SPAM NATION

裸奔的隐私

你的资金、个人隐私甚至生命安全正在被侵犯!

[美] 布莱恩·克雷布斯（Brian Krebs） ◎著
曹　烨　房小然　◎译

写给互联网＋及大数据时代的网络安全读本

“万物互联”时代，
互联网用户如何应对有预谋、有组织的网络犯罪？

南方出版传媒
广东人民出版社

SPAM NATION

裸奔的隐私

你的资金、个人隐私甚至生命安全正在被侵犯！

〔美〕布莱恩·克雷布斯（Brian Krebs）◎著
曹　烨　房小然　◎译

SPM
南方出版传媒
广东人民出版社
·广州·

图书在版编目（CIP）数据

裸奔的隐私：你的资金、个人隐私甚至生命安全正在被侵犯！/（美）克雷布斯著；曹烨，房小然译．—广州：广东人民出版社，2016.2

ISBN 978-7-218-10630-4

Ⅰ．①裸… Ⅱ．①克… ②曹… ③房… Ⅲ．①计算机网络－安全技术－研究 Ⅳ．①TP393.08

中国版本图书馆 CIP 数据核字（2015）第 298067 号

Luo Ben de Yin Si

裸奔的隐私

[美] 布莱恩·克雷布斯 著　　曹　烨　房小然　译　　版权所有　翻印必究

出 版 人：曾　莹

策　　划：中资海派
执行策划：黄　河　桂　林
责任编辑：肖风华　古海阳　张　静
特约编辑：王　影　王利军
版式设计：王　雪
封面设计：WONDERLAND Book design 仙境 QQ:344581934

出版发行：广东人民出版社
地　　址：广州市大沙头四马路 10 号（邮政编码：510102）
电　　话：（020）83798714（总编室）
传　　真：（020）83780199
网　　址：http：//www.gdpph.com
印　　刷：深圳市福圣印刷包装有限公司
开　　本：787mm × 1092mm　1/16
印　　张：17　　**字　　数**：19.6 千
版　　次：2016 年 2 月第 1 版　2016 年 2 月第 1 次印刷
定　　价：39.80 元

如发现印装质量问题，影响阅读，请与出版社（020-83795749）联系调换。
售书热线：（020）83795240

权威推荐

《纽约时报》（*New York Times*）

克雷布斯报道了互联网极其阴暗的角落：利益至上的网络犯罪。罪犯通过医药销售、恶意软件、垃圾邮件、欺诈和劫持攫取数十亿美元的非法利润。最近，奥多比、塔吉特和内曼·马库斯等公司就深受网络劫持之害，克雷布斯先生就是第一个发现并揭露这些问题的人。很少有人像克雷布斯先生那样，勇敢地将网络地下世界曝光于世。

《今日美国》（*USA Today*）

垃圾邮件为何日益泛滥？作者作出了有趣而且惊心动魄的深刻探讨……从此，《裸奔的隐私》的读者将用不一样的眼光看待收件箱里的垃圾邮件。

《波士顿环球报》（*Boston Globe*）

《裸奔的隐私》是一本很强势的新书……错综复杂、扑朔迷离。克雷布斯为我们揭示了网络犯罪团体构建的邪恶地下世界；让我们吃惊地发现，在当今信息世界中，每个人的电脑都是黑客的猎物。

《彭博新闻周刊》（*Bloomberg Businessweek*）

克雷布斯在曝光网络安全弱点时所展露的才华，为他在 IT 界赢得了声誉，也令他在网络犯罪界引发强烈愤慨……他对独家新闻的追踪记录，使他成为少数以顽强地报道新闻而知名的博主之一。

《科克斯书评》（*Kirkus*）

克雷布斯带领读者游览了网络犯罪的地下世界。这是一个关于黑客、垃圾邮件制造者和网络诈骗犯的故事，一个充满了险恶情节的警世故事……这是一本令人大开眼界的著作，它令人沉浸在当前有组织网络犯罪的痛苦中难以自拔。

