

Index

A

- ABetterInternet adware, 74–76
- AbortSystemShutdown command, 64
- accept all cookie option, cookie privacy settings, 262
- access settings
 - Norton Personal Firewall, 115
 - ZoneAlarm Pro firewall, 113
- active content, Web pages
 - delivery and insertion methods, 53–54
 - discussed, 8–9
- Active Registry Monitor program, infestation detection and repair, 61
- Active Server Pages (ASP), 128
- ActiveX Controls, browser security, 243, 257
- AdBuster toolbar, pop-up blockers, 137
- address books, sender verification, 200
- Address Resolution Protocol (ARP), 93
- addresses. *See also* IP addressing
 - broadcast, 97
 - destination, 101
 - network, 97
 - numeric, 95
 - spoofed, 192
- Advanced tab (Windows Firewall), 108–109
- advertisements
 - spam, 193
 - spyware, 9
- adware. *See also* anti-adware
 - ABetterInternet, 74–76
 - defined, 10, 16
 - infestation repair and detection help options, 79
 - pop-up invasions, stopping, 10–12
 - scanners, 60, 145–147
 - spyware and, 10
- Ad-Aware SE anti-adware program, 150
- alerts
 - malware, 34–35, 39–40
 - spyware, 159
- alternate mailbox options, spam filtering services, 197
- always allowing pop-up setting, 136
- ALWIL avast! anti-virus program, 171, 181–182
- AnalogX Web site, 240
- annual security measures, 323–324
- anonymous logon, authentication security settings, 259
- Anthrax viruses, 23
- anti-adware. *See also* adware
 - Ad-Aware SE program, 150
 - Bazooka Adware and Spyware scanner, 161
 - defined, 142–143
 - discussed, 141–142
 - multiple blockers, 162
 - Pest Scan scanner, 148
 - reasons for, 143–145
 - resources, 163
 - Spy Sweeper 3.0 program, 150
 - X-Cleaner program, 148
- anti-spyware. *See also* spyware
 - Bazooka Adware and Spyware scanner, 161
 - discussed, 141–142
 - installing, 152–154
 - multiple blockers, 162
 - Pest Scan scanner, 148
 - reasons for, 142–145
 - resources, 163
 - Spy audit scanners, 148, 161
 - Spy Sweeper 3.0 program, 150
- anti-virus tools. *See also* viruses
 - ALWIL avast! program, 171, 181–182
 - Anti-Virus Review Web site, 184
 - clean system checks, 79
 - firewalls and, 167–168
 - F-Port, 20
 - F-Secure, 81
 - Grisoft AVG Anti-Virus program, 170
 - LiveUpdate services, 169

continued

anti-virus tools *continued*

- McAfee products, 170
- multiple packages, running, 183
- NAV (Norton AntiVirus) program, 171–175
- reasons for, 166–167
- resources, 184
- signature detection, 168
- Symantec products, 169
- virus definition updates, 71–72
- VirusScan program, 170, 177–179
- application label, malware prefixes, 36
- Application layer, TCP/IP, 93–94, 102–103
- applications, infection activities, 63
- ARP (Address Resolution Protocol), 93
- ASP (Active Server Pages), 128
- ASR (Automated System Recovery), 55
- attachments, e-mail, blocking, 223–226
- attacks
 - denial-of-service, 68
 - malware prefixes, 37
 - phishing, 233
- AuditMyPC Web site, 321
- audits, security, 321–322
- authentication security settings, 259–260
- Automated System Recovery (ASR), 55
- automation
 - automated replies, spam, 193–194
 - invocation, insertion and delivery methods, 50–52
 - logons, authentication security settings, 259
 - program controls, Norton Personal Firewall, 115
 - security, 308
- auto-protect option (Norton Anti-Virus program), 174
- AVG Anti-Virus program (Grisoft), 170
- avoiding
 - spoofs, 232–233
 - uncertain e-mail messages, 3

B

- backups
 - Norton Ghost utility, 62, 81
 - registry keys, 227–228
 - security measures, 306–307
- banners, 12–13

baselining systems

- overview, 271
- performance metrics, 280
- process inventory, 272–274
- resources, 293–294
- snapshots, 280–283
- tasklist command output, 274–278
- version differences, comparing, 284–288
- .bat file extension, 19
- Bazooka Adware and Spyware scanner, 161
- BBB (Better Business Bureau), 266
- Beagle malware attack, 24
- BGP (Border Gateway Protocol), 93
- BHO (Browser Help Object), 74–75, 77
- bizarre gibberish, spam, 194
- blacklisting, spam filtering services, 198
- blended threats, 25–26
- block all cookies option, privacy settings, 262
- blocked senders, sender verification, 200
- Blocked Zone, ZoneAlarm Pro firewall, 112
- blocking e-mail attachments, 223–226
- blocking pop-ups. *See also* pop-ups
 - AdBuster toolbar, 137
 - filter levels, 134
 - Google Toolbar, 137
 - intelligent blockers, 129–131
 - killing browsers, 130
 - multiple blockers, running, 139
 - Pop This! program, 137
 - Pop-up Killer Review Web site, 138
 - PopUpCheck Web site, 138
 - PopupTest Web site, 138
 - resources, 139–140
 - serial blockers, 130
 - SP2 (Service Pack 2), Windows XP, 120, 133–135
 - testing, 138
 - trainable blockers, 130
 - Window Shades program, 137
- blocking spam. *See also* spam
 - blacklisting, 198
 - Cloudmark SpamNet program, 215
 - e-mail basics, 187–191
 - filtering services, 197–201

