KINGPIN

马克斯·维京：地下网络犯罪之王

掘金黑客

[美] 凯文·保尔森（Kevin Poulsen）著

王军 王凯 译

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
http://www.phei.com.cn

掘金黑客

KINGPIN

马克斯·维京：地下网络犯罪之王

【美】凯文·保尔森 著　　王 军 王 凯 译

電子工業出版社
Publishing House of Electronics Industry
北京·BEIJING

版权贸易合同登记号 图字：01-2012-6282

图书在版编目（CIP）数据

掘金黑客——马克斯·维京：地下网络犯罪之王/（美）保尔森（Poulsen,K.）著；王军等译.—4版.—北京：电子工业出版社，2012.11
书名原文：Kingpin：How One Hacker Took Over the Billion-Dollar Cybercrime Underground
ISBN 978-7-121-18488-8
Ⅰ.①掘… Ⅱ.①保… ②王… Ⅲ.①计算机网络-安全技术-普及读物
Ⅳ.①TP393.08-49

中国版本图书馆CIP数据核字（2012）第214839号

书　　名：掘金黑客——马克斯·维京：地下网络犯罪之王

作　　者：【美】凯文·保尔森（Kevin Poulsen）
策划编辑：胡　南
责任编辑：李　影　　特约编辑：张　冉
印　　刷：三河市鑫金马印装有限公司
装　　订：三河市鑫金马印装有限公司
出版发行：电子工业出版社
　　北京市海淀区万寿路173信箱　　邮编：100036
开　　本：720×1000　1/16　印张：17.5　　字数：270千字
印　　次：2012年11月第1次印刷
定　　价：49.00元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：(010) 88254888。

质量投诉请发邮件至zlts@phei.com.cn，盗版侵权举报请发邮件至dbqq@phei.com.cn。

服务热线：(010) 88258888。

作 者 介 绍

过去十年来，曾经的黑客、现今出色的调查记者凯文 · 保尔森，已经在网络犯罪报道领域树立起权威。在本书中，他利用自己的专业背景和能接触到事件核心的独特优势，展现了一个扣人心弦的“猫鼠游戏”，并对 21 世纪的新式组织犯罪做出了深刻披露。

凯文 · 保尔森（Kevin Poulsen），连线（Wired）网站的高级编辑和《连线》杂志的撰稿人。他主持连线网站的网络犯罪、隐私及政治报道等版面，备受赞誉的博客“威胁等级”（Threat Level）由他于 2005 年创建并维护。

内 容 介 绍

如同某种势不可挡的新型病毒，地下黑客圈子流言四起：某个聪明绝顶、胆大妄为的家伙发动了对线上犯罪网络的恶意接管，这个犯罪网络足以从美国经济中攫取数十亿美元。

联邦调查局展开了雄心勃勃的秘密行动，矛头直指这位崭露头角的头号人物，决心将其缉拿归案；世界各地的情报机构也安排了几十位“鼹鼠”和双面间谍。与此同时，网络警察笼络了许多尚未纳入黑名单的黑客为其所用。然而，他们的头号猎物展现出不可思议的能力，总是能够识破他们的卧底、看穿他们的计谋。

他们追查的这位头号人物，并不像个犯罪分子：他是一名出色的程序员，具有嬉皮士和超级恶棍的双重人格。作为著名的“白帽”黑客，“维京”马克斯 · 巴特勒曾是整个程序设计领域的明星，甚至还担任过联邦调查局的顾问。但作为“黑帽”黑客的“冰人”，他入侵了美国各地的数千台电脑，轻而易举地将数百万信用卡资料尽收囊中。他和一名诡计多端的骗子一道，掌控着一个现实世界的大规模犯罪产业链。

字里行间，我们被带入巨大的网络诈骗交易市场，里面充斥着信用卡号码、假支票、假护照、被窃银行账户和秘密情报点。我们会了解到黑客活动的运作机制——浏览器漏洞利用程序、网络钓鱼攻击、木马等——诈骗犯们使用这些手段从事非法勾当，通过复杂的流程，把被盗信息变成巨额的真金白银。多亏了作者对警方和犯罪分子的深入洞察，我们才得以窥见执法部门和诈骗犯之间神秘莫测、险象环生的斗争场面。