《出版商周刊》（*Publishers Weekly*）

克雷布斯利用长期不和的黑客和网络诈骗犯发来的大量信息武装自己，探究了垃圾邮件制造者如何以及为何可以如此猖獗地游走于法律之外。通过揭露的网络弱点，并跟随着财富的步伐，作者呈现了一个精彩、愉快的警世故事。在现今这个依赖网络的时代，克雷布斯的著作非常及时，蕴藏深刻的教育意义。

美国波音特媒体研究中心（The Poynter Institute），**新闻评论机构**

作为一名独立科技记者，布莱恩凭借一己之力，击败了网络的腐烂面……他在全世界网络罪犯和犯罪打击者之间布下情报网络，就像一名小说里的侦探那样一步步揭开真相。

《华盛顿自由灯塔》（*The Washington Free Beacon*）

在《裸奔的隐私》这本书中，作者布莱恩·克雷布斯带领读者游览有组

织网络犯罪者构建的令人生畏的技术世界……从某种程度上来说，天才黑客以及他们背后的机器人大军将是未来战争的主要诱因。而现在，幸好我们有布莱恩作为向导以及垃圾邮件过滤软件保护收件箱的安全。

《联邦电脑周刊》（*Federal Computer Week*）

《裸奔的隐私》是一本强大的编年史，剖析了发送垃圾邮件的龌龊勾当如何以及为何能够成功。

倾斜点（Slashdot），**科技资讯网站**

布莱恩·克雷布斯极其出色地讲述了这个故事一个重要的方面，并告诉你那些可以带来巨大改变的小事情。区区 200 多页，《裸奔的隐私》可谓一本轻巧的巨著。

先闻网站（Before It's News）

布莱恩·克雷布斯是一位著名的网络安全专家，他带我们深入探究这个地下世界，了解垃圾邮件行业的历史和文化，并谈及黑客团伙对网络犯罪行为的参与，包括身份盗用、僵尸网络、洗钱、数据破坏等。

《自动收货时代》杂志（*Vending Times*）

想要了解黑客犯罪和网络盗窃世界的秘密，这本书是最好的答案。

科利·多克托罗（Cory Doctorow）

“波音波音”（Boing Boing）**博客联席主席**

《裸奔的隐私》对垃圾邮件和网络犯罪的技术、伦理、经济、全球政治及商业的深刻剖析，作者的研究透彻，字里行间蕴藏巨大的人文关怀与热情。

田俊国，用友大学校长

用友网络科技股份有限公司副总裁

在人们尽情享受互联网带来的各种便利的同时，网络安全的隐忧始终如影随形，几乎人人都受到过垃圾邮件的骚扰、木马病毒的威胁，人人都承受着身份信息被盗、重要数据遭窃取的网络危害。布莱恩·克雷布斯在本书中大胆而无情地向我们揭露了网络安全背后的黑幕，又用类小说体将原本很专业、很枯燥的情节描述地形象生动。事关网民生存安危，又通俗易懂，可视作为网络安全普及读本。

SPAM NATION

目 录

第1章

向网络犯罪宣战

Parasite

你的邮箱是否经常塞满垃圾邮件？可曾想过这些垃圾邮件为何会进入你的收件箱？而点击邮件中的推销广告后，电脑运行速度却变得越来越慢？只要受到廉价商品的诱惑开始购买垃圾邮件中推销的商品，你的个人信息就会被神不知鬼不觉得收集起来！

深度剖析僵尸网络

莫斯科闹市区，一辆深蓝色宝马760缓缓驶过某十字路口的斑马线；另一辆黑色保时捷卡宴与它并排停下。正值2007年9月2日下午两点，苏哈列夫广场旁往常拥堵不堪的街道却稍显冷清，只有稀稀落落的游客和本地居民在两旁宽阔的人行道上信步闲逛。条条街道沐浴在午后尚有余温的阳光下，古旧建筑也开始竞相投射出长长的阴影。

宝马车驾驶员是本地臭名昭著的网络诈骗专家，黑客名为恰克。那一天，恰克初为人父，他刚刚和车上的乘客痛饮伏特加，来庆祝人生中这一重大时刻。此时天时地利具备，他准备和保时捷驾驶员一较高下。二人心照不宣同时发动引擎，准备在这直道上短短地赛一程，终点就是前方的城市广场。

