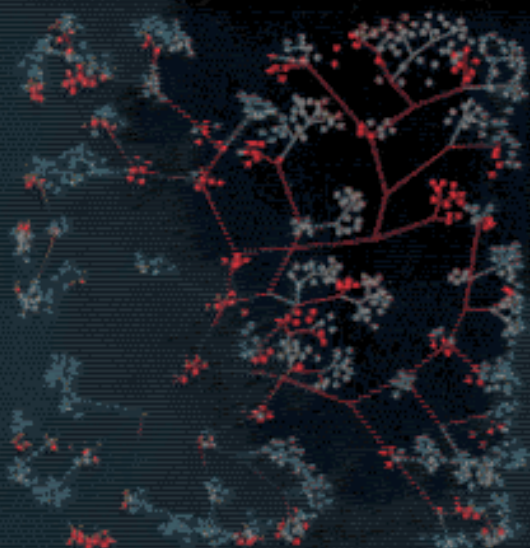


ARTECI HOUSE
COMPUTER SECURITY SERIES

*Defense and Detection
Strategies against*
Internet Worms



JOSE NAZARIO

Contents

Foreword	<i>xvii</i>
Preface	<i>xxi</i>
Acknowledgments	<i>xxvii</i>

1

Introduction	1
1.1 Why worm-based intrusions?	2
1.2 The new threat model	3
1.3 A new kind of analysis requirement	4
1.4 The persistent costs of worms	5
1.5 Intentions of worm creators	6
1.6 Cycles of worm releases	7
References	8

Part I Background and Taxonomy	9
--	---

2

Worms Defined	11
2.1 A formal definition	12
2.2 The five components of a worm	12
2.3 Finding new victims: reconnaissance	14
2.4 Taking control: attack	15
2.5 Passing messages: communication	15
2.6 Taking orders: command interface	16

2.7	Knowing the network: intelligence	17
2.8	Assembly of the pieces	18
2.9	Ramen worm analysis	19
2.10	Conclusions	21
	References	21

3 Worm Traffic Patterns 23

3.1	Predicted traffic patterns	23
3.1.1	<i>Growth patterns</i>	23
3.1.2	<i>Traffic scan and attack patterns</i>	25
3.2	Disruption in Internet backbone activities	26
3.2.1	<i>Routing data</i>	26
3.2.2	<i>Multicast backbone</i>	27
3.2.3	<i>Infrastructure servers</i>	28
3.3	Observed traffic patterns	28
3.3.1	<i>From a large network</i>	28
3.3.2	<i>From a black hole monitor</i>	30
3.3.3	<i>From an individual host</i>	31
3.4	Conclusions	34
	References	34

4 Worm History and Taxonomy. 37

4.1	The beginning	38
4.1.1	<i>Morris worm, 1988</i>	39
4.1.2	<i>HI.COM VMS worm, 1988</i>	41
4.1.3	<i>DECNet WANK worm, 1989</i>	42
4.1.4	<i>Hacking kits</i>	43
4.2	UNIX targets	44
4.2.1	<i>ADMwOrm-v1, 1998</i>	44
4.2.2	<i>ADM Millennium worm, 1999</i>	45
4.2.3	<i>Ramen, 2000</i>	46
4.2.4	<i>Ii0n worm, 2001</i>	47
4.2.5	<i>Cheese worm, 2001</i>	48
4.2.6	<i>sadmind/IIS worm, 2001</i>	48
4.2.7	<i>X.c: Telnetd worm, 2001</i>	49
4.2.8	<i>Adore, 2001</i>	49

4.2.9	<i>Apache worms, 2002</i>	50
4.2.10	<i>Variations on Apache worms</i>	51
4.3	Microsoft Windows and IIS targets	53
4.3.1	<i>mIRC Script.ini worm, 1997</i>	53
4.3.2	<i>Melissa, 1999</i>	54
4.3.3	<i>Love Letter worm, 2001</i>	54
4.3.4	<i>911 worm, 2001</i>	55
4.3.5	<i>Leaves worm, 2001</i>	56
4.3.6	<i>Code Red, 2001</i>	56
4.3.7	<i>Code Red II, 2001</i>	58
4.3.8	<i>Nimda, 2001</i>	59
4.3.9	<i>Additional e-mail worms</i>	60
4.3.10	<i>MSN Messenger worm, 2002</i>	60
4.3.11	<i>SQL Snake, 2002</i>	61
4.3.12	<i>Deloder, 2002–2003</i>	62
4.3.13	<i>Sapphire, 2003</i>	62
4.4	Related research	63
4.4.1	<i>Agent systems</i>	64
4.4.2	<i>Web spiders</i>	64
4.5	Conclusions	65
	References	65

