



21世纪信息安全大系

# 僵尸网络 网络程序杀手

Craig A. Schiller, Jim Binkley, David Harley

Gadi Evron, Tony Bradley, Carsten Willems, Michael Cross 著

邢健 党开放 刘孜文 译

Botnets

The Killer Web App



科学出版社



号 117200 : 字国

# Botnets The Killer Web App

## 僵尸网络 网络程序杀手

This is a translated version of Botnets: The Killer Web App by Craig A. Schiller. Copyright © 2008 by Addison-Wesley. ISBN 10: 0744413877 ISBN 13: 978-0-321-51387-7 All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording, or by any information storage and retrieval system, without permission in writing from the publisher.

本册本册	AUTHOR	作者: 克雷格·A·希勒
译者: 王宇	译者: 王宇	译者: 王宇
ISBN 7-111-21720-0	ISBN 7-111-21720-0	ISBN 7-111-21720-0
定价: 39.00元	定价: 39.00元	定价: 39.00元
科学出版社	科学出版社	科学出版社

科学出版社

定价: 39.00元

北京

图字：01-2008-2322 号

This is a translated version of

**Botnets: The Killer Web App**

Craig A. Schiller, et al.

Copyright © 2007 Elsevier Inc.

ISBN 10: 1-59749-135-7

ISBN 13: 978-1-59749-135-8

All rights reserved.

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system, without permission in writing from the publisher.

AUTHORIZED EDITION FOR SALE IN P. R. CHINA ONLY

本版本只限于在中华人民共和国境内销售

**图书在版编目(CIP)数据**

僵尸网络：网络程序杀手/(美)席勒(Schiller, C. A.)等著；邢健、党开放、刘孜文译. —北京：科学出版社，2009

(21世纪信息安全大系)

书名原文：Botnets: The Killer Web App

ISBN 978-7-03-024943-2

I. 僵… II. ①席…②邢…③党…④刘… III. 计算机网络-程序设计-安全技术 IV. TP393.09

中国版本图书馆 CIP 数据核字 (2009) 第 112700 号

责任编辑：田慎鹏 霍志国/责任校对：包志虹

责任印制：钱玉芬/封面设计：耕者设计工作室

**科学出版社出版**

北京东黄城根北街16号

邮政编码：100717

<http://www.sciencep.com>

**骏志印刷厂印刷**

科学出版社发行 各地新华书店经销

\*

2009年8月第一版 开本：787×1092 1/16

2009年8月第一次印刷 印张：19 1/4

印数：1—4 000 字数：450 000

**定价：48.00 元**

(如有印装质量问题，我社负责调换〈环伟〉)

## 作者简介

**Craig A. Schiller** (CISSP-ISSMP, ISSAP) 波特兰州立大学首席信息安全官；鹰眼安全培训有限公司总裁；最早的公认系统安全准则 (GASSP) 的主要作者，与他人合著 *Handbook of Information Security Management, Data Security Management* 的特约作者。Craig 先生也参与编写了 *Combating Spyware in the Enterprise* (Syngress, ISBN: 1597490644) 和 *Winternals Defragmentation, Recovery, and Administration Field Guide* (Syngress, ISBN: 1597490792)。他是高级网络安全工程师并负责美国宇航局航空情报服务处信息安全组。他负责美国俄勒冈州 hillisboro 警察局警察储备专家部门。

**Jim Binkley** 波特兰州立大学高级网络工程师和网络安全研究人员、Ourmon 软件的制作人。Jim Binkley 有 20 多年的 TCP/IP 经验和 25 年的 UNIX 操作系统经验，在波特兰州立大学从事网络管理、网络安全和 UNIX 操作系统的教学工作，为大学提供各种网络监测手段，并提供网络设计的咨询工作。曾与 John McHugh 一起参与了波特兰州立大学的“安全移动网络”项目（美国国防高级研究计划局资助）。Jim Binkley 获得华盛顿州立大学计算机专业硕士，专门从事无线网络技术及网络异常监测包括开源 Ourmon 网络监测和异常监测系统。

## 致 谢

感谢以下人士在本书出版过程中的热心支持。

在这里感谢银行家、律师以及财务工作人员似乎有点奇怪，但他们中的每个人对 Syngress 的成功出版发行起了重要的作用，感谢 Jim Barbieri, Ed Remondi, Anne Marie Sharpe, 以及他们在 Holbrook 的工作团队；

