

---

Subject: [Server code] 4.1 patch 2 private chat hook  
Posted by [iRANian](#) on Sun, 05 Oct 2014 12:20:00 GMT  
[View Forum Message](#) <> [Reply to Message](#)

---

The previous version stopped working because the prologue of the TT chat code I'm hooking changed, seems to be because 4.1 uses a newer C++ compiler.

```
int TTChatHookAddress = 0;
int TTChatHookJMPAddress = 0;
int TTPrologueFuncCallAddress = 0;

bool ReadMemory(int Address, void* Buffer, int Size)
{
    bool ret = 1;
    DWORD OldProtect;
    HANDLE Process = OpenProcess(PROCESS_VM_READ | PROCESS_VM_WRITE |
PROCESS_VM_OPERATION, false, GetCurrentProcessId());
    VirtualProtectEx(Process, (LPVOID)Address, Size, PAGE_EXECUTE_READWRITE,
&OldProtect);
    if (!ReadProcessMemory(Process, (LPVOID)Address, Buffer, Size, NULL))
    {
        Console_Output("Reading process memory address 0x%x failed\n", Address);
        Console_Output("GetLastError() = %d\n", GetLastError());
        ret = 0;
    }
    VirtualProtectEx(Process, (LPVOID)Address, Size, OldProtect, NULL);
    CloseHandle(Process);
    return ret;
}

bool WriteMemory(int Address, const void* Buffer, int Size)
{
    bool ret = 1;
    DWORD OldProtect;
    HANDLE Process = OpenProcess(PROCESS_VM_READ | PROCESS_VM_WRITE |
PROCESS_VM_OPERATION, false, GetCurrentProcessId());
    VirtualProtectEx(Process, (LPVOID)Address, Size, PAGE_EXECUTE_READWRITE,
&OldProtect);
    if (!WriteProcessMemory(Process, (LPVOID)Address, Buffer, Size, NULL))
    {
        Console_Output("Hooking address 0x%x failed\n", Address);
        Console_Output("GetLastError() = %d\n", GetLastError());
        ret = 0;
    }
    VirtualProtectEx(Process, (LPVOID)Address, Size, OldProtect, NULL);
    CloseHandle(Process);
    return ret;
}
```

```

}

void Install_Hook(char OpCode, int Addr, int Glue, char *Padding)
{
    int HookAddress = Addr;
    int Offset = Glue - HookAddress - 5;
    WriteMemory(HookAddress, &OpCode, 1);
    WriteMemory(HookAddress+1, &Offset, 4);
};

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

    ReadMemory(JMPStartAddress, OpCodes, 5);
    Console_Output("BYTES READ: 0x%x 0x%x 0x%x 0x%x 0x%x \n", OpCodes[0],
OpCodes[1], OpCodes[2], OpCodes[3], OpCodes[4]);

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

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

bool _cdecl Private_Chat_Hook(int PlayerID, int Type, wchar_t *Message, int TargetID)
{
    if (TargetID == -2 || Type != 2) { return true; } // Only trigger on valid private chat

    Console_Output("PlayerID = %d, TargetID = %d, type = %d, Message = %S\n", PlayerID,
TargetID, Type, Message);

    return false;
}

void _declspec(naked) PrivateChatHook_Glue()
{
    _asm
    {
        push esi
        mov eax, esi
        mov esi, ecx // save ecx

        push [ecx+06C0h] // arg 4, TargetID
        push [ecx+06BCh] // arg 3, Message
        push [ecx+06B8h] // arg 2, Type
        push [ecx+06B4h] // arg 1, PlayerID
    }
}

```

```
call Private_Chat_Hook
add esp, 16;

mov ecx, esi // restore ecx

test al, al
jz Block_Private_Chat

call TTPrologueFuncCallAddress
jmp TTChatHookJMPAddress
```

Block\_Private\_Chat:

```
pop esi
retn
}
}
```

// install function, OnLoadGlobalINISettings is a good place to install, the plugin constructor doesn't work

```
void TriggerbotAntiCheat::OnLoadGlobalINISettings(INIClass *SSGMINi)
{
    TTChatHookAddress = Calculate_Address_From_Displacement(0x004B5C10); // Hook from
    cCsTextObj::Act(void)
    TTChatHookJMPAddress = TTChatHookAddress+8;
    TTPrologueFuncCallAddress = Calculate_Address_From_Displacement(TTChatHookAddress +
    3);

    Install_Hook('\xE9', TTChatHookAddress, (int)&PrivateChatHook_Glue, "");
}
```