Flow Ruler Web site, 214
 high filter level, 202
 low filter level, 202
 medium filter level, 202
 multiple spam blockers, 216–217
 Norton AntiSpam utility, 116, 202–205
 plug-ins, 201
 Qurb 2.0 program, 215
 reasons for, 192
 resources, 217–218
 Rules Wizard (Outlook), 206–210
 screening services, 195
 SP1 (Service Pack 1), 211–213
 Spam Inspector program, 215
 Spamarrest program, 215
 SpamCop program, 215
 spamXpress Web site, 214
 standalone programs, 201
 when to block, 194–196
 bloodhound option (Norton AntiVirus program),
 175
 bogus Microsoft security updates, 56
 booting
 boot-record infectors, viruses, 19
 safe mode, 65, 72
 Border Gateway Protocol (BGP), 93
 Brightmail Web site, 217
 broadcast addresses, IP addresses, 97
 Browser Help Object (BHO), 74–75, 77
 browsers
 active Web content, delivery and insertion
 methods, 53
 Firefox, 54, 244
 Mozilla, 54, 244
 Opera, 54, 245–246
 security, 243–247
 selection considerations, 54
 buffer overflows, vulnerabilities, 51
 bulletins
 bogus security updates, 56
 malware, 34–35, 39–40
 Virus Bulletin Web site, 40, 80
 bytes, IP addresses, 95

C

carbon copies, e-mail, 191
Catch-22 (Joseph Heller), 59
 Category 1 measure, malware, 30
 Category 2 measure, malware, 31, 66
 Category 3 measure, malware, 31
 Category 4 measure, malware, 31, 312
 Category 5 measure, malware, 31
 CAUCE (Coalitions Against Unsolicited Commercial
 E-mail), 217
 CDT (Central Daylight Time), 191
 CERT computer security, incident and vulnerability
 reporting, 33
 character data, 192
 chatting, 54
 Check Point Software Technologies, ZoneAlarm Pro
 firewall, 110–114
 CIAC (Computer Incident Advisory Center), 240
 Class A, IP addresses, 96–98
 Class B, IP addresses, 96–98
 Class C, IP addresses, 96–98
 Class D, IP addressed, 97
 Class E, IP addresses, 97
 Class ID (CLSID), 75
 clean system checks, PC infestation detection and
 repair, 79
 clearinghouses, malware, 29–30, 33
 ClientMan.msdaim spyware, 77–78
 closing pop-ups, 5
 Cloudmark SpamNet program, spam blockers,
 215
 CLSID (Class ID), 75
 CNET Downloads Web site, 52
 Coalitions Against Unsolicited Commercial E-mail
 (CAUCE), 217
 code additions, malware, 27
 COM (Common Object Model), 75, 243
 .com file extension, 19
 Comer, Douglas E. (*Internetworking with TCP/IP:
 Principles, Protocols, and Architecture*), 122,
 333
 command content, TCP/IP Application layer, 103

commands

- AbortSystemShutdown, 64
- Content-type, 192
- ipconfig, 96
- MIME-version, 192
- net share, 67
- netstat, 104
- nslookup, 234
- ntldr, 55
- tasklist, 279
- X-Mailer, 192
- Common Object Model (COM), 75, 243
- Common Vulnerabilities and Exposures (CVE), 34, 39
- Compare Files menu, WinDiff utility, 287
- Computer Emergency Readiness Team Web site, 25
- Computer Incident Advisory Center (CIAC), 240
- confidential information, virus alerts, 26
- configuration
 - controls and, Norton Personal Firewall, 115
 - default changes, infection activities, 63
- content security zone, Internet, 248
- Content-type command, 192
- cookies
 - defined, 4, 260
 - managing, 8
 - passive, 7
 - privacy settings, 261–264
 - resources, 269
- credit card purchases, money exchanges, 266
- curiosity claims, spam, 194
- current software maintenance, 302–306
- CVE (Common Vulnerabilities and Exposures), 34, 39
- Cyber Sentinel software program, 88
- Cyberpunk: Outlaws and Hackers on the Computer Frontier* (Katie Hafner and John Markoff), 40, 333
- CYBERSitter software program, 88

D

- dam malware suffix, 37
- damage headings
 - malware, 30
 - viruses, 26

- Damage metric, malware, 312
- data collecting programs, 7
- data offset, TCP/IP Transport layer, 102
- date and time information, malware reports, 33
- deceptive software, spyware, 8
- definition updates, viruses, 71–72
- Definitive Solutions Web site, 75
- deleting registry entries, 72–73
- delivery and insertion methods
 - active Web content, 53–54
 - automatic invocation, 50–52
 - e-mail attachments, 49
 - file transfers, 52–53
 - invitation only approach, 56
 - media-based infections, 55
 - pop-ups, 48
 - resources, 57
- denial-of-service attacks, 68
- deny access settings, ZoneAlarm Pro firewall, 113
- descriptions, malware reports, 34
- destination IP addresses, 101
- destination port, TCP/IP Transport layer, 102
- detection and repair, PC infestations
 - ABetterInternet adware, 74–76
 - Active Registry Monitor program, 61
 - clean system checks, 79
 - ClientMan.msdaim spyware, 77–78
 - ERD (emergency repair disk), 55
 - full-system scans, 72
 - help options, 78–79
 - hoaxes, 80
 - infection activities, 62–64
 - overview, 59
 - professional techniques and procedures, 61–62
 - registry entries, 72–73
 - Registry Watch program, 61
 - resources, 80–81
 - safe mode booting, 72
 - scanners, 60
 - System Restore utility, 69–71, 73–74
 - test machines, 61–62
 - virus definition updates, 71–72
 - W32.Randex.ATX file, 66–69

dialog windows, pop-ups, 128–129
 Disable option (Security Settings dialog box), 256
 discounted offers, spam, 194
 distribution measures, malware, 30
 Distribution metric, malware, 312
 DLLs (dynamic link libraries), 278
 DNS (domain name system), 99
 documentation, malware reports, 32
 dotted decimal forms, IP addresses, 95–96
 downloads
 drive-by, 7
 insertion and delivery methods, 52–53
 risky, 292–293
 safe download sites, 334
 security settings, 258
 dr malware suffix, 37
 drive-by downloads, 7
 drug violation, spam, 193
 dynamic link libraries (DLLs), 278
 dynamic port numbers, 103

