<<密战>>

图书基本信息

书名：<<密战>>

13位ISBN编号：9787111332657

10位ISBN编号：7111332652

出版时间：2011-3-10

出版时间：机械工业出版社华章公司

作者：Joseph Menn

页数：211

译者：徐旭铭

前言

2004年当我第一次遇到Barrett Lyon的时候，我正在旧金山的办公室里为《洛杉矶时报》撰稿，稿件内容正是关于互联网安全的。
他的故事实在是太吸引人了（完全能满足记者的好奇心），乍听之下我几乎很难相信他说的都是真的。

一年以来，我一直都在和紧迫但又复杂的故事搏斗。
基本上每个星期我都要介绍一个在全世界范围里产生影响的新生计算机病毒。
其中很多确实造成了实质性的冲击，致使大量公司的网络瘫痪或者是在电子邮箱里塞入太多的垃圾邮件，最终导致它们开始拒收合法邮件。
即便如此，有时候也会很难在下一天的报纸截稿之前把问 题解释清楚——特别是在病毒利用了一些很隐蔽的软件漏洞的情况下，即使是专业的研究人员也仍然需要时间努力设法理解它们。

棘手的不仅仅是技术上的阐述。
那时除了仅有的几个不方便给出名字的痴迷研究员以外，几乎没有英雄人物。
而罪犯则通常都神龙见首不见尾。
如果他们真的被抓到，你会发现他们往往都是一些游离在边缘社会的青少年。

然而时代总是在不断发展变化的。
当我们的世界越来越多地被计算机连接起来，并且在更多的事情上依赖它们的时候，不法分子也开始蠢蠢欲动。
更糟糕的是，仅仅是为了恶作剧而释放出来的病毒正在被那些用来敛财的病毒所替代。

接着就出现了一系列新型的互联网攻击，这些攻击从技术上比之前的病毒要容易理解得多，它们展现了一种全新的犯罪形式。
匿名的攻击者只需要用大量伪造的流量来冲击商业网站即可令其彻底瘫痪。
要想停止攻击，他们要求受害人至少汇3万美元到某些东欧国家去。

我拜访了一些受害公司，想要找到一些线索来完善我的故事，这样读者就可以从中学习到有用的东西。
很快地我就听到了计算机防御专家Barrett Lyon这个名字。

当时他还是一个谦虚的年轻人，但是非常聪明，善于表达自己。
他曾与那些攻击者进行过交谈。
没错，他知道其中一些人的名字。
或许他碰巧还保留了一些对话的记录？
你猜对了。
不要以为警察会对这些东西有兴趣，通常他们在碰到计算机犯罪的时候很容易就放弃了。
你想问为什么？
因为无论是在英国还是俄罗斯，都有 FBI、特工，以及国家有关部门来打理。
这些传说愈演愈烈，最终我们看到了一幅有组织犯罪的全景图。

然了，Barrett擅长抵御的那类攻击只是一个更大的迅速扩散的问题中比较引人注意的一个方面而已——技术进步给犯罪带来的帮助甚至比它们为消费者带来的好处还要大。
在线欺诈和身份盗窃的数量不断猛增，一个完整的地下产业也在不断成长。
类似针对信息经纪商ChoicePoint和零售商T. J. Maxx这样的大规模数据掠夺的消息已经多次登上报纸头条了。

到2009年为止，30%的美国人都成为了身份盗窃的受害者，公司和个人每年在互联网犯罪这一项上要损失大约一万亿美元，人们对于电子化经济的信任以及信息基础设施的稳定都在不断消磨。
它不再光是钱的问题，而是事关国际政治和计算机战争事务了。

私家研究人员或许可以解释一个病毒和之前的版本有什么区别，执法部门可以抱怨针对身份盗窃的起诉一旦离开本国就会被拖延到无人问津，相当一部分学者教授谈 论起东欧的政策时也可以滔滔不绝。

