客（Cracker）。他们坐在计算机前，试图非法进入别的计算机系统，窥探别人在网络上的秘密。他们有可能在网络上截取商业秘密要挟他人；或者盗用电话号码，使电话公司和客户蒙受巨大损失；也有可能盗用银行账号进行非法转账等等。这类人已经滑入了犯罪的轨道了。

在《中国黑客内幕》一书中，我们不希望简单地告诉读者什么是中国黑客，在某个事件中的中国黑客是对是错，是好是歹。我们希望读者在看过我们对包括“五一中美黑客大战”在内的客观事件报道，听到了包括黑客在内社会各界对“黑客”的诠释以后，自己来回答这两个问题。

其次，在想写一本讲中国黑客的书以前，很多同行还会遇到另外一个麻烦：到底该写什么？我们同样遇到了这样的问题。一开始，我们想写的是一本纯粹讲黑客文化的书。但是，在这以后，我们遭遇过各式各样木马，险些让人偷走了我们的书稿。而我们为本书做的市场调查报告显示：一半以上的网民毫无安全意识，他们甚至不知道单机上网以前需要关掉“系统资源共享”（否则，任何人可以轻松的拿到你上网的账户和密码）。 于是我们希望再为读者写一部“网络安全防卫手册”。在天极网（www.yesky.com）的大力支持以及搭档熊杰先生（前黑客，原国内著名的网络安全栏目天极网 “安全之路” 主编现在负责《电脑报》“防黑秘籍”、“局域网”栏目）的鼎力协助下，《中国黑客内幕》中的“上网安全防卫手册”有望成为国内现有图书中最全面、最实用的安全防卫手册。

正如大家所见，我们在《中国黑客内幕》一书中花了很大的篇幅去写黑客常用的攻击伎俩。我们认为，这样做是值得的。其实，在日常生活中，黑客与常人往往并没有霄壤之别。他们因技术漏洞而产生，如果不讲讲黑客到底利用的是什么漏洞，又是用什么样的伎俩突破层层防线，“直捣黄龙”，不讲讲“网络警察”是如何追踪黑客，会让很多喜欢刨根问底的读者感到失望。于是我们编写了“黑客常用攻击伎俩”这部分内容。与其他黑客内容图书不同，我们不强调技术的基本原理。我们希望用通俗易懂的语言剖析黑客的惯用伎俩，并向读者传授基本而实用的防范对策。与本书“网络安全防卫手册”部分不同的是：前者以普通用户可能遇到的安全隐患为线索展开，重点讨论如何防范“技术含量”较低，但在互联网上最常见的“低能”黑客攻击，而后者以黑客实际攻击流程为线索展开，重点在讨论如何防范黑客中的“江洋大盗” 。

有人可能会认为《中国黑客内幕》的技术部分基本可以作为一本“黑客教程”。这使我们想起《金瓶梅》的原序：“...余尝曰：读《金瓶梅》而生怜悯心者，菩萨也；生畏惧心者，君子也；生欢喜心者，小人也； 生效法心者，乃禽兽耳...”。其实写一部“黑客教程”是我们一开始就反对的做法。我们希望告诉读者真实的中国黑客，讨论如何加强个人网络安全意识、增强对黑客攻击的“免疫”能力。希望读者能体恤我们的一片苦心。

Preface

Millions of words have been written about hackers, but none coming down to their Chinese branches, where an enormous population hides Hidden Dragons and Crouching Tigers. So let us be the first group to unmask them, an unknown detachment of the cyber world. Time goes by, and we've found it is no easy task to wade through such a muddy field.

The identification of a hacker proves to be the first challenge. Who, in China, deserve the "honor" of being listed as a hacker? Hunters searching for system bugs? Naughty boys playing software tricks? Or college guys addicted to hacker techniques? Or rather those with mail – bombs and password cracking?

At last, we agree upon one definition, a definition of our own: **Hacker comes out of the information age, a natural product of the IT development due to the imperfect technology and the incomplete laws with it.**

In his book *Heroes of the Computer Revolution* published in 1984, Steven Levy pointed out that " Because of their ethic and unconventional style, hackers like Jobs and Wozniak were able to launch the ' computer revolution, ' resulting in the first personal computer (the Apple), which was easy to use and which put programming power in the individual's hands. "

Hackers change with time. Most hackers of 1950s were typical " bug hunters", proud of finding system bugs, but shamed of destroying data or systems.

Although hackers today have different means, they have at least one thing in common: their purpose is accessing computers of the others illegally, some of them keeping in mind the motto of their originators: **Access to computers and hardware should be complete and total Information wants to be free Mistrust Authority. You can create truth and beauty**

on a computer. Computers can change your life for the better (Steven Levy: *Heroes of the Computer Revolution*) .