关于东西文库

东西文库致力于“第三种文化”（TTC）的思考、传播与交流；注重在互联网、科技、商业、媒体、电子阅读等领域的互动；包括但不限于：纸质、电子出版，版权引进、策划，文化论坛。

已出版《失控》、《技术元素》、《比特素养》、《掘金黑客》等图书。

本书由东西文库策划执行　特约编辑：克里斯　傅丰元

东西文库网站：http://welib.us/

献给劳伦，

我生命中未被起诉的同谋。

警察与卡贩

马克斯·维京，本名马克斯·巴特勒，以“冰人”的名号打理着“卡贩市场”网站。他使用的其他名头还有“幽灵23”、“乐善好施”、“数字”、“阿飞”和“大侠”。

克里斯托弗·阿拉贡，又名“悠闲生活”、“卡马”和“花花公子”，是马克斯在“卡贩市场”的合作伙伴，掌控着一个利润丰厚的信用卡伪造团伙，以马克斯窃取的信息为货源。

“脚本”，乌克兰人，被盗信用卡信息的卖家，第一个卡贩论坛“卡贩天地”的创始人。

“亚瑟王”，东欧的网络钓鱼者，自动柜员机套现老手，从“脚本”手里接管了“卡贩天地”网站。

“马克西克”，乌克兰卡贩马克西姆·雅斯洛姆斯基，他取代了“脚本”，成为地下网络中被盗信用卡信息的最大卖家。

艾伯特·冈萨雷斯，又名“康巴乔尼”和“落汤纳粹”，网站“幽灵帮”的管理员，

该网站在被美国特勤局取缔之前，一直是网络上最大的犯罪站点。

大卫·托马斯，又名“街头乐手”，是一名惯骗，打理着一个名为“诈骗犯”的信用卡交易论坛，为美国联邦调查局（FBI）搜集情报。

约翰·詹诺内，又名“斑马”、“给力”、“马克有钱”和“小子”，是一位来自长岛的年轻卡贩，与马克斯在网上合作，与克里斯·阿拉贡在现实生活中合作。

基思·穆拉斯基，又名“斯普林特老师”、帕维尔·卡明斯基，联邦调查局匹兹堡分部的特工，在一次风险很大的秘密行动中接管了网站“黑市”。

格雷格·克拉布，一位美国邮政稽查员，基思·穆拉斯基的良师益友，花了很多年跟踪地下隐藏的国际犯罪头目。

布雷特·约翰逊，又名“咕噜姆乐”（Gollumfun[①]），“幽灵帮”网站的创始人，后来又继续担任“卡贩市场”的管理员。

“茶”，又名阿伦卡，曾格尔才兹克·才曾德尔格，蒙古移民，在位于橙县的安全藏身处帮助管理“卡贩市场”。

“吉利”，瑞努坎斯·苏布拉马尼亚姆，斯里兰卡裔的英国公民，创办了“黑市”网站（Dark Market）。

“马提克斯001”，马库斯·克勒雷尔，德国人，“黑市”网站的管理员。

“地窖”，劳埃德·李斯科，加拿大黑客，后来成为温哥华警方的线人。

“堕落分子”，以前是一名毒品贩子和游戏性黑客，担任“卡贩市场”的管理员。

① Gollum 是指环王中的怪物。——译者注

楔　子

的士没有熄火，在旧金山市中心的一家便利店门前停了下来[1]。马克斯·维京付了车费，从车子的后座探身出来，他身高 1.95 米，浓密的黑发扎成一条粗长的马尾辫。他走进便利店，等着的士在街头消失后再次现身，步行走过两条街，回到自己的安全藏身处。