但即便恐惧的气氛上升到就连总统巴拉克·奥巴马也要发表演讲来讨论计算机犯罪、计算机间谍，以及计算机战争的大规模危机，几乎没有人可以从全局上讲出一个所以然来。

Barrett Lyon又一次证明了自己的能力。

我了解到他那时就已经成功渗透了俄罗斯和美国的帮派，而且还能保护自己的身份不泄露，他借用的是FBI的马甲。

这些工作一直到现在才被披露出来。

接着，我们又遇到了英国特工Andy Crocker，他手里的线索让他比之前任何西方人都更深入地渗透苏联——而他的历险之前从未被详细报道过。

我们一起回忆了历史上最大规模的跨国计算机犯罪追捕行动，就好像一名俄罗斯秘密警察在杯酒交盏之间现身说法一般。

他们的故事加在一起是目前为止对这个规模数倍于贩毒的影子经济最大的曝光。

这个影子经济早已影响到了国家政府，甚至可能会逐渐削弱西方社会的富裕和安定。

本书描述了两个男人所完成的前无古人的伟大成就。

但同时这也是对早已在酝酿中的灾难所发出的警告。

2009年年中的时候，在政府的一些秘密小圈子里关于Barrett Lyon和Andy Crocker的事迹被传得满天飞。

他们甚至被邀请飞往华盛顿去给美国政府及其盟友的一百多名顶尖间谍授课。

即使是这样，仍然有很多官员抓不到其中的重点。

最终我们的两位英雄只好选择向政府辞职。

针对计算机犯罪，不应该指望专业人士能处理好一切。

读过本书后你就能理解其中的缘由了。

<<密战>>

内容概要

2004年的时候，加利福尼亚的计算机高手Barrett Lyon注意到一名多次攻击商业网站的黑客。
在尽可能不引起对方警觉的情况下，他展开了一场跟踪调查，并发掘出一帮俄罗斯黑帮。
计算机犯罪一直以来都在不断演化升级。
它不再是过去那种小偷小摸的把戏，而是早就形成了严密的帮会组织。
最初他们只会攻击一些公司的网站，但是现在正越来越多地开始偷取客户的商业数据，甚至政府的国防机密。

在Barrett调查这项高科技犯罪的时候，美国政府也正在迎头赶上。
不过在英国，情况则完全不同。
在20世纪90年代末，女王亲自将安全的电子商务列为国家安全的头等大事。
伦敦国家高科技犯罪小组的探员找到Barrett，希望得到他的帮助。
他们还派出了Andrew Crocker探长（他之前在威尔士当过拳击手）前往俄罗斯跟踪抓捕黑客，并设法找出他们究竟是在为谁工作。

本书揭露了俄罗斯网络暴徒和美国黑手党之间在互联网上爆发的大规模冲突。
从旧金山到哥斯达黎加，再到伦敦和俄罗斯，本书引导读者深入了黑客阴暗的地下世界。
展示了Barrett Lyon和Andrew Crocker是怎样步步接近这些之前从未有人成功接近的地下经济大鳄。
这些故事将会告诉你计算机犯罪远比你想象的更糟糕，以及为什么互联网有可能会无法生存。

作者简介

梅恩（Joseph Menn），十年前就开始为《洛杉矶时报》报道计算机安全以及其他的技术问题，现在则是《金融时报》的撰稿人。
他是2003年出版的《All the Rave：The Riseand Fall of Shawn Fanning SNapster》一书的作者，同时还曾两次角逐GeraldLoeb奖（商业报道里的最高奖项）。

