Subject: Re: Blockable change team hook
Posted by iRANian on Thu, 28 Jun 2012 12:34:00 GMT
View Forum Message <> Reply to Message

Done, took me a bit to figure the displacement out. :/

Doesn't trigger on TEAM2 and TEAM but you can just replace them (and have them call the original console commands):

```
Hook *TeamChangeHook = new Hook;
int TTHookAddress = 0;

bool __cdecl ChangeTeamHook(int ID)
{
 Console_Output("playerid = %d\n", ID);
 return true;
}

void _declspec(naked) TeamChangeHook_Glue()
{
 _asm
 {

  mov  edi, ecx
  push [edi+6B4h]
  call ChangeTeamHook
  add esp, 4;
  mov ecx, edi

  test al, al
  jz BlockTeamChange

  mov edi, TTHookAddress
  jmp edi

BlockTeamChange:
  retn
 }
}

Toys::Toys()
{
 char OpCodeBuffer[5];
 Hooking::ReadMemory(0x004B4910, OpCodeBuffer, 5); // 0x004B4910 is where the JMP opcode (E9) starts, next 4 are the displacement/relative address

 int Displacement;
```

```
 memcpy(&Displacement, OpCodeBuffer+1, sizeof(OpCodeBuffer)); // OpCodeBuffer+1 or we'll
also read the JMP opcode

 TTHookAddress = 0x004B4910 + 5 + Displacement;
 Console_Output("displacement = %x, function address = 0x%X\n", Displacement,
TTHookAddress);

 TeamChangeHook->Install('\xE9', 0x004B4910, (int)&TeamChangeHook_Glue, "");
}
```
