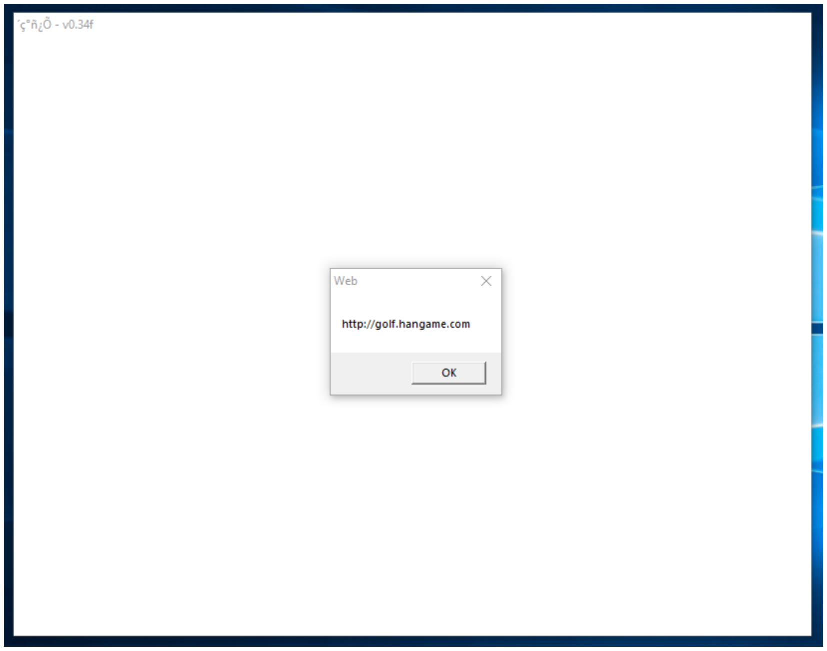
Daniel Hoynoski

Golf King Client Version: v0.34f

Turn In (Extended): May 4th, 2018

Game Crack 1 - Removing Nag When Opening DangGol.exe

When trying to launch the game directly from the executable, I am presented with the following error message:



http://golf.hangame.com

This is shown because Korean games make you sign into the games website in order to launch the game. Obviously, since this game has been abandoned for nearly 13 years, these services don't exist anymore.

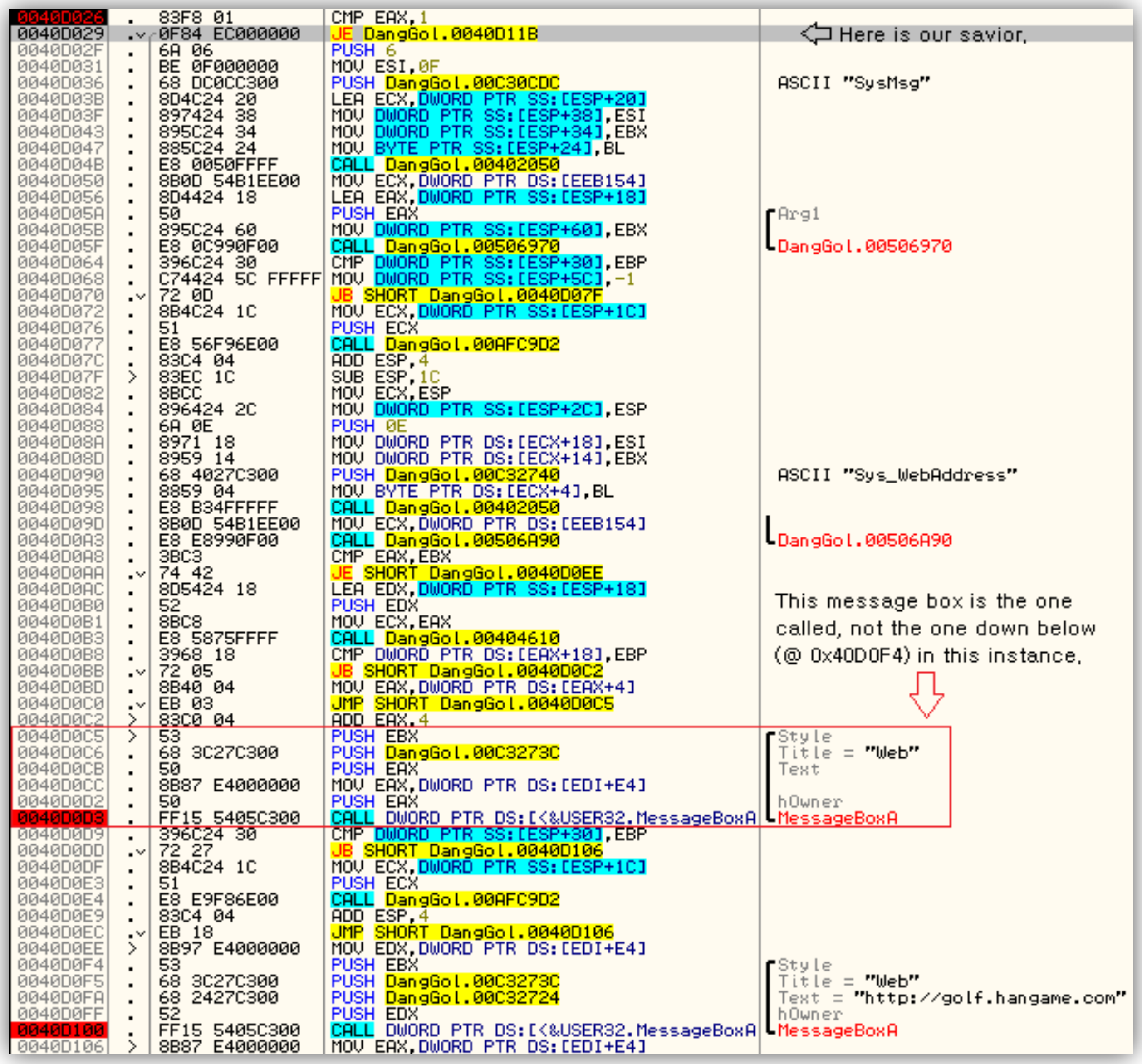
This is the definition of a nag dialog box, so it should be easy to remove with OllyDBG! When I breakpointed all of the intermodular calls of "MessageBoxA" and then ran the executable it halted at the assembly code of the nagging dialog box of "http://golf.hangame.com." We found it! After looking at the jump statements, they either jump to the dialog box (i.e. the *nag box*) or they just jump a couple lines down, but still on the path to the *nag box*. If you keep looking further up you will arrive at the jump statement that reads

