INDEX

A

aarch64, 292
Acer ransomware attack, 245
Active Directory, 183, 184, 219, 229
  abuse, 184–185
  authentication, 184
  authorization, 184
  BloodHound, 185, 212
  collecting environment information, 190
  decrypting password hashes from domain computers, 190
  Domain Administrator, 185, 212, 216, 217
    privileges, 191
  Domain Controller, 184, 224–225
    secretsdump, 191, 192
  domain trust relationship, 225
  dumping authentication data with Impacket, 193
  enumeration, 212, 215–218
  forest, 225
  Game of Active Directory, 214, 224, 242
  Group Policies, 142, 224–229
  groups, 218
  information collection, 190
  inherent trust, 185
  Kerberos, 185, 191, 192
  Lightweight Directory Access Protocol, 216
    `ldapsearch` command, 216
  LM hashes, 192, 193, 196
  Local Security Authority, 192, 193
  NTDIS.dit file, 192
  NTLM hashes, 191–193, 195, 196, 221
  resource management, 184
  Security Accounts Manager, 192, 193
  Service Principal Name, 185
  SharpHound, 185
AdFind, 212, 217, 317
administrators of ransomware, 247
AES256 encryption, 65–67
AES encryption, 172, 177, 178
  initialization vector, 179
affiliates, 7, 191, 219, 247
aggressor scripts, 171, 322
Ahmia, 6
AI. *See* artificial intelligence
AIDS trojan, 244
Ailurophile Stealer, 83
ALPHV, xxiv, 8, 254, 295
  access token, 309
  BlackCat, 192
  concurrency, 304
  configuration data, 304
  deleting virtual machine snapshots, 307
  excluding virtual machines from encryption, 305, 307
  file and directory traversal, 306
  killing processes and services, 259, 307
  Linux/ESXi locker, 304–309
  Morph obfuscation toolkit, 306
  privilege escalation, 256
  ransom negotiation, 309
  ransom notes, 308
  RemCom, 192
  skipping files, folders, or extensions, 258, 306–307
  SmartPattern encryption, 255
  Sphynx, 192
AMSI (Antimalware Scan Interface), 241

Android malware
AccessibilityService API abuse, 110–113
activity, 111
Android manifest, 111, 113
callbacks, 112
Cerberus banking trojan, xxii, 113–116, 125
creating malicious overlays, 112–113
Google Play Protect, 110, 124
injections, 108, 114
overlays, 108, 114
services, 111
SettingsRead function, 112, 114
SharedPreferences storage system, 112, 114
View, 110
WebView, 112
Anna-senpai, 73
anti-analysis techniques, 55–57
Beacon Object Files, 166–167
benign string insertion, 133
BunnyLoader, 70–71
string obfuscation, 63–67
crypters, 128, 164
dynamically obtaining function pointers, 146
import resolution, 57
junk code insertion, 134–136, 141, 144
Metasploit evasion modules, 163, 207
nonsense string insertion, 133, 144
obfuscation, xxii, 128, 141, 146, 164, 172, 248
code, 43, 45
ESXi ransomware, 310
function obfuscation, 57
minification, 43, 163
string, 57, 63–67
XOR cipher, 74, 96, 103, 175
opaque predicates, 57, 136
requiring passwords to decrypt, 261
sandbox detection, 71, 77
SmokeLoader, 58–62
string encryption
Sodinokibi, 263
StealBit, 234–235
virtual machine detection, 55–57, 58, 71, 77
anti-debugging techniques, 55–57
ESXi ransomware, 310
using the PEB, 59, 232
anti-hooking, 57
Antimalware Scan Interface (AMSI), 241
antivirus evasion, 203–204, 207, 211, 225
in command-and-control frameworks, 165–167, 186
AnyDesk, 222, 317
use for data exfiltration, 223
Applocker, 163
Archiveus, 244
ARM, 292
artificial intelligence (AI), 320–321
large language models, 321
ransom negotiation, 322
assembly changers, 128
asymmetric encryption, 172, 244, 251, 252
private keys, 251, 252
public keys, 172, 251, 252
RSA, 172, 174, 177
Atera, 222
Atomic Shell Archive (ASAR) file, 36
attribution, 164, 318
authentication protocol, Kerberos, 185
Avaddon, 256

