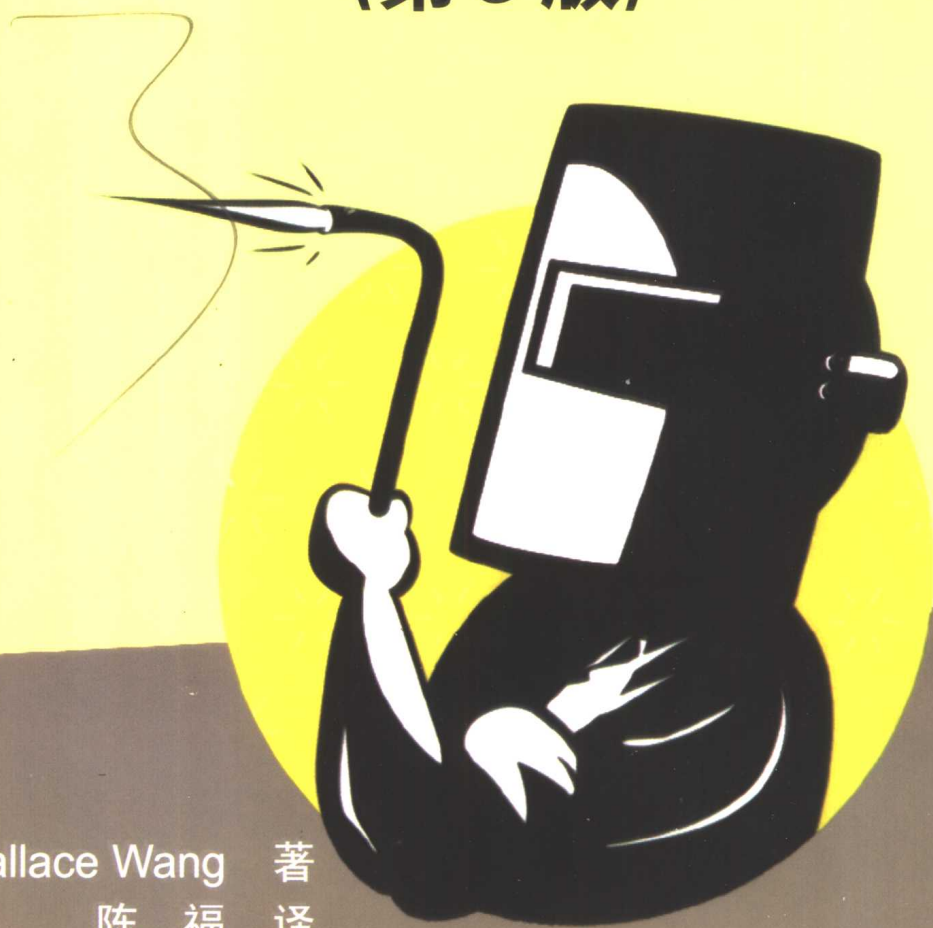


STEAL THIS COMPUTER BOOK 3

谁动了我的电脑

(第3版)



(美) Wallace Wang 著
陈福译



清华大学出版社

谁动了我的电脑

(第 3 版)

(美)Wallace Wang 著

陈 福 译

清华大学出版社

北 京

内 容 简 介

个人计算机和 Internet 的普及使世界融为一体,网络为人们带来了速度、效率与便捷,但同时也带来了众多隐忧。本书从社会和技术角度分析 Internet 所存在的问题,深入剖析其运作方式,内容涉及计算机系统的安全性问题、技术的局限性以及解决方案。本书并没有具体讲解黑客技术,而是引导您从黑客的角度分析问题,从而试图改变您对网络世界的认知。

本书内容翔实、见解独到,是网络管理员、程序员以及所有关注网络安全问题的计算机爱好者难得的参考书。

Wallace Wang

Steal This Computer Book 3

EISBN: 1-59327-000-3

Copyright© 2003 by No Starch Press.

Authorized translation from the English language edition published by No Starch Press.