Memory:	**Opcode:**	**Assembly Instruction:**
0040D026	**0F84 EC000000**	**JE DangGol.0040D11B**

This statement jumps right over the *nag box,* which is what we want! ☺ If you run the app and put a breakpoint at this instruction and then change the zero flag we can hop over the *nag box* and success! The *nag box* is gone!

PATCHING:

Change the **JE**, jump if equal too, to a **JMP**, jump always. The comparison of **EAX** and the number **0x01h** is obviously not equal here, for a reason I am not sure of at this time, so it will not take this jump. Patch the code to remove this bastard.

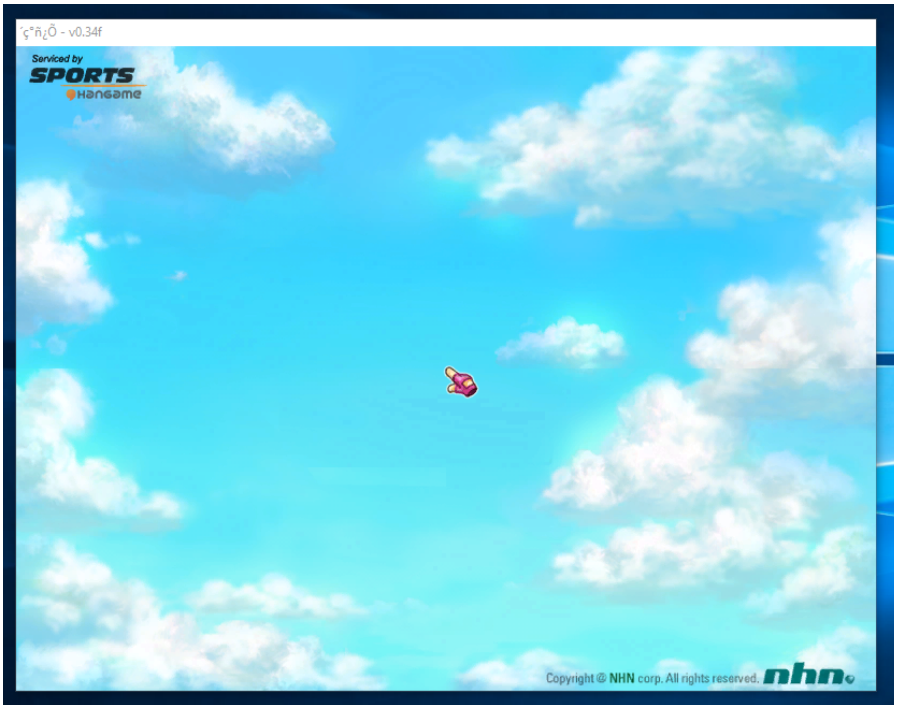


```
0040D026  .    83F8 01          CMP EAX,1
0040D029  .v   0F84 EC000000    JE DangGol.0040D11B                        ⇦ Here is our savior.
0040D02F  .    6A 06            PUSH 6
0040D031  .    BE 0F000000      MOV ESI,0F
0040D036  .    68 DC0CC300      PUSH DangGol.00C30CDC                      ASCII "SysMsg"
0040D03B  .    8D4C24 20        LEA ECX,DWORD PTR SS:[ESP+20]
0040D03F  .    897424 38        MOV DWORD PTR SS:[ESP+38],ESI
0040D043  .    895C24 34        MOV DWORD PTR SS:[ESP+34],EBX
0040D047  .    885C24 24        MOV BYTE PTR SS:[ESP+24],BL
0040D04B  .    E8 0050FFFF      CALL DangGol.00402050
0040D050  .    8B0D 54B1EE00    MOV ECX,DWORD PTR DS:[EEB154]
0040D056  .    8D4424 18        LEA EAX,DWORD PTR SS:[ESP+18]
0040D05A  .    50               PUSH EAX                                   Arg1
0040D05B  .    895C24 60        MOV DWORD PTR SS:[ESP+60],EBX
0040D05F  .    E8 0C990F00      CALL DangGol.00506970                      DangGol.00506970
0040D064  .    396C24 30        CMP DWORD PTR SS:[ESP+30],EBP
0040D068  .    C74424 5C FFFFF  MOV DWORD PTR SS:[ESP+5C],-1
0040D070  .v   72 0D            JB SHORT DangGol.0040D07F
0040D072  .    8B4C24 1C        MOV ECX,DWORD PTR SS:[ESP+1C]
0040D076  .    51               PUSH ECX
0040D077  .    E8 56F96E00      CALL DangGol.00AFC9D2
0040D07C  .    83C4 04          ADD ESP,4
0040D07F  >    83EC 1C          SUB ESP,1C
0040D082  .    8BCC             MOV ECX,ESP
0040D084  .    896424 2C        MOV DWORD PTR SS:[ESP+2C],ESP
0040D088  .    6A 0E            PUSH 0E
0040D08A  .    8971 18          MOV DWORD PTR DS:[ECX+18],ESI
0040D08D  .    8959 14          MOV DWORD PTR DS:[ECX+14],EBX
0040D090  .    68 4027C300      PUSH DangGol.00C32740                      ASCII "Sys_WebAddress"
0040D095  .    8859 04          MOV BYTE PTR DS:[ECX+4],BL
0040D098  .    E8 B34FFFFF      CALL DangGol.00402050
