Daniel Hoynoski

Golf King Client Version: v0.34f

Turn In (extended): Friday, May 4th, 2018

Game Crack 2 - Buttons!

Amazing!!!! I am finally able to have a working screen up! Yes there is no server, but alas it is the login in page! To begin, after the last success I noticed that a gameguard updating box appear in the upper left hand corner. It would disappear, sometimes right away and sometimes in a couple seconds and then an error message would come up saying:

Korean-

Title: 게임가드 에러: 380

Message: "게임가드 업데이트 서버 접속에 실패하였습니다. 잠시 후 재시도 해보거나, 게인 방화벽이 있다면 설정을 조정해 보시기 바랍니다."

English-
Title: GameGuard Error: 380
Message: "Failed to connect to the GameGuard update server. Try back later, or if the firewall settings to adjust the gain, please."

And then once we clicked okay, our lovely nag box from the last success would appear (It had a second location for this bastard, but it located easily right under our original one). Now thinking GameGuard, I went to search for all referenced test strings and at the top of the list there were many GameGuard related strings, plus some "HackShield" strings too. After placing a breakpoint at them I was able to halt the program and figure out what was going on. Pacing through the code brought me to a very special call. It was the call to our GameGuard Application. It is located at (0x00404B97, but may vary depending on the systems). If we go over it, the application opens then closes, the stack is not altered. But thinking about how we can get rid of that text box that comes after this application, if we continue downward we see two jump statements:

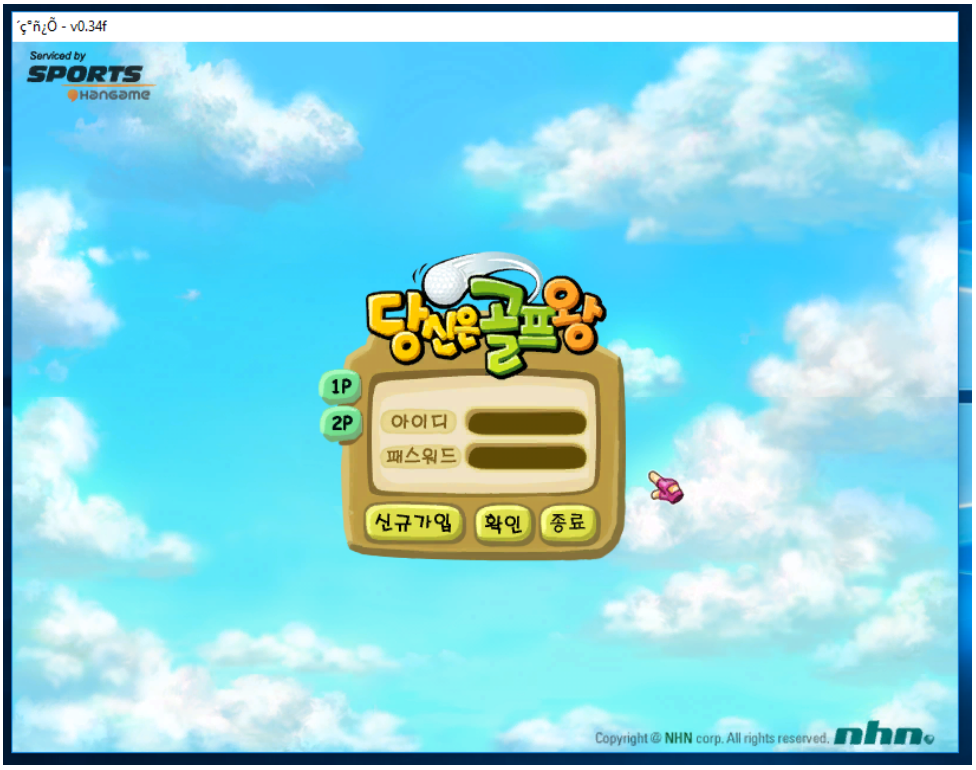
Memory:	Opcode:	Assembly Instruction:
0040514B	74 64	JE SHORT DangGol.004051B1
0040514D	85F6	TEST ESI, ESI
0040514F	74 60	JE SHORT DangGol.004051B1

If we set the zero flag we skip our stupid message that displays the details as reported above. Next if we continue we will come to **Jump If Not Zero** instruction and the next line below it pushes the ascii code "InitHackSheild() return FALSE!!!" Well in this case it was not going to take that jump. Now if we let it continue onward it would give us our old nag box and then halt but if we jump this code we succeed and it brings us to a nice login screen. This is our bastard here! Patch it by making this jump all the time!

```
006752BC  .  85C0          TEST EAX,EAX
006752BE  .v 75 16         JNZ SHORT DangGol_.006752D6      <= patch this line by always jumping to succeed!
006752C0  .  68 A478C800   PUSH DangGol_.00C878A4           ASCII "InitHackShield() return FALSE!!!□"
006752C5  .  6A 10         PUSH 10
006752C7  .  E8 B4F6D8FF   CALL DangGol_.00404980
006752CC  .  83C4 08       ADD ESP,8
006752CF  .  33C0          XOR EAX,EAX
006752D1  .v E9 2B010000   JMP DangGol_.00675401
006752D6  >  68 8C78C800   PUSH DangGol_.00C8788C           ASCII "InitHackShield() - end□"
```

Result:

There is a bit of unresponsiveness in the beginning, but I attribute this to the server checking looping that is contained within the program. But after a tiny bit, we are greeted with a login screen:



If the servers were still alive, this would have essentially bypassed the anti-hacking software in the game.