All rights reserved. For sale in the People's Republic of China only.

Chinese simplified language edition published by Tsinghua University Press.

本书中文简体字翻译版由 No Starch 出版社授权清华大学出版社在中华人民共和国境内(不包括中国香港、澳门特别行政区和中国台湾地区)独家出版发行。未经许可之出口视为违反著作权法,将受法律之制裁。未经出版者预先书面许可,不得以任何方式复制或抄袭本书的任何部分。

版权所有,翻印必究。

本书封面贴有清华大学出版社激光防伪标签,无标签者不得销售。

北京市版权局著作权合同登记号 图字:01-2003-5401

图书在版编目(CIP)数据

谁动了我的电脑(第3版)/(美)王(Wang,W.)著;陈福译.—北京:清华大学出版社,2004

书名原文:Steal This Computer Book 3

ISBN 7-302-08291-X

I. 谁… II. ①王…②陈… III. 计算机网络—安全技术 IV. TP393.08

中国版本图书馆 CIP 数据核字(2004)第 019131 号

出 版 者:清华大学出版社

地 址:北京清华大学学研大厦

<http://www.tup.com.cn> 邮 编:100084

社 总 机:010-62770175 客户服务:010-62776969

组稿编辑:曹康

文稿编辑:李阳

封面设计:康博

版式设计:康博

印 刷 者:北京昌平环球印刷厂

装 订 者:三河市化甲屯小学装订二厂

发 行 者:新华书店总店北京发行所

开 本:185×260 印张:16.75 字数:347 千字

版 次:2004 年 4 月第 1 版 2004 年 4 月第 1 次印刷

书 号:ISBN 7-302-08291-X/TP·5978

印 数:1~5000

定 价:30.00 元

本书如存在文字不清、漏印以及缺页、倒页、脱页等印装质量问题,请与清华大学出版社出版部联系调换。联系电话:(010)62770175-3103 或(010)62795704

前言

本书从社会和技术角度分析有关 Internet 鲜为人知的阴暗面，内容涉及黑客、病毒编写者、政治活动者、审查机构、种族主义、政府、宗教和企业宣传，并介绍了一些伪装为新闻、广告和通讯稿的实例。

本书分析计算机黑客，但不讨论黑客技术，书中并未详细介绍黑客如何潜入计算机，也未从技术角度分析在任何特定操作系统类型中所有固有的安全漏洞。如果您正在查找有关 Red Hat Linux 最新版本的安全缺陷，或要了解如何配置 Cisco 路由器使企业网络免受攻击，请阅读其他相关书籍。

有人觉得本书倒胃，令人不快且隐藏危险。还有人借用本书信息大搞破坏，制造麻烦。我们认为，这两种做法都是错误的。

本书无意将您训练为黑客，而是引导您从黑客的角度分析问题，它将动摇您以前形成的是非观念，并冲破所属地区和文化形成的思想束缚。最终，它将拓展您的思维空间，带您跨入一个崭新世界。

个人思维的革命

当今世界风波不断，本书并未责备政府、国际组织、同种同文化民族、性偏好、多元文化组织、思想信仰、宗教机构或政党，而是宣扬一种个人革命，即自我思维的一场革命。本书认为：

- 若更改了自我思维方式，自我行为也将随之改变。
 - 若更改了自我行为方式，就可更改他人的行为和思考方式。
 - 若更改了他人的行为和思考方式，这种方式就会不断扩展，从而逐渐改变世界。
- 不过，这一切都是从您开始的。

之所以强调个人思想的革命，原因就在于此。在寻求真理的道路上，必须认识到，每个人的知识都是有限的，需不断调整自我，开阔知识视野，逐步积累。

无论是您(或您的父母、老板、配偶、家庭、政府或教会)还是我，都不可能通晓一切。不必为知识的缺憾而叹息，而要以装腔作势为辱。无论职位、居住地、信仰或所属国家如何，皆应互相学习，取长补短。为使世界更加美好，就需要开放、坦诚的交流，就需要个人思想的不断升华与变革，这正是本书的宗旨所在。

