

INDEX

A

Adminius, 22, 238, 242
air gaps, 90, 93–94, 99–100
AntiY, 118–119
Ars Technica, 104

B

baker's yeast (*Saccharomyces cerevisiae*), xxi, 229
banking trojans
 evolution beyond banking,
 167–169
 initial classification, 155
 transition to access brokers,
 216, 218
Bitcoin, 188
Botnetium, 156, 238, 242
Buchanan, Ben, 130
buffer overflow, 41, 46, 53, 184

C

C2. *See* command-and-control
CaddyWiper, 151
centrifuges, uranium-enrichment,
 84, 86, 94–95, 101
Centrifugium, 84, 238, 242
China
 attribution speculation, 37
 GhostNet campaign, 76–80
Chosun Expo, 197
CIH virus, 99
CISA (Cybersecurity and
 Infrastructure Security
 Agency), 217
Code Red II, 33
command-and-control (C2),
 65, 66, 71–72, 121–122, 162,
 210–211

Computer Fraud and Abuse Act, 18
Conti, 166
Controllor, 64, 236
CrackedCantil, xiv–xv
CrashOverride. *See* Industroyer
critical infrastructure, 104, 135,
 147–152, 223
Cryptor, 178, 235, 236
CrySyS, 117–121
Cutler, Silas, 123
CVE-2010-2568, 89
CVE-2010-2729, 90
CVE-2010-2743, 90
CVE-2010-3338, 90
CVE-2017-0144, 183, 190
cyber attribution, 104, 130,
 149–150, 196–197,
 217–218, 226
cyber espionage
 GhostNet campaign,
 76–80
 reconnaissance platforms,
 106–108
 state-sponsored surveillance,
 125, 131–132
Cybersecurity and Infrastructure
 Security Agency (CISA), 217
CyOTE, 148–149

D

Darwin, Charles, xxiv
Davis–Besse nuclear power
 plant, 56
de Guzman, Onel, 12–13
Denior, 42, 236
Destroyer, 84, 236
digital certificates, stolen
 or forged, 92, 102, 116–117,
 130–131

DLL injection, 70, 162–163, 207
 DoublePulsar, 184–186, 191
 Dridex, 218
 dual-use software, xxi
 Dunaev, Vladimir, 173
 Duqu, 106–107
 Dyre, 168

E

electrical grid attacks, 141–148
 Electronic Commerce Act of
 2000, 14
 email
 credential harvesting, 162
 ILOVEYOU message, 6
 as propagation vector, 17,
 27–28, 69, 161, 198
 Emotet, 161
 ESET, 150
 espionage. *See* cyber espionage
 EternalBlue, 183–184, 190–191
Eternalblueium, 178, 242
 Eurojust, 173
 Evil Corp, 218

F

Fararo Paya, 94
 FBI (Federal Bureau of
 Investigation), 217
 fermentation, xvi
 Flame (sKyWIper)
 adaptation, 120, 132
 anatomy, 112–115
 attribution, 128–130
 Bluetooth surveillance, 119–120
 CLAN database, 121
 forged certificates, 116–117,
 130–131
 Lenaean classification, 112
 Lua scripting, 120
 MD5 collision attack, 117
 modular architecture, 119–120
 self-removal, 123

G

Gh0stius, 64, 238, 242
 Gh0st RAT
 adaptation, 80
 anatomy, 64–68
 command protocol, 71–72
 descendants, 78–80
 infection vectors, 69–70
 Lenaean classification, 64
 modular architecture, 73–74
 persistence, 71
 remote-control capabilities,
 72–73
 GhostNet, 76–77
 GodRAT, 79, 81
 GRU (Russian military
 intelligence), 149–150, 218
 Guerrero-Saade, Juan Andrés, 123

H

hidden file extensions, 7, 27
 Hutchins, Marcus, 194–195

I

ICS. *See* industrial control systems
 IEC 60870-5-101, 142
 IEC 60870-5-104, 142, 150
 IEC 61850, 142–143
 IEDs (intelligent electronic
 devices), 142
 IIS (Internet Information
 Services), 26, 29, 33
 ILOVEYOU (Love Bug)
 anatomy, 2–6
 economic impact, 15–16
 email message, 6
 file types targeted, 9–10
 legal response, 12–14
 Lenaean classification, 2
 and Morris worm, 17
 patient zero, 11–13
 persistence mechanisms, 8, 10

propagation, 7–10
and VBScript, 7
industrial control systems (ICS),
83, 99, 105, 142, 144, 146.
See also PLCs; SCADA
industrial protocols, 142, 150
industrial sabotage, 94–97, 106–108
Industroyer (CrashOverride)
adaptation, 151
anatomy, 136–140
attribution, 149–151
circuit breakers, 143, 144
industrial protocols, 142, 150
Lenaean classification, 136
Pivnichna substation attack,
141, 148
and Sandworm, 149–151
Ukraine grid blackout, 141,
147–148
wiper component, 151
Industroyer2, 150–151, 153
Infectior, 2, 22, 236
intelligent electronic devices
(IEDs), 142
Internet Explorer, 10, 27
Internet Information Services
(IIS), 26, 29, 33
Iran
cyber operations, 102, 125,
127–128
nuclear program, 84, 92, 96