B

Babuk Locker, 287–289, 314, 318
ESXi locker, 314
network attached storage, 287
backdoors, 311
Background Intelligent Transfer Service (BITS), 219
banking trojans, xxii, 10, 108–113
Android malware
abusing AccessibilityService API, 110–113
accessibilityDataSensitive property, 110

creating malicious overlays, 112–113
isAccessibilityTool property, 110
Cerberus, xxii, 113–116, 125
DanaBot, 108
Emotet, 108, 116, 319
injections, 108
overlays, 108, 119
TrickBot, 116–123, 319
baselining, 241
Bassterlord, 191–192
Networking Manual, 191
Beacon Object Files (BOFs), xxiii
anti-analysis techniques, 166–167
C2 frameworks, 163, 164, 186, 317
Cobalt Strike, 171
custom, 166
benign string insertion, 133
best practices
malware handling, 16–18
OPSEC, 2–6
big game hunting attacks, 245
Bitcoin, 244, 245, 249, 254
Bitdefender, 253, 286
BITS (Background Intelligent Transfer Service), 219
bitsadmin tool, 219
BlackMatter, 1, 253, 261, 287, 318
encryption flaw, 254
ExMatter, 229
printing ransom notes, 260
ransom negotiation, 309
rebranding, 254
BlackSuit ransomware, 217
BloodHound, 185, 212, 217–218, 317
BOFMask, 166
BOFs. *See* Beacon Object Files
botnets, xxii, 71–76
bootstrapping, 73
bot herders, 71
centralized, 72
CosaNostra, xxii, 77–78
Gameover Zeus, 244
infection process, 72
Mirai, xxii, 73–76, 310, 318, 322
IoT, 73
MisakaNetwork, 73
P2P, 72
wormable, 72
BreachForums, 320
browser data theft, xxii, 89, 95–96, 119, 190
PostGrabber, 109
browser engines, 37
brute forcers, xxi, 33–34
Brute Ratel, 166, 169
bypassing EDR hooks, 166
C4, 166
cracked license, 171
Bumblebee loader, 217
BunnyLoader, xxii, 62–71
anti-analysis techniques, 70–71
string obfuscation, 63–67
fileless download and injection capability, 67–70
loading capabilities, 67–70
Burp Suite, 22
bypassing execution policy in PowerShell, 211

C

C2 framework. *See* command-and-control framework
C2 servers, 163, 276, 297
centralized botnets, 72
Cerberus Android banking trojan, xxii, 113–116, 125
AccessibilityService permission, 113
Android manifest, 113
callbacks, 113
injections, 114
overlays, 114, 115
SettingsRead function, 114
SharedPreferences storage system, 114
checkers, xxi, 32–33
TMChecker, xxii, 35–38
CIS (Commonwealth of Independent States), 102, 257
clipboard data, 55, 63, 78
clipper, 63
CMSTP (Connection Manager Profile Installer), Microsoft, 256

Cobalt Strike, 179
aggressor scripts, 171
Beacon implant, 165, 171
Beacon Object Files, 171
custom, 166
beacon type, 174
BOFMask, 166
C2 callback interval, 165
C2 protocol, 171–172
configuration data extractor, 173
cracked license, 168
jitter, 165
obfuscation, 172
pipename configuration block, 175
post-ex configuration block, 175
Sleep Mask, 167
Team Server, 171–172
code obfuscation, 43, 45
minification, 43, 163
XOR cipher, 74, 146, 172
Colonial Pipeline ransomware attack, xix, 254
COM (Component Object Model) objects, 194, 256
COM interface, 194, 280
command-and-control (C2) framework, 162–164, 218, 222, 318
antivirus evasion, 165–167, 186
beacon, 162
Beacon Object Files, 163, 164, 186, 317
custom, 166–167
built-in stealth capabilities, 166
C2 server, 163
client console, 163
Cobalt Strike, xxiii, 161, 164, 165, 166, 168
C2 protocol, 171–172
cracked license, 168–171
Impacket, 317
implant, 162
jitter, 162
Metasploit, 161, 163–165, 317
session, 162
Sliver, 162, 167
built-in obfuscation capabilities, 165
C2 protocol, 180
interactive shell, 165
OPSEC, 166
`psexec` command, 166
`shell` command, 166
transport encryption protocol, 181
stagers, 165
Commonwealth of Independent States (CIS), 102, 257
concurrency, 230, 254, 269, 304
input/output completion ports, 254, 272
named pipe, 255
threading, 255
Conti, 219, 254, 286, 317, 318
leaked documents, 219
Windows Restart Manager, 286
CosaNostra botnet, xxii, 77–78
anti-analysis techniques, 77–78
sandbox detection, 77
virtual machine detection, 77
Covenant C2, 186, 317
Cracked forum, 319
cracked license, 164, 168–171
CRC32 hash, 301
credential access, 113. *See also* stealers
financial credentials, 108
Golden Kerberos Ticket, 164
infostealers, 82
Kerberos, 191, 192, 222
LM hash, 192, 193, 196
Local Security Authority, 192, 193
Local Security Authority Subsystem Service, 221, 222
malware logs, 90
Mimikatz, 212, 221, 222
NTDIS.dit, 192
NTLM hashes, 191–193, 195, 196, 221
ProcDump, 212
Security Accounts Manager, 192, 193
credential-stuffing attack, 34
cross-compilation, 292, 294
crypters, 128–142, 311, 316
Fully UnDetectable, 128, 316
indicators, 139
benign string insertion, 133