<<密战>>

书籍目录

章节摘录

第1章 战争游戏　　在到达哥斯达黎加之后，Barrett Lyon已经迫不及待地想要见到他的新客户了。
那是在2003年圣诞节之后的第二天，这名来自加利福尼亚塔霍湖旁边的25岁的计算机专家即将会受到英雄般的欢迎。
这架早班飞机飞离了旧金山国际机场穿过冬日的云层冲上云霄。
Barrett看了一眼身边美丽的深褐色头发的女孩，感到自己正迈向美好生活的一个全新阶段。
BetcRIs（Bet Costa Rica International Sports）不但为他支付了旅行的全部费用，连他女友Rachelle Sterling的费用也一并支付了。
这是他们第一次一起飞行，也是她第一次出国。
他希望这可以缓解过去六个星期以来的紧张情绪。
　　Barrett知道自己现在对BetCRIs的热情一定是很不理智的，因为他要保护这家素未谋面的哥斯达黎加公司免受攻击，敌人不但看不见，而且极可能身在别的国家。
在他们，位于萨克拉门托的狭小公寓里，Rachelle绝大多数时候看到的Barrett都是他把自己六英尺高的身躯蜷缩在环形办公桌的后面。
Barrett每天至少有20个小时睡眼惺忪地坐在计算机前，紧紧盯着他正在跟踪的网络攻击。
甚至连他答应过她的感恩节家庭聚会都忘记了。
因为他正在忙着完善自己的程序和配置。
他实在是太专心了，当女友带给他打包的感恩节火鸡时，甚至连谢谢都忘记说，更别提向女友解释他到底在做什么了㈢。
　　对Barrett来说，这是一场多年难得一见的战斗，这让他想起了《战争游戏（warGames）》，这是一部1983年的老电影，在他的墙上还有一张当年的电影海报。
在电影中，一个从未上过学的天才儿童在玩线上游戏的时候无意中闯入政府的超级计算机，几乎引发了第三次世界大战。
Barrett认为他略过了那些刚开始的错误，直接跳到了好玩的部分。
他正在试图阻止一场计算机战争，这场战争可能会导致现实生活中的人们失去工作和金钱。
　　BetCRls每年在体育博彩上投入成百上千万的美元，这让它成为全世界最大的博彩公司之一。
并且它还是第一个尝试为来自美国的客户寻找合法的海外避难所的公司。
然而在旺季的时候，它的网站不断地遭到恶意攻击并致使网站崩溃，这让赌客放弃在它的网站上继续下注，BetCRIS每天为此的损失高达500万美元。
Barrett并不知道那些高科技罪犯是受雇于其他竞争的博彩公司还是出于他们自己的本意。
但无论是哪种情况他们都在试图向公司敲诈钱财——计算机时代勒索保护费的典型案例。
如果这些不法分子成功的话，他们一定会变本加厉地去攻击其他公司。
　　去年春天，BetCRIS网站最初出现问题的时候还没有引起公司总经理Mickey Richardson的警觉。
在哥斯达黎加的首都圣何塞，有一栋七层楼高的大厦，大厦的外部是黑色的玻璃，它不但可以隔热还能阻隔人们好奇的目光。
在那里，电话像往常一样响个不停。
但是通过800电话的下注只占公司业务的很小一部分。
一年多以来绝大多数的赌资都来自于网络，赌客们坐在家里或办公室中就可以下注了。
然而在那个春天的某一周，BetCRIS开始收到很多网页访问缓慢的投诉。
“网站到底是怎么回事？
”Miekey失控地大声吼遭，只要不是涉及钱的问题他还算是一个不错的人。
工程师Glenn Lebumfacil查看了日志，发现虽然存在大量的访问记录，但是那些都不是真的赌客。
来自全世界各地的计算机访问都诵向BetCRIS.com然后又立即离开。
Glenn对其中的原因完全摸不着头脑。
这种神秘的情况持续了好几天。