E

eEye Digital Security Web site, 318
 Electronic Privacy Information Center, 10
 e-mail
 attachments, blocking, 223–226
 bogus security updates, 56
 carbon copies, 191
 EmailAbuse Web site, 217
 from line, 191
 hoaxes, recognizing, 230–231
 insertion and delivery methods, 49
 large scale e-mailing, virus alerts, 26
 mass mailers, 23
 Norton AntiVirus program options, 175
 phishing attacks, 233
 privacy policies, 237
 Received keyword, 191
 return path, 191
 safety resources, 237–240
 scams, 233–236
 screening, 229–230
 sender spoofing, 222

SMTP (Simple Mail Transfer Protocol), 94, 187
 spam blockers, 187–191
 spoofs, 231–233
 subject lines, 191
 time stamps, 191
 transit message time, 191
 uncertain messages, avoid opening, 3
 uncertain messages, spyware potential, 9
 viruses, 23–24
 Web-based, 223
 Emperor viruses, 23
 Enable option (Security Settings dialog box), 256
 ERD (emergency repair disk), 55
 Ethernet adapter connection, IP addressing, 99
 Eudora Web site, 214
 eWeek Web site, 316
 Exceptions tab (Windows Firewall), 107
 exclamation points in subject lines, hoax potential,
 230
 exclusions options (Norton AntiVirus program),
 175
 .exe file extension, 19
 exploits
 defined, 32
 exploit headings, malware, 30
 Extensible Markup Language (XML), 149

F

false familiarity, spam, 194
 Family malware suffix, 38
 Federal Trade Commission Web site, 8, 266
 File command, WinDiff utility, 286
 file deletion
 infection activities, 63
 malware, 27
 virus alerts, 26
 file extensions, 19
 file infectors, malware, 18
 file sharing sources, spyware, 8
 file systems, infection activities, 63
 File Transfer Protocol (FTP), 94
 file transfers, insertion and delivery methods,
 52–53

files

- .pst (personal store), 334
- svchost.exe, 278

filters

- e-mail, 237
- pop-up blockers, 134
- spam, 197–201

Firefox browser, 54, 244

firewalls

- anti-virus tools and, 167–168
- defined, 87–88
- Gibson Research Web site, 119
- Home PC Firewall Guide, 109
- ICF (Internet Connection Firewall), 106
- installing, 117–118
- Kerio Personal Firewall, 110
- multiple, running, 121
- network hubs, 122
- Norton Personal Firewall, 114–117
- packet inspections, 105
- resources, 122–123
- security scanners, 119
- Security Space Web site, 119
- Sygate Personal Firewall, 110
- TCP/IP and, 89–93
- Tiny Firewall 6.0, 110
- Windows, 106–109
- ZoneAlarm Pro, 110–114

flags

- IP header layout, 101
- TCP/IP Transport layer, 102

floppy disks, jump start, 20–22

Flow Ruler Web site, 214

forwardings, repeated, hoaxes, 231

F-Port anti-virus tool, 20

fragment offset, IP header layout, 101

Free Downloads Center Web site, 52

Frisk Software, malware sources, 39

from line, e-mail, 191

F-Secure anti-virus vendor, 81

FTP (File Transfer Protocol), 94

G

games, free, spyware potential, 8

Gates, Bill (Trustworthy Computing Initiative), 85–86, 122

gen malware suffix, 38

General tab (Windows Firewall), 106–107

GeoBytes Web site, 236

Gibson, Steve

- computer security merits, 16
- Gibson Research Web site, 119
- ShieldsUp! security scan, 132

GMT (Greenwich Mean Time), 191

Google Toolbar, pop-up blockers, 137

Grisoft AVG Anti-Virus program, 170

GUI (graphical user interface), 126–127

H

HackerWacker Web site, 119

Hafner, Katie (*Cyberpunk: Outlaws and Hackers on the Computer Frontier*), 40, 333

header layout, IP addressing, 100–101

Heller, Joseph (*Catch-22*), 59

help options, PC infestation repair and detection, 78–79

high filter levels

- cookie privacy settings, 262
- pop-up blockers, 134
- spam blockers, 202

Hill, Timothy (*Windows NT Shell Scripting*), 309

historical trends, spyware, 9

hives, defined, 76

hoaxes

- Hoax Busters Web site, 230, 240
- recognizing, 230–231
- repeated forwardings, 231
- resources, 80, 339
- social engineering, 80
- TruthOrFiction Web site, 240
- Vmyths Web site, 80

Home PC Firewall Guide, 109

Honeycutt, Jerry (*The Windows XP Registry Guide*),
81, 239, 294, 333
Host-to-Host layer, TCP/IP, 93
Housecall scanners, 60
HTML (Hypertext Markup Language), 149
HTTP (Hypertext Transfer Protocol), 94
HTTPS (Secure HTTP), 264
hustles, spam, 193
hybrid viruses, 25–26
HyperSafe Web site, 292
Hypertext Markup Language (HTML), 149
Hypertext Transfer Protocol (HTTP), 94

