

# Index

## A

- Address Resolution Protocol (ARP), 215
- AES Cipher, 199
  - AesTest.py script, 264–265
  - AesUdpReceiver.py script, 266
  - AesUdpSender.py script, 265
  - approach, 267
  - brute-force attack, 266
  - PyCrypto and PyCryptodome libraries, 264
- Application Programming Interface (API)
  - hooking techniques
- API patching
  - advantages, 310
  - algorithm, 314
  - CTest and TestApplication, 311, 315
  - Deviare framework, 316
  - disadvantages, 311
  - GetAt method, 315
  - MySpyMgr.cpp file, 313
  - out.txt log file, 312
  - ProcessParam function, 313, 315
  - steps, 310
  - TextOutA WinAPI
    - function, 309, 312
  - VirtualQuery and VirtualProtect functions, 309
  - WinAPI, 309
- monitor tool, 302

Monitor v2, 19

proxy DLL, 302

AutoHotKey language, 18

AutoIt analysis functions

co-ordinate modes, 38

hexadecimal representation, 39

pixels changing, 42

programming languages, 18

specific pixel, 38

StretchBlt function, 44

## B

Bots

community classification, 7

comparison

community and developer, 13

compiler execution, 14

in-game, 13

input device, 15

memory, 14

network, 14

OS libraries, 15

out-game, 13

output device, 14

parameters, 13

data embedding, 12

developer classification, 9

game application, 3

in-game bot, 7

## INDEX

### Bots (*cont.*)

- out-game bots, 8
- purpose of
  - cheats and hacks, 2
  - deathmatch, 1
  - FPS games, 1
  - MMORPG games, 2
  - video game evolution, 1
- types of, 7

## C

- Cheat Engine, 97
- Cipher Block Chaining (CBC), 261
- Clicker bots
  - developer tools
    - analysis tool, 19
    - API hooking, 19
    - image processing
      - methods, 17–18
    - programming languages, 18
    - source code editors, 19
  - embedded system (*see* Embedded system/operating system)
  - Lineage 2 (*see* Lineage 2 game)
  - output device capture
    - AutoIt, 38
    - FastFind library, 46
    - GDI windows, 36
    - ImageSearch library, 54
    - output, 56
  - protection system
    - actions, 72
    - algorithm, 94
    - client-side part, 70
    - keyboard state check, 89
    - process scanner, 81
    - server-side part, 70

- steps, 70
- test application, 71

- CloseHandle function
  - DebugBreak, 185
  - debugger detection, 184
  - demonstrates, 185
  - try-except statement, 185–186
- ColorPix, 19
- CreateProcess function
  - algorithm, 189
  - inter-process communication, 190
  - parent and child processes, 188
  - possibilities, 186
  - SelfDebugging.cpp application, 187
- Cryptographic system, 252

## D

- Data Encryption Standard (DES), 259
- Debugger, 96
- Device Depended Bitmap (DDB), 37
- Device Independent Bitmap (DIB), 44
- Diablo 2 game
  - bot implementation, 160
    - AutohpBot.cpp source file, 166
    - character object, 161
    - details, 160
    - game process, 160
    - GetForegroundWindow, 161
    - GetWindowThreadProcessId
      - function, 161
    - health parameter, 164
    - IsArrayMatch function, 164
    - PostMessage function, 166
    - ScanSegments function, 163–164
  - bot overview, 145
    - advantages and disadvantages, 170
    - approach, 168

- articles, 169
- hotkey panel, 167
- keyIndex variable, 168
- process memory, 168
- UsePotion function, 169
- WriteWord function, 169
- game window, 142–143
- memory analysis, 146
  - artifacts, 147
  - experience points, 147
  - object, 154
  - parameters, 146
  - stamina value, 147
  - windowed mode, 146
- player parameter window, 144
- PostMessage function, 168
- Discretionary access control list (DACL), 197
- Dynamic-link libraries (DLL), 99

## E

- Embedded system/operating system
  - HAL, 22
  - high-level subroutines, 22
  - kernel, 22
  - keyboard stroke simulation, 23
    - active window, 23
    - AutoIt function, 25
    - inactive window, 28
  - mouse simulation
    - active window, 32
    - inactive window, 34
  - Native API, 22
  - simulate actions, 36
  - Win32 application, 22
  - Windows resources via
    - system API, 21

## F

- FastFind library, 18
  - AutoIt script, 46
  - C++ application, 47
  - explicit library linking, 48
  - FFBestSpot.au3 script, 50
  - FFLocalizeChanges.au3 script, 51–52
  - FFLocalizeChanges function, 53
  - FFSnapShot function, 53
  - implicit library linking, 48
  - MMORPG game Lineage 2, 49
  - parameters of (FFBestSpot function), 50
  - screenshot, 49
  - script, 52
  - SnapShots abstraction, 52
  - test.cpp source file, 47
- First-person shooter (FPS) games, 1