J

JMicron Technology, 92

K

kill switch, 194–195
Kyiv, 141, 148

L

ladder logic, 88, 93
Lazarus Group, 196–197

Lenaean Taxonomy.

See also Malmons

adaptation to malware, xix
definition of malware, xx
function orders, 235–237
location and year, 239–241
operating system prefixes,
232–233
origin of name, xix, 230
philosophy, 243–245
structure, 230–232
trait epithets, 237–239
type kingdoms, 233–235
Linnaeus, Carl, xix, 229, 230
Litchfield, David, 59
living off the land, 163, 207–208
loaders, 70, 116, 161–162, 209,
212–213

Loador, 202, 236

Love Bug. *See* ILOVEYOU

Loveletterius, 2, 238, 242

M

Malmons (Malware Monsters)

defined, xxiii–xxiv
ecological roles, 231
functions summarized, 236
habitats summarized, 232
in Lenaean taxonomy, 230–232
lessons from, 222–224
morphological transcription, xxiv
specimens summarized, 242
traits summarized, 238
types summarized, 234
malware. *See also* Lenaean

Taxonomy

behavior, ecological view, xviii
definition, Lenaean, xx
naming, xix, 230, 243–245
phylogeny, 18
as (un)natural, xviii–xxii
Manufacturing Message
Specification (MMS), 143

MAPI, 8
 MD5 chosen-prefix collision,
 117, 131
 Melissa virus, 15
 Microsoft Outlook, 8, 15
 Microsoft SQL Server, 41, 46–47,
 51, 53, 55, 57
 Mimikatz, 159
 MITRE ATT&CK, 149
 MMS (Manufacturing Message
 Specification), 143
 monster-in-the-browser attacks, 164
 morphological transcription, xxiv
 Morris worm, 17–18
 MS02-039, 53
 MS10-046, 89
 MS10-061, 90
 MS10-073, 90
 MS10-092, 90
 MS17-010, 183, 191

N

Natanz enrichment facility, 96
 National Health Service (NHS),
 193–194
 National Security Agency (NSA),
 184, 190–191, 217
 naturalist framing, xxiv–xxv,
 224, 228
 network shares, 26, 28–31
The New York Times, 104
 NHS (National Health Service),
 193–194
 Nimda
 anatomy, 23–25
 authorship, unresolved, 37–38
 and Code Red II, 33
 IIS exploitation, 26, 29, 33
 Lenaean classification, 22
 multivector propagation,
 26–31, 38
 network impact, 34–36
 and 9/11 attacks, 33–34

 persistence, 31–32
 README.exe attachment, 26–28
 North Korea, 196–197
 NSA (National Security Agency),
 184, 190–191, 217

O

OPC (Open Platform
 Communications), 142–143
 Operation Olympic Games, 104

P

Park Jin Hyok, 196–197
 patch management, 53, 57–58
 pathogen, as biological parallel,
 xx–xxii
 patient zero, 11–13
 persistence mechanisms, 8, 10,
 31–32, 71, 164, 187
 Philippines, 11, 13–14
 Electronic Commerce Act
 of 2000, 14
 Manila, 12–13
 PLCs (programmable logic
 controllers), 83, 88–94
Powergridium, 136, 242
 proof-of-concept exploit code,
 59–60

Q

QNAP devices, 210
Qnapium, 202, 238, 242

R

ransomware
 autonomous spread, 177
 encryption, 188
 infrastructure, 166
 payment tracking, 194
 Raspberry Robin
 as access broker, 212, 216–217
 adaptation, 207