I

I am Not a Geek Web site, 293
IANA (Internet Assigned Numbers Authority), 105,
218
ICF (Internet Connection Firewall), 106
ICMP (Internet Control Message Protocol), 93, 108
ICSA (International Computer Security Association),
184
identification, IP header layout, 101
identify theft, spam, 193
in the wild terminology, malware, 29
InaQuick (IQ) utility, 81
infestations, detecting and repairing
 ABetterInternet adware, 74–76
 Active Registry Monitor program, 61
 clean system checks, 79
 ClientMan.msdaimg spyware, 77–78
 ERD (emergency repair disk), 55
 full-system scans, 72
 help options, 78–79
 hoaxes, 80
 infection activities, 62–64
 overview, 59
 professional techniques and procedures, 61–62
 registry entries, deleting, 72–73
 Registry Watch program, 61
 resources, 80–81
 safe mode booting, 72
 scanners, 60
 System Restore utility, 69–71, 73–74
 test machines, 61–62
 virus definition updates, 71–72
 W32.Randex.ATX file, 66–69
information gathering, malware reports, 32
insertion and delivery methods
 active Web content, 53–54
 automatic invocation, 50–52
 e-mail attachments, 49
 file transfers, 52–53
 invitation only approach, 56
 media-based infections, 55
 pop-ups, 48
 resources, 57
installing
 anti-spyware, 152–154
 personal firewalls, 117–118
 WinDiff utility, 284–286
instant messaging windows, 14
int malware suffix, 38
intelligent pop-up blockers, 129–131
International Computer Security Association (ICSA),
184
Internet
 content security zone, 248
 IANA (Internet Assigned Numbers Authority),
 105, 218
 ICF (Internet Connection Firewall), 106
 ICMP (Internet Control Message Protocol), 93,
 108
 Internet crash of 1988, 24
 Internet Official Protocol Standards, 90
 Internet Zone, ZoneAlarm Pro firewalls, 112
 IR (Internet Relay Chat), 54
 ISAKMP (Internet Security Association and Key
 Management Protocol), 104
Internet Explorer
 security settings, 247–251
 toolbars, 6

Internet layer, TCP/IP, 92–94
 Internet Protocol. *See* IP addressing
Internetworking with TCP/IP: Principles, Protocols, and Architecture (Douglas E. Comer), 122, 333
 Intranet, local content security zone, 249–251
 invisible Web pages, 4
 invitation only approach, delivery and insertion methods, 56
 IP (Internet Protocol) addressing
 broadcast addresses, 97
 bytes, 95
 Class A, 96–98
 Class B, 96–98
 Class C, 96–98
 Class D, 97
 Class E, 97
 destination, 101
 dotted decimal forms, 95–96
 Ethernet adapter connection, 99
 header layout, 100–101
 location lookups, 236
 logical numeric addresses, 95
 network addresses, 97
 octets, 95
 overview, 94
 physical numeric addresses, 95
 source, 101
 symbolic names, 95
 IP2Location Web site, 236
 ipconfig command, 96
 IQ (InaQuick) utility, 81
 IRC (Internet Relay Chat), 54
 ISAKMP (Internet Security Association and Key Management Protocol), 104

J
 Java
 Java programming language, 244
 JavaScript scripting language, 244
 JSP (Java Server Pages), 128
 JVM (Java Virtual Machine), 245, 258
 JIT (Just-In-Time) compiler, 54

 .js file extension, 19
 JSP (Java Server Pages), 128
 jump start floppy disks, 20–22
 Just-In-Time (JIT) compiler, 54
 JVM (Java Virtual Machine), 245, 258

K

Kasperksy Virus Encyclopedia, 24
 Kerio Personal Firewall, 110
 keyfilev1.txt directory, 287
 keyfilev2.txt directory, 287
 keys and values additions, infection activities, 63
 KeyWallet Web site, 292
 killing browsers, pop-up blockers, 130
 Knittel, Brian (*Windows XP Under the Hood: Hardcore Windows Scripting and Command Line Power*), 309

L

laboratories, infestation detection and repair, 61
 language, malware prefixes, 37
 Last Known Good Configuration (LKGC) option, 65
 layers, TCP/IP
 Application, 93–94, 102–103
 Host-to-Host, 93
 Internet, 92–94
 Network Access, 92–93
 Process, 93
 Transport, 93–94, 102
 LiveUpdate service
 anti-virus tools, 169
 virus definition updates, 71
 LKGC (Last Known Good Configuration) option, 65
 local content security zone, Intranet, 249–251
 location lookups, IP addressing, 236
 logical numeric (IP) addresses, 95
 logons, authentication security settings, 259
 low filter levels
 cookie privacy settings, 262
 pop-up blockers, 134
 spam blockers, 202

M

- @m malware suffix, 37
- macro viruses
 - defined, 20
 - malware prefixes, 36
- mail. *See* e-mail
- mailbox cleaning, spam filtering services, 197
- mailing lists, sender verification, 200
- Main tab (ZoneAlarm Pro firewall), 112
- malware
 - alerts, 34–35, 39–40
 - Beagle attack, 24
 - bulletins, 34–35, 39–40, 56
 - Category 1 measure, 30
 - Category 2 measure, 31, 66
 - Category 3 measure, 31
 - Category 4 measure, 31, 312
 - Category 5 measure, 31
 - clearinghouses, 29–30, 33
 - code additions, 27
 - damage headings, 30
 - Damage metric, 312
 - defined, 6, 17
 - distribution measures, 30
 - Distribution metric, 312
 - exploits, 30, 32
 - file deletion, 27
 - in the wild terminology, 29
 - naming, 36–38
 - Netsky attack, 24
 - payload headings, 30
 - prefixes, 36–37
 - propagation techniques, 303
 - reporting, 32–36, 39
 - risk assessment measures, 30–31
 - Sasser malware attack, 24, 35
 - scanners, 60
 - strange system activities, 27–28
 - system changes, monitoring, 27–29
 - threats, 32
 - Trojan horses, 25
 - vulnerabilities, 31–32, 34
 - Welchia attack, 24
 - Whatis Web site, 17
 - Wild metric, 312
 - worms, 24
- Malware: Fighting Malicious Code* (Ed Skoudis and Lenny Zelster), 40, 334
- manual entry, security software inventory, 299
- manual scan option (Norton AntiVirus program), 174
- Markoff, John (*Cyberpunk: Outlaws and Hackers on the Computer Frontier*), 40, 333
- mass mailers, e-mail, 23
- MBCA (Microsoft Security Baseline Analyzer), 303
- MBR (master boot record), 19
- McAfee
 - anti-virus products, 170
 - malware sources, 39
 - VirusScan program, 177–179
- media-based infections, insertion and delivery
 - methods, 55
- medium filter levels
 - cookie privacy settings, 262
 - pop-up blockers, 134
 - spam blockers, 202
- Melissa virus, 20
- message inspection, spam filtering services, 198
- message type, TCP/IP Transport layer, 102
- messages, e-mail
 - bogus security updates, 56
 - spyware, 9
 - uncertain, avoid opening, 3
 - uncertain, spyware potential, 9
- Microsoft
 - bogus security updates, 56
 - malware sources, 39
 - MBCA (Microsoft Security Baseline Analyzer), 303
 - Passport, 318–319
 - Windows 2000 Scripting Guide*, 309
- MIME-version command, 192
- @mm malware suffix, 37
- .mnu file extension, 19
- modeless dialog windows, pop-ups, 128–129