## G

- Game application
  - algorithm, 5
  - client application, 4
  - client-server architecture, 5
  - computing processes, 3
  - elements of, 3
  - input device, 4
  - memory sandbox, 3
  - operating system, 3
  - output device, 5
  - single mode, 6
- Graphics Device Interface (GDI)
  - bitmap, 37
  - concepts, 36
  - device contexts, 36
  - graphical objects and
    - devices, 37

## H

Hardware abstraction layer (HAL), 22

Heap access, 139

- CreateToolhelp32Snapshot, 140

- Heap32ListFirst, 140

- Heap32ListNext, 140

- HeapTraverse.cpp application, 140

- ListProcessHeaps function, 141

HeapMemView freeware, 97

Human Interface Device (HID), 278

Hypertext Transfer Protocol  
(HTTP), 221

## I, J

ImageSearch library, 18

- AutoIt script, 54

- ImageSearch function, 55

- Notepad icon, 54

- Search.au3 script, 54

- steps, 55

In-game bots

- access

- current process, 125

- heap access, 139

- open process, 117

- read and write operations, 121

- target process, 133

- TEB and PEB access, 124

- approaches against bots

- AES cipher, 199

- check correctness, 204

- CheckHash function, 206

- hashing, 204

- hide game data, 197

- protection algorithm, 197

- security descriptors, 197

- XOR cipher, 198

debugger, 96

Diablo 2 (*see* Diablo 2 game)

memory analyzing tools, 97

process memory analysis

- base address, 99

- 32-bit application, 107

- 64-bit application, 113

- blocks/segments, 99

- components, 98

- control flow, 106

- heap segments, 100

- launched process (ending), 104

- layout, 100

- linear address, 106

- machine code, 97

- memory map, 103

- memory segmentation model, 106

- OllyDbg and WinDbg

- debuggers, 117

- overview, 97

- process address space, 102

- random-access memory, 98

- real process, 105

- runtime, 98

- segment and description, 101

- stack segment, 100

- static libraries, 99

- thread, 99

- type system encode, 98

- variable offsets, 106

- variable searching algorithm, 106

programming language, 95

protection methods

- approaches against bots, 197

- CloseHandle, 184

- CreateProcess, 186

- IsDebuggerPresent, 178

- register manipulations, 190

- test application, 171
  - use of, 171
- register manipulations
  - BeingDebugged.cpp application, 193
  - debugger via checking registers, 191
  - \_\_forceinline keyword, 192
  - inline assembler, 190
  - Int3.cpp file, 197
  - IsDebug function, 196
  - IsDebuggerPresent
    - function, 190–191, 195
  - OllyDbg, 194
  - preprocessor macro, 193
- test application
  - algorithm, 172
  - analysis of, 173
  - bot actions, 175
  - main function, 174
  - memory map, 175
  - physical storage, 178
  - segment flags, 177
  - SimpleBot.cpp application, 175
  - steps, 173
  - TestApplication.cpp code, 172
- tools, 95
- Initialization vector (IV), 261
- Input device emulation
  - drivers directory, 275–276
  - emulate keyboard and mouse
    - action codes, 291
    - ControlKeyboardMouse.au3
      - script, 294, 296
    - keyboard-mouse.ino application, 291
    - readBytes method, 293
    - readBytesUntil method, 293
    - read method, 294
    - SendArduinoMouse function, 296
- hardware features, 275
- IDE, 276
- installation process, 276
- keyboard
  - application and script, 277
  - architecture, 276–277
  - Arduino board, 277
  - CommAPI files, 279
  - ControlKeyboard.au3 script, 279
  - HID compatible protocol, 278
  - keyboard.ino application, 277
  - loop function, 278
  - OpenPort function, 281
  - script, 281
  - SendArduino function, 282
- modifier keys
  - bytes, 283
  - ControlKeyboardCombo.au3
    - script, 284
  - keyboard-combo.ino application, 282
  - loop function, 284
- mouse device
  - Arduino IDE version, 285
  - ControlMouse.au3 script, 289
  - current cursor position, 285
  - descriptor, 286
  - formula symbols, 288
  - \_hidReportDescriptor array, 286
  - loop function, 288
  - Mouse.cpp file, 286
  - mouse.ino application, 286
- tools, 275
- Internet protocols
  - communication tasks
    - ARP tools, 215
    - local networks, 215
    - MAC address, 214
    - network hosts, 213
    - network packet, 213, 216