美国波士顿 Ruberto, Israel & Weiner 律师事务所的 Gene Landy, Amy Mastrobattista 和 Beth Grazio;

Morgan & Morgan (PC in Hingham, 马萨诸塞州) 的 Timothy D. MacLellan 及其助手 Darci Miller Nadeau。

## 贡献作者

**Tony Bradley** (CISSP-ISSAP) 《纽约时报》旗下 About.com 因特网安全网站主管，在许多网站和刊物上发表多篇文章，如 PC World、SearchSecurity.com、WindowsNetworking.com、智能计算杂志 (*Smart Computing magazine*) 和信息安全杂志 (*Information Security magazine*)。目前是一家世界财富 100 强公司的网络安全顾问及设计师，积极推动世界财富 500 强企业的反病毒及网络安全事件响应的策略及技术，也为小规模公司提供技术支持和网络管理。著有 *Essential Computer Security: Everyone's Guide to E-mail, Internet, and Wireless Security* (Syngress, ISBN: 1597491144)。

Tony 获得过多种认证，包括 CISSP、ISSAP、MCSE、MCSA、MCP 等。由于在 Windows 安全技术上的贡献，被授予微软“最有价值专家”称号 (MVP)。

在 About.com 网站上，平均每月有超过 600 000 的浏览量，并且有 25 000 个固定用户。Tony 还创办了 10-part Computer Security 101 课程，至今已培训数千人并赢得口碑流行起来。除此之外，Tony 还曾参编多部有关计算机安全的书籍，如 *Hacker's Challenge 3* (ISBN: 0072263040)、*Winternals: Defragmentation, Recovery, and Administration Field Guide* (ISBN: 1597490792)，以及 *Combating Spyware in the Enterprise* (ISBN: 1597490644)。Tony Bradley 撰写了本书第 4 章。

**Michael Cross** (MCSE、MCF+I、CAN、Network+) 因特网专家/尼亚加拉警察局 (NRPS) 计算机取证分析师。他检查涉嫌犯罪的计算机，协助处理与计算机或因特网相关的案件。除了在 [www.nrps.com](http://www.nrps.com) 上设计并维护 NRPS 网站和 NRPS 内联网以外，Michael Cross 提供编程、硬件和网络管理等方面的支持。他所在的信息技术团队，为一个 800 多个民间用户和军方用户的用户群提供支持。他认为，如果用户带枪，解决问题的动力就会更大。Michael 还拥有 KnightWare ([www.knightware.ca](http://www.knightware.ca))，可以提供与计算机有关的服务，如网页设计、Bookworms ([www.bookworms.ca](http://www.bookworms.ca))，可以在这个网站上在线购买收藏品和一些有趣的东西)。他作为自由作家已经有好几年了，在许多书籍和文选当中发表了 30 多篇文章。目前和妻子 Jennifer 以及一对可爱的儿女 (儿子 Jason，女儿 Sara) 居住在加拿大安大略省圣凯瑟琳市。Michael Cross 撰写了本书第 11 章。

**Gadi Evron** 是 Beyond Security 公司的安全专家，该公司位于美国弗吉尼亚州 McLean，为客户提供漏洞评估和漏洞管理解决方案；同时也是网络安全资讯公司 SecuriTeam 的主编。Gadi Evron 是因特网安全技术领域特别是针对僵尸网络和网络钓鱼领域方面的安全专家，也是零日紧急响应小组 (ZeroDay Emergency Response Team, ZERT) 的创始人，著名的针对企业间谍破坏活动的安全专家。他曾担任以色列政府因

特网安全行动组的经理，曾经是以色列政府计算机安全应急响应组（Computer Emergency Response Team, CERT）的创始人和经理。Gadi Evron 撰写了本书第 3 章。

**David Harley** (BA, CISSP) 主编并与他人合编了许多计算机安全技术方面的书籍，如 *Viruses Revealed* 和即将出版的 *AVIEN*（防病毒信息交换网络）、*Malware Defense Guide for the Enterprise*。他是一位经验丰富且德高望重的反病毒研究人员，同时具有多项资质认证如安全审计（BS7799 主任审核员）、ITIL 管理认证和医学资讯。他为一家主要医学研究基金会进行安全分析并管理英国国家健康中心的威胁评估中心，特别是针对 malware 和电子邮件的安全管理。David 参与编写了第 5 章。