modem activity, infestation and infection signs, 46
 money exchanges, security options, 264–267
 monitoring system security, 289–290
 monthly security scans, 300
 Mozilla browser, 54, 244
 music sources, spyware, 8
 mutexes, 64

N

naming malware, 36–38
 NAV (Norton AntiVirus) program, 171–175
 .NET Framework security settings, 257
 Net Nanny software program, 88
 net share command, 67
 Netsky malware attack, 24
 netstat command, 104
 Network Access layer, TCP/IP, 92–93
 network addresses, IP addresses, 97
 network hubs, firewalls, 122
 network interface activity, infestation and infection signs, 46
 networking controls, Norton Personal Firewall, 115
 networking model, TCP/IP, 92–93
 news, security sources, 315
 NNTP (Network News Transport Protocol), 94
 normal startup timing activities, 280
 Norton

- AntiSpam utility, 116, 202–205
- NAV (Norton AntiVirus) program, 171–175
- Norton Ghost utility, 62, 81
- Norton Personal Firewall, 114–117

 nslookup command, 234
 ntlldr command, 55
 numeric addresses, IP addresses, 95

O

OASIS (Organization for the Advancement of Structured Information Standards), 268
 octets, defined, 95
 OLE (object linking and embedding), 243
 One_Half viruses, 23

Opera browser, 54, 245–246
 ordinary windows, pop-ups, 128
 Organization for the Advancement of Structured Information Standards (OASIS), 268
 OSPF (Open Shortest Path First) protocol, 94
 Outlook

- Rules Wizard, 206–210
- SP1 (Service Pack 1), 211–213

 overflows, buffers, 51
 Overview page, ZoneAlarm Pro firewall, 111–112
 .ovl file extension, 19

P

Pacific Daylight Time (PDT), 191
 packet inspections, firewalls, 105
 Packet Internetnetwork Groper (PING), 94
 Panda Software, malware sources, 39
 Passport (Microsoft), 318–319
 passwords

- password handling, 290–292
- Password Safe Web site, 292
- resources, 336

 patches, for vulnerabilities, 303
 payload headings

- malware, 30
- viruses, 26

 PC infestations, detecting and repairing

- ABetterInternet adware, 74–76
- Active Registry Monitor program, 61
- clean system checks, 79
- ClientMan.msdaim spyware, 77–78
- ERD (emergency repair disk), 55
- full-system scans, 72
- help options, 78–79
- hoaxes, 80
- infection activities, 62–64
- overview, 59
- professional techniques and procedures, 61–62
- registry entries, deleting, 72–73
- Registry Watch program, 61
- resources, 80–81

- safe mode booting, 72
- scanners, 60
- System Restore utility, 69–71, 73–74
- test machines, 61–62
- virus definition updates, 71–72
- W32.Randex.ATX file, 66–69
- PDT (Pacific Daylight Time), 191
- performance
 - slow, potential spyware infestation, 9
 - system baselining, 280
 - virus alerts, 26
- personal firewalls. *See* firewalls
- personal store (.pst) files, 306
- Pest Scan scanners, 60, 148
- phishing attacks, 233
- physical numeric IP addresses, 95
- .pif file extension, 19
- PING (Packet Internet Groper), 94
- platform name, malware prefixes, 36
- plug-ins, spam blockers, 201
- Point-to-Point Tunneling Protocol (PPTP), 93
- pop-uppers, 12
- Pop-up Killer Review Web site, 138
- PopUpCheck Web site, 127, 138
- pop-ups. *See also* blocking pop-ups
 - always allowing setting, 136
 - banners and, 12–13
 - closing, 5
 - continuous streams, 12
 - defined, 126–127
 - delivery and insertion methods, 48
 - infestation and infection signs, 48
 - instant messaging windows, 14
 - modeless dialog windows, 128–129
 - ordinary windows, 128
 - pop-uppers, 12
 - sexual related, 10
 - spyware, 9
 - stopping invasions, 10–12
 - synthesized windows, 128
 - temporarily allowing setting, 136
 - unfathered windows, 129
- PopupTest Web site, 138
- porn solicitation, spam, 193
- ports
 - destination, 103
 - dynamic port numbers, 103
 - IANA (Internet Assigned Numbers Authority), 105, 218
 - registered port numbers, 103
 - source, 103
 - well-known port numbers, 103
- potential infestation, spyware, 9
- PPPoE (PPP over Ethernet) protocol, 93
- PPTP (Point-to-Point Tunneling Protocol), 93
- prefixes, malware, 36–37
- .prg file extension, 19
- privacy
 - cookies, 261–264
 - e-mail settings, 237
 - Electronic Privacy Information Center, 10
- process changes, stop and start functions, infection activities, 64
- process inventory, system baselining, 272–274
- Process layer, TCP/IP, 93
- professional techniques and procedures, PC infestation, detection and repair, 61–62
- program controls
 - Norton Personal Firewall, 117
 - ZoneAlarm Pro firewall, 114
- Prompt option (Security Settings dialog box), 256
- propagation techniques, malware, 303
- protocol suite, defined, 89
- protocols
 - ARP (Address Resolution Protocol), 93
 - BGP (Border Gateway Protocol), 93
 - FTP (File Transfer Protocol), 94
 - HTTP (Hypertext Transfer Protocol), 94
 - ICMP (Internet Control Message Protocol), 93, 108
 - NNTP (Network News Transport Protocol), 94

continued

protocols *continued*

- OSPF (Open Shortest Path First) protocol, 94
- PPTP (Point-to-Point Tunneling Protocol), 93
- RIP (Routing Information Protocol), 94
- services and, 89
- SMTP (Simple Mail Transfer Protocol), 94, 187
- UDP (User Datagram Protocol), 94
- X.25 protocol, 93