## INDEX

### Internet protocols (*cont.*)

- network switch, 214
- OSI model, 217
- ports, 216
- protocol meaning, 215
- router/gateway, 215
- stack of protocol, 216
- wireless connections (WiFi), 216

### NetChess (*see* NetChess application)

### packet analysis, 221

### packet capture

- active network adapters, 226
- capture data packet, 230
- display filter expression dialog, 228
- steps, 226, 232
- TCP packets, 231
- test application, 227
- TestTcpSender.py script, 230
- three-way handshake, 229

### TCP/IP stack

- Cerf, Vinton, 217
- Ethernet, 220
- fragmentation, 220
- Internet layer, 220
- IPv4 protocol, 220
- Kahn, Robert, 217
- layers, 218
- OSI model, 218
- topmost layer, 221
- transport layer, 220
- user datagram protocol, 220
- Wireshark window, 219

### test application

- algorithm, 221–222
- IPv4 and TCP protocols, 224
- listen method, 224
- loopback interface, 225
- network socket/socket, 222

### parameters, 224

### Python scripts, 222

### settimeout method, 225

### TestTcpReceiver.py script, 223

### TestTcpSender.py script, 222, 224–225

### UDP connection, 233

### algorithm, 233

### bytes, 235

### recv method, 234

### settimeout method, 234

### TestUdpReceiver.py script, 234–235

### IsDebuggerPresent function

### algorithm, 180

### assemble dialog, 182

### binary file, 183

### CheckRemoteDebuggerPresent function, 184

### EAX dialog modification, 181

### JE instruction, 182

### JNE instruction, 183

### OllyDbg plug-ins, 183

### OllyDumpEx, 183

### source code, 178

### steps, 181

### WinAPI function, 179

## K

### Kernel memory, 102

## L

### Lineage 2 game

### advantages, 69

### blind bot

### BlindBot.au3 script, 60

### BlindBotFunc.au3 script, 62

### hotkeys, 60

- shortcut panel, 59
- /target command, 61
- while loop, 61
- bot implementation, 58
  - algorithm, 58
  - blind bot, 59
  - bot with conditions, 63
  - improvements, 67
- bot with conditions
  - AnalysisBot.au3 script, 65
  - Attack functions, 66
  - FFBestSpot function, 63
  - IsTargetExist function, 64
  - LogWrite Function, 63
  - SelectTarget functions, 66
  - tracing, 63
- disadvantages, 69
- farming, 56
- improvements
  - aggressive monsters, 67
  - Attack and Move functions, 68
  - IsTargetExist function, 69
  - pseudorandom numbers, 69
  - SelectTarget function, 67
- interface, 57
- overview, 56
- Rpg-Club server, 58

## M

- Massively multiplayer online role-playing games (MMORPGs), 1

## N

- NetChess application
  - accept dialog, 238
  - advantages and disadvantages, 251

- benefits, 251
- bot implementation, 247
- bot overview, 239
- client configuration dialog, 237
- connection confirmation, 238
- server and client, 236
- server configuration dialog, 237
- StartGameBot.py script, 247
- steps, 236
- traffic analysis, 239
- window, 235–236

## O

- OllyDbg debugger, 96
- Open Systems Interconnection (OSI)
  - model, 217
- Operating system (OS), *see* Embedded system/operating system
- Optimal Asymmetric Encryption Padding (OAEP), 269
- OS-level interception data, 297
  - advantages, 317
  - Deviare, 297
  - DLL import, 299
  - DLL Wrapper Generator, 297
  - test application, 298
  - tools, 297
- Out-game bots
  - internet protocols (*see* Internet protocols)
    - cryptographic library, 209
    - installation variants, 211
    - modules, 209
    - PyCryptodome library, 210
    - PyCrypto library, 210
  - network analyzer, 211
  - protection approaches, 252

## INDEX

### Out-game bots (*cont.*)

- AES cipher, 264
  - cryptographic system, 252
  - decryption, 255
  - detection, 273
  - encryption, 252, 255
  - RSA cipher, 267
  - test application, 253
  - TestStringUdpSender.py script, 253
  - Triple DES cipher, 259
  - XOR cipher, 254
  - XorCrack.py script, 258
  - XorTest.py script, 255
  - XorUdpReceiver.py script, 256
  - XorUdpSender.py script, 256
- Python language, 209
- tools, 209
- windows configuration, 211–212