计算机行业并非完美无缺

计算机的组成原理很复杂，令人困惑，使用起来也非易事，不过，它代表着通信技术的巨大飞跃，其重要性不亚于字母表或印刷机的发明。

个人计算机和 Internet 的普及使世界融为一体，人们可收发邮件，搜索信息，并与全球各地的网友交流意见，其优越性毋庸置疑。但是，计算机行业也并非像市场炒作的那样完美无缺，它充满了销售部门不愿论及的隐忧：特洛伊木马、电子间谍、远程计算机监控、敌意组织、行骗者、恋童癖者、色情和恐怖主义——单击鼠标，它们便可能探出头来。

本书揭开了各种危险的面纱，并深入剖析其创建方式。帮助您理解之，认识之，避开威胁，或与之斗争。

真理是一种观点

本书不是资源大全，无法包容 Internet 上所有可能的合法和非法活动。本书所提供的信息是一把双刃剑，可用作帮助别人的工具，也可用作侵害他人的利器。不过，是正义之举，还是邪恶行为，这要取决于判断的标准和取向。同样是攻击网络，如果破坏的是政府计算机网络，您可能背上恐怖分子的罪名；如果破坏的是敌方网络，政府可能授予您英雄称号。所以，学会自我分析才是面对世界的最有力武器。

目 录

第 1 章 搜索引擎的魔力	1
1.1 搜索引擎	1
1.1.1 Meta 搜索引擎	2
1.1.2 专业搜索引擎	2
1.1.3 为儿童设计的搜索引擎	3
1.1.4 多媒体搜索引擎	4
1.1.5 区域搜索引擎	4
1.1.6 查找更多的搜索引擎	6
1.2 使用搜索引擎的一些技巧	7
1.2.1 在类别中搜索	7
1.2.2 使用具体的关键字	7
1.2.3 使用多个关键字	7
1.2.4 使用布尔运算符	7
1.2.5 留意搜索引擎返回的结果	8
1.3 搜索引擎的局限性	8
第 2 章 新闻和信息的其他来源	9
2.1 在线报纸	9
2.2 在线杂志	12
2.3 在线新闻机构	13
2.4 更多的新闻源	14
2.5 公司化运作对新闻的影响	15
2.6 新闻媒体只对已掌握的信息进行报道	16
2.7 已经成为历史的新闻	16
2.8 通过阅读来学习	17
第 3 章 黑客活动：网上活动	18
3.1 通过电子邮件和 Web 站点发表评论	19
3.2 将 Internet 用作媒体	20
3.2.1 将计算机病毒作为活动消息	20

3.2.2 通过活动消息毁损 Web 页面	22
3.2.3 在线破坏	23
3.3 计算机恐怖分子的威胁	24
第 4 章 黑客在何方	26
4.1 黑客站点	26
4.2 计算机安全站点	27
4.3 黑客杂志	28
4.4 寻找更多的黑客站点	29
4.4.1 黑客搜索引擎	29
4.4.2 黑客站点列表	30
4.4.3 Web ring	30
4.5 黑客 Usenet 新闻组	30
4.5.1 一般的黑客新闻组	30
4.5.2 计算机病毒新闻组	31
4.5.3 加密新闻组	31
4.5.4 破解新闻组	31
4.6 在 IRC 上查找黑客	31
4.7 黑客大会	32
4.8 不用恐慌：黑客也是人	32
第 5 章 病毒和蠕虫	34
5.1 不同的病毒如何感染计算机	36
5.1.1 传播感染文件的病毒	36
5.1.2 传播引导病毒	38
5.1.3 传播多元复合型病毒	39
5.1.4 传播宏病毒	40
5.2 病毒如何避免检测	41
5.2.1 感染方法	41
5.2.2 隐形	42
5.2.3 多态性	42
5.2.4 反击者	43
5.3 蠕虫的感染方法	43
5.4 关于病毒的虚妄和恶作剧	44
5.4.1 连锁信病毒恶作剧	44
5.4.2 作为宣传手段的病毒恶作剧	45

