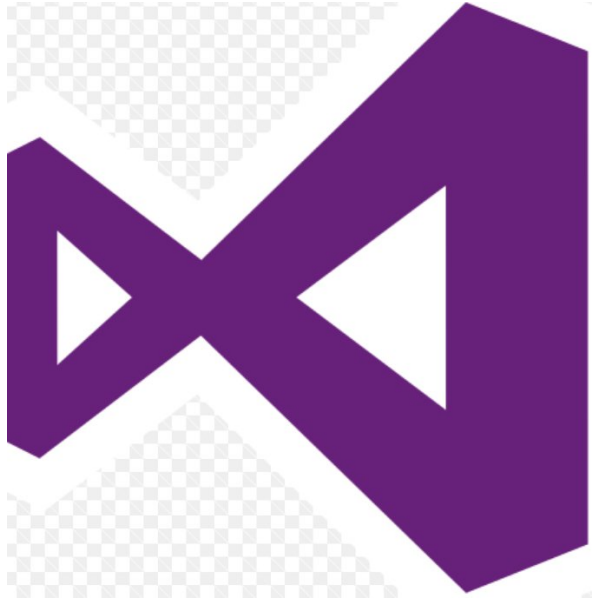


VON STEVEN
KOVACS

C# Pong mit Ballansteuerung durch externe Assemblerinjektion



Verwendete Software

Visual Studio 2013 Ultimate
Monogame Erweiterung (Ursprünglich XNA)

Cheat Engine 6.6
Debugger
Assembler Codeeditor

Bestandteile/Funktionsweise

C# Pong Software

Fügt hinzu:

- Benutzeroberfläche
- Beweglicher Spieler
- Automatisierter Bot
- Ergebnisanzeige
- Knopf
- Ballvisualisierung

Ließt RAM/
schreibt RAM



Windows Debugging Software

Integrierte Assemblerentwicklungsumgebung

Auto Assembler ließt:

- Spieler/Bot-Positionen

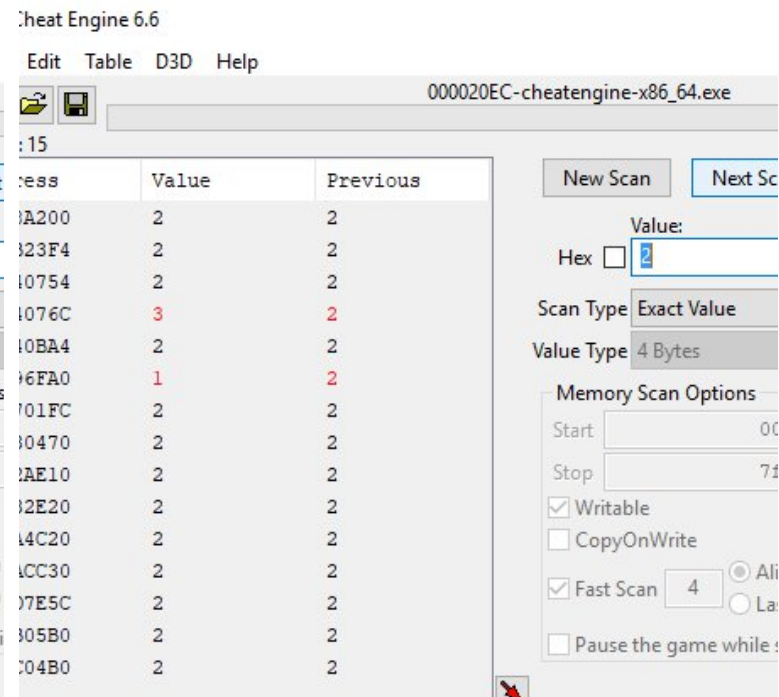
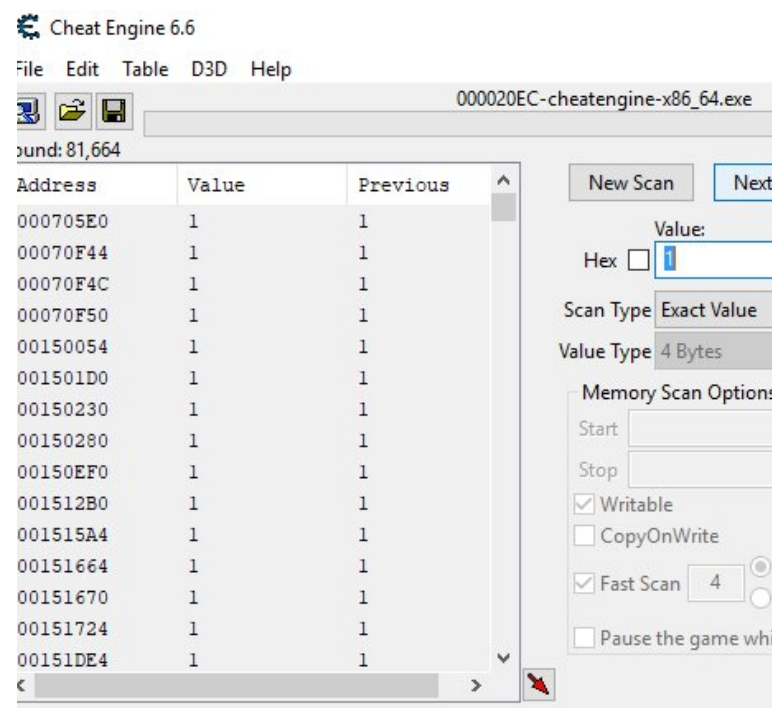
Auto Assembler schreibt:

- Ball position
- Spieler/Bot-Punktzahl

Wie wird die Kommunikation ermöglicht?

- Speicher finden
- Verweis auf neuen Speicher erstellen

Address	Bytes	Opcode
aobPlayerY	E9 B3 1EA4F6	jmp 007E0000
09D9E14D	90	nop
09D9E14E	DB 46 24	fild dword ptr [esi+24]
Protect:Execute/Read/Write Base=09D9E000		
address	48 49 4A 4B 4C 4D 4E 4F 50 51 52 53	
09D9E148	E9 B3 1E A4 F6 90 DB 46 24 D9 5D D	



The following opcodes accessed 03479CF0

C...	Instruction
10	0AA24542 - 83 7B 18 0A - cmp dword ptr [ebx+18],0A
651	0AA24571 - 8B 43 18 - mov eax,[ebx+18]
1	0A58699A - 89 51 18 - mov [ecx+18],edx
518	0AA2332D - 83 7E 18 0A - cmp dword ptr [esi+18],0A
10	0AA2332A - FF 46 18 - inc [esi+18]

0AA23323 - 77 08 - ja PongGame.PongGame.MainHandler::Update+E5

Replace

Show disassembler

Add to the codelist

More information

increment by 1