So that is the Hacker Ethic.

Some hackers are even known as cyberbunkers, somewhat like those hippies, trouble – making in the cyber place their greatest pleasure. Some hackers, also known as crackers, use their computing skill only to violate laws, peeping into business secretes and stealing account passwords.

They commit crimes.

We do not intend to judge between right and wrong. We lay bare the cases and facts, and leave the decisions and judgements to our readers. Let them judge and let them answer. So objectivity is one of the distinct features of our book.

This is the first publication in China to place ' hacker culture' and ' hacker technique' together. At first, we want to write a book of pure ' hacker culture'. But during our writing, hackers kept attacking our computers, and some even tried to steal the Book via Trojan.

Meanwhile, a nation – wide survey shows weak public awareness of the importance of Internet security.

So we invited into our group XiongJie, a famous ex – hacker in China, who wrote *How to Defend Your PC*, a chapter telling you how to treat snaky hackers. We hope this technical part will be both practical and precise.

And our editor Zhu Yunkai, an excellent editors with the CPCW, a knowledgeable and popular IT weekly that enjoys the biggest circulation in China, is introducing to our readers a New World, the Empire of China Hackers.

We hope you'll enjoy.

Editor in Chief: Ximu Chen

July 5, 2001

软件授权书

金山软件股份有限公司授权《电脑报》社在《中国黑客内幕》一书配套光盘中收录“金山毒霸《中国黑客内幕》特别版”。在功能上，该特别版与市面上最新版本（版本号）的“金山毒霸”完全一致。在试用期上，该特别版的试用期为 90 天（普通的试用版为 30 天）。

2001 年 6 月 28 日

"五一"假期，中美数万网络黑客，在虚拟空间竞相角逐，数千家网站被黑。虽然这些攻击行为的象征意义大于实际意义，但也算是给国人上了一堂生动的网络安全教育课

中国黑客内幕　采用纪实的形式为你全面撩开中国黑客神秘面纱，曝光中国黑客真实生活，报道历年来黑客典型案例，同时，我们站在客观的立场剖析种种黑客现象，让你洞悉国内黑客常用伎俩，进而保卫个人网络安全

无论你对黑客的存在是否认同，通过本书，你能够全方位地了解中国黑客，清醒地认识到网络时代我们所面临的严重安全危机从而防范于未然

本书部分精彩内容

五·一中美黑客大战
初次出击，中国黑客战印尼
海信挑战全球黑客
"少年黑客天才"现形记
狂人日记
黑客这样过一天
近距离聚焦中国黑客
"黑客杀手"许榕生妙论黑客
网络警察护一方净土
"傻瓜式"黑客工具一瞥
基本的攻击手段
剖析攻击的实例
如何追踪黑客
网络病毒典型案例分析要症状
木马攻防战
安全地管理邮件
聊天软件的安全
网吧管理软件与安全
个人安全必备工具

斑马多媒体工作室（ZEBRA MULTIMEDIA）

在非洲的大草原上，斑马是食草动物群落的先行者，它们通常总是第一个进入闷热而潮湿的草原地带。斑马工作室，愿意陪伴读者进入每一个未知的领域，共同发掘这崭新时代的秘密。

陈绍木：本书主编兼第一作者，现为《电脑报》记者、编辑，曾经采访过美国IDG公司总裁麦戈文、美国杜比实验室负责人Bill Jasper、美国红软公司CEO邓辉、"超级解霸"作者梁肇新、KV3000软件作者王江民、金山公司创始人求伯君等许多国内外IT届知名人士。近年来，他在大陆《北京青年报》、《电脑报》、等知名平面媒体以及天极网（www.yesky.com）、人民网（《人民日报》网络版）、新浪网（www.sina.com.cn）等网络媒体上发表了数十篇文章。

朱云凯：本书第二作者，现为《电脑报》企业、财经栏目编辑。作为一名专业记者和新闻编辑，他对计算机网络安全有独到而深入的见解。同时，他与近几年主要黑客事件中的当事人有过深入的探讨。近年来，在《电脑报》等国内多家知名媒体上发表了大量的新闻作品。

熊杰：本书第三作者，现为《电脑报》防黑秘籍、局域栏目编辑。熊杰曾是一名黑客，之后他长期从事网络安全工作，在计算安全领域有很大的影响力。他曾经代表天极成功组织了中国第一次黑客大会。熊杰先生以前负责的天极网安全之路栏目，是国内IT网站访问量最高的栏目之一。

王润武：本书的特约编辑，现为天极网设计在线栏目主编，在《电脑报》等知名媒体上多次发表文章，并出色地完成过不少计算机图书的编辑工作。

目　录

上卷

展，人们已提出了基于太空的第四国防。随着网络应用的日益重要，基于网络的国家安全称为第五国防……

下卷