在他的周围，阴沉沉的天空下，小店和报摊开始营业。高层写字楼的上层影影绰绰，俯瞰着西装革履的上班族们鱼贯而入。马克斯也要开工了，但他要干的活儿并不像常人那样，忙完九个小时就能回家美美睡一觉。这一次他要闭关修炼一阵子。一旦他将计划付诸行动，就不再回家，也不会外出吃饭。在这间一应俱全的屋子里，没日没夜地忙活个不停，心无旁骛，直到完工。

这一天是他宣战的日子。

他阔步来到邮政街大楼前，临街的一面，五横十四纵的窗格嵌在一模一样的凸窗上，清一色地漆着与金门大桥一样的橘色。这栋公寓可短期租住，租金低廉，

吸引了不少交换生在此租住。他来到这栋公寓大楼已经几个月了，尽力和交换留学生们打成一片。但没有人知道他的名字——至少没有人知道他的真实姓名。而且，没有人了解他的过去。

在这里，他不是马克斯·巴特勒，那个在小镇里过不了几天安生日子，就要变着花样折腾的捣蛋鬼；也不是马克斯·维京，那位每小时 100 美元报酬，专为硅谷的公司加强网络安全的计算机安全专家。当马克斯登上公寓大楼的电梯，就变成了另一个人："冰人"——犯罪组织里一位崭露头角的小头目，这个组织要为美国的公司和消费者被窃的数十亿美元负责。

"冰人"已经急不可待了！

几个月以来，他一直在"造访"全国各地的商家，窃取了大量的信用卡号码等信息。这些信息本该在黑市里卖到数十万美元，但市场垮了。两年前，特勤局的特工人员发动了凌厉的网络清理行动，摧毁了最大的地下网络犯罪窝点，用枪指着那些头目将他们逮捕，剩下的喽啰们都躲到聊天室和那些不起眼的网络论坛去了。这些聊天室和网络论坛暗藏了许多安全漏洞，联邦政府人员和卧底充斥其间，局面一片混乱。

无论地下网络犯罪圈子对这些情况清楚与否，他们都需要一位强势的头目来统一号令，重整秩序。

下了电梯，马克斯在走廊里慢慢踱步，看看有没有尾巴跟着，然后来到自己的房门前，进了这套租来的单间公寓。屋内闷热难耐是这个安全藏身处的最大问题，房间里堆满了服务器和笔记本电脑，散发出大量的热量，整个房间热浪滚滚，灼人心肺。夏天的时候，他搞了些风扇来，但仍无济于事。产生的高额电费反而让公寓管理员怀疑他在鼓捣无土栽培毒品的勾当。但屋内有的只是这些机器而已，磕头碰脑地码放在电缆中，主电缆曲里拐弯地连接到巨大的抛物面天线上，天线像狙击步枪一样对准窗外。

马克斯对这些不便之处并不在意，他坐在电脑旁，将程序植入到一些计算机罪犯聚集的网络论坛，诸如“黑市”和“谈钱说财”一类的虚拟“酒馆”。两天了，他不停地入侵各个网站，手指在键盘上飞舞着：突破网站的防护，窃取网站信息、用户名、密码和电子邮件地址。觉得累了，就倒在公寓的折叠床上眯上一两个小时，然后睡眼惺忪地接着干。

他敲了几下键盘，如同纵火犯轻轻擦燃一根火柴那样，彻底删除了网站的数据库。2006 年 8 月 16 日，马克斯群发了一封没有丝毫歉意的邮件，收信人是那些被他破坏的网站的网民。在邮件中，马克斯告诉他们：如今，他们都是“冰人”掌管的网站“卡贩市场”（CardersMarket.com）的成员！世界上最大的犯罪据点横空出世，拥有 6000 名用户，并将是地下网络里唯一的交易平台。

马克斯只敲了一下键盘，执法部门多年来兢兢业业的成果就化为乌有，十亿美元的地下犯罪网络又恢复了元气。

在俄罗斯、乌克兰、土耳其和英国，在美国各地的公寓、办公室和家庭里，罪犯们意识到这是地下网络首度出现的不友善的接管。他们中的一些人将枪放在床头柜中，用来保护他们价值数百万的赃物，但对于这种盗窃方式，他们的枪支却毫无用武之地。联邦调查局和特勤局的特工们曾花了数月乃至数年时间，渗透到眼下已被肃清的地下论坛，如今他们会同样惊愕地获悉这条消息。刹那间，所有的人：黑客骨干、暴虐的俄罗斯犯罪团伙成员、伪造身份证的老手，以及发誓抓住他们的警察，都在不约而同地思考着同一个问题：