交通信号灯转绿之际，橡胶轮胎与水泥路面摩擦的刺耳声迅速传到数百米外的广场之上。路人纷纷停下脚步，转身回望。两辆车如离弦之箭冲出十字路口，争先恐后冲向终点。

正以超过 200 公里时速掠过赛程中点的宝马车却突然失去控制，与保时捷发生侧撞，之后一头斜插到路边的灯柱上。比赛瞬间结束，不过双方都不是赢家。宝马被灯柱切成两半，保时捷也变成一堆废铁，在旁边静静地燃烧着。两辆车的司机爬了出来，一瘸一拐地逃离事故现场。但宝马车上的乘客却惨遭不幸：一位名为尼古拉·马克罗的 23 岁青年当场死亡。他就职于一家互联网公司，前途无量，此时却被压在这辆报废的豪车之下，身首异处。

被朋友们称为柯里亚的尼古拉·马克罗其实在互联网犯罪圈子中小有名气，他还是家族企业马克罗互联网公司（与他的姓氏相同）史上最年轻的员工。当全世界的执法机关如梦初醒，开始意识到有组织的网络犯罪正在对众多金融机构和企业组织造成威胁时，马克罗互联网公司早就在这个法律真空地带赚足了名声：网络骗子们可以租用马克罗互联网公司的服务器放心大胆地开立商铺、尽情投资、构筑阴谋，根本不必担心国外执法机关找自己的麻烦。

就在柯里亚殒命之时，世界上通过“机器人网络”发送垃圾邮件的肮脏生意正如火如荼地进行，而像马克罗互联网公司之流的虚拟主机运营商就是这些生意的最大母巢。遭到黑客攻击或被恶意软件[①]侵染的个人电脑群组往往被冠以僵尸网络[②]之名，能够为黑客们提供远程操作的便利。通常，这些电脑的主人就算被征用为“傀儡”也会浑然不觉。

在马克罗互联网公司操控之下的僵尸网络每天都会向外辐射数以千万计的垃圾邮件，封堵电脑用户的邮箱和垃圾邮件过滤器。不过，

①恶意软件，指在计算机系统上执行恶意任务的病毒、蠕虫和特洛伊木马的程序。

②僵尸网络，指采用各种传播手段使大量主机感染 bot 程序（僵尸程序）病毒，从而在控制者和被感染主机之间形成一个可一对多控制的网络。

马克罗互联网公司的服务器却不会编写、发送任何垃圾邮件，否则便会吸引网络警察和西方执法机构的注意，成为众矢之的。相反，它仅会利用僵尸主控机远程操控全球数以百万计的个人电脑，驱使它们成为喷吐垃圾邮件的傀儡机[①]。

当医护人员清理了车祸现场后，这血腥的场面就被人上传到他的朋友及客户频繁造访的俄罗斯网上论坛。率先上传柯里亚死讯的是来自 Crutop.nu 的用户。Crutop.nu 是一个坐拥 8 000 余名会员的俄语黑客论坛，豢养着垃圾邮件界臭名昭著的巨头们。Crutop.nu 中的部分成员是马克罗互联网公司虚拟主机的忠实客户，他们在互联网上宣布了柯里亚的死讯，其中包括文字信息和图片文件。很多人还自发（或是在论坛管理员的奚落下良心发现）担负了柯里亚的丧葬费和家庭赡养费。这在当时算得上是网络犯罪界的一件大事。

数天后，莫斯科一群制造电子垃圾的乌合之众前往柯里亚的葬礼吊唁。葬礼在柯里亚 23 年前出生时受洗的教堂举行。吊唁者包括当今世界最大的垃圾邮件制造者，也是本书的两个关键人物：SpamIt 和 GlavMed 的共同管理员，“Desp”伊戈尔·古谢夫以及“圣徒 D”德米特里·斯图平。

前去扶灵的还包括德米特里·奈奇伍德，此人也是一名黑客，绰号“古格”，当年 25 岁，是 Cutwail 僵尸网络的核心成员之一。Cutwail 堪称网络犯罪界的大杀器，曾在全世界内感染，并且暗中操控数以千万计的家庭计算机，代之发送海量垃圾邮件。奈奇伍德也借此牟取暴利，单是为 GlavMed 和 SpamIt 两家主顾捉刀，就能足