entropy, 136, 230
JMP address, 140
junk code insertion, 134–136, 141, 144
memory allocation and manipulation functions, 140, 141, 146, 151
nonsense string insertion, 133, 144
section names, 138, 230
section sizes, 137, 230
PolyCrypt, 128
polymorphism, 128, 322
Theattacker-Crypter, 130–131
crypting services, 132
cryptocurrency, 244
Bitcoin, 244, 245, 249, 254
mixing, 248
CryptoLocker, 244–245
CryptoWall, 245
cryptowallet data theft, xxii, 55, 63, 82, 89, 190
Raccoon Stealer, 100–101
cURL, 222
CursedChrome, 189–190, 318
Cyber Kill Chain, xxi, 14, 163

D

DanaBot, 108
DarkSide, 245, 266, 287
checking default language, 257
Colonial Pipeline ransomware attack, xix, 254
encryption flaw, 253
Windows Restart Manager, 286
dark web
administrators, 247
affiliates, 7, 191, 219, 247
bot herders, 71
cracked software, 164, 168–171
know your customer, 169
data, 9
exploit builders, 30–31
finding sites, 7
forums
banning ransomware, 249
BreachForums, 320
Cracked, 319
Exploit, 249
Genesis Market, 190, 318, 319
Nulled, 319
reappearing after takedown, 320
XSS, 35
guarantors, 13
initial access brokers, xxii, 26–27, 35, 191, 247
operators, 7, 113
OPSEC best practices, 2–6
reputation, 8
Bitcoin, 249
vouches, 249, 319
search engines, 6
vouch copies, 63
dark web services for sale, 11–12
bulletproof hosting, 12
buying loaders, 54–55
DDoS for hire, 11
tutorials, 12, 164, 167–168
for C2 frameworks, xxii, 167–168, 317
for post-exploitation toolkits, 186–189
dark web tools for sale, 10–11
data encryption, 184
data exfiltration, 90, 213, 222–224, 238–240
AnyDesk, 223
malware logs, 90
PowerShell, 211
ransomware, 213, 238–240, 248
Revix, 298
Sodinokibi, 276–277
StealBit, 229, 230, 238–240
stealers, 82
Vermilion Strike, 177
DDoS (distributed denial-of-service) attacks, 71, 73, 80, 247, 323
decompilers, 20–22
decrypting service tickets, Kerberos, 185
denial-of-service (DOS) servers, 248
dictionary attacks, 33
disabling antivirus software, 226, 227, 311

disassembler, 20
Distributed Component Object Model (DCOM), 194, 220
  CLSID, 194
  CMSTPLUA, 256
  COM elevation moniker, 256
  COM interface, 194, 280
  COM objects, 194, 256
  IID, 194
distributed denial-of-service (DDoS) attacks, 71, 73, 80, 247, 323
DLL injection, 67
  reflective, 117, 318
Domain Administrator, 185, 212, 216, 217
  privileges, 191
Domain Controller, 184, 224–225
  secretsdump, 191, 192
DOS (denial-of-service) servers, 248
`dsquery` command, 215–217, 317
DuckDuckGo, 6
dynamic analysis
  debuggers, 22
  network analysis tools, 22
  system and process monitoring tools, 23
  x64dbg, 58–62

E

effective user ID (EUID), 176
Egregor, 261
Elliptic Curve Integrated Encryption Scheme (ECIES), 270
Emotet, 108, 116, 319
Empire, 222
Emsisoft, 253, 287
encryption algorithms
  asymmetric, 251
    RSA, 172, 174, 177
  Elliptic Curve Integrated Encryption Scheme, 270
  flawed, 253–254, 292, 312, 318
  hybrid, 252–253, 270
  initialization vector, 179, 292
  key generation, 250–253, 269–271
  symmetric, 250–251
    AES, 172, 177, 178
    AES256, 65–67
    RC4, 235, 263, 266, 281
    Salsa20, 271
Enigma Protector, The, 133
entropy, 136–137, 230
enumerating network resources, 212, 213–215
  Active Directory, 214
  `net` command, 213
  `smbclient` command, 213
  SMB shares, 213
  Snaffler, 212, 214–215
ESXi, 292
  Active Directory, 294
  antivirus, 294
  device files, 300
  `DisplayName` field, 299
  hypervisors, 293, 310
    type, 1–2, 293
  locker, 314
  misconfiguration, 294
  ransomware, xxiii, 292–295
    anti-analysis techniques, 310
    obfuscation, 310
    shutting down virtual machines, 298–299, 307, 310
    targeting, 294
  vCenter Server, 293
  vSphere, 293
    hardening guidance, 294
  `WorldID` field, 299
ESXiArgs, 312–314
  data encryption, 313
  decryptors, 312
  file and directory traversal, 313
EUID (effective user ID), 176
Evil-WinRM, 212, 220, 317
exclusive or cipher. *See* XOR cipher
exploit builders, 30–31
Exploit forum, 249
exploits, xx, xxi, 322
  buffer overflow, 165
  CVE-2018-8453, 266
  CVE-2020-1472 (Zerologon), 191
  Metasploit exploit modules, 163, 206
  privilege escalation, 256

