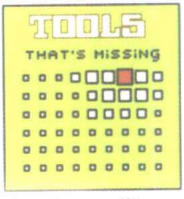
网络文化丛书

新刺客

网络时代的黑客

张奇志 谢春雷
●编著



世界图书出版公司

新　刺　客

——网络时代的黑客

张奇志　谢春雷　编著

世界图书出版公司
上海·西安·北京·广州

图书在版编目(CIP)数据

新刺客/张奇志,谢春雷编著. - 上海:上海世界图书出版公司,2001.3
(网络文化丛书)
ISBN 7-5062-4899-9

Ⅰ.新... Ⅱ.①张...②谢... Ⅲ.计算机网络 - 普及读物 Ⅳ.TP393.49

中国版本图书馆 CIP 数据核字(2000)第 86288 号

网络文化丛书

新 刺 客

——网络时代的黑客

张奇志 谢春雷 编著

上海世界图书出版公司出版发行
上海市武定路 555 号
邮政编码 200040
上海竟成印刷厂印刷
各地新华书店经销

开本:850×1168 1/32 印张:9.125 字数:204 000
2001 年 3 月第 1 版 2001 年 3 月第 1 次印刷
印数:1—5 100
ISBN 7-5062-4899-9/Z·133
全套定价:60.00 元(共 4 册,每册 15.00 元)

目　录

第一章　危机笼罩的网络时代

一个幽灵，一个网络时代的幽灵，在新的世纪游荡。

这个幽灵隐藏在田园诗一般的网络空间，随时可能使世界秩序分崩离析。

这个幽灵是一个电脑迷，或者说是一个电脑程序迷。

它的英文名叫 HACKER，它的中文名叫黑客。

HACK 本意为“砍”，所以“黑客”就指那些通过高超的技能入侵系统的人。黑客作一些事情常常只是为了挑战自己的智力，或者为了一己之乐，但是他们的行为与社会另外的群体利益安全是如此的关系重大，以至于不少黑客因为过人天赋而使自己陷入政治或法律的斗争与惩罚之中。

所有的黑客几乎都是身份平凡的程序员或编程爱好者，但他们的破坏力往往远远超过声名显赫的政客。

他们祭起个人英雄主义的大旗，试图证明自己超凡的智慧和过人的能力。有不少的电脑青年以做黑客为荣。

邻家那个忧郁的男孩，公司里那个迷恋电脑的年轻工程师，你身边的他或她，也许就是“大闹天宫”里的“现代孙悟空”——黑客。

第一节　网络攻击战的预演

1．想像《黑客帝国》时代

故事发生在22世纪。和许多电脑迷一样，程序员尼奥(Neo)也常常入侵一些系统。他是一个黑客。他并没意识到他会担任拯救人类的重任。像他这样的玩家当然还有很多，整个世界似乎在有条不紊地运行。

但是，一些玩家逐渐发现了，自己和周围的人全部生活在一个程序之中。也就是说，每个人的生活似乎都在正常进行，但实际上所有的进程和发展都由一个程序在进行管理和控制，人们实际上没有了选择和创造生活的权利。

由于资源的枯竭以及生存环境的恶劣，实际上地球已经不再具备人类生存的条件了。

统治者为了稳定人心，编写了一个叫“Matrix”的程序来管理这个世界。绝大多数人们并不知道自己正生活在一个程序之中，一个虚拟的世界里，他们的生活似乎还跟以前一样。但是从局外人看来——比如，假设在遥远的星球有一群生物正注视着地球的人类，在他们的眼睛里——整个地球人类的发展就像MUD游戏，每个人都是玩家，而统治者则是对任何玩家都有生杀予夺权利的“巫师”。玩家们苦苦奋斗却不知早已被牢牢控制。

为了夺回对“Matrix”的管理权，实际上为了从虚拟世界解放中获取自由，包括Neo在内的黑客联合起来向统治者发起攻击……

这就是美国大片《黑客帝国》(也曾译作《22世纪杀人网络》)的故事梗概。该片原名Matrix,直译是"矩阵"。Neo们最终成功地通过攻击Matrix程序的破绽,改写了程序。

可能大多数的人们还认为影片情节太过虚幻,但实际上并不尽然。当我们的生存步入数字化之后,谁能说这种情况不会出现呢?