**Chris Ries** VigilantMinds 公司的安全工程师，在匹兹堡从事安全服务培训及专业咨询。主要从事软件漏洞的检测、利用和修补以及恶意代码的分析和安全软件的评估，并在这些研究工作基础上发表了多篇文章和技术白皮书，也参与了一些信息安全方面的书籍编写工作。Chris 拥有 Colby 大学计算机专业学士学位，辅修数学，在大学期间完成了自动恶意代码检测研究工作。Chris 也是美国国家网络辩论和训练联盟的分析研究人员（NCFTA），为相关法律实施提供技术支持。Chris 为本书第 8 和 9 章进行了技术编辑。

**Carsten Willems** 独立软件研发人员，具有 10 年的工作经验，特别是针对恶意软件的安全工具的研发。他是 SWSandbox 沙盒工具（一种恶意软件自动分析工具）的创立者。该工具是他在亚琛工业大学计算机专业硕士论文的一部分，现在已经被 sunbelt 软件公司用于 Clearwater 和 FL 中。目前他正在曼海姆大学从事博士研究工作，课题为“恶意软件自动分类”。2006 年 11 月，他的“恶意程序行为的自动分析”获得安全应用技术学会三等奖。此外 Carsten 还创建了一些官方及电子商务产品。最近，他研发的 SAGE GS-SHOP（一种在线 shopping 客户端服务器）已经被安装 10 000 多次。本书的第 10 章由 Carsten 编写。

**Gadi Evron** 是 Beyond Security 公司的安全专家，该公司位于以色列的 Be'er Sheva。他为各方提供管理网络安全方案，同时也是互联网安全专家。Gadi Evron 是网络安全技术领域以色列国家应急响应组（National Computer Emergency Response Team, NCERT）的创始人，著名的针对企业网络安全活动的以色列政府

# 目 录

<b>第 1 章 僵尸网络：呼吁行动</b> .....	1
前言.....	2
网络程序杀手.....	3
问题有多大？.....	3
僵尸网络的概念史.....	4
僵尸病毒的新闻案例.....	11
业界反响.....	15
小结.....	15
快速回顾.....	16
常见问题.....	17
<b>第 2 章 僵尸网络概述</b> .....	19
什么是僵尸网络？.....	20
僵尸网络的生命周期.....	20
漏洞利用.....	21
召集和保护僵尸网络客户端.....	24
等候命令并接受 payload.....	27
僵尸网络究竟做什么？.....	28
吸收新成员.....	28
DDoS.....	31
广告软件（Adware）和 Clicks4Hire 的安装.....	33
僵尸网络垃圾邮件和网络钓鱼连接.....	35
存储和分配偷窃或非法（侵犯）知识产权的信息资料.....	37
勒索软件（Ransomware）.....	41
数据挖掘.....	41
汇报结果.....	41
销毁证据，放弃（僵尸）客户端.....	41
僵尸网络经济.....	42
垃圾邮件和网络钓鱼攻击.....	42
恶意广告插件和 Clicks4Hire 阴谋.....	43
Ransomware 勒索软件.....	45
小结.....	45
快速回顾.....	46
常见问题.....	48



<b>第 3 章 僵尸网络 C&amp;C 的替换技术</b> .....	51
简介：为什么会有 C&C 的替换技术？ .....	52
追溯 C&C 的发展历史 .....	53
DNS 和 C&C 技术 .....	53
域名技术 .....	54
多宿 (Multihoming) .....	54
可替换控制信道 .....	55
基于 Web 的 C&C 服务器 .....	55
基于回声的僵尸网络 .....	55
P2P 僵尸网络 .....	57
即时消息 (IM) C&C .....	57
远程管理工具 .....	58
降落区 (drop zone) 和基于 FTP 的 C&C .....	58
基于 DNS 的高级僵尸网络 .....	60
小结 .....	61
快速回顾 .....	62
常见问题 .....	62
<b>第 4 章 僵尸网络</b> .....	63
简介 .....	64
SDBot .....	64
别名 .....	64
感染途径 .....	65
被感染的标志 .....	65
注册表项 .....	66
新生成的文件 .....	67
病毒传播 .....	67
RBot .....	68
别名 .....	68
感染途径 .....	68
被感染的标志 .....	68
Agobot .....	72
别名 .....	72
感染途径 .....	72
被感染的标志 .....	73
传播 .....	75
Spybot .....	76
别名 .....	76
感染途径 .....	76

