Câu 1.1.exe

Đặt thử breakpoint tại 004014A6 . E8 5B080000 CALL <JMP.&user32.GetDlgItemTextA> ; \GetDlgItemTextA

Thử nhập key là abcdefgh, key sẽ được lưu vào địa chỉ 0040332C

Ta thấy từ 00401506 - 0040155B, key sẽ được lấy để làm vài việc.

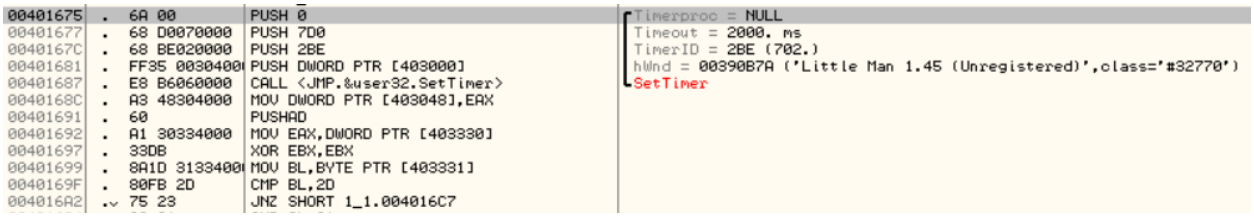
```
00401506  >  A1 2C334000   MOV EAX,DWORD PTR [40332C]
0040150B  .  8B1D 3033400( MOV EBX,DWORD PTR [403330]
00401511  .  A3 E6324000   MOV DWORD PTR [4032E6],EAX
00401516  .  891D EA32400( MOV DWORD PTR [4032EA],EBX
0040151C  .  E8 C8040000   CALL 1_1.004019E9
00401521  .  893D 4B33400( MOV DWORD PTR [40334B],EDI
00401527  .  A1 4B334000   MOV EAX,DWORD PTR [40334B]
0040152C  .  8B1D 3033400( MOV EBX,DWORD PTR [403330]
00401532  .  A3 E6324000   MOV DWORD PTR [4032E6],EAX
00401537  .  33C0          XOR EAX,EAX
00401539  .  891D EA32400( MOV DWORD PTR [4032EA],EBX
0040153F  .  60            PUSHAD
00401540  .  68 ADDE0000   PUSH 0DEAD
00401545  .  58            POP EAX
00401546  .  68 EFBE0000   PUSH 0BEEF
0040154B  .  5B            POP EBX
0040154C  .  68 AFAAAA0A   PUSH 0AAAAAAF
00401551  .  59            POP ECX
00401552  .  0FC9          BSWAP ECX
00401554  .  0FC9          BSWAP ECX
00401556  .  61            POPAD
00401557  .  0C 01         OR AL,1
00401559  .  0BC0          OR EAX,EAX
0040155B  .v 0F85 8F00000( JNZ 1_1.004015F0
```

Để ý từ 00401557-0040155B, câu lệnh này luôn nhảy, vì vậy, dòng lệnh để hiển thị "Your are Registered" sẽ không được gọi.