proof of concept, 27–30
CVE-2023-34362 (MoveIT), 28
CVE-2024-34102, 28
extortion, 213, 245, 323
contacting customers, 247, 323
distributed denial-of-service attack, 247, 323
novel tactics, 323
third-party, 247

F

FickerStealer, 294
`file` command, 19
fileless malware, 210
fisherstell, 42
FLARE-VM, 16
forests in Active Directory, 225
Forti VPN Bruter, 34
Fully UnDetectable (FUD), 83, 128, 316
function hooking, 119, 140
bypassing EDR hooks, 166
calculating code jumps, 122
creating function hooks, 121
modifying memory permissions, 121
function obfuscation, 57
fuzzing, 164

G

Game of Active Directory (GOAD), 214, 224, 242
Gameover Zeus, 244
Genesis Market forum, 190, 318, 319
Ghidra, 16, 142
Entropy tool, 136
fixing Rust string references, 295
Script Manager, 173
Shannon entropy, 137
string data analysis, 93–95
string representation, 94
string value, 94
GNU Debugger (GDB), 22
Go, 137, 292, 294, 295, 316
Golden Kerberos Ticket, 164
GootLoader, 54
GPCode, 244
GPOs. *See* Group Policy Objects
Greatness Hub, 42, 48
Greatness phishing kit, 42–50, 316
multifactor authentication interception, 48
payload generation, 45–47
retooling, 48–49, 316
Group Policies, 142, 224
abuse, 225–229
disabling antivirus software, 226, 227
modifying update time, 228
Group Policy Editor, 227
gpedit.msc file, 226
Group Policy Objects (GPOs), 224–229
cmdlets, 225
computer configuration, 226
Policies directory, 225
scheduled tasks, 225
user configuration, 226
Groups in Active Directory, 184, 218
guarantors, 13, 34

H

hash-based message authentication code (HMAC), 177
Hashcat, 185
hashing algorithms
MD5, 192
SHA256, 66, 177, 178
`hashlib` module, 67
heuristic malware detection, 128
hidden virtual network computing (HVNC), 109
Hidden Wiki, The, 6
Hive, 245
Honig, Andrew, 22
HTML application (HTA) files, 54
HTTP proxy, 189
hybrid encryption, 252–253
Elliptic Curve Integrated Encryption Scheme, 270
Sodinokibi, 270
hypervisors, 293

I

IABs (initial access brokers), xxii, 26–27, 35, 191, 247
icon changers, 128

ICS (industrial control system), 323
Impacket, xxiii, 212, 317
  bypassing EDR, 188
  collecting Active Directory environment information, 190
  command-and-control framework, 317
  dumping authentication data with, 193
  executing commands, 190
  `impacket-psexec` command, 201
  `impacket-secretsdump` command, 193, 196
  `impacket-services` command, 205
  `impacket-wmiexec` command, 195, 196, 197
  obtaining credential information, 190
  pass-the-hash attack, 188, 192, 194, 196
  pass-the-ticket attack, 192
  psexec, 188, 192, 199–205, 206, 218
  rdp_check.py module, 186
  remote code execution, 199–202
  secretsdump, 191–194
  smbexec, 192
  wmiexec, 188, 192, 194–198, 199, 218
import resolution, 57, 264
industrial control system (ICS), 323
initial access brokers (IABs), xxii, 26–27, 35, 191, 247
initial access techniques, xxi, 212
  buying access, 26–31
    exploit builders, 30–31
    exploit proof of concept, 27–30
  credential access, 32–34
    brute forcers, xxi, 33–34
    checkers, xxi, 32–33
    credential-stuffing attack, 34
    dictionary attack, 33
    Forti VPN Bruter, 34
    TMChecker, 35–38
  guarantors, 34
  phishing kits, 38–42
in-memory execution, 117, 210, 218
  fileless malware, 210
integrity level, 267
internet of things (IoT), 323
IoT botnet, Mirai, 73

J

Java Naming and Directory Interface (JNDI), 50
JBS Foods ransomware attack, 263
John the Ripper, 185
junk code insertion, 134–136, 141, 144