141	被感染的标志	77
141	注册表项	77
141	不正常的流量	79
141	传播	79
141	Mytob	80
141	别名	80
141	感染途径	81
141	被感染的标志	81
141	系统文件夹	81
141	不正常的流量	81
141	传播	81
141	小结	82
141	快速回顾	83
141	常见问题	84
141	<b>第 5 章 僵尸网络检测：工具和技术</b>	87
141	简介	88
141	滥用	88
141	垃圾邮件和滥用	91
141	网络设施：工具和技术	92
141	SNMP 和网络流：网络监控工具	94
141	防火墙和日志	97
141	第二层的交换机和隔离技术	98
141	入侵检测	101
141	主机的病毒检测	104
141	作为 IDS 例子的 Snort	109
141	Tripwire	112
141	暗网、蜜罐和其他陷阱	114
141	僵尸网络检测中的取证技术和工具	116
141	过程	117
141	事件日志	119
141	防火墙日志	125
141	反病毒软件日志	127
141	小结	134
141	快速回顾	134
141	常见问题	137
141	<b>第 6 章 Ourmon：概述和安装</b>	139
141	简介	140
141	案例分析：在黑暗中跌撞前行的事情	141

37	案例 1: DDoS (分布式拒绝服务)	141
37	案例 2 外部并行扫描	143
37	案例 3 僵尸客户端	144
37	案例 4 僵尸服务器	145
38	Ourmon 如何工作	146
38	Ourmon 的安装	149
38	Ourmon 安装提示和窍门	151
38	小结	153
38	快速回顾	153
38	常见问题	154
	<b>第 7 章 Ourmon: 异常检测工具</b>	157
38	简介	158
38	Ourmon 网页接口	158
38	原理简介	162
38	TCP 异常检测	163
38	TCP 端口报告: 30 秒视图	164
38	TCP 蠕虫图表	170
38	TCP 每小时摘要	171
38	UDP 异常检测	173
38	E-mail 异常检测	175
38	小结	177
38	快速回顾	178
38	常见问题	179
	<b>第 8 章 IRC 和僵尸网络</b>	181
38	简介	182
38	IRC 协议	182
38	Ourmon 的 RRDTOOL 统计与 IRC 报告	185
38	IRC 报告的格式	185
38	检测 IRC 僵尸网络客户端	190
38	检测 IRC 僵尸网络服务器	194
38	小结	197
38	快速回顾	197
38	常见问题	198
	<b>第 9 章 ourmon 高级技术</b>	201
38	简介	202
38	自动包捕获	202
38	异常检测触发器	203
38	触发器应用实例	205

845	Ourmon 事件日志 .....	209
845	搜索 Ourmon 日志的技巧 .....	209
845	嗅探 IRC 消息 .....	212
845	优化系统 .....	215
845	买一个双核 (Dual-Core) CPU .....	216
845	使用不同的电脑, 分开前端与后端 .....	216
845	买一个双核, 双 CPU 的主板 .....	217
845	扩大内核的环缓存 .....	217
845	减少中断 .....	218
845	小结 .....	218
845	快速回顾 .....	218
845	常见问题 .....	220
	<b>第 10 章 使用沙盒工具应对僵尸网络</b> .....	221
845	简介 .....	222
845	CWSandbox 介绍 .....	223
845	组件介绍 .....	226
845	检查分析报告的样本 .....	231
845	<analysis>部分 .....	231
845	分析 82f78a89bde09a71ef99b3ced b991bcc. exe .....	232
845	分析 Arman. exe .....	233
845	解释分析报告 .....	237
845	僵尸病毒是如何安装的? .....	238
845	病毒如何感染新主机 .....	239
845	僵尸病毒如何保护本地主机和自己? .....	240
845	联系哪个 C&C 服务器以及如何联系 .....	243
845	僵尸病毒如何更新? .....	244
845	进行了什么样的恶意操作? .....	245
845	在线沙盒对僵尸病毒的监测结果 .....	249
845	小结 .....	251
845	快速回顾 .....	252
845	常见问题 .....	253
	<b>第 11 章 情报资源</b> .....	255
845	简介 .....	256
845	辨别企业/大学应该尽力收集的信息 .....	256
845	反汇编 .....	258
845	可找到公用信息的地方/组织 .....	260
845	反病毒、反间谍软件、反恶意软件的网页 .....	260
845	专家和志愿者组织 .....	261