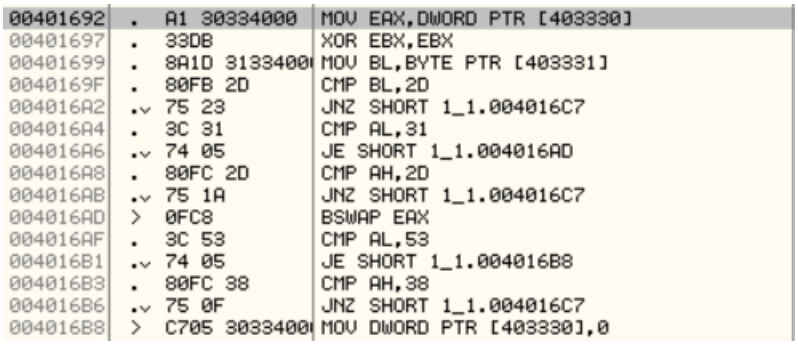
Từ 00401598-004015EB, là đoạn lệnh cho phép hiện “Registered”. Làm sao để vào được đoạn lệnh này?

```
00401585  >  6A 40         PUSH 40                                 Style = MB_OK|MB_ICONASTERISK|MB_APPLMODAL
00401587  .  68 7A154000   PUSH 1_1.0040157A                       Title = "Good Work!"
0040158C  .  68 63154000   PUSH 1_1.00401563                       Text = "Your are Registered!"
00401591  .  6A 00         PUSH 0                                  hOwner = NULL
00401593  .  E8 98070000   CALL <JMP.&user32.MessageBoxA>          MessageBoxA
00401598  >  6A 00         PUSH 0                                  Enable = FALSE
0040159A  .  FF35 6030400( PUSH DWORD PTR [403060]                 hWnd = 00260D6C (class='Edit',parent=00390B7A)
004015A0  .  E8 31070000   CALL <JMP.&user32.EnableWindow>         EnableWindow
004015A5  .  6A 01         PUSH 1                                  Enable = TRUE
004015A7  .  FF35 6030400( PUSH DWORD PTR [403060]                 hWnd = 00260D6C (class='Edit',parent=00390B7A)
004015AD  .  E8 24070000   CALL <JMP.&user32.EnableWindow>         EnableWindow
004015B2  .  6A 00         PUSH 0                                  Enable = FALSE
004015B4  .  FF35 6430400( PUSH DWORD PTR [403064]                 hWnd = 00100DA6 (class='Edit',parent=00390B7A)
004015BA  .  E8 17070000   CALL <JMP.&user32.EnableWindow>         EnableWindow
004015BF  .  8D05 CC10400( LEA EAX,DWORD PTR [4010CC]
004015C5  .  83E8 1F       SUB EAX,1F
004015C8  .  50            PUSH EAX                                lParam => 4010AD
004015C9  .  6A 00         PUSH 0                                  wParam = 0
004015CB  .  6A 0C         PUSH 0C                                 Message = WM_SETTEXT
004015CD  .  FF75 08       PUSH DWORD PTR [EBP+8]                  hWnd
004015D0  .  E8 67070000   CALL <JMP.&user32.SendMessageA>         SendMessageA
004015D5  .  8D05 AE32400( LEA EAX,DWORD PTR [4032AE]
004015DB  .  83C0 0F       ADD EAX,0F
004015DE  .  50            PUSH EAX                                lParam => 4032BD
004015DF  .  6A 00         PUSH 0                                  wParam = 0
004015E1  .  6A 0C         PUSH 0C                                 Message = WM_SETTEXT
004015E3  .  68 CA000000   PUSH 0CA                                ControlID = CA (202.)
004015E8  .  FF75 08       PUSH DWORD PTR [EBP+8]                  hWnd
004015EB  .  E8 46070000   CALL <JMP.&user32.SendDlgItemMessageA>  SendDlgItemMessageA
```

Từ 00401675-004016A2, xử lý WM_TIMER message



Nhận thấy từ 00401692-004016B8, đây là đoạn lệnh có tác động tới 00403330 (tức là: 0040332C+4), vì thế nếu key là abcdefgh tại 0040332C thì tại 00403330 sẽ là efgh



Ta phân tích đoạn mã trên với key là abcdefgh:

00401692 mov eax, [403330] //eax=”hgfe”

00401697 xor ebx, ebx

00401699 mov bl, byte ptr [403331] //ebx=’f’

0040169F cmp bl, 2Dh //so sánh bl==’-’

004016A2 jnz short loc_4016C7 //nếu không bằng, nhảy tới 4016C7

004016A4 cmp al, 31h //al==’1’? //ta không xét nhiều về so sánh này

004016A6 jz short loc_4016AD

004016A8 cmp ah, 2Dh //ah==bl==’-’

004016AB jnz short loc_4016C7

004016AD bswap eax //đảo => eax=”efgh”

004016AF cmp al, 53h // al=='S'? => ‘h’==’S’ //nếu bằng => đúng

004016B1 jz short loc_4016B8

004016B3 cmp ah, 38h //hoặc ah=='8' => ‘g’==’8’ //nếu bằng => cũng đúng

004016B6 jnz short loc_4016C7

Từ đoạn mã trên, ta có thể suy ra quy luật key:

Key: *****-*S*** (với * có thể là ký tự bất kỳ)

Hoặc:

Key: *****-8**** (với * có thể là ký tự bất kỳ)

Ví dụ:

Key: 12345-1S234

Hoặc:

Key: 12345-81234