K

Kaseya ransomware attack, 245, 263
Kerberoasting, 185
Kerberos, 185, 191, 192, 222
key generation, 250–253, 269–271
keyloggers, 54, 55, 63, 77, 78
key-scheduling algorithm, Salsa20, 271
killing processes and services
  ALPHV, 259, 307
  ransomware, 245, 255, 259–260, 310
  Revix, 297
  Sodinokibi, 267–269, 279, 280–281
know your customer (KYC), 169

L

large language models (LLMs), 321
lateral movement, 194, 196–198, 212–213, 218–221
  `bitsadmin` command, 219
  Windows Remote Shell, 220
law enforcement takedowns, 108, 190, 244, 248, 263, 287
  Operation Talent, 319–320
  Operation Tovar, 245
`ldapsearch` command, 216
leak sites, ransomware, 246
Lightweight Directory Access Protocol (LDAP), 216, 317
  distinguished name, 216
Linux, 292
Linux.Encoder, 292
living-off-the-land techniques, xxiii, 162, 210–212
  dual-use tools, 210, 223, 241
  LOLBAS Project, 210, 241
  LOLBins, 210, 214, 223, 229, 242

mitigations, 240–241
mshta.exe program, 55
PowerShell, 210–212, 225, 228
shadow copy deletion with `wmic`, 260
Windows Management Instrumentation command line, 212, 219–220, 241
LLMs (large language models), 321
LM hash, 192, 193, 196
LNK file, 31, 55
loaders, xxii, 54–57, 164, 311
analysis challenges, 55–57
Bumblebee, 217
BunnyLoader, xxii, 62–71
fileless download and injection capability, 67–70
buying on the dark web, 54–55
GootLoader, 54
loader builders, 54
QakBot, 54
Raspberry Robin, 54
SmokeLoader, 54, 57–62
SocGholish, 54
Local Security Authority (LSA), 192, 193
Local Security Authority Subsystem Service (LSASS), 221, 222
LockBit, xxiii, 227, 262
disabling Windows Defender, 227
LockBit 2.0, 227
LockBit 3.0, 227, 228
modifying Group Policy update time, 228
printing ransom notes, 260
requiring password to decrypt, 262
StealBit, xxiii, 227, 229–240, 317
lockers, 250
Log4Shell, 50–52
logging utilities. *See also* Sysmon
security information and event management, 197
Windows Event Logs, 197, 198, 206
LOLBins, 210, 214, 223, 229, 242
Lumma Stealer, 82

M

macOS ransomware, 294
malware analysis basics, 15–23
dynamic analysis, 22–23
static analysis, 18–22
decompilers, 20–22
disassemblers, 20
inlining, 21
turning off Windows Defender, 17–18
malware-as-a-service (MaaS), 82
malware delivery, xxii
botnets, xxii, 71–76
deploying loaders with, 72
Gameover Zeus, 244
loaders, xxii, 54–57, 164
analysis challenges, 55–57
Bumblebee, 217
loader builders, 54
Metasploit encoder modules, 163
malware deployment, 224–229, 322
malware handling best practices, 16–18
malware logs, 90
man-in-the-browser (MITB) attack, 124
man-in-the-middle (MITM) attack, 124
Master Boot Record (MBR), 245
Master File Table (MFT), 245
Maze, 245
MD5 hash, 192
MediaMarkt ransomware attack, 245
MegaSync, 222
Metasploit, 118, 161, 317, 318
antivirus evasion, 165
modules
auxiliary, 164
encoder, 163
evasion, 163, 207
exploit, 163, 206
payload, 163
post, 164
webexec.rb, 206
psexec, 206
scanning, 164
Meterpreter, 163
Microsoft Connection Manager Profile Installer (CMSTP), 256
Mimikatz, 212, 221, 222, 317

minidump file, 222
Mirai, 73–76, 79–80
  default credential addition, 74
  distributed denial-of-service attack, 73
  IoT botnet, 73
  login process, 75–76
  scanning for devices, 74–75
MisakaNetwork botnet, 73
MITB (man-in-the-browser) attack, 124
MITM (man-in-the-middle) attack, 124
MITRE ATT&CK, 15
Monti, 254
Morph obfuscation toolkit, 306
mshta.exe program, 55

N

named pipes, 199, 201, 202, 239, 255
`net` command, 213
NETLOGON, 191
`netsh` utility, 280
network attached storage (NAS), 287, 292
Network Level Authentication (NLA), 226
NEW Cooperative ransomware attack, 8
Nmap, 188
no-distribute sites, 131
nonsense string insertion, 133, 144
NotPetya, 245
NSIS (Nullsoft Scriptable Install System), 157
NTDIS.dit file, 192
NTLM hashes, 191–193, 195, 196, 221
Nulled forum, 319

