Subject: [CODE] Blockable Team Change hook
Posted by iRANian on Mon, 02 Jul 2012 21:57:59 GMT
View Forum Message <> Reply to Message

For those who missed me posting it in the TT forums. Doesn't trigger on TEAM or TEAM2 so just replace those with a custom version.

```
Hook *TeamChangeHook = new Hook;
int TTHookAddress = 0; // Will be loaded with the calculated address of script 4.0's suicide hook code

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

void _declspec(naked) TeamChangeHook_Glue()
{
 _asm
 {
  mov  edi, ecx // save ecx

  push [edi+6B4h] // First argument, the ID of the player attempting to suicide
  call ChangeTeamHook
  add esp, 4; // Manually re-align the stack (our hook is __cdecl)

  mov ecx, edi // restore ecx

  test al, al // Check the return value of our hook
  jz BlockTeamChange // If the return value is zero (return false), jump to BlockTeamChange

  mov edi, TTHookAddress // Otherwise move the address of scripts 4.0's hook
  jmp edi // And jump to it

BlockTeamChange:
  retn // Return immediately without doing the team change
 }
}

int Calculate_Address_From_Displacement(int JMPStartAddress)
{
 char OpCodes[5];
 int Displacement, Address;

 Hooking::ReadMemory(JMPStartAddress, OpCodes, 5); // 0x004B4910 is where the JMP opcode (E9) starts, next 4 are the displacement/relative address
```

```
 memcpy(&Displacement, OpCodes+1, sizeof(char)*4); // OpCodeBuffer+1 or we'll also read the
JMP opcode

 Address = JMPStartAddress + 5 + Displacement;
 return Address;
}

 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(char)*4); // 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, "");
```