009	..... 邮件列表和讨论团体 .....	263
009	会员组织以及如何获得资格 .....	263
019	..... 审查成员 .....	264
019	保密协议 .....	264
019	..... 什么可以共享 .....	264
019	..... 什么不能共享 .....	264
019	..... 违背协议的潜在影响 .....	265
019	..... 利益冲突 .....	265
019	获取信息时如何处理 .....	266
019	情报收集在法律相关的执行方面扮演的角色 .....	267
019	小结 .....	267
039	快速回顾 .....	268
039	常见问题 .....	269
<b>12</b>	<b>第 12 章 应对僵尸网络 .....</b>	<b>271</b>
039	简介 .....	272
039	放弃不是一个选项 .....	272
039	为什么会有这个问题? .....	273
039	..... 刺激需求：金钱，垃圾邮件，以及网络钓鱼 .....	274
039	..... 法律实施问题 .....	275
039	..... 软件工程的棘手问题 .....	276
039	..... 缺乏有效的安全策略或者过程 .....	277
039	..... 执行过程中的挑战 .....	278
039	我们应该做什么? .....	279
039	..... 有效的方法 .....	279
039	..... 如何应对僵尸网络? .....	282
039	..... 报告僵尸网络 .....	283
039	..... 绝地反击 .....	284
039	..... 法律的实施 .....	288
039	..... 暗网、蜜罐和僵尸网络颠覆 .....	288
039	战斗的号角 .....	290
039	小结 .....	291
039	快速回顾 .....	291
039	常见问题 .....	293
069	..... 信息前嫌划代到以强半大)业命限有 .....	
069	..... 能下可 .....	
069	..... 地址\改取前息寄田公院数新 .....	
069	..... 或网自科野意基又,行群数可划,备内云 .....	
069	..... 址能许题志请家特 .....	

# 第 1 章

## 僵尸网络：呼吁行动

### 本章主要内容：

■ 网络程序杀手

■ 问题有多大？

■ 业界反响

✓ 小结

✓ 快速回顾

✓ 常见问题

### 前言

整个 2006 年，科技安全大会都在讨论最新的“网络程序杀手”。不幸的是，这种技术主要是为一些不法分子服务的。新一代高智商而缺乏道德责任感的黑客们，在一些有组织的犯罪集团以及垃圾邮件制造商的资助下，创造了一种致命的摧毁性病毒——僵尸网络。来自威廉玛丽学院的 Norman Elton 和 Matt Keel 在 2005 年“谁拥有你的网络？”的报告中称，僵尸网络是“人类面对的一个最大的威胁”。这似乎有些夸张，但是说僵尸网络是网络社会所面临的巨大威胁却是有据可依的。John Canavan 在名为“恶意 IRC<sup>①</sup> 的进化”的白皮书中提到，僵尸网络是“最危险和最广为传播的 Win32 病毒威胁”。

2006 年 10 月 16 日 e-Week 杂志封面称，我们“正在输掉”与僵尸网络的战争。Ryan Naraine 在“与僵尸网络的战争已经失败？”一文中介绍了僵尸网络环境现状：僵尸网络是“组织严谨的全球犯罪链中的关键核心。它利用僵尸工具盗用带宽，并通过非法网络活动谋取利益”（更多信息参考 [www.eweek.com/article2/0,1895,2029720,00.asp](http://www.eweek.com/article2/0,1895,2029720,00.asp)）。而与之形成鲜明对比的是，相应的安全措施刚刚起步，少数安全软件厂商发行了与僵尸网络相关的产品（第一版）。紧缺急需的情报信息被封锁起来，仅传递给需要它的安全专家，只有信息安全专家清楚地了解安全问题。有安全专家宣称：“这（指僵尸网络）是不存在的”。一位供货商告诉我们，他们产品的质量取决于他们情报资源的质量，然而接下来却说，他们不能给我们确保情报资源质量的任何信息。