O

OAuth, 190
`objdump` command, 19
offcut references, 295
OllyDbg, 22
opaque predicates, 57, 61, 136
OpenBullet, 10
operational technology (OT) network, 323
Operation Talent, 319–320
Operation Tovar, 245
operators, 7, 113
OPSEC (operational security), 2–6, 166
Oracle VirtualBox, 293

P

P2P botnets, 72
packers, 165, 157–160
  Enigma Protector, The, 133
  NSIS, 157
  self-extracting archives, 128
  7Zip, 157
    building an SFX archive, 158
  Themida, 132
  UPX, 139, 157
    compressing a file, 159
  VMProtect, 133
pass-the-hash attacks, 188, 192, 194, 196
pass-the-ticket attacks, 185, 192
password-cracking utilities, 185
password database entry, 176
PE-bear, 20
persistence, 311
PE Studio, 20
Petya, 245
phishing, 322
  payload, 31
phishing kits, xxi, 11, 38–42, 316
  Greatness, 42–50, 316
    multifactor authentication interception, 48
    payload generation, 45
    retooling, 49, 316
  Zphisher, xxii, 38–41
pointer resolution
  using `InLoadOrderModuleList` field, 155, 232
  via shellcode, 150
PolyCrypt, 128
polymorphism, 128, 322
post-exploitation, 15, 180, 184, 322. *See also names of individual tools*
  Active Directory enumeration, 212, 215–218
    `dsquery` command, 215
  data exfiltration, 90, 213, 222–224, 238–240

disabling antivirus software, 226, 227, 311
dropping additional tools, 184
enumerating network resources, 212, 213–215
net command, 213
smbclient command, 213
framework, 162
lateral movement, 194, 196–198, 212–213, 218–221
bitsadmin command, 219
malware deployment, 224–229, 322
persistence, 311
privilege escalation, 163, 212, 221–222, 311
remote code execution, 199–202
reverse shell, 163, 219
system information collection, 211
post-exploitation toolkits, xxiii, 11, 186–190, 218, 222. *See also* Impacket
Metasploit, 206–207
psexec, 206
webexec.rb module, 206
wmiexec-Pro, 198
PowerShell, 210–212, 241
BunnyLoader, 67
command encoding, 163, 211
data exfiltration, 211
Evil-WinRM, 220
execution policy, 211, 241
Group Policy abuse, 225, 228
hiding console windows, 211
profile, 211
system information collection, 211
PowerSploit, 222
Practical Malware Analysis (Sikorski and Honig), 22
privilege escalation, 221–222, 255–256, 266–267, 310
CMSTPLUA COM interface, 256
exploiting vulnerabilities, 256
rerunning as administrator, 256, 267
ProcDump, 212, 221–222
dumping LSASS process memory, 221
Process Explorer, 23, 242
process hollowing, 69–70
process injection, 68, 117–119
reflective DLL injection, 117
shellcode, 118
process listing, 117
Process Monitor, 23, 242
psexec, 199, 206
PyCryptodome library, 67

Q

QakBot, 54

R

RaaS. *See* ransomware-as-a-service
Raccoon Stealer, xxii, 82, 83, 266, 317
affiliate panel, 84
autofilling passwords, 97
browser data theft, 95–96
checking installed programs, 101–102
cryptowallet data theft, 100–101
screenshots, 98–100
string obfuscation
stack strings, 96
XOR cipher, 95, 103
system information collection, 102–103
Ragnar Locker, 246
ransom notes, 302, 308
printing, 260
ransomware, 212–229, 243–289, 323. *See also names of individual ransomware*
administrators, 247
affiliates, 219, 229, 247
anti-analysis techniques, 261–263
big game hunting, 245
Bitcoin, 244, 245, 254
concurrency, 230, 254
input/output completion ports, 254
named pipes, 255
threading, 255
data exfiltration, 213, 238–240, 248
decryptors, 253, 286–287, 289, 312
deleting or emptying folders, 260, 275–276
mapping contents into memory and overwrite, 275