让我们来虚妄地设想一个完全数字化生存的时代。在这个时代,我们的个人记录储存在电脑里,我们的货币是电子货币(实际上是银行电脑里一串数据),我们的交易也通过网络来实现,甚至,我们的人际交往也通过电脑网络来进行,意味着我们可能有很多朋友,可是我们又素昧平生。倘若有一天,一位技术高超的黑客恶作剧地侵入系统删除了你的资料(也可能是电脑糊里糊涂丢失了你的记录),于是,你失去了网络社会的身份,你无法再通过网上交易获得生活物品,无法再通过网络与别人交流,你作为物理的人仍然存在着,但是实际上你已经被宣告在网络社会里死亡,即使走在大街上也没有人认识你相信你,当然也不会帮助你,因为在他们的(网络)世界根本没有你这个人。

有人说网络化生存是人类未来发展的一种必然趋势。可是我们怎样约束黑客的行为来保证社会秩序的安全?如果我们消灭黑客,我们又怎样监督网络社会统治者的行为以保证人类个体的权利?

不少人开始认为网络网住了未来,"未来的世界和在未来世界中生活工作的人,将离不开网络,就像离不开空气、水和钱一样"。

不过网络也是脆弱的,它不能也不应该被神化。网络的确使我们的生活变得更为快捷便利,但是如同许多新技术变

革都在带来方便与实惠的同时也会带来更大的风险一样，网络的出现和发展也使人类在享受现代技术服务的同时面临更大的风险。自工业革命以来，交通工具在陆、海、空方面无不取得飞速发展，但与此同时，频繁的交通事故也在发生。一种技术在一个领域应用，一般只带来这个领域的利益和风险；一种技术在社会各个领域应用，就会带来各个领域的利益和风险。网络是属于后者。迄今为止，还没有任何一种技术像互联网这样深入地影响人类社会的各个领域，但是网络系统只要不是100%的安全，就意味着人类社会各个领域都面临风险。

黑客不是网络安全的最大敌人。网络安全的最大敌人是系统本身的破绽。千里长堤，溃于蚁穴，系统一个微小破绽也许就会酿成系统的崩溃。南半球一只蝴蝶搧动翅膀激起的气流，到北半球有可能形成一场龙卷风，这种"洛伦兹效应"谁说它一定不会出现在网络系统？如果网络系统真没有破绽也未必就是好事，《黑客帝国》里的 Neo 恰恰是利用程序的破绽才修改了程序，拯救了人类。

在每一个时刻，总会有人推动技术发展，而另一些人关注着技术的弊端，两者使技术与社会最为合理地向前进步。

怕就怕，强权与独裁进入数字社会，那是比黑客入侵更为悲哀的事！

2. 网络攻击战的预演

1999 年底 2000 年初，好莱坞推出的以网络为主题的影片《黑客帝国》风靡全球。

这部影片虽然只是科幻，但是他对人们思想的震撼和影响仍然是极其巨大的。一个 14 岁的泰国小男孩 Withit Kham-

phirarak 看完这部影片后走火入魔，上吊自杀。

正当人们对影片的描述觉得荒诞之时，黑客攻击战却在现实生活中出现了！

美国东部时间 2000 年 2 月 7 日上午 9 时 15 分，全世界各地成千上万的国际互联网用户跟平常一样打开电脑，准备登录雅虎网站。雅虎网站是继美国在线之后排名第二的大网站，现有注册用户达 1 亿个，平均每天传送的资料多达 4.65 亿页，每月吸引的访问者多达 4200 万人。

但是这一天，许多人都感觉到情况有所不妙，有超乎寻常的大量数据在同时向“雅虎”涌来。“雅虎”遭袭击了！大惊失色的技术人员赶紧采取紧急措施，一边查明黑客的袭击手段，一边立即进行紧急补救。此时正是一年中网上购物最活跃的时候，如果不能及时恢复服务的话，那么就意味着数百万美元的交易将落空。

