Subject: PowerupGameObj::Grant() and C4GameObj::Detonate()
Posted by iRANian on Sun, 01 Jul 2012 10:57:19 GMT
View Forum Message <> Reply to Message

After talking to StealthEye he told me that ::Grant() isn't jump hooked to the FDS' function, instead the function calling them being replaced completely (::Think() for both IIRC), and it seems to be the same for C4GameObj::Detonate().

Could a jump hook for the FDS' original functions for these replacements be added, so I can grab the address of 4.0's replacement functions in memory by checking the JMP at the start of the original functions?

PowerupGameObj::Grant() is at 0x006F1100
and C4GameObj::Detonate() is at 0x0070BE90

I'm not sure if the 4.0 replacement functions are called in 4.0's replacement ::Think().