Nish Patel

Part 2 Documentation

Completed both requirements.

Methodology to Bypass Authentication:

Banner: To fulfill requirement #1 (*launch without "Expired Trial Period" on top*), I used breakpoints and debugging to find the code section of branches regarding the application window banner (around address 0x0076B0A7). My method of disabling the expired trial banners was modifying the first conditional jump to skip directly to the branch that selects the text " (Unregistered Copy) ". This was done by replacing the instruction with a (nonconditional) jmp to the desired location.

Popup: To fulfill option #2 (*launch without "31-Day Trial Expiration" Popup*), I used more breakpoints to find where the popups occur (around address 0x008163B5). This took time, because the process of enabling the popup takes considerably more subroutine calls than the banner branches. Ultimately, using a combination of step-overs and step-ins, the proper function was isolated. Similar to my approach for option #1, I chose to skip over the call entirely to cease the popup (and hopefully skip as much "unnecessary" code as possible). To be precise, I modified the instruction just before the call to skip the subroutine…

```
mov     eax, off_863454
mov     eax, [eax] ; Modified this instruction
call    sub_81637C
```

I did not add or delete instructions, simply modified bytes (opcodes and operands).

Instructions Changed: Format (Address: Original → **New Instruction**)

Option 1 (Banner):

1) (`0076B0A7`: `je short loc_76B0B8` → **`jmp short loc_76B0F6`**)
    a. *Bytes*: `74 0F` → **`EB 4D`**

Option 2 (Popup):

1) (`00858C8E`: `mov eax, [eax]` → **`jmp short loc_858CB9`**)
    a. *Bytes*: `8B 00` → **`EB 29`**