5.5	更多地了解病毒和蠕虫	45
第 6 章	特洛伊木马：警惕笑里藏刀的杀手	47
6.1	特洛伊木马的传播方式	47
6.1.1	把特洛伊木马物理地复制到计算机	47
6.1.2	从站点下载软件	48
6.1.3	从电子邮件附件接收特洛伊木马	48
6.1.4	从聊天室或即时消息传递服务发布特洛伊木马	48
6.2	特洛伊木马的种类	49
6.2.1	玩笑木马程序	49
6.2.2	破坏性的木马程序	49
6.2.3	盗取密码和其他敏感信息的木马程序	51
6.2.4	远程访问的特洛伊木马	52
6.3	黑客编写特洛伊木马的方式	55
6.4	阻止特洛伊木马	55
6.4.1	回滚程序	56
6.4.2	反病毒程序	56
6.4.3	防火墙	57
6.4.4	反特洛伊木马程序	57
6.4.5	黑客的反特洛伊木马工具	58
6.5	进一步认识特洛伊木马	59
第 7 章	网上骗局	60
7.1	区号骗局	60
7.2	尼日利亚骗局	61
7.3	金字塔骗局	62
7.4	家庭业务骗局	65
7.4.1	填充信封	65
7.4.2	自制工具箱	66
7.4.3	成为独立承包人	66
7.4.4	欺诈性销售	66
7.4.5	庞氏骗局	67
7.4.6	一贯正确的预报员	67
7.5	征友骗局	68
7.6	包嗅探器、Web 欺骗、phishing 和按键记录器	68
7.6.1	包嗅探器	69

7.6.2	Web 欺骗	69
7.6.3	phishing	70
7.6.4	按键记录器	71
7.7	重定向 Internet 连接	71
7.8	利用在线拍卖进行欺诈	72
7.9	Internet 商场谬论	73
7.10	城市传说	73
7.11	信用卡欺诈	73
7.12	自我保护	74
第 8 章	确定目标	77
8.1	war-dialing	77
8.2	端口扫描	78
8.2.1	ping sweeping	80
8.2.2	端口扫描	81
8.2.3	识别操作系统	82
8.3	war-driving	83
8.4	在找到进入计算机的方式之后	86
第 9 章	入侵计算机	87
9.1	请求并接收：社会工程的艺术	87
9.1.1	匿名电话	87
9.1.2	以个人身份使用社会工程策略	88
9.2	破解密码	89
9.2.1	盗取密码	89
9.2.2	用字典攻击工具猜测密码	93
9.2.3	暴力攻击密码程序	94
9.3	软件的漏洞和缺陷	94
9.3.1	缓存区溢出	95
9.3.2	隐藏的后门程序	96
9.3.3	默认设置	96
9.3.4	查找更多可利用的软件功能	97
9.4	闯入无线网络	97
9.5	密码：第一道防线	98

第 10 章 探索	99
10.1 清理日志文件	99
10.2 破坏监视软件	100
10.2.1 种植特洛伊程序	101
10.2.2 可加载的核心模块(LKM)rootkit	102
10.3 打开后门	103
10.4 嗅探更多的密码	103
10.5 摧毁 rootkit	104
第 11 章 计算机的购买预算	106
11.1 进行计算机的购买预算	106
11.1.1 整修的计算机	106
11.1.2 商店的陈列品和被退回的商品	108
11.1.3 在线拍卖	108
11.1.4 政府拍卖	108
11.1.5 再生计算机	109
11.1.6 自己组装	109
11.1.7 购买新计算机	110
11.1.8 升级旧的计算机	110
11.2 节约购买打印机设备的成本	111
11.3 总是免费的软件	112
11.3.1 共享件和免费软件	112
11.3.2 在学术机构以大折扣的价格购买软件	113
11.3.3 升级	113
11.3.4 低价的 Microsoft Office 替代品	114
11.3.5 盗版软件	114
11.3.6 解密软件	116
11.4 免费音乐	117
11.4.1 MP3 播放器	117
11.4.2 MP3 刻录程序	118
11.4.3 MP3 搜索引擎	118
11.5 免费的 Internet 访问	119
11.6 免费的电子邮件	119
11.7 免费的传真服务	119
11.8 免费的 Web 站点宿主	120
11.9 节省费用	120