然而，袭击在不断升级，最高峰的时候，雅虎网站平均每秒钟遭受一千兆字节数据的猛烈攻击，这一数据量相当于普通网站一周的数据量！面对如此猛烈的攻击，“雅虎”的技术人员束手无策，只能眼睁睁地看着泛滥成灾的电子邮件垃圾死死地堵住了雅虎用户们上网必经的路由器。

10 时 15 分，汹涌而来的垃圾邮件堵死了雅虎网站除电子邮件服务等三个站点外所有的路由器，雅虎公司大部分网络服务陷入瘫痪，公司不得不将网站入口关闭。此时，美国的雅虎用户根本无法登录雅虎的任何站点，而世界各地其他的用户也只能登录“雅虎”59% 的站点。

13 时 25 分，雅虎公司的技术人员终于设法识别出了电子邮件的数据类型，并且加上新的邮件过滤器将其滤去，这才部分恢复了正常的服务，有 70% 的网站重新为用户提供服务。

然而，恶梦才刚刚开始。

第二天，黑客攻击越发疯狂。著名网上零售商店“亚马逊”传出遭黑客围攻的消息，下午5点前后，该零售网站的服务器速度大幅下降，运行速度慢得跟蜗牛爬一般。过了15分钟后，只有平时1.5%的网客能够进入网址，直到1小时后才恢复正常。美国有线新闻网(CNN)的网站也因遭到攻击，从下午7点一直瘫痪到晚上9点。而拍卖网站ebay也开始出现问题，网站从下午3点20分开始遭到攻击，瘫痪的时间差不多长达一天，许多人无法进行买卖。

截至1999年底，ebay网站的注册用户高达1000万，每个月的点击率高达15亿次。遭到黑客攻击后，ebay发言人瑟埃尔女士表示：“初步迹象显示，我们遇到了所谓的瘫痪服务攻击问题，但仅发生在静态网页，并未影响到我们的搜索、竞标或开价功能。”瑟埃尔说，ebay于格林尼治时间9日凌晨0点01分左右在网站上张贴公告，通知用户发生问题的信息。随后ebay发表声明说，在美国标准时间晚上7点以前，除了若干图形档案，所有服务均已全部恢复。

最惨的还是刚上市的超市网站Buy.com。Buy.com网站从上午10点50分出现罕见的大塞车现象，直到下午2点才恢复正常，被黑客足足折腾了3个小时。该公司认为黑客是有备而来，以大量的垃圾霸占网站，令他人无法进入。

2月9日，黑客继续对一些著名网站发难。ZDNet不得不于上午7时暂时关闭。E-Trade在上午也遇到了塞车问题，黑客直到10点才陆续撤退。

3. 攻击手段极其简单

此次网络攻击，黑客使用了一种名为“拒绝服务”(“DDOS”

手段)的方式入侵网页:在不同计算机上同时用连续不断的服务器电子请求来"轰炸"网站,泛滥成灾的电子请求堵塞了帮助上网者找到所需目标的路由器,造成网络瘫痪。这种方式类似于有人通过不停地拨打某公司电话来阻止其他电话打进,从而导致公司通信发生故障。据悉,雅虎网受袭击期间,其网站每秒有10亿字节的信息蜂拥而至,数量超过一般商业网站一年处理的信息量。

看起来有人可能只需坐在温暖的家中敲击几下键盘就可以使全球范围内的电子商务经营活动陷入混乱。

可以造成这种破坏作用的软件使用起来非常简单,而且可以很容易在遍布因特网的地下黑客网站上获得。登录这些黑客网站的人可以下载一个小程序,然后将它植入世界各地的计算机。此后只需按下某个按钮,这些个人计算机就会被激活并且"投入战斗",向某个网站发送一个简单的登录请求,并且不断重复,每秒钟可以重复发送几千次。