ransomware (*continued*)
distributed denial-of-service attacks, 247, 323
encryption speed, 254, 269, 272–273, 280, 284
ESXi, 291–310
evolution, 323
excluding sensitive locations, 257, 264–265
extortion, 213, 245
file and directory traversal, 237–238, 254
flawed encryption algorithms, 253–254, 292, 312, 318
history, 244–247
key generation, 250–253, 269–271
killing processes and services, 245, 255, 259–260, 310
leak sites, 246
lockers, 250
modifying login permissions, 226
partial encryption, 255
printing ransom notes, 260
privilege escalation, 255–256, 310
process enumeration, 259
ransom negotiation, 309, 322
ransom payments, 244, 245
rebranding, 316
self-deletion, 230, 236
service enumeration, 260
shadow copy deletion, 219, 226, 227, 245, 260
vssadmin.exe utility, 260, 269
with `wmic` command, 260
skipping files, folders, or extensions, 230, 238, 257–258, 260
ransomware-as-a-service (RaaS), xxiii, 247–249. *See also names of individual services*
administrators, 247
developers, 247
initial access brokers, 247
ransom negotiation, 322
rules for attacking victims, 248
Raspberry Robin, 54
RC4, 235, 263, 266, 281
Rclone, 222
RDP (Remote Desktop Protocol), 186, 222
`readelf` command, 19–20
reconnaissance, 26, 55
reflective DLL injection, 117, 318
RemCom, 192, 199, 200, 201
REMnux, 17
remote access trojans (RATs), 123, 184, 218, 311
remote code execution (RCE), 199–202
vulnerability, 28
Remote Procedure Call (RPC), 199
Remote Server Administration Tools (RSAT), 215
remote shell, 192, 195, 197, 199, 203
interactive shell, 165, 201
reverse proxy, 190
reverse shell, 163, 219
REvil, 248–249, 286–287
Acer ransomware attack, 245
JBS Foods ransomware attack, 263
Kaseya ransomware attack, 245, 263
Revix, 296
Sodinokibi, xxiii, 248, 255, 263–286
Revix, 296–303
C2 server, 297
data encryption, 297, 299–301
data exfiltration, 298
deleting virtual machine snapshots, 298
encryption statistics, 302
encryption threads, 298
file and directory traversal, 300
killing processes and services, 297
modifying file permissions, 301
parsing configuration data, 297
ransom note, 300, 302
shutting down virtual machines, 298–299
silent mode, 298
skipping files, folders, or extensions, 300

system information collection, 301–302
terminating processes, 299
rootkits, 311
RPC (Remote Procedure Call), 199
RSA encryption, 172, 174, 177
RSAT (Remote Server Administration Tools), 215
Rubeus, 185
Rust, 137, 254, 292, 316
ALPHV, 304
FickerStealer, 294
fixing string references, 295
Ryuk, 217
Infostealer, 229

S

Salsa20, 271
sandbox detection, 71, 77
SapphireStealer, 105–106
scanning, 74–75, 164
ScreenConnect, 222
screenshots, 54, 55, 78, 89, 98–100
secretsdump, 191–194
Securities and Exchange Commission (SEC), 260
Security Accounts Manager (SAM), 192, 193
Security Information and Event Management (SIEM), 197
Sellix, 319
Server Message Block (SMB), 196, 200, 213
Service Principal Name (SPN), 185
service tickets, Kerberos, 185
7Zip, 157, 222
building an SFX archive, 158
SHA256, 66, 177, 178
shadow copy deletion, 219, 226, 227, 245, 281
Shannon entropy, 137
SharpHound, 185, 317
shellcode, 149, 163, 165, 167, 266
pointer resolution via, 118
resolving API calls via, 150
Shodan, 322
SIEM (security information and event management), 197
signature-based malware detection, 128
Sikorski, Michael, 22
Sliver, 317
Sliver C2 framework, 165–166, 167–168, 180–181, 185, 186
antivirus evasion, 165
built-in obfuscation capabilities, 165
interactive shell, 165
OPSEC, 166
protocol, 180
`psexec` command, 166
`shell` command, 166
transport encryption protocol, 181
tutorial, 167
SMB (Server Message Block), 196, 200, 213
`smbclient` command, 213
SmokeLoader, 54, 57–62, 71, 232
anti-analysis techniques, 58–62
byte insertion, 61–62
control flow obfuscation, 62
opaque predicate, 61
Snaffler, 212, 214–215, 317
SocGholish, 54
SOCKS proxy, 37, 181
Sodinokibi, xxiii, xxiv, 248, 255, 263–286
C2 server, 276
command line options, 279
configuration data, 263
data encryption, 269, 271–272, 280, 284–286
data exfiltration, 276–277
decryptor, 286
deleting or emptying folders, 275–276
encryption keys, 269–271, 277, 284
excluding sensitive locations, 264
import resolution, 264
killing processes and services, 267–269, 279, 280–281
network discovery, 280
privilege escalation, 266–267
process enumeration, 268
ransom notes, 275, 278
safe mode, 279, 282
service enumeration, 280