- anatomy, 203–205
- attribution, 217–218
- infection via USB drives,
 - 206, 218
- Lenaeon classification, 202
- living off the land, 207–208
- msiexec.exe* abuse,
 - 207–208, 210
- obfuscation layers, 208–209
- and QNAP devices, 210
- and Unit 29155, 217–218
- RATs (remote-access trojans), 63
- Realtek Semiconductor, 92
- Reconnaissance General Bureau, 196
- Red Canary, 201
- remote-access trojans (RATs), 63
- remote terminal units (RTUs), 142
- removable media.
 - See* USB drives
- reverse engineering, xiii, xv–xvii,
 - 221, 226
- Rid, Thomas, 130
- Russia
 - annexation of Crimea, 147
 - GRU (Russian military intelligence),
 - 149–150, 218
 - invasion of Ukraine, 150–151
- Ryuk, 166
- S**
- Saccharomyces cerevisiae* (baker's yeast), xxi, 229
- Sandworm, 149–150
- Sapphire. *See* Slammer
- SCADA (supervisory control and data acquisition), 96, 147
- Sequelium*, 42, 238, 242
- Server Message Block (SMB),
 - 165, 183–184
- Shadow Brokers, 190–191
- Siemens
 - S7-300 PLCs, 94
 - SIPROTEC relays, 145
 - Step7 software, 92–93
 - WinCC, 90
- Skyptium*, 112, 242
- sKyWIper. *See* Flame
- Slammer (SQL Slammer;
 - Sapphire)
 - adaptation, 46
 - anatomy, 43–46
 - buffer overflow exploitation,
 - 46, 55
 - and Davis–Besse nuclear plant, 56
 - Lenaeon classification, 42
 - network congestion, 51, 56–57
 - patch availability, 53, 57–58
 - pseudorandom scanning,
 - 48–50
 - SQL Server Resolution Service, 42, 53, 59
 - UDP port 1434, 46, 55, 59
- SMB (Server Message Block),
 - 165, 183–184
- social engineering, 1, 6–8, 25–28,
 - 132, 177
- Sony Pictures Entertainment, 197
- spear phishing, 68–69, 78
- Spyor*, 112, 236, 242
- SQL Slammer. *See* Slammer
- Stealor*, 156, 236, 242
- Stuxnet
 - air gaps, 90, 93–94, 99–100
 - anatomy, 85–88
 - attribution, 103–104
 - centrifuge sabotage, 94–97
 - digital certificates stolen,
 - 92, 102
 - Duqu and Flame relation,
 - 106–108
 - industrial rootkit, 96
 - Lenaeon classification, 84

Stuxnet (*continued*)
 Operation Olympic Games, 104
 PLC manipulation, 92–94
 Siemens systems targeted, 92–93
 zero-day vulnerabilities, 89, 104

SugarGh0st, 79, 81

supervisory control and data acquisition (SCADA),
 96, 147

surveillance
 audio and Bluetooth, 119–120
 remote, 72–77
 state-sponsored, 125, 131–132

Symantec, 92

Systema Naturae, 229

T

Tor

command-and-control,
 210–211
 payment infrastructure,
 185, 188

TrickBot

as access broker, 168, 174
 adaptation, 155, 166–167
 anatomy, 157–160
 and Dunaev, 173
 and Emotet, 161
 Lenean classification, 156
 modular architecture, 162–163
 monster-in-the-browser
 attacks, 164
 persistence, 163
 ransomware, enabling, 166,
 169, 171
 takedown, 172–174
 web injection, 162, 164

trojans. *See* banking trojans

trust

browser trust, 28–30
 certificate trust, counterfeited,
 116–118

digital trust relationships,
 11, 17–18
 in industrial infrastructure,
 102–106
 social trust exploited, 6–8
 in software, 10, 28–31

U

Ukraine

grid blackout, 141, 147–148
 Russian invasion, 150–151

Unit 29155, 217–218

Unit 74455, 149

(Un)Natural concept, xv–xviii,
 xxii, 222, 226

USB drives

crossing air gaps, 90, 99–100
 as infection vectors, 201, 204,
 206, 218
 removable media attacks, 117

US Cyber Command, 172

US Department of Justice, 12–13,
 149, 196

V

Vacon, 94

VBScript, 7

W

WannaCry

anatomy, 178–182
 attribution, 196–197
 and DoublePulsar, 184,
 185–186
 encryption scheme, 187–189
 and EternalBlue, 183–184,
 190–191
 kill switch, 194–195
 and the Lazarus Group,
 196–197
 Lenean classification, 178
 NHS disruption, 193–194

persistence, 187
propagation, 185–187
and the Shadow Brokers,
190–191
SMBv1 vulnerability,
183–184, 192
The Washington Post, 104
web injection, 162, 164
Windows Registry, 10, 31, 70–71,
145, 163, 187
Windows Update, 117
Wintrojan, 234–235
Winwareia, 234–235

Winwormia, 234–235

worms
early internet worms,
17–18, 38
multivector, 24–26, 38–39
propagation speed, 53–54,
59–60
ransomware convergence, 198

Z

zero-day vulnerabilities,
89–90, 102