Subject: Re: Syncing or changing BuildingGameObj 'IsDetroyed' state for clients
Posted by iRANian on Fri, 02 Aug 2013 09:04:34 GMT
View Forum Message <> Reply to Message

I checked the game's code and saw it exports and imports the IsDstroyed flag in BuildingGameObj::Import_Rare() and BuildingGameobj::Export_Rare(). However when importing it only calls BuildingGameObj::On_Destroyed() when the servers sends that the BuildingGameObj IsDetroyed is true and when on the client it's still alive (IsDetroyed set to false). I fixed the issue with building revival by setting the IsDestroyed on the client to what the server sends after that code (at the end of the function).

Here's my memory patched client code for TT's BuildingGameObj::Import_Rare(), using the space for alignment to add my patch:

```
561A8A63   84DB           TEST BL,BL // contains IsDestroyed sent by server
561A8A65   74 17          JE SHORT tt.561A8A7E // if false jump past this code to Out
561A8A67   80BE 70070000 00 CMP BYTE PTR DS:[ESI+770],0 // Check client IsDetroyed
561A8A6E   75 0E          JNZ SHORT tt.561A8A7E // if IsDestroyed is true jump to Out, only execute the below call if false
561A8A70   8B56 F8        MOV EDX,DWORD PTR DS:[ESI-8]
561A8A73   8B82 94000000    MOV EAX,DWORD PTR DS:[EDX+94]
561A8A79   8D4E F8        LEA ECX,DWORD PTR DS:[ESI-8]
561A8A7C   FFD0           CALL EAX // call BuildingGameObj::On_Destroyed()

// Out:
561A8A7E   889E 70070000    MOV BYTE PTR DS:[ESI+770],BL // I memory patched this in, this sets client IsDetroyed with what server sends
561A8A84   90             NOP
561A8A85   90             NOP
561A8A86   90             NOP
561A8A87   5F             POP EDI // Normal epilogue
561A8A88   5E             POP ESI
561A8A89   5B             POP EBX
561A8A8A   8BE5           MOV ESP,EBP
561A8A8C   5D             POP EBP
561A8A8D   C2 0400        RETN 4
```

So the issue can be fixed by 4.0 by patching BuildingGameObj::Import_Rare() to set the client IsDestroyed flag with what the server sends at the end of the function.

Note that the IsDestroyed offset is BuildingGameObj + 0x770, NOT 0x778 like I previously thought. The offset seems to be diffeerent between server versions and they handle Import_Rare() and Export_Rare() a bit differently.