

Contents

Chapter 1 Botnets: A Call to Action.	1
Introduction	2
The Killer Web App	3
How Big Is the Problem?	4
A Conceptual History of Botnets	6
GM	7
Pretty Park	7
SubSeven Trojan/Bot	8
GT Bot	8
SDBot	9
Agobot	10
From Code-Based Families to Characteristic-Based Families	11
Spybot	12
RBot	14
Polybot	15
Mytob	15
Capabilities Coming to a Bot Near You	15
Cases in the News	16
“THr34t-Krew”	16
Axel Gembe	17
180Solutions Civil Law Suit	17
Operation Cyberslam: Jay Echouafni, Jeanson James Ancheta	18
Anthony Scott Clark	20
Farid Essebar	21
Christopher Maxwell	21
Jeffrey Parson	21
The Industry Responds	22
Summary	24
Solutions Fast Track	25
Frequently Asked Questions	26
Chapter 2 Botnets Overview	29
What Is a Botnet?	30
The Botnet Life Cycle	31
Exploitation	31
Malicious Code	31
Attacks against Unpatched Vulnerabilities	32
Backdoors Left by Trojan Worms or Remote Access Trojans	33
Password Guessing and Brute-Force Access Attempts	34
Rallying and Securing the Botnet Client	37
Waiting for Orders and Retrieving the Payload	41

What Does a Botnet Do?	42
Recruit Others	42
DDoS	46
Installation of Adware and Clicks4Hire	49
The Botnet-Spam and Phishing Connection	51
Storage and Distribution of Stolen or Illegal Intellectual Property	55
Ransomware	60
Data Mining	61
Reporting Results	61
Erase the Evidence, Abandon the Client	62
Botnet Economics	62
Spam and Phishing Attacks	62
Adware Installation and Clicks4Hire Schemes	63
Ransomware	69
Summary	70
Solutions Fast Track	70
Frequently Asked Questions	73
Chapter 3 Alternative Botnet C&Cs	77
Introduction: Why Are There Alternative C&Cs?	78
Historical C&C Technology as a Road Map	79
DNS and C&C Technology	81
Domain Names	81
Multihoming	82
Alternative Control Channels	82
Web-Based C&C Servers	83
Echo-Based Botnets	83
Connect & Forget	84
File Data	84
URL Data	84
Command-Based Botnets	84
P2P Botnets	86
Instant Messaging (IM) C&Cs	86
Remote Administration Tools	87
Drop Zones and FTP-Based C&Cs	87
Advanced DNS-Based Botnets	89
Dynamic DNS	90
Fastflux DNS	90
Future Outlook	91
Summary	93
Solutions Fast Track	94
Frequently Asked Questions	95

Chapter 4 Common Botnets	97
Introduction	98
SDBot	98
Aliases	99
Infection	99
Signs of Compromise	100
System Folder	100
Registry Entries	101
Additional Files	102
Unexpected Traffic	103
Propagation	104
RBot	104
Aliases	105
Infection	105
Signs of Compromise	105
System Folder	105
Registry Entries	106
Terminated Processes	106
Unexpected Traffic	107
Propagation	108
Using Known Vulnerability Exploits	110
Exploiting Malware Backdoors	111
Agobot	111
Aliases	112
Infection	113
Signs of Compromise	113
System Folder	113
Registry Entries	113
Terminated Processes	114
Modify Hosts File	114
Theft of Information	114
Unexpected Traffic	115
Vulnerability Scanning	116
Propagation	116
Spybot	118
Aliases	118
Infection	118
Signs of Compromise	119
System Folder	119
Registry Entries	119
Unexpected Traffic	122
Keystroke Logging and Data Capture	122
Propagation	122
Mytob	123
Aliases	123

Infection	124
Signs of Compromise	124
System Folder	124
Registry Entries	125
Unexpected Traffic	125
Propagation	125
Summary	128
Solutions Fast Track	129
Frequently Asked Questions	131

Chapter 5 Botnet Detection: Tools and Techniques 133

Introduction	134
Abuse	134
Spam and Abuse	139
Network Infrastructure: Tools and Techniques	140
SNMP and Netflow: Network-Monitoring Tools	143
SNMP	144
Netflow	146
Firewalls and Logging	148
Layer 2 Switches and Isolation Techniques	151
Intrusion Detection	155
Virus Detection on Hosts	160
Heuristic Analysis	165
Snort as an Example IDS	168
Installation	169
Roles and Rules	169
Rolling Your Own	170
Tripwire	173
Darknets, Honeypots, and Other Snares	176
Forensics Techniques and Tools for Botnet Detection	179
Process	181
Event Logs	184
Firewall Logs	192
Antivirus Software Logs	198
Summary	208
Solutions Fast Track	208
Frequently Asked Questions	213

