

---

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, "");
```

---

---

Subject: Re: [CODE] Blockable Team Change hook  
Posted by [Gen\\_Blacky](#) on Tue, 03 Jul 2012 07:15:24 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

Server crashes if you return true.

---

---

Subject: Re: [CODE] Blockable Team Change hook  
Posted by [iRANian](#) on Tue, 03 Jul 2012 07:34:34 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

I've updated the code I posted, try again, I just tested the code and it works with return true.

---

---

Subject: Re: [CODE] Blockable Team Change hook  
Posted by [iRANian](#) on Tue, 03 Jul 2012 08:18:33 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

Blacky confirmed it's working now when I spoke to him.

---

---

Subject: Re: [CODE] Blockable Team Change hook  
Posted by [Gen\\_Blacky](#) on Tue, 03 Jul 2012 08:21:00 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

Lies, but it works.

---

---

Subject: Re: [CODE] Blockable Team Change hook  
Posted by [Gen\\_Blacky](#) on Tue, 03 Jul 2012 15:06:01 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

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

void Console(const char *Format, ...)
{
    char buffer[256];
    va_list va;
    _crt_va_start(va, Format);
    vsnprintf(buffer, 256, Format, va);
    va_end(va);
    Console_Input(buffer);
}

bool __cdecl ChangeTeamHook(int ID)
{
    int GDIPlayers = (Tally_Team_Size(1));
    int NodPlayers = (Tally_Team_Size(0));
    int difference = GDIPlayers - NodPlayers;
    int Team = Find_Player(ID)->Get_Player_Type();
    StringClass side;
    if ( Team == 0 )
    {
        side = "GDI";
        Team = 1;
    }
    else
    {
        side = "Nod";
        Team = 0;
    }

    if ( GDIPlayers == NodPlayers )
    {
        Console("ppage %d Teams are Even!", ID);
        return false;
    }
    else if ( difference == 1 && NodPlayers != 0 )
    {
        Console("ppage %d GDI only has one more player then Nod!", ID);
        return false;
    }
}
```

```

else if ( difference == -1 && GDIPlayers != 0)
{
    Console("ppage %d Nod only has one more player then GDI!", ID);
    return false;
}
else if ( GDIPlayers > NodPlayers && Team == 1 )
{
    Console("ppage %d GDI has more player's then Nod!", ID);
    return false;
}
else if ( GDIPlayers < NodPlayers && Team == 0 )
{
    Console("ppage %d Nod has more player's then GDI!", ID);
    return false;
}

Change_Team(Get_GameObj(ID), Team);
Console_Output("%S Changed to Team %s\n", Find_Player(ID)->PlayerName, side);
Console("msg %S Changed to Team %s\n", Find_Player(ID)->PlayerName, side);
Find_Player(ID)->Set_Deaths(Find_Player(ID)->Get_Deaths() - 1 );
return false;
}

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, TeamChangeHookAddress // 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;
}
```

```
TeamChangeHookAddress = Calculate_Address_From_Displacement(0x004B4910);
Console_Output("[HOOK] TT TeamChangeHook address = 0x%X\n",
TeamChangeHookAddress);
TeamChangeHook->Install('\xE9', 0x004B4910, (int)&TeamChangeHook_Glue, "");
```

---