第 12 章	保护数据和隐私	121
12.1	保护数据	121
12.1.1	密码保护	121
12.1.2	数据加密	121
12.1.3	挫败加密	123
12.1.4	隐藏硬盘上的文件	123
12.1.5	在图形中加密	124
12.2	监视自己的计算机	125
12.2.1	用网络摄像机监视	126
12.2.2	用软件监视	127
12.3	掩盖自己的痕迹	127
12.3.1	停用 cookie	127
12.3.2	清理 Web 浏览器缓存	129
12.4	保护自己的隐私	130
12.4.1	匿名浏览	131
12.4.2	以他人的名义浏览	131
12.4.3	发送匿名电子邮件	132
12.4.4	使用重邮器	132
12.4.5	Private Idaho	134
12.4.6	匿名聊天	134
12.5	保护身份	134
12.5.1	保护个人信息	135
12.5.2	如果个人信息被侵犯了, 该怎么办	136
第 13 章	向垃圾邮件宣战	138
13.1	公司会在 Internet 上发送垃圾邮件的原因及发送方法	139
13.1.1	获取电子邮件地址	139
13.1.2	掩饰身份	140
13.1.3	查找批量电子邮件发送程序	141
13.2	保护自己不受垃圾邮件的侵扰	142
13.2.1	向垃圾邮件发送者投诉	142
13.2.2	向垃圾邮件发送者的 ISP 投诉	142
13.2.3	向国内税收署投诉	143
13.2.4	使用电子邮件过滤器	143
13.2.5	查找垃圾邮件发送者的邮政地址	144
13.2.6	处理伪装的电子邮件地址	145

13.2.7	DNS 查找程序	148
13.2.8	伪装 Web 站点上的电子邮件地址	150
13.2.9	避免接收垃圾邮件的最后一招	151
13.3	反垃圾邮件资源	151
第 14 章	Web 窃听器、广告软件、弹出广告和间谍软件	153
14.1	警惕 Web 窃听器	153
14.1.1	跟踪用户浏览的 Web 站点	153
14.1.2	在垃圾邮件中使用 Web 窃听器	154
14.1.3	窃听新闻组	154
14.1.4	保护自己不受 Web 窃听器的伤害	155
14.2	广告软件——内置了广告的软件	156
14.2.1	对抗广告软件	157
14.2.2	广告软件和 Ad-aware	158
14.2.3	在 AOL 即时消息器中删除广告	158
14.3	阻止弹出广告	159
14.4	检测间谍软件	160
14.5	保护隐私的惟一确保有效的方法	162
第 15 章	防火墙、入侵检测系统和 honeypot	163
15.1	防火墙：第一道防线	163
15.1.1	防火墙的工作原理	163
15.1.2	防火墙是如何失败的	166
15.1.3	加固操作系统	167
15.2	入侵检测系统	168
15.2.1	入侵检测系统的工作原理	168
15.2.2	入侵检测系统是如何失败的	169
15.3	honeypot	169
15.4	跟踪黑客	170
第 16 章	计算机法医学：恢复和删除数据	173
16.1	删除数据	173
16.1.1	文件切碎程序	174
16.1.2	文件切碎的安全级别	174
16.1.3	自我摧毁的电子邮件	177
16.2	查找被删除的数据	178
16.2.1	键盘缓存区	178