Chapter 6 Ourmon: Overview and Installation 217

Introduction	218
Case Studies: Things That Go Bump in the Night	220
Case Study #1: DDoS (Distributed Denial of Service)	220
Case Study #2: External Parallel Scan	222
Case Study #3: Bot Client	224
Case Study #4: Bot Server	226

How Ourmon Works	227
Installation of Ourmon	232
Ourmon Install Tips and Tricks	236
Summary	239
Solutions Fast Track	240
Frequently Asked Questions	241
Chapter 7 Ourmon: Anomaly Detection Tools	245
Introduction	246
The Ourmon Web Interface	247
A Little Theory	252
TCP Anomaly Detection	255
TCP Port Report: Thirty-Second View	255
Analysis of Sample TCP Port Report	262
TCP Work Weight: Details	265
TCP Worm Graphs	267
TCP Hourly Summarization	269
UDP Anomaly Detection	272
Detecting E-mail Anomalies	275
Summary	279
Solutions Fast Track	279
Frequently Asked Questions	283
Chapter 8 IRC and Botnets	285
Introduction	286
Understanding the IRC Protocol	286
Ourmon's RRDTOOL Statistics and IRC Reports	290
The Format of the IRC Report	292
Detecting an IRC Client Botnet	298
Detecting an IRC Botnet Server	304
Summary	309
Solutions Fast Track	309
Frequently Asked Questions	311
Chapter 9 Advanced Ourmon Techniques	313
Introduction	314
Automated Packet Capture	314
Anomaly Detection Triggers	317
Real-World Trigger Examples	319
Ourmon Event Log	324
Tricks for Searching the Ourmon Logs	325
Sniffing IRC Messages	329
Optimizing the System	334
Buy a Dual-Core CPU for the Probe	335
Separate the Front End and Back	
End with Two Different Computers	336
Buy a Dual-Core, Dual-CPU Motherboard	336

Make the Kernel Ring Buffer Bigger	336
Reduce Interrupts	337
Summary	339
Solutions Fast Track	339
Frequently Asked Questions	343
Chapter 10 Using Sandbox Tools for Botnets	345
Introduction	346
Describing CWSandbox	348
Describing the Components	352
Cwsandbox.exe	354
Cwmonitor.dll	356
Examining a Sample Analysis Report	359
The <analysis> Section	359
Analysis of 82f78a89bde09a71ef99b3cedb991bcc.exe	360
Analysis of Arman.exe	363
Interpreting an Analysis Report	368
How Does the Bot Install?	369
Finding Out How New Hosts Are Infected	371
How Does the Bot Protect the Local Host and Itself?	372
Determining How and Which C&C Servers Are Contacted	375
How Does the Bot Get Binary Updates?	376
What Malicious Operations Are Performed?	378
Bot-Related Findings of Our Live Sandbox	383
Summary	385
Solutions Fast Track	387
Frequently Asked Questions	390
Chapter 11 Intelligence Resources	391
Introduction	392
Identifying the Information an	
Enterprise/University Should Try to Gather	392
Disassemblers	395
PE Disassembler	395
DJ Java Decompiler	396
Hackman Disassembler	396
Places/Organizations Where Public Information Can Be Found	398
Antivirus, Antispyware, and Antimalware Sites	398
Viewing Information on Known Bots and Trojans	399
Professional and Volunteer Organizations	400
EDUCAUSE	400
NANOG	401
Shadowserver	401
Other Web Sites Providing Information	402
Mailing Lists and Discussion Groups	402
Membership Organizations and How to Qualify	403

Vetting Members	404
Confidentiality Agreements	404
What Can Be Shared	405
What Can't Be Shared	405
Potential Impact of Breaching These Agreements	406
Conflict of Interest	407
What to Do with the Information When You Get It	407
The Role of Intelligence Sources in Aggregating Enough Information to Make Law Enforcement Involvement Practical	409
Summary	411
Solutions Fast Track	411
Frequently Asked Questions	414
Chapter 12 Responding to Botnets	417
Introduction	418
Giving Up Is Not an Option	418
Why Do We Have This Problem?	420
Fueling the Demand: Money, Spam, and Phishing	421
Law Enforcement Issues	423
Hard Problems in Software Engineering	425
Lack of Effective Security Policies or Process	426
Operations Challenges	428
What Is to Be Done?	429
Effective Practices	430
Practices for Individual Computer Users	430
Enterprise Practices	432
How Might We Respond to Botnets?	434
Reporting Botnets	436
Fighting Back	437
The Saga of Blue Security	438
Some Observations about the Blue Frog Affair	442
Law Enforcement	443
Darknets, Honeynets, and Botnet Subversion	444
A Call to Arms	445
Summary	447
Solutions Fast Track	448
Frequently Asked Questions	451
Appendix A: FSTC Phishing Solutions Categories	453
Index	459