5 Construction of a Worm 69

5.1	Target selection	69
5.1.1	<i>Target platform</i>	70
5.1.2	<i>Vulnerability selection</i>	71
5.2	Choice of languages	72
5.2.1	<i>Interpreted versus compiled languages</i>	72
5.3	Scanning techniques	74
5.4	Payload delivery mechanism	75
5.5	Installation on the target host	76
5.6	Establishing the worm network	77
5.7	Additional considerations	78
5.8	Alternative designs	78
5.9	Conclusions	80
	References	80

Part II Worm Trends 81

6 Infection Patterns 83

6.1	Scanning and attack patterns	83
6.1.1	<i>Random scanning</i>	83
6.1.2	<i>Random scanning using lists</i>	85
6.1.3	<i>Island hopping</i>	86
6.1.4	<i>Directed attacking</i>	87
6.1.5	<i>Hit-list scanning</i>	88
6.2	Introduction mechanisms	89
6.2.1	<i>Single point</i>	89
6.2.2	<i>Multiple point</i>	90
6.2.3	<i>Widespread introduction with a delayed trigger</i>	90
6.3	Worm network topologies	91
6.3.1	<i>Hierarchical tree</i>	91
6.3.2	<i>Centrally connected network</i>	93
6.3.3	<i>Shockwave Rider-type and guerilla networks</i>	94
6.3.4	<i>Hierarchical networks</i>	95
6.3.5	<i>Mesh networks</i>	96
6.4	Target vulnerabilities	97
6.4.1	<i>Prevalence of target</i>	97
6.4.2	<i>Homogeneous versus heterogeneous targets</i>	98
6.5	Payload propagation	99
6.5.1	<i>Direct injection</i>	99
6.5.2	<i>Child to parent request</i>	100
6.5.3	<i>Central source or sources</i>	101
6.6	Conclusions	102
	References	102

7 Targets of Attack 103

7.1	Servers	103
7.1.1	<i>UNIX servers</i>	104
7.1.2	<i>Windows servers</i>	104
7.2	Desktops and workstations	105
7.2.1	<i>Broadband users</i>	105
7.2.2	<i>Intranet systems</i>	107

7.2.3	<i>New client applications</i>	107
7.3	Embedded devices	108
7.3.1	<i>Routers and infrastructure equipment</i>	109
7.3.2	<i>Embedded devices</i>	109
7.4	Conclusions	110
	References	110

8

	Possible Futures for Worms	113
8.1	Intelligent worms	113
8.1.1	<i>Attacks against the intelligent worm</i>	117
8.2	Modular and upgradable worms	118
8.2.1	<i>Attacks against modular worms</i>	121
8.3	Warhol and Flash worms	122
8.3.1	<i>Attacks against the Flash worm model</i>	125
8.4	Polymorphic traffic	126
8.5	Using Web crawlers as worms	127
8.6	Superworms and Curious Yellow	129
8.6.1	<i>Analysis of Curious Yellow</i>	130
8.7	Jumping executable worm	130
8.8	Conclusions	131
8.8.1	<i>Signs of the future</i>	132
8.8.2	<i>A call to action</i>	132
	References	132

Part III Detection 135

9

	Traffic Analysis	137
9.1	Part overview	137
9.2	Introduction to traffic analysis	138
9.3	Traffic analysis setup	139
9.3.1	<i>The use of simulations</i>	141
9.4	Growth in traffic volume	142
9.4.1	<i>Exponential growth of server hits</i>	143
9.5	Rise in the number of scans and sweeps	143
9.5.1	<i>Exponential rise of unique sources</i>	145
9.5.2	<i>Correlation analysis</i>	147

9.5.3	<i>Detecting scans</i>	148
9.6	Change in traffic patterns for some hosts	148
9.7	Predicting scans by analyzing the scan engine	150
9.8	Discussion	156
9.8.1	<i>Strengths of traffic analysis</i>	156
9.8.2	<i>Weaknesses of traffic analysis</i>	156
9.9	Conclusions	158
9.10	Resources	158
9.10.1	<i>Packet capture tools</i>	158
9.10.2	<i>Flow analysis tools</i>	158
	References	159

10 Honeypots and Dark (Black Hole) Network Monitors 161

10.1	Honeypots	162
10.1.1	<i>Risks of using honeypots</i>	163
10.1.2	<i>The use of honeypots in worm analysis</i>	163
10.1.3	<i>An example honeypot deployment</i>	164
10.2	Black hole monitoring	164
10.2.1	<i>Setting up a network black hole</i>	166
10.2.2	<i>An example black hole monitor</i>	167
10.2.3	<i>Analyzing black hole data</i>	167
10.3	Discussion	170
10.3.1	<i>Strengths of honeypot monitoring</i>	170
10.3.2	<i>Weaknesses of honeypot monitoring</i>	171
10.3.3	<i>Strengths of black hole monitoring</i>	171
10.3.4	<i>Weaknesses of black hole monitoring</i>	172
10.4	Conclusions	172
10.5	Resources	173
10.5.1	<i>Honeypot resources</i>	173
10.5.2	<i>Black hole monitoring resources</i>	173
	References	173

