

INDEX

A

- accessibility abuse, 144–145, 150–151
- accuracy, measuring, 175
- activities, 78–79, 91, 183
- ad fraud, 24–25
 - Android.Click.312.origin, 57–58
 - attribution fraud, 25
 - Cheetah Mobile, 58–59
 - click fraud, 25
 - impression fraud, 25
 - installation attribution fraud, 58
 - Judy, 45–46
- AndroidManifest.xml*, 10
- Android Package (APK), 10
- Android Studio, 117–119
- anomaly detection, 163
- antifraud SDK, 59–60
- API calls, 184
- API packages, 186
- app entry points, 78, 90–91, 95–98, 129–130
- application subclasses, 80–81
- area under the ROC curve (AUC), 176

B

- backdoor apps, 12–13
 - CoolReaper, 42
- banking trojans, 235
 - BankBot, 236
 - Cerberus, 236
 - FakeSpy, 236
 - vs. goodware, 238–242
 - Marcher, 237, 241, 244
 - case study, 246–249
 - Medusa, 237
 - vs. other malware, 242–245
 - Xbot, 237
 - Zitmo, 237
- broadcast receivers, 79–80, 91, 96

C

- call fraud, 24
- categories, malware, 10–26
- classification algorithms, 162, 166–174
 - bagging and random forest, 169–170
 - decision trees, 167–169
 - ExtraTrees, 210
 - k-nearest neighbors, 172
 - naive Bayes, 172–174
 - support vector machines, 170–172
- command-and-control
 - communications, 102, 131–132, 138–141
- correlation graphs, 201–202
 - community detection algorithm, 201–203
 - generation, 201
- cryptocurrency malware, 40–41

D

- defense techniques
 - anti-analysis, 81–82, 118–119, 286–288
 - Base64-encoded strings, 38, 44, 85, 97
 - cloaking, 51
 - code obfuscation, 48, 57
 - device administrator abuse, 37
 - nonstandard programming
 - language, 39, 50, 84
 - opaque predicates, 86
 - package squatting, 54
 - reflection, 82, 87
 - string encryption, 50, 57, 85
- denial of service (DoS), 11–12
- dynamic (code) analysis, 115–116
 - vs. static, 116
 - tools, 119–120
- dynamic features, 184–186

E

- early Android malware, 28–42
- exploits
 - EasyRoot, 51
 - Rage Against the Cage (CVE-2010-EASY), 29

F

- F1 score, 176
- feature clustering, 199–201
 - aggregation algorithm, 200–201
 - generation, 199–200
- feature vectors, 163–164
- filesystem changes, 122–123
- Frida, 120, 127–128
 - Frida scripting, 129–131, 135–138
 - installation, 120
 - malware analysis with Frida, 127–131
 - running frida-server, 128
 - using frida-trace, 128–129, 142–144

G

- Gini value, 169
- gray zone apps, 162

H

- hostile downloader, 18–19

I

- impression fraud, 25
- installation attribution fraud, 58
- International Mobile Equipment Identity (IMEI), 17, 31

L

- landmark-based features, 195–198
 - clustering-based selection, 196
 - generation, 198
 - maximum distance heuristic selection, 196–197

M

- machine learning
 - algorithms, 162–163
 - challenges, 177–179
 - methods, 162–177, 291–293

- models, evaluating, 174–177
 - accuracy, 175
 - area under the ROC curve (AUC), 176
 - F1 score, 176
 - false negatives, 175
 - false positives, 175
 - precision, 175
 - recall, 176
 - receiver operating characteristic (ROC) curve, 176
 - true negatives (TNs), 175
 - true positives (TPs), 175

- malicious functionality, detecting, 121–122
- method call features, 186–187

N

- name unmangling, 98–100
- network traffic
 - analyzing, 125–126
 - capturing, 124–125
- non-Android malware, 25–26
 - Ramnit, 49

O

- outlier detection, 163
- over-the-air (OTA) update providers, 63
 - Adups, 64–65
 - Digitime, 65–67
 - GMobi, 63–64
 - Redstone, 65

P

- permissions
 - ACCESS_FINE_LOCATION, 224
 - ACCESS_WIFI_STATE, 212, 214, 256, 270
 - BIND_ACCESSIBILITY_SERVICE, 144
 - BIND_NOTIFICATION_LISTENER_SERVICE, 77
 - CALL_PHONE, 224, 244, 275
 - CHANGE_NETWORK_STATE, 241
 - dangerous, 183
 - DIAGNOSTIC, 260
 - DISABLE_KEYGUARD, 240
 - GET_PACKAGE_SIZE, 211, 214
 - GET_TASKS, 211, 214, 222, 241, 255, 270
 - INSTALL_PACKAGES, 211, 214, 255