早期对抗网络僵尸的方法是消灭僵尸服务器，即“对毒蛇的斩首行动”。针对近期的僵尸网络的安全措施研究文献中称，我们不是和普通的蛇而是和“九头蛇”战斗。它不仅仅有一个头，而是很多个，除去一个，将产生两个来取代它，因而这个斗争失败了很多次。文章中，几个安全专家承认与僵尸网络的战斗已经失败。在实际战斗中，军官必须对抗的是敌人，但重要的是必须鼓舞士气，必须有斗志（必须与己方低迷的士气作战）。率先与僵尸网络作战的安全专家（先驱）在意识到“斩首行动”（消灭 C&C 服务器）不再和昔日一样有效时，非常沮丧。设想进攻的先前军队遇见城堡，城堡主对围城塔、弹弩或迫击炮的感受。然而随着这些武器的引入，城堡自身设计也在改变：由一面环绕城堡的墙变成一系列的墙；城堡形状由规则方形变成不规则形状以便避开而不是挡住敌人的武器。武器的失败并不意味着战斗的失败，只有军官沮丧，使得士兵士气削弱且不懂得变通因地制宜才会导致失败。

本书意在为对抗僵尸网络而增加新士兵和新武器。为此，作者希望挖掘“士气”削弱的根源，帮助专业技术安全人士重新获得信心，为进一步探索研究打下基础。

本章介绍了现状以及为什么会到这步田地。用户计算机水平千差万别，为此我们必须从最基础的开始。什么是僵尸网络？它最简单的形式是一群感染了病毒的计算机执行“傀儡牧人”的命令。“傀儡牧人”就是利用僵尸网络谋取利益或攻击其他计算机的黑客。

<sup>①</sup> Internet Relay Chatting——译注。

## 网络程序杀手

僵尸网络如何成为“网络程序杀手”？创造和管理僵尸网络的软件使得僵尸网络危害程度要远远高于以前的恶意脚本那一代。它不仅仅是病毒，而是病毒的病毒。僵尸网络是模块化式的，一个模块利用找到的漏洞来控制目标系统。然后，它下载另一个模块，该模块通过阻止反病毒软件和防火墙来保护新僵尸病毒。第三个模块可能开始扫描其他有漏洞的系统。僵尸网络具有自适应功能。它可以设计成下载不同的模块，以便于利用它所发现的系统漏洞。新的攻击手段一出现，就能被加入到模块中去，这使得防病毒软件的工作更为复杂。找到僵尸网络的一个组件，发现不了其他组件的特性。因为这个组件能够选择任意数量的模块进行下载，以完成僵尸网络运行每个阶段所需要的功能。这也使得反病毒软件受到质疑，当反病毒软件遇到并清除了多重组件的僵尸病毒的一个组件后就显示系统病毒已清除干净了。因为首次感染后，需要每个组件时就下载，因而系统遭遇零天攻击的可能性会变大。如果你处于企业环境中，清除恶意代码不彻底，会有把僵尸病毒带回（循环）的危险。为了降低这个危险性，许多IT部门选择了从已知的干净镜像文件来重装（重新镜像）系统。

僵尸网络可选择目标攻击。就是说，黑客能够将一个公司或者市场部门作为攻击目标。尽管僵尸网络能够随机产生，他们也可以专门设计选择一系列潜在用户组成的僵尸网络。傀儡牧人能够配置僵尸客户端，以限制他们在设定的因特网协议（IP）地址范围内对主机的扫描。由于具有这种定位特性带来了特定（根据客户需求）攻击的市场需求。僵尸网络的目标定位也有自适应能力。僵尸客户端能够检查新感染的主机以知道如何利用漏洞。例如，确定主机的主人是电子黄金账户的顾客，僵尸客户端能够下载一个组件，该组件在下次客户进行交易时利用 piggyback<sup>①</sup>。当主机的主人链接上电子黄金账户时，僵尸病毒就会利用漏洞，通过发送转账申请从账户取走现金。