.pst (personal store) files, 306

public malware reports, 35

Q

Qurb 2.0 program, spam blockers, 215

R

Received keyword, 191

recognition capabilities, spam, 195–196

recovery, ASR, 55

registered port numbers, 103

registry entries, deleting, 72–73

registry keys

- backing up, 227–228

- discussed, 281

Registry Watch program, infestation detection and repair, 61

repair and detection, PC infestations

- ABetterInternet adware, 74–76

- Active Registry Monitor program, 61

- clean system checks, 79

- ClientMan.msdaim spyware, 77–78

- ERD (emergency repair disk), 55

- full-system scans, 72

- help options, 78–79

- hoaxes, 80

- infection activities, 62–64

- overview, 59

- professional techniques and procedures, 61–62

- registry entries, 72–73

- Registry Watch programs, 61

- resources, 80–81

- safe mode booting, 72

- scanners, 60

- System Restore utility, 69–71, 73–74

- test machines, 61–62

- virus definition updates, 71–72

- W32.Randex.ATX file, 66–69

repeated forwardings, hoax potential, 231

reports, malware

- CERT computer security, incident and vulnerability reporting, 33

- date and time information gathering, 33

- detailed descriptions, 34

- information gathering, 33

- publicizing, 35

- repair and recovery tools and techniques, 34

- resources, 39

Requests for Comments (RFCs), 90

resources

- adware, 163

- books and articles, 333–334

- cookies, 269

- delivery and insertion methods, 57

- download sites, 334

- e-mail safety, 239–240

- firewalls, 122–123

- hoaxes, 80, 339

- Microsoft Knowledge Base articles, 333

- password management, 336

- PC infestation detection and repair, 78–81

- pop-up blockers, 139–140

- scanners, 334

- security, 268–270

- software, 339

- spam, 217–218, 335

- spyware, 16, 163

- system baselining, 293–294

- TCP/IP, 122–123

- virus tools, 184

restart timing activities, 280

restoration, System Restore utility
 normal operation, returning to, 73–74
 overview, 69–71
 restore points, 71

Restricted Zone
 Internet options, 253
 Norton Personal Firewall, 115

return path, e-mail, 191

RFCs (Requests for Comments), 90

RIP (Routing Information Protocol), 94

risk assessment measures, malware, 30–31

RoboForm Web site, 292

Rules Wizard (Outlook), 206–210

runtime environment, infection activities, 64

S

safe mode booting, 65, 72

safety. *See* security

Sasser malware attack, 24, 35

scams
 e-mail, 233–236
 ScamBusters Web site, 236
 spam, 193

scanners
 adware, 60, 145–147
 Bazooka Adware and Spyware, 161
 full-system scans, 72
 HackerWacker Web site, 119
 Housecall, 60
 malware, 60
 monthly security scans, 300
 PC infestations, detection and repair, 60
 Pest Scan, 60, 148
 resources, 334
 ShieldUp!, 132
 Spy audit, 60, 148, 161
 Spybot-Search & Destroy program, 145–147
 spyware, 60, 145–147
 VirusScan program, 177–179

Schweitzer, Douglas (*Securing the Network From Malicious Code*), 184, 334

.scr file extension, 19

screening services
 e-mail, 229–230
 spam, 14, 195

Scrimger, Rod (*TCP/IP Bible*), 123, 334

scripts
 active Web content, delivery and insertion methods, 53
 script blocking option (Norton AntiVirus program), 174
 security controls, 259

SearchSmallBizIT Web site, 217

Secunia Web site, 317

Secure Data Manager Web site, 292

Secure HTTP (HTTPS), 264

Secure Sockets Layer (SSL), 264

Securing the Network From Malicious Code (Douglas Schweitzer), 184, 334

security
 annual, 323–324
 audits, 321–322
 authentication, 259–260
 automated, 308
 backups, 306–307
 bogus Microsoft updates, 56
 browser, 243–247
 CERT computer security, incident and vulnerability reporting, 33
 cookies, 260–264
 download settings, 258
 e-mail, 237–239
 Electronic Privacy Information Center, 10
 general sources of, 315
 ICSA (International Computer Security Association), 184
 Internet Explorer, 247–251
 ISAKMP (Internet Security Association and Key Management Protocol), 104
 MBCA (Microsoft Security Baseline Analyzer), 303