- KILL_BACKGROUND_PROCESSES, 211, 226, 256
 - mapping APIs to, 76
 - MOUNT_UNMOUNT_FILESYSTEMS, 212, 214, 223, 255
 - PROCESS_OUTGOING_CALLS, 275
 - READ_CALL_LOG, 245
 - READ_CONTACTS, 76
 - READ_EXTERNAL_STORAGE, 226
 - READ_LOGS, 214, 256, 259
 - READ_PHONE_STATE, 212, 216, 222, 240, 256, 268
 - READ_SMS, 222, 238, 242, 270, 275
 - RECEIVE_BOOT_COMPLETED, 212, 216, 241, 256
 - RECEIVE_SMS, 222, 238, 242, 258, 270, 275
 - RECORD_AUDIO, 225
 - REQUEST_INSTALL_PACKAGES, 255
 - RESTART_PACKAGES, 214, 256, 259
 - SEND_SMS, 222, 238, 258, 270, 275
 - in static analysis, 74, 90, 95
 - SYSTEM_ALERT_WINDOW, 212, 222, 240, 256, 270
 - VIBRATE, 240
 - WAKE_LOCK, 244
 - WRITE_CONTACTS, 244
 - WRITE_EXTERNAL_STORAGE, 226
 - WRITE_SMS, 222, 238, 242, 258, 270, 275
 - phishing, 17–18
 - Gaiaphish, 44–45
 - Xenomorph, 115, 120, 185
 - precision, measuring, 175
 - preinstalled malware, 42, 62, 289–290
 - privilege escalation, 19–21, 205
- R**
- ransomware, 21–22, 251–252
 - Anubis, 255, 265
 - Chiffon, 252–253, 257, 265
 - vs. goodware, 255–258
 - Jisut, 253, 257, 265
 - LeakerLocker, 253, 257, 265
 - vs. other malware, 258–260
 - Police, 253, 257, 265
 - SimpleLocker, 253, 257, 265
 - Simplocker, 253, 255–257
 - case study, 261–264
 - Svpeng, 253, 255, 265
 - recall, calculating, 176
 - remote access trojans (RATs), 15–16
 - reverse engineering tools
 - adb, 118
 - Android emulator, 117–118, 123–124
 - CyberChef, 132–135
 - Frida, 120
 - jadx, 73–74, 130
 - logcat, 126–127
 - tcpdump, 119, 124
 - Wireshark, 120
 - rooting apps, 13–14, 205
 - DroidDream, 29
 - case study, 216–218
 - Dvmap, 206
 - vs. goodware, 208–214
 - vs. other malware, 214–216
 - Rootnik, 208, 210, 213–214
 - Tizi, 206
 - ZNIU, 206
- S**
- services, 80, 91, 96–97
 - sideloaded malware, 35, 60, 290–291
 - smishing, 236
 - SMS fraud, 22–23, 267
 - BadNews, 36–37
 - BeeKeeper, 33–35, 267, 275
 - case study, 277–279
 - Camera, 30–31, 267
 - DeathRing, 42
 - DroidSMS, 28–29
 - vs. goodware, 268–274
 - HDC Bookmark, 61–62
 - Joker, 47–49, 267, 280
 - Moundial, 268
 - vs. other malware, 275–279
 - RuFraud, 35–37, 267
 - RuPlay, 36–37, 267, 275
 - Taicliphot, 41–42, 267
 - Wallpaper, 29–30, 267
 - WallySMS, 38–39, 267
 - software development kit (SDK), 25
 - spam, 24
 - Dogowar, 35

- spyware, 16, 219
 - Acecard, 220
 - Cricketland, 31–32
 - Dougaleaker, 32–33
 - DroidDream Light, 35, 41
 - vs. goodware, 220–224
 - HeHe, 220
 - OneAudience, 56–57
 - vs. other malware, 224–227
 - Pincer, 220
 - Qibla Compass Ramadan, 220
 - case study, 227–232
 - UaPush, 219
 - USBCleaver, 220
 - UUPay, 42
- stalkerware, 16–17
- static (code) analysis, 72
 - vs. dynamic, 116
 - guided vs. unguided analysis, 72
 - permissions, 74, 90, 95
- static features, 182–184
- string encryption, breaking, 87–89,
101–102, 131–138
- supply chain malware, 49, 289–290
- system logs, 126–127

T

- toll fraud apps, 23
 - Joker, 47–49
 - Mono WAP, 39–40
 - Turkish Clicker, 42–43

- tracking techniques, 31. *See also*
 - International Mobile Equipment Identity
- training sample, 164
- training set, 164–166
- triadic suspicion graph (TSG), 187–188
 - features, 192–195
 - suspicious rank, 191–192
 - suspicious scores, 189–191
 - window-based segmentation,
193–195
- trojan apps, 14
 - Chamois, 51
 - DressCode, 46–47
 - DroidDream, 29
 - case study, 216–218
 - EagerFonts, 62–63
 - Ghost Push, 36
 - Gooligan, 52–53
 - Hummingbad, 53
 - Loapi, 60
 - OldBoot, 42
 - Podec, 60
 - Shuabang, 44
 - Snowfox, 52–53
 - Triada, 49–51
 - Xinyinhe, 53
 - YouTube Downloader, 54

W

- Windows malware, 284–286
 - vs. Android malware, 285–286