美国联邦调查局属下的国家基础建设保护中心,在去年12月已向各大网站发出警告,称有证据显示黑客会使用一种在全球各地电脑潜伏、伺机同时发难攻击的"DDOS"手段,进行网上攻击。由于这些工具很容易在网络找到和下载,所以根本防不胜防,加上黑客从不同的地方万箭齐发,攻击点太多,并且全是假冒的网址,实在很难找到躲藏在背后发动攻袭的黑客。

电脑专家称,使用"DDOS"的黑客,会在攻击数天以致数月前,先在多部大型服务器电脑(通常为大学电脑)内秘密安装"袭击程序",在发难时,才向它们发出信号,共同轰炸一个目标,情形就像数以千万计的人同时打一个电话号码,令真正要打电话者无法打通。

一名专家指出，黑客使用“DDOS”技术进行的“拒绝服务攻击”，其实早在多年前已经存在，只是近来技术不断进步，令攻击者可以通过多部电脑同时进行，网站所面对的威胁也与日俱增。

从神秘黑客的施袭手段来看，他们明显地并不打算窃取消费者客户的任何敏感资料（如信用卡资料），而是旨在令多家大型网上商贸公司无法营运。有报道指出，黑客挑选 buy.com 施袭，极可能与该公司于 8 日首日挂牌上市有关。虽然 buy.com 股价首日收市报 25.125 美元，急升了 93%，不过该公司总裁霍金斯承认，袭击事件确令网站蒙受了经济收入损失。网站持续许多小时无法进入，妨碍了顾客购物，影响了销售额，也影响网站点击率，从而影响了广告收入。至于黑客袭击 ebay，相信是要令这家刚宣布跟美国迪斯尼公司 go.com 合作发展流行电影和相关纪念品网站的网上公司出丑。

华尔街一些分析家认为，这类攻击不会对上述公司的股价或信誉造成冲击，其影响比公司系统受损或资料被盗要小。然而电脑安全专家忠告说，业内人士应当小心，否则会对电子商贸构成影响。因为互联网发展仍处于很脆弱的阶段，但电子商贸的发展却远比互联网快。

不过，黑客在短短几天内的攻击造成的损失仍是令人震惊的。

据美国著名的研究和咨询公司扬基集团发表的报告，黑客对美国 8 家大型网站袭击所造成的经济损失可能在 1 2 亿美元以上。

报告说，黑客袭击造成的网站中断服务从 45 分钟、2 小时到 5 小时不等。受影响的公司及其因特网合作伙伴为了更新安全设施，将要另外花费 1 到 2 亿美元。这次袭击还将给受

害公司的品牌声誉、合作关系以及未来的客户造成损害。

4. 黑客骚扰克林顿

黑客袭击也激怒了美国政府。

2000年2月9日,美国司法部和联邦调查局宣布向网站攻击者开战。

司法部长雷诺说:"我们发誓要用各种方法追出元凶,让有意干扰电子商务行为的黑客接受司法审判。"有关官员还表示,美国联邦调查局等机构已对黑客展开"地毯式"搜寻,如果抓到黑客,司法部准备以联邦法的第十八条起诉,若多项罪名成立,最高可处以10年监禁,罚金最高可达受害人经济损失的两倍。

联邦调查局将网络专家分成小组派往各地分头行动。负责此次调查行动的美国国家基础设施保护中心,隶属联邦调查局,是美国最厉害的网络警察机构。

"地毯式"搜索随即在全美展开,寻找罪犯的"数码足迹"。上百个国内外的黑客被列入了重点调查的黑名单中。

克林顿总统2月11日接受3家美国报纸采访时表示,他已邀请受害的几家网站等民间高科技公司与政府专家15日在白宫召开网络高级安全会议,共商对策,防止网络再遭袭击。

就在白宫召开电脑安全会议的前一天,克林顿接受CNN的网上在线采访。然而,克林顿的第一次网上接受采访却成了黑客大显身手的日子。

尽管提交总统的所有问题都经过了仔细的筛选,一些不够尊敬的问题还是被贴了上去,而且至少有两个黄色贴子突破CNN设计的网络过滤系统,并以克林顿的名义贴了上去。