11 Signature-Based Detection 175

11.1	Traditional paradigms in signature analysis	176
11.1.1	<i>Worm signatures</i>	177
11.2	Network signatures	177

11.2.1	<i>Distributed intrusion detection</i>	179
11.3	Log signatures	180
11.3.1	<i>Logfile processing</i>	181
11.3.2	<i>A more versatile script</i>	184
11.3.3	<i>A central log server</i>	188
11.4	File system signatures	190
11.4.1	<i>Chkrootkit</i>	190
11.4.2	<i>Antivirus products</i>	192
11.4.3	<i>Malicious payload content</i>	194
11.5	Analyzing the Slapper worm	195
11.6	Creating signatures for detection engines	198
11.6.1	<i>For NIDS use</i>	198
11.6.2	<i>For logfile analysis</i>	200
11.6.3	<i>For antivirus products and file monitors</i>	201
11.7	Analysis of signature-based detection	204
11.7.1	<i>Strengths of signature-based detection methods</i>	204
11.7.2	<i>Weaknesses in signature-based detection methods</i>	205
11.8	Conclusions	206
11.9	Resources	206
11.9.1	<i>Logfile analysis tools</i>	206
11.9.2	<i>Antivirus tools</i>	207
11.9.3	<i>Network intrusion detection tools</i>	207
	References	208

Part IV Defenses 209

12 Host-Based Defenses 211

12.1	Part overview	211
12.2	Host defense in depth	213
12.3	Host firewalls	213
12.4	Virus detection software	214
12.5	Partitioned privileges	216
12.6	Sandboxing of applications	219
12.7	Disabling unneeded services and features	221
12.7.1	<i>Identifying services</i>	221
12.7.2	<i>Features within a service</i>	223

12.8	Aggressively patching known holes	223
12.9	Behavior limits on hosts	225
12.10	Biologically inspired host defenses	227
12.11	Discussion	229
12.11.1	<i>Strengths of host-based defense strategies</i>	229
12.11.2	<i>Weaknesses of host-based defense strategies</i>	229
12.12	Conclusions	230
	References	230

13 Firewall and Network Defenses 233

13.1	Example rules	234
13.2	Perimeter firewalls	236
13.2.1	<i>Stopping existing worms</i>	237
13.2.2	<i>Preventing future worms</i>	238
13.2.3	<i>Inbound and outbound rules</i>	238
13.3	Subnet firewalls	239
13.3.1	<i>Defending against active worms</i>	239
13.4	Reactive IDS deployments	239
13.4.1	<i>Dynamically created rulesets</i>	240
13.5	Discussion	242
13.5.1	<i>Strengths of firewall defenses</i>	242
13.5.2	<i>Weaknesses of firewall systems</i>	242
13.6	Conclusions	242
	References	243

14 Proxy-Based Defenses 245

14.1	Example configuration	246
14.1.1	<i>Client configuration</i>	248
14.2	Authentication via the proxy server	249
14.3	Mail server proxies	249
14.4	Web-based proxies	251
14.5	Discussion	253
14.5.1	<i>Strengths of proxy-based defenses</i>	253
14.5.2	<i>Weaknesses of proxy-based defenses</i>	253
14.6	Conclusions	254

14.7 Resources	254
References	254

15 **Attacking the Worm Network** **257**

15.1 Shutdown messages	259
15.2 "I am already infected"	260
15.3 Poison updates	261
15.4 Slowing down the spread	262
15.5 Legal implications of attacking worm nodes	263
15.6 A more professional and effective way to stop worms	264
15.7 Discussion	266
15.7.1 <i>Strengths of attacking the worm network</i>	266
15.7.2 <i>Weaknesses of attacking the worm network</i>	266
15.8 Conclusions	267
References	267

16 **Conclusions** **269**

16.1 A current example	269
16.2 Reacting to worms	270
16.2.1 <i>Detection</i>	271
16.2.2 <i>Defenses</i>	272
16.3 Blind spots	273
16.4 The continuing threat	273
16.4.1 <i>Existing worms</i>	274
16.4.2 <i>Future worms</i>	274
16.5 Summary	275
16.6 On-line resources	275
16.6.1 <i>RFC availability</i>	275
16.6.2 <i>Educational material</i>	275
16.6.3 <i>Common vendor resources</i>	275
16.6.4 <i>Vendor-neutral sites</i>	276
References	277

About the Author **279**

Index **281**