## 问题有多大？

2006年9月，Symantec发布的最新因特网威胁报告称，2006年1~6月期间，每天有57 717台活跃的僵尸网络计算机。Symantec也声称，已经发现了超过450万台活动明显的僵尸网络计算机。根据我们在学术领域的经验，很多看到的僵尸病毒通常是检测不到的，除非傀儡牧人放弃该计算机。一旦僵尸客户端停止运行，就能检测出其残留。这就是说，实际数量远远大于Symantec报告中的数量，再加上僵尸客户端还有一种模块能关闭反病毒软件，并阻止用户访问反病毒软件供应商的网站进行更新或下载杀毒工具。

11月17日发行的e-Week在线杂志声称俄罗斯的傀儡牧人操纵了7000多台主机进行垃圾邮件和黑客行为，如果这种情形继续下去，正如猖獗的犯罪以及非法的毒品影响社会经济前景那样，这场僵尸网络灾祸就可能威胁未来的网络。

<sup>①</sup> 寄生术，是指跟随其他用户的合法访问操作混入计算机系统作案的一种方法——译注。



仔细查看 McAfee 公司 Ken Baylor 和 Chris Brown 的白皮书“Killing Botnets——A View from the trenches”中特别的案例。即使文章结尾明显是有商业目的，其所收集的案例确是真实和有潜在可能的。2006 年 3 月，McAfee 被要求从一个数目庞大的僵尸网络中收回美国国家中心的电信基础设施。在协议的第一周，McAfee 记录了 690 万次攻击，其中 95% 是与 IRC 有关的僵尸病毒。国家电话公司报告了其引起的问题：

- 无数网络停机达 6h

- 面对客户诉讼威胁

- 客户交易中断

- 银行 ATM 服务漫长的停机

自 2005 年 1 月份以来，微软公司开始给用户提供 Windows 恶意软件去除工具 (Windows Malicious Software Removal Tool)。15 个月后，微软宣称已经从将近 600 万的单台计算机上删除了 1600 万次恶意软件事例。根据微软的报告“Progress Made, Trends Observed” (取得进展，洞察趋势)，主要删除的恶意软件是僵尸病毒。用户可以自愿使用该工具，也就是说，绝大多数的微软用户并没有运行该工具。在赞同这些数据之前，记住这种行为是反应行为——计算机被感染后，先投入使用然后才被发现和删除。2006 年的最后一周内，微软发行了一个补丁，3 天后，对该补丁的漏洞利用 (攻击) 已经遍布网络。

看僵尸网络攻击的威力——分布式拒绝服务攻击 (DDoS)。一个具有 10000 个僵尸客户端 (上载速度为 128 Kb/s) 的小型僵尸网络每秒可产生 1.3 Gb 的数据量。据 McAfee 称，具备这种能量的 2~3 个大型的 (超过 100 万) 僵尸网络就能够“威胁许多国家的基础设施”。这些大型的僵尸网络可能强大到摧毁大多数财富 500 强的公司。

### 僵尸网络的概念史

与如今因特网上的很多东西一样，僵尸开始作为有用的工具而没有其他恶意。僵尸最初作为虚拟的个体开发研究。它可以加入 IRC 信道，在主人忙于其他事务时为其服务。IRC 是 1988 年 8 月由芬兰奥卢大学的 Jarkko WiZ Oikarinen 创建的。图 1.1 追溯了僵尸技术的发展进化历程。

#### GM

最初的 IRC 僵尸 (或者 robot user)，Wikipedia 称之为 GM，是由 IRC 服务器操作员 Greg Lindahl 于第二年 (1989 年) 开发的。这个善意的僵尸能够和 IRC 用户玩 Hunt the Wumpus 游戏。最早的僵尸是真正的 robot user，对于其余的 IRC 用户来说他们也只是用户，帮助用户享用并管理自己的 IRC 连接，不同于今天的僵尸网络客户端。

从这个简单的例子，其他程序员意识到，可以为用户和 IRC 操作员创造 robot user 来执行很多目前由人类来完成的工作，如处理全天 24h 的用户请求。对僵尸一项重要的研究开发就是当操作员忙于其他事情时，僵尸能够保持信道畅通并防止恶意用户控制该信道。为了协助 IRC 操作员，僵尸必须能够像信道操作员一样工作。僵尸已经从最初的帮助单个用户，发展为管理和运行 IRC 信道并为所有用户提供服务。服务的术语表