0040D09D  .    8B0D 54B1EE00    MOV ECX,DWORD PTR DS:[EEB154]
0040D0A3  .    E8 E8990F00      CALL DangGol.00506A90                      DangGol.00506A90
0040D0A8  .    3BC3             CMP EAX,EBX
0040D0AA  .v   74 42            JE SHORT DangGol.0040D0EE
0040D0AC  .    8D5424 18        LEA EDX,DWORD PTR SS:[ESP+18]
0040D0B0  .    52               PUSH EDX
0040D0B1  .    8BC8             MOV ECX,EAX
0040D0B3  .    E8 5875FFFF      CALL DangGol.00404610
0040D0B8  .    3968 18          CMP DWORD PTR DS:[EAX+18],EBP
0040D0BB  .v   72 05            JB SHORT DangGol.0040D0C2
0040D0BD  .    8B40 04          MOV EAX,DWORD PTR DS:[EAX+4]
0040D0C0  .v   EB 03            JMP SHORT DangGol.0040D0C5
0040D0C2  >    83C0 04          ADD EAX,4
0040D0C5  >    53               PUSH EBX                                   Style
0040D0C6  .    68 3C27C300      PUSH DangGol.00C3273C                      Title = "Web"
0040D0CB  .    50               PUSH EAX                                   Text
0040D0CC  .    8B87 E4000000    MOV EAX,DWORD PTR DS:[EDI+E4]
0040D0D2  .    50               PUSH EAX                                   hOwner
0040D0D3  .    FF15 5405C300    CALL DWORD PTR DS:[<&USER32.MessageBoxA    MessageBoxA
0040D0D9  .    396C24 30        CMP DWORD PTR SS:[ESP+30],EBP
0040D0DD  .v   72 27            JB SHORT DangGol.0040D106
0040D0DF  .    8B4C24 1C        MOV ECX,DWORD PTR SS:[ESP+1C]
0040D0E3  .    51               PUSH ECX
0040D0E4  .    E8 E9F86E00      CALL DangGol.00AFC9D2
0040D0E9  .    83C4 04          ADD ESP,4
0040D0EC  .v   EB 18            JMP SHORT DangGol.0040D106
0040D0EE  >    8B97 E4000000    MOV EDX,DWORD PTR DS:[EDI+E4]
0040D0F4  .    53               PUSH EBX                                   Style
0040D0F5  .    68 3C27C300      PUSH DangGol.00C3273C                      Title = "Web"
0040D0FA  .    68 2427C300      PUSH DangGol.00C32724                      Text = "http://golf.hangame.com"
0040D0FF  .    52               PUSH EDX                                   hOwner
0040D100  .    FF15 5405C300    CALL DWORD PTR DS:[<&USER32.MessageBoxA    MessageBoxA
0040D106  >    8B87 E4000000    MOV EAX,DWORD PTR DS:[EDI+E4]
```

This message box is the one called, not the one down below (@ 0x40D0F4) in this instance.

Let’s Launch Again:

Once this is patched, launch the executable, revealed a new screen:



However, the game freezes and then crashes soon after. This is lightly due to it caught in a loop of repeatedly trying to contact servers that do not exist anymore.