Sodinokibi (*continued*)
setting desktop background, 277
shadow copy deletion, 269, 279, 281
skipping files, folders, or extensions, 273–275
string encryption, 263
Sphynx, 192
SPN (Service Principal Name), 185
stack strings, 96
static analysis
decompilers, 20–22
disassemblers, 20
file attributes tools, 19–20
inlining, 21
PE analysis utilities, 20
`strings` command, 18
static linking, 294
StealBit, xxiii, 227, 229–240, 317
anti-analysis techniques, 230–235
concurrency, 230
configuration options, 229–230
data exfiltration, 229, 230, 238–240
debugger checks, 231
file and directory traversal, 237–238
hiding, 230, 235
import resolution, 232
self-deletion, 230, 236
skipping files, folders, or extensions, 230, 238
string encryption, 234–235
StealC, 82
stealer affiliate panel, 84
stealers, 10, 55, 311, 323. *See also* credential access
Ailurophile Stealer, 83
browser data theft, xxii
cryptowallet data theft, xxii
data collection, 88–89
deployment and execution, 85–92
download lures, 86–88, 311
FickerStealer, 294
infostealers, 82
Lumma Stealer, 82
Raccoon Stealer, xxii, 82, 83, 93–103, 266, 317
SapphireStealer, 105–106
StealC, 82
TTP retooling, 104
Vidar, 82
string obfuscation, 57
stack strings, 96
XOR cipher, 96, 175
string representation, 94
string value, 94
symmetric encryption, 172, 250–251, 252
AES, 172, 177, 178
encryption key, 172, 252
RC4, 235, 263, 266, 281
Salsa20, 271
Sysinternals tool suite, 17, 221
Process Explorer, 242
Process Monitor, 242
Sysmon, 196, 201, 206, 242
`ParentCommandLine` field, 197
PipeEvent rule (Pipe Connected) (Event 18), 202
PipeEvent rule (Pipe Created) (Event 17), 202, 240
process creation (Event 1), 197, 202, 204
RegistryEvent rule (Value Set) (Event 13), 202, 204
`WmiEventConsumer` activity detected (Event 20), 198
system information collection, 102–103, 176, 211, 301–302

T

Theattacker-Crypter, 130–131
Themida, 132
threading, 255
ticket granting service (TGS), 185
TMChecker, xxii, 35–38
Tofsee, 142
Tor, xxi, 258
entry guard, 4
exit node, 4
.onion site, 309
Whonix, xxi, 3–6
Tor Browser, 3–6, 258
Torch, 6
TrickBot, xxii, 116–123, 318, 319
browser data theft, 119

function hooking, 119
calculating code jumps, 122
creating function hooks, 121
modifying memory permissions, 121
in-memory execution, 117
overlays, 119
process injection, 117–119
reflective DLL injection, 117, 318
shellcode, 118
`webinject` module, 117–119
trojans, 311
AIDS, 244
TTP retooling by threat actors, 130, 316
Greatness phishing kit, 48–49
stealers, 104

U

UPX, 139, 157, 159

V

vCenter Server, 293
Vermilion Strike, xxiii, 180, 299, 318
beacon type, 174
configuration data decryption, 172–175
data exfiltration, 177
implant tasking, 178–180
string deobfuscation, 175–176
victim metadata collection, 176–177
Vidar, 82
virtual machines (VMs)
deleting snapshots, 298, 307
detection, 55–57, 58, 71, 77
excluding from encryption, 305, 307
shutting down, 298–299
Virtual Machine eXecutable (VMX), 299
virtual private network (VPN), 190
VirusTotal, 131
VMProtect, 133
VMWare Workstation, 293
vouch copies, 63
vSphere, 293
hardening guidance, 294
vulnerabilities, xxi, 322
CVE-2018-8453, 266
CVE-2020-1472 (Zerologon), 191
CVE-2021-44228 (Log4Shell), 50–52
CVE-2023-34362 (MoveIT), 28
CVE-2024-34102, 28
fuzzing, 164
remote code execution, 28

W

web shell, 311
Whonix, xxi, 3–6
WinDbg, 22, 221
Windows Cryptographic API, 65–67, 97, 234
Windows Defender, 142, 201, 215, 226
disabling, 17–18, 227
Windows Event Logs, 197, 198, 206
Windows Internet library (*wininet.dll*), 119, 120, 238
Windows Management Instrumentation (WMI), 194, 198, 280, 281
living-off-the-land techniques, 212, 219–220, 241
management services interface, 195
/root/cimv2 namespace, 195
Windows Management Instrumentation command line (WMIC), 212, 219–220, 241
Windows Registry, 197
Windows Remote Management (WinRM), 220, 221
TrustedHosts, 220
Windows Remote Shell (WinRS), 220
Windows Restart Manager, 284–286
Windows Server Update Service (WSUS), 219
Windows Service Control Manager, 199
Windows Sysinternals, 17
WinLock, 244
WinRAR, 222
WinSCP, 222
Wired, 82
Wireshark, 17, 22, 77

wmiexec, 188, 192, 194–198, 199, 218
wmiexec-Pro, 198

X

x32dbg, 142
x64dbg, 16, 58–62, 142, 147
    breakpoint, 147, 148, 152
    Follow in Dump, 147
    `savedata` command, 149
XOR (exclusive or) cipher
    code obfuscation, 74, 146, 173
    string obfuscation, 95–96, 103, 175
XSS forum, 35

Z

Zphisher, xxii, 38–41