continued

- security *continued*
- money exchanges, 264–267
 - monthly scans, 300
 - .NET Framework, 257
 - news sources, 315
 - Norton Personal Firewall control levels, 116
 - password handling, 290–292
 - resources, 268–270
 - scripting, 259
 - Security Settings dialog box, 256
 - security suite products, 328–330
 - software inventory, 298–299
 - system security, monitoring, 289–290
 - third-party threat information, 316–318
 - updates, 267
 - U.S. Securities and Exchange Commission Web site, 236
 - vendor-specific sources, 315
 - virus alerts, 26
 - ZoneAlarm Pro firewall control levels, 113
- Security Focus Web site, 40, 318
- Security Space Web site, 119
- Security Zones (Internet Explorer), 54
- senders
- classifications, spam filtering services, 197
 - sender spoofing, 222
 - verification, 200
- sequence numbers, TCP/IP Transport layer, 102
- serial pop-up blockers, 130
- Service Pack 1 (SP1), Outlook, 211–213
- Service Pack 2 (SP2), Windows XP, 86, 120
- services and protocols, 89
- sexual content
- pop-ups, 10
 - spam, 193
- Shareware Web site, 52
- ShieldsUp! security scan, 132
- signature detection, anti-virus tools, 168
- sites. *See* Web sites
- Skoudis, Ed (*Malware: Fighting Malicious Code*), 40, 334
- slow performance, potential spyware infestation, 9, 46
- SMTP (Simple Mail Transfer Protocol), 94, 187
- snapshots
- infestation detection and repair, 61
 - system baselining, 280–283
- social engineering, hoaxes, 80
- software
- Cyber Sentinel program, 88
 - CYBERSitter program, 88
 - infestation detection and repair, 61
 - keeping current, 302–306
 - Net Nanny program, 88
 - resources, 339
 - security software inventory, 298–299
- source domain name, TCP/IP Application layer, 103
- source IP addresses, 101
- source port, TCP/IP Transport layer, 102
- spam. *See also* blocking spam
- advertisements, 193
 - automated replies, 193–194
 - bizarre gibberish, 194
 - curiosity claims, 194
 - defined, 14, 16
 - discounted offers, 194
 - drug violations, 193
 - false familiarity, 194
 - hustles, 193
 - identity theft, 193
 - porn solicitation, 193
 - recognition capabilities, 195–196
 - resources, 335
 - scams, 193
 - screening services, 14
 - sender verification, 200
 - sexual content, 193
 - solutions to, 14
 - Spam Inspector program, 215
 - spambots, 14
 - spamXpress Web site, 214

- special offers, 194
- strange character sets, 194
- Whatis Web site, 14
- special offers, spam, 194
- SP1 (Service Pack 1), Outlook, 211–213
- spoofing
 - avoiding, 232–233
 - e-mail, 231–233
 - sender, 222
 - spoofed addresses, 192
- SP2 (Service Pack 2), Windows XP, 86, 120
- Spy audit scanners, 60, 148, 161
- Spy Sweeper 3.0 anti-adware/anti-spyware program, 150
- Spybot-Search & Destroy program, 145–147
- spyware. *See also* anti-spyware
 - advertisements, 9
 - adware and, 10
 - alerts, 159
 - ClientMan.msdaimg, 77–78
 - deceptive software, 8
 - defined, 7, 16
 - drive-by download, 7
 - examples of, 8–9
 - historical trends, 9
 - infestation repair and detection help options, 79
 - pop-ups, 9
 - potential infestation, 9
 - resources, 16
 - scanners, 60, 145–147
 - Spyware Guide Web site, 40
 - Whatis Web site, 7–8
- Spyware Info Web site, 317
- Spyware Warrior Web site, 317
- SSL (Secure Sockets Layer), 264
- standalone programs, spam, 201
- standards, Internet Official Protocol Standards, 90
- startup, normal startup timing activities, 280
- statistics, Norton Personal Firewall, 115

- stop and start process changes, infection activities, 64
- strange character sets, spam, 194
- strange system activities, malware, 27–28
- subject lines, e-mail, 191, 230
- suffixes, malware, 37–38
- Surfer Beware Web site, 317
- svchost.exe file, 278
- Sygate Personal Firewall, 110
- Symantec
 - anti-virus products, 169
 - malware sources, 39
 - Symantec Virus Encyclopedia, 24
- symbolic names, IP addresses, 95
- synecdoche naming mechanism, TCP/IP, 90
- synthesized windows, pup-ups, 128
- .sys file extension, 19
- system baselining
 - overview, 271
 - performance metrics, 280
 - process inventory, 272–274
 - resources, 293–294
 - snapshots, 280–283
 - tasklist command output, 274–278
 - version differences, comparing, 284–288
- system changes, monitoring, 27–29
- system infectors, viruses, 19
- system instability, virus alerts, 26
- System Restore utility
 - enabling/disabling, 69–70
 - normal operation, returning to, 73–74
 - restore points, 71
- system security, monitoring, 289–290

T

- Task Manager (Windows), 11
- tasklists
 - tasklist command, 279
 - tasklist command output, system baselining, 274–278

- TCP/IP Bible* (Rod Scrimger), 123, 334
 - TCP/IP (Transmission Control Protocol/Internet Protocol)
 - Application layer, 93–94, 102–103
 - capabilities of, 90
 - Host-to-Host layer, 93
 - Internet layer, 92–94
 - Network Access layer, 92–93
 - networking model, 92–93
 - port numbers, 103–105
 - Process layer, 93
 - protocol suite, 89
 - resources, 122–123
 - RFCs (Requests for Comments), 90
 - synecdoche naming mechanism, 90
 - TCP/IP stack, 91–94
 - Transport layer, 93–94, 102
 - TCP (Transmission Control Protocol), 90, 94
 - TechTarget Web site, 316
 - temporarily pop-up setting, 136
 - Tequilla viruses, 23
 - testing
 - pop-up blockers, 138
 - test machines, infestation detection and repair, 61–62
 - threats
 - defined, 32
 - Norton AntiVirus program, 175
 - potential trouble, avoiding, 320–321
 - third-party threat information, 316–318
 - vendor threat information, 318–320
 - time
 - time and date information, malware reports, 33
 - time stamps, e-mail, 191
 - time zones, 191
 - Tiny Firewall 6.0, 110
 - toolbars, Internet Explorer, 6
 - TOS (Type of Service), 100
 - trainable pop-up blockers, 130
 - transferring files, insertion and delivery methods, 52–53
 - transit message time, e-mail, 191
 - Transmission Control Protocol/Internet Protocol.
 - See* TCP/IP
 - Transmission Control Protocol (TCP), 90, 94
 - Transport layer, TCP/IP, 93–94, 102
 - Trend Micro Virus Encyclopedia, 24
 - Trojan horses
 - defined, 25
 - infestation repair and detection help
 - options, 79
 - Trusted Zone
 - Internet options, 252
 - Norton Personal Firewall, 115
 - ZoneAlarm Pro firewall, 112
 - Trustworthy Computing Initiative (Bill Gates), 85–86, 122
 - TruthOrFiction Web site, 240
 - Tucows Web site, 53
 - Type of Service (TOS), 100
- ## U
- UCT (Universal Coordinated Time), 191
 - UDP (User Datagram Protocol), 94
 - uncertain e-mail messages
 - avoid opening, 3
 - spyware potential, 9
 - unfathered windows, pop-ups, 129
 - Universal Coordinated Time (UCT), 191
 - updates
 - bogus Microsoft security, 56
 - security reasons, 267
 - vulnerabilities, 303
 - urgent subject lines, hoax potential, 230
 - U.S. Securities and Exchange Commission
 - Web site, 236
 - US-ASCII character data, 192
 - User Datagram Protocol (UDP), 94