## P, Q

### Process Environment Block (PEB), 102

### Process identifier (PID), 117

### Process memory

- access
  - current process, 125
  - heap access, 139
  - open process, 117–121
  - read and write operations, 121
  - target process algorithm, 118, 133
  - TEB and PEB access, 124
- base address, 99
- 32-bit application
  - algorithm, 112
  - Cheat Engine scanner, 108
  - Cheat Engine window, 109
  - ColorPix window, 107
  - memory map, 111

### OllyDbg debugger, 110

### process list dialog, 108

### segment, 110

### stages, 108

### subtraction, 112

### TEB dump, 113

### 64-bit application

### attach to process dialog, 115

### memory map, 116

### resource monitor process, 117

### WinDbg, 114

### window (resource monitor), 114

### components, 98

### current process

### compiler intrinsics, 127

### descriptor table, 126

### GetTeb function, 125, 127

### NtCurrentTeb function, 129

### ntdll.lib file, 132

### NtQueryInformationThread, 130

### NT\_TIB structure, 128

### portable version, 128

### pragma directive, 132

### protected processor mode, 126

### segment addressing, 126

### TEB structure, 126

### WinAPI Function, 131

### winternal.h header file, 126

### heap segments, 100

### launched process (ending), 104

### machine code, 97

### memory blocks/segments, 99

### OllyDbg and WinDbg debuggers, 117

### overview, 97

### process address space, 102

### random-access memory, 98

### real process, 105

### runtime, 98



- segment and description, 101
  - stack segment, 100
  - static libraries, 99
  - target process
    - application, 133
    - console output, 135
    - CreateToolhelp32Snapshot, 136
    - ListProcessThreads function, 138
    - OpenProcessToken functions, 135
    - SetPrivilege functions, 135
    - TebPebMirror.cpp application, 133, 135, 139
    - TebPebTraverse.cpp application, 136
    - Thread32First, 136
    - Thread32Next, 136, 139
  - type system encode, 98
  - thread, 99
  - Protection system
    - algorithm, 94
    - keystrokes, 89
      - InitKeyHooks function, 91
      - KeyboardCheckProtection.au3 script, 90
      - \_KeyHandler procedure, 92
      - LLKHF\_INJECTED flag, 92
      - virtual device drivers, 92
      - VirtualMachineBot.au3 script, 93
      - WinAPI, 92
  - process scanner
    - AutoHotKey compiler window, 84
    - HT editor, 88–89
    - interpreter, 82
    - Md5ScanProtection.au3 script, 85
    - modules, 86
    - ProcessList function, 82, 86
    - ProcessScanProtection.au3 Script, 81
    - ScanProcess function, 86
    - SimpleBot.ahk script, 83
    - SimpleBot.au3 script, 82
    - SimpleBot.exe and AutoHotKey.exe files, 86
    - steps, 83
  - Proxy DLL
    - actions, 308
    - advantages, 305
    - bot algorithm, 306
    - disadvantages, 305
    - gdi32 subdirectory, 306
    - steps of, 303
    - TextOutA function, 303, 306
    - WinAPI, 302
  - Python language
    - cryptographic library, 209
    - installation variants, 211
    - modules, 209
    - PyCryptodome library, 210
    - PyCrypto library, 210
- ## R
- Random-access memory (RAM), 98
  - Read and write operations, 121
  - Role-playing game (RPG), 2
  - RSA cipher
    - chosen-plaintext attack, 269
    - game client, 267
    - importKey function, 271
    - PyCrypto and PyCryptodome libraries, 268
    - RsaOaepTest.py script, 269
    - RsaTest.py script, 268
    - RsaUdpReceiver.py script, 271
    - RsaUdpSender.py script, 270
    - session key, 272

## INDEX

### S

- SciTE editor, 19
- Static libraries, 99
- Structured Exception
  - Handling (SEH), 185

### T

- Thread Environment Block
  - (TEB), 101
- Thread Information Block
  - (TIB), 101
- Transmission Control
  - Protocol (TCP), 220
- Triple DES (3DES)
  - algorithm, 259
  - attacker, 260
  - 3DesTest.py script, 260
  - 3DesUdpReceiver.py script, 263
  - 3DesUdpSender.py script, 262
  - input parameters, 261
  - meet-in-the-middle attack, 260
  - random module, 261

### U

- Uniform Resource Locator (URL), 221
- User Datagram Protocol (UDP), 220

### V

- Virtual device drivers, 93
- Virtual machine (VM), 10

### W

- WinAPI functions, 19
- Win32 application, 22
- WinDbg freeware, 96
- Windows Application Programming
  - Interface (API), 21
- Wireless connections (WiFi), 216
- World Wide Web (WWW), 221

### X, Y, Z

- x64dbg debugger, 96
- XOR cipher, 198, 254