有一天早上Miekey在查看邮件时，收到了一个令人大吃一惊的解释外加一封勒索信。
一位匿名黑客洋洋得意地宣称是他策划了针对Mickey网站的’拒绝服务攻击，这是一种利用大量虚假的信息请求来冲击网页的攻击手段。
和那些在互联网泡沫时期致使雅虎和eBay网站瘫痪来吸引眼球的青少年黑客不同，他只要球对方一次性通过在线支付服务e-Gold支付500美元就行了。
“小意思”，Mickey太声说道。
他在当地_的一个寿司店里随便一个晚上就能花掉那么多。
Mickey决定付钱。
但是他想，亡羊补牢，为时未晚。
下一次的代价可能会更太。
所以Micker打电话给他认识的最厉害的技术专业人士，在需要抵御这种攻击的时候可以到哪里去寻求帮助。
当他找到拉斯维加斯顶尖的博彩公司Don Best Sports的时候，这位商业盟友向他介绍了这个来自加利福尼亚韵孩子，并对他赞不绝口。
说他在一年前帮助他们抵御了一场类似的攻击——这个热情又亲切的网络高手就是Barrett Lyon。
Mickey给Barrett打了个电话解释了一下事情的经过。
因为事情还不到不可收拾的地步（BetCRIS还能够运营），BalTett给了他一些免费的建议。
他告诉Mickey从马萨诸塞州一家专业生产阻碍恶意网络流量设备的公司Top Layer购买两台机器。
Miekey花了2万美元购买设备，然后Barrett帮助Glenn把设备配置好。
如果这种情况再次发生，我们也不用担心了，Mickey想6几个月以后，Mickey开始从好朋友那里听到了一些流言。
新的计算机攻击席卷了他的竞争对手，经过了最初的一些抵抗后，绝大多数海外受注网站都选择了破财免灾。
“这些混蛋太野蛮了，根本没办法阻止他们。
”其中一个朋友警告道。
没有付钱的一些网站被迫关闭了将近：一个月。
他们蒙受了巨大的损失，因为赌客都转向了其他网站，令他们失去收入。
有些网站再也没能重开，因为愤怒的赌客无法收回他们账户中的资金，并且控诉他们欺诈。
现在那些敲诈犯要求每年支付3万美元来免受攻击。
Mickey暗自偷笑，因为他只付出了500美元和一些新设备的代价而已。
接着厄运再次降临到他的头上。
就在感恩节前一个星期六的早上八点之前，他收到了一封电子邮件。
“你韵网站将会遭到攻击。
”信中要求他在第三天中午之前支付4万美元来换取一年的平安。
一年中最大的博彩周即将开始，不但有职业的和大学的橄榄球比赛，还有篮球比赛。
“如果你选择不付钱，那么你可能就无法再继续运营，因为在未来的二十个星期里每个周末你都会受到攻击。
”信中说道。
Mickey问Glenn，Top Layer的设备能不能抵御攻击。
“我们应该是安全的，我觉得我们的网络状况良好。
”Glenn说道。
但他完全不知道那些不法分子比去年强了多少倍。
他们已经控制了成百上千台电脑来进行“分布式”拒绝服务攻击（也叫做DDoS），这就是说恶意的流量会从世界各地同时涌过来。
一旦电脑被转变成僵尸，或者说受控于隐身的主人，它们能以多种方式发动攻击。
Top Layer的设备只能阻止一些基本的攻击方式。

在Mickey拒绝回应攻击者的第一封电子邮件后，一场巨犬的拒绝服务攻击席卷而来，不出十分钟Top Layer的机器就被攻陷了，BetCRIS的网站也随之瘫痪。
这轮攻击同时还击溃了BetCRIS的互联网服务商Digital Solutions以及哥斯达黎加一半的博彩公司。
Digital Solutions很快不得不把BetCRIS从网络上断开，暂时取消网站的访问。
……

媒体关注与评论

“《密战》准确地揭露了神秘的跨国计算机企业寡头以及他们价值数亿美元的生意，证明了计算机犯罪不但可以获利，而且利润惊人。
” ——Richard A.Clarke美国前总统小布什的计算机安全特殊顾问《Against All Enemies：Inside America.S War on Terror》一书的作者 “作者将我们领入一个真实的地下世界。
在这里，罪犯的身份、恶意代码和攻击行动时时刻刻都在发生变化。
他敏锐犀利的旁自令读者无法释卷，而他对计算机犯罪和国家安全之间界线模糊的全球事务的解析将迫使公司、执法人员，以及普通大众重新思考如何安全地浏览和保护我们早已混乱不堪的互联网。
” ——Gbeg Garcia 美国国家安全局计算机安全与通信前助理秘书Garcia Strategies.LLC总裁“作者引领我们深入当今计算机安全威胁和干扰背后的特质与政治。
对这种均衡的迫切需求突显出为什么未来的互联网更需要仰赖人性的善良，而不是什么技术上的银弹。
” ——Jonathan Zinrain哈佛法学院法律教授Berkman Center for Internet&Society联合创始人《The Future of the Internet And How to Stop It》一书的作者

<<密战>>

编辑推荐

《密战：网络犯罪大追踪》是一部惊心动魄的网络犯罪追踪小说，《福布斯》、《商业周刊》等众多主流媒体热评好书！

一部惊心动魄的网络犯罪追踪小说，《福布斯》、《商业周刊》等众多主流媒体热评好书！

版权说明