V

- .vb file extension, 19
- .vbe file extension, 19
- .vbs file extension, 19
- vendor threat information, 318–320
- vendor-specific security sources, 315
- versions
 - difference comparisons, 284–287
 - IP header layout, 100
- Virus Bulletin Web site, 40, 80
- viruses. *See also* anti-virus tools
 - Anthrax, 23
 - blended threats and, 25–26
 - boot-record infectors, 19
 - categorizing, 23
 - Computer Emergency Readiness Team Web site, 25
 - damage headings, 26
 - defined, 18
 - definition updates, 71–72
 - denial-of-service attacks, 68
 - e-mail, 23–24
 - Emperor, 23
 - file infectors, 18
 - F-Port anti-virus tool, 20
 - hybrid, 25–26
 - infestation repair and detection help options, 79
 - Kaspersky Virus Encyclopedia, 24
 - macro, 20, 36
 - Melissa, 20
 - One_Half, 23
 - payload headings, 26
 - scanning for, 28
 - Symantec Virus Encyclopedia, 24
 - system infectors, 19
 - Tequilla, 23
 - Trend Micro Virus Encyclopedia, 24
 - Whatis Web site, 18
 - W97M.Jedi, 27

- VirusScan program, 170, 177–179
- Vmyths Web site, 80
- vulnerabilities
 - buffer overflows, 51
 - CERT computer security, 33
 - CVE (Common Vulnerabilities and Exposures), 34, 39
 - overview, 31–32
 - patches for, 303
 - updates, 303

W

- Web pages
 - active content, 8–9, 53–54
 - invisible, 4
- Web sites
 - AnalogX, 240
 - Anti-Virus Review, 184
 - AuditMyPC, 321
 - Brightmail, 217
 - CNET Downloads, 52
 - Computer Emergency Readiness Team, 25
 - Definitive Solutions, 75
 - eEye Digital Security, 318
 - EmailAbuse, 217
 - Eudora, 214
 - eWeek, 316
 - Federal Trade Commission, 8, 266
 - Flow Ruler, 214
 - Free Downloads Center, 52
 - GeoBytes, 236
 - Gibson Research, 119
 - HackerWacker, 119
 - Hoax Busters, 230, 240
 - HyperSafe, 292
 - I am Not a Geek, 293
 - IP2Location, 236
 - KeyWallet, 292

continued

Web sites *continued*

- Password Safe, 292
- PopUpCheck, 127, 138
- Pop-up Killer Review, 138
- PopupTest, 138
- RoboForm, 292
- ScamBusters, 236
- SearchSmallBixIT, 217
- Secunia, 317
- Secure Data Manager, 292
- Security Focus, 40, 318
- Security Space, 119
- Shareware, 52
- spamXpress, 214
- Spyware Guide, 40
- Spyware Info, 317
- Spyware Warrior, 317
- Surfer Beware, 317
- TechTarget, 316
- TruthOrFiction, 240
- Tucows, 53
- U.S. Securities and Exchange Commission, 236
- Virus Bulletin, 40, 80
- Vmyths, 80
- Web-based e-mail, 223
- Welchia malware attack, 24
- well-known port numbers, 103
- Whatis Web site
 - e-mail virus definition, 23
 - malware definition, 17
 - pop-up definition, 127
 - spam definition, 14
 - Trojan horse definition, 25
 - virus definition, 18
- Wild metric, malware, 312
- WinDiff utility
 - closing, 288
 - Compare Files menu, 287
 - discussed, 81
 - File command, 286

- installing, 284–286

- launching, 286

- Window Shades program, pop-up blockers, 137

- `window.open()` operator, 128

Windows

- runtime environment, infection activities, 64

- Task Manager, 11

- Windows Firewall, 106–109

- Windows XP Service Pack 2 (SP2), 86, 120

- Windows NT Shell Scripting* (Timothy Hill), 309

- Windows registry, infection activities, 63

- Windows 2000 Scripting Guide* (Microsoft Corporation), 309

- The Windows XP Registry Guide* (Jerry Honeycutt), 81, 239, 294, 333

- Windows XP Under the Hood: Hardcore*

- Windows Scripting and Command Line*

- Power* (Brian Knittel), 309

- `window.showModelessDialog()` operator, 128

- WinLogo key sequences, 71

- WinTasks program, 294

worms

- Beagle malware attack, 24

- infestation repair and detection help options, 79

- Internet crash of 1988, 24

- Netsky malware attack, 24

- Norton AntiVirus program options, 175

- Sasser malware attack, 24, 35

- Welchia malware attack, 24

- `.ws` file extension, 19

- `.wsc` file extension, 19

- `.wsf` file extension, 19

- W32.Randex.ATX file, 66–69

X

- X-Cleaner program, anti-adware, 148

- X-Mailer command, 192

- XML (Extensible Markup Language), 149

- X.25 protocol, 93

Z

Zelster, Lenny (*Malware: Fighting Malicious Code*),
40, 334

zombies, defined, 68

ZoneAlarm Pro firewall

access settings, 113

Block Zone, 112

Check Point Software Technologies, 110

Internet Zone, 112

Main tab, 112

Overview page, 111–112

Program Control window, 114

security control levels, 113

Trusted Zone, 112

Zones tab, 112