①傀儡机，被黑客远程操控的机器。黑客通过黑客软件进行攻击，如果计算机被感染，病毒会在系统开一个后门，方便黑客在需要时对计算机进行控制。

不出户轻松赚取数百万美元。虽然主管职位几度易手，但时至今日，Cutwail 仍是世界上规模最大且最为活跃的僵尸网络之一。现在它正由几位赫赫有名的人物管理维护。

在这起网络犯罪里程碑式的事件中，我们为什么要着重介绍以上三位人物？因为他们（柯里亚及其数以百计的同侪们）匠心独运的杰作将以一种怪异但却至关重要的方式影响着地球上每个人的日常生活——垃圾邮件。

毋庸争辩，垃圾邮件的出现确实推动了恶意软件（即每天攻击你和我以及所有人的家用电脑的恶意程序）的长足发展。通过垃圾邮件，黑客得以定位我们的身份，攻陷我们的安全防护机制，将我们的经济状况、家庭信息甚至社交圈子摸得一清二楚。作为网络世界的虚拟寄生虫，僵尸网络亟须殷切的护理和持续的“喂养”才能在技术上保持先进，从而领先杀毒工具和杀毒软件企业，即帮助家庭计算机杜绝网络侵害的企业。为了保持“宿主”旺盛的生命力，垃圾邮件制造者（或称为“僵尸主控机”，这两个术语可以互换）必须贡献出持之以恒的努力来传播“数字疾病”并辅以变异，借以寻求技术支持。由于杀毒程序能够清剿“宿主”中的恶意程序，僵尸网络运营商必须向新“宿主”发动持续攻击，夺得控制权，并探寻新途径，将以往的“宿主”再次拉下水。

为避开日益升级的杀毒软件以及垃圾邮件防御系统的围追堵截，这场技术上的军备竞赛需要不断开发、生产和分配隐蔽性极强的恶意软件。因此，黑客们通常会将垃圾邮件赋予“自保”属性。为了感染更多的计算机，喷吐老式垃圾邮件的僵尸网络通常会被用来散布包含新版恶意软件的电子邮件。另外，邮件制造者也会将一部分收入用于

再投资，来开发破坏力更强、更加隐秘的恶意软件，借以攻破杀毒软件、防垃圾邮件软件以及防火墙的三重围剿。这种在技术和社会双重意义上的犯罪机器俨然已成为一个自给自足的生态系统。

迄今为止，传播海量“数字疾病”的网络罪犯已鲸吞了网络安保企业羽翼下的大片安全领土。杀毒软件企业曾做出过一份报告，声称他们平均每天要将 8.2 万种新型恶意软件进行分类并予以查杀，而网络罪犯开发恶意软件的根本目的就是感染家用电脑，使之沦为傀儡机，以供网络犯罪者远程操纵。杀毒软件大鳄迈克菲（McAfee）也曾发表声明，仅在 2013 年第一季度，该公司就检测出 1 400 万种新型恶意软件。

不过对垃圾邮件制造者来说，这样一套生态系统造价不菲。以 Cutwail 为例，系统的维护需要软件开发以及技术支持团队 7×24 小时连轴运转。像 Cutwail 这样的大型僵尸网络通常都会承担一些外包业务，而承租者（即其他垃圾邮件制造者）为了满足犯罪目的，经常会要求进行代码调整或开发附加组件以维持僵尸程序正常运转。

伊戈尔·维什涅夫斯基是莫斯科人。他 30 多岁时，正在为 Cutwail 效力，也是奈奇伍德的亲密战友，在黑客界声名煊赫。不过后来维什涅夫斯基决定开创自己的事业，开发了一个新系统与 Cutwail 分庭抗礼，喷吐垃圾邮件、承接外包生意。在本书中，他成为我们的导游，带领我们探索邮件制造者构筑的庞大、神秘又不为人知的地下世界。在一次即时消息会话中，维什涅夫斯基曾提道：“我们为了支持古格（即奈奇伍德，他的绰号与 Google 的读音有异曲同工之妙），曾为他单独设立一间办公室，并提供编码员和其他技术支持。有时候我会去拜访他，但从不在那里工作。”据他讲，为满足客