16.2.2	清除 Web 浏览器高速缓存	178
16.3	计算机法医工具	179
16.3.1	文件恢复程序	179
16.3.2	16 进制编辑器	179
16.3.3	磁性感应器和电子显微镜	180
16.3.4	磁盘的拼接	181
16.4	使用法医工具	181
16.4.1	免费的法医工具	182
16.4.2	商业法医工具	182
16.5	自我保护	183
第 17 章	保护计算机	184
17.1	给计算机上锁	184
17.2	保护计算机部件	185
17.2.1	反盗窃机箱	185
17.2.2	报警器	186
17.3	保护笔记本电脑	186
17.3.1	笔记本电脑的警报器	187
17.3.2	远程跟踪服务	187
17.4	用生物测定技术阻止访问	188
17.4.1	生物测定设备	188
17.4.2	击败生物测定设备	190
附录 A	软件	192
A.1	程序类型	192
A.2	安装支持	192
A.2.1	解压缩	192
A.2.2	实用程序	193
A.3	匿名程序	193
A.4	反骗局软件	194
A.5	反间谍软件	194
A.6	反特洛伊木马程序	195
A.7	反病毒软件	196
A.8	批量发送电子邮件的程序	197
A.9	高速缓存和 cookie 清理程序	197
A.10	桌面保护程序	198

A.11	反汇编程序	198
A.12	DNS 查询程序	198
A.13	密码破解程序	199
A.14	文件加密程序	199
A.15	文件完整性检查程序	200
A.16	文件切碎程序	201
A.17	法医程序	202
A.18	16 进制编辑器	202
A.19	honeypot 诱捕程序	203
A.20	入侵检测程序	203
A.21	IRC 客户程序	204
A.22	按键记录程序	205
A.23	MP3 工具	206
A.24	数据包嗅探器	207
A.25	家长监控软件	207
A.26	密码恢复程序	207
A.27	端口扫描程序	208
A.28	读取器	209
A.29	远程监视程序	209
A.30	回滚程序	210
A.31	反垃圾邮件程序	210
A.32	数据隐藏程序	211
A.33	系统锁定程序	211
A.34	系统恢复程序	212
A.35	声音加密程序	212
A.36	易受攻击的扫描程序	213
A.37	Web 站点保护程序	213

附录 B 黑客的攻击工具库 214

B.1	因特网黑客工具	214
B.1.1	AOHell	214
B.1.2	BO2K-Back Orifice	215
B.1.3	Crack Whore	216
B.1.4	Death'n Destruction	216
B.1.5	ICQ War 2000	217
B.1.6	John the Ripper	217

B.1.7	NetBus	218
B.1.8	Nmap	219
B.1.9	SubSeven	220
B.1.10	UpYours	220
B.2	电话线路盗用工具	221
B.2.1	Master Credit Card Generator	221
B.2.2	CyberPhreak	222
B.2.3	Shit Talker	223
B.2.4	ToneLoc	223
B.3	病毒	224
B.3.1	AIDS 病毒	224
B.3.2	Ambulance 病毒	225
B.3.3	Boza 病毒	225
B.3.4	Casino 病毒	226
B.3.5	Senna Spy Internet Worm Generator 2000	226
B.3.6	VBS Monopoly 蠕虫	227
B.3.7	VBS 蠕虫生成器	228
B.3.8	病毒制造机	229
附录 C	电话线路盗用的简史和其他欺诈手段	230
C.1	电话线路盗用的简史	230
C.2	电话盗用的真实故事	231
C.2.1	洛杉矶的卫生纸危机	232
C.2.2	Santa Barbara 的核子骗局	233
C.2.3	总统的秘密	234
C.3	入门	235
C.3.1	“偷看”电话卡号码	236
C.3.2	电话音调盒	236
C.4	音调盒子程序	238
C.5	War 拨号程序和恶作剧程序	238
C.6	语音邮箱的入侵	239
C.7	便携式电话欺诈和卫星电视干扰	240
附录 D	术语表	241