“冰人”是谁？

第一章　钥　匙

敞篷小货车一开上马路牙子[2]，几个坐在人行道上休息的少年极客就知道麻烦来了。“他妈的拨浪鼓儿！”其中一名牛仔朝窗外骂道。车上飞出一只啤酒瓶，砸在人行道上。那些极客们离开了俱乐部，避开音乐的喧闹声在这里海侃神聊。这阵势，他们以前都曾领教过。1988 年，在博伊西市的公共场所，如果被人发现没有系宽大的皮带扣、没有戴牛仔帽，就会遭到啤酒瓶的攻击。

其中一名极客做了让牛仔们出乎意料的事：他站了起来。马克斯·巴特勒身材高大，肩膀很宽，看上去镇定自若、仪表堂堂，一头直立的朋克摇滚硬发，又为他平添了几分风采，使他的身高蹿升了七八公分。马克斯平静地问道：“什么拨浪鼓儿？”假装对这个博伊西的俚语词一无所知，这个词是专指那些新浪潮摇滚乐迷和其他各类发烧友的。“你算什么玩意儿？”那两个牛仔气势汹汹地破口大骂起来，骂骂咧咧了好一阵才驱车离开，轮胎擦着地面发出刺耳的尖啸声，挡泥板剧烈地颤动着。

自打初中认识以来，爱达荷州默里迪恩的电脑迷们聚会的时候，马克斯就俨然成了大伙的非正式保镖。那时默里迪恩是一个中等社区，距博伊西八英里，一路上都是些零散的农场。一个世纪以前，小镇的先辈们将此地取名为默里迪恩，因为它的位置正好位于博伊西经线上。在美国陆地测量系统中，由 37 条南北向的无形的线构成 Y 轴，这条经线就是其中的一条。这大约是这个小镇唯一的掌故了，在小镇上，中学的牛仔竞技队吸引了所有的姑娘。

马克斯的父母年纪轻轻就结了婚[3]，在他还是个婴儿的时候，他们就从凤凰城搬到了爱达荷州。在某些方面，马克斯继承了父母双方最出色的品质：他的父亲罗伯特·巴特勒是一名越战老兵[4]和热心的技术迷，他在博伊西经营了一家电脑店。他的母亲纳塔莉·斯考拉普斯基是乌克兰移民的女儿，她是一位人道主义者和反战分子，喜欢看天气频道和关于自然界的纪录片[5]来放松自己。马克斯继承了母亲严谨的生活观念，除了一时鬼迷心窍尝试过嚼烟之外，他不吃牛羊肉、不吸烟、不喝酒，也不吸食毒品。从父亲身上，马克斯继承了对计算机的酷爱。从可以当办公桌用的大型商业机，到手提箱大小的 IBM 第一代便携式兼容机，各式各样琳琅满目的机器伴随着马克斯成长，马克斯八岁时就开始用 BASIC 语言编程。

在他 14 岁那年，父母离婚了，他平静的心绪消失了。他的父亲去了博伊西，而马克斯和母亲及妹妹莉萨在默里迪恩生活。父母的离异，使这位少年悲痛欲绝，也似乎使他形成双重的行为模式：一种是气定神闲，另一种是疯狂十足[6]。当他疯狂的一面发作时，没人能赶得上他；他的大脑以光速运转，像激光一样专注于眼前的任何任务。在他拿到驾照后，他驾着他那辆银色的尼桑车，把踩油门当成按开关一般，在停车标志牌之间超速行驶，他还戴着实验室护目镜，像一个正在做物理试验的疯狂科学家一样。

就像马克斯保护他的朋友一样，他的朋友也极力保护马克斯。他最好的伙伴