第1章 搜索引擎的魔力

关于信息存在两个问题：不充分的信息和过多的信息。对于一个主题而言，不充分的信息容易导致错误的判断，而过多的信息使得查找相关信息的过程相当耗时且乏味，这会鼓励人们仅凭直觉来进行快速而不准确的判断。

设法找出与主题相关且足够有用的信息而不去过多关注太多无关紧要的信息是一个平衡的策略。如果想根据推理和信息(而不是情绪和无知)作出英明的决策，那么您必须花时间来全面研究主题。

作为一个研究工具，Internet 为我们提供了极其丰富的信息，几乎可以涵盖每一个您可能遇到的主题。遗憾的是，利用 Internet 进行研究的同时也引发了一些问题：

- 如何找到您所需要的信息？
- 如何了解您找到的信息是否准确、是否过时、是否易产生误导、是否存在一般性错误？

在 Internet 上查找信息相当简单：您只需要在搜索引擎中输入一个或多个关键字，然后搜索引擎就会列出所有与之相关的 Web 站点。

从不同的 Web 站点查找所需的信息相对简单。困难的是要确定找到的信息是否可靠，知道每一个信息源如何选择性地报道信息、忽略信息。因为人们都倾向于根据个人经验和偏见来看待问题，所以如果您得到的结论与他人得到的结论完全不同，这一点也并不奇怪。

某一观点可能在有些时候是正确的，而在有些时候却是错误的，但是更可能出现的情况是，没有一个观点是完全正确或者完全错误的。您所做出的判断是否就是正确的答案，这取决于您个人的观点。

1.1 搜索引擎

在 Internet 上搜索信息的关键是搜索引擎的使用。如果您利用不同的搜索引擎搜索相同的信息，那么每一个搜索引擎返回的结果可能都是不尽相同的。不要局限于只使用单一的搜索引擎，尝试下文介绍的搜索引擎也许会令您发现曾经遗漏的信息。

此外，在使用多个搜索引擎的过程中，您还会发现，某一搜索引擎在查找特定类型的数据或特有领域的信息时具有特别的优势。例如，Teoma 搜索引擎会根据主题把搜索结果归类。如果您搜索的关键字是“Mustang”，Teoma 会把找到的结果根据“Ford

Mustang”和“Mustang horses”进行分类。下面我们要介绍一些功能更为强大的搜索引擎：

About	http://about.com
AlltheWeb	http://www.alltheweb.com
AltaVista	http://www.altavista.com
AOLSearch	http://search.aol.com
Ask Jeeves	http://www.askjeeves.com
Google	http://www.google.com
Hotbot	http://www.hotbot.com
LookSmart	http://www.looksmart.com
MSN	http://www.msn.com
Open Directory Project	http://dmoz.org
Teoma	http://www.teoma.com
Yahoo!	http://www.yahoo.com

1.1.1 Meta 搜索引擎

Meta 搜索引擎会把您的查询请求发送给两个或多个通用搜索引擎并删除重复结果，从而节省您访问多个搜索引擎的时间。下面是一些流行的 meta 搜索引擎：

DogPile	http://www.dogpile.com
Mamma	http://www.mamma.com
MetaCrawler	http://www.metacrawler.com
Search.com	http://www.search.com

1.1.2 专业搜索引擎

最后，不要忽略了用来搜索特定领域信息的专业搜索引擎。通过这些专业搜索引擎，通常可以找到通用搜索引擎遗漏的 Web 站点。专业搜索引擎几乎包罗万象，其范围从养鱼到最新的嫁接技术。下面是一些有趣的专业搜索引擎：

- **AvatarSearch** 搜索一些神秘的超自然的主题，如魔法、吸血鬼、异教仪式、占星术、占卜纸牌等(<http://www.avatarsearch.com>)。
- **Black Web Portal** 查找黑人感兴趣的 Web 站点(<http://www.blackwebportal.com>)。
- **Crime Spider** 搜索提供各种犯罪和法律实施的 Web 站点，Web 站点信息通过主题分类，如连环谋杀、都市传奇和电脑犯罪等(<http://www.crimespider.com>)。