## Flag:

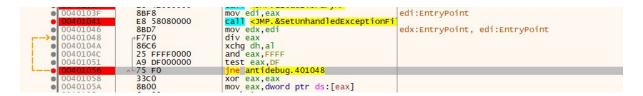
# "NtQu3ry1nf0rm@t10nPr0(355R@!s33xc3pt!onD3bugPr1v1l3g3 St@ckT1m3CCS3lf-P3BF1ndW1nd0wH1d1ng@nt1-R3v3rs3"

### Mô tả:

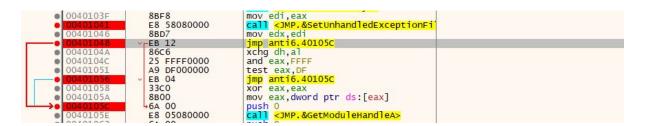
- Chương trình kiểm tra xem có trong chế độ debug k? có => exit
- Chương trình tồn tại lỗi => sinh lỗi => lỗi, exit
- Cần tìm input đầu vào sao cho sau khi press "check" button, ta thu được 100

## Debug - danh sách lỗi và sửa lỗi:

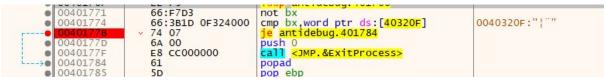
#### 1. SetUnhandledExceptionFilter



- Khi debug, hàm trả về NULL (0) => eax = 0 => lỗi khi div eax
- 0x401056: Nếu khác không => nhảy đến 0x401048 (div eax) => bỏ qua 2 lệnh này, jmp đến phần lệnh tiếp theo



#### 2. Bug



#### => je thành jmp



## 3. IsDebuggerPresent

- return 0, nếu process không chạy trong luồng debug
- return khác 0, nếu process chay trong luồng debug

```
pusn gword ptr ds:[4U3/ZU]
call <JMP.&SendMessageA>
call <JMP.&IsDebuggerPresent>
                                              E8 74070000
E8 1B070000
0040114F
00401155
                                                                                            call <JMP.&IsDebuggerPresent>
test eax, eax
jne antidebug.401256
mov ebx,dword ptr ::[30]
cmp dword ptr ds:[ebx+68],0
jne antidebug.401256
mov eax,dword ptr ds:[ebx+18]
cmp dword ptr ds:[eax+c],2
jne antidebug.401256
cmp dword ptr ds:[eax+t0],0
jne antidebug.401256
lea esi,dword ptr ds:[40109A]
mov al,47
                                             85C0
0F85 EF000000
    0040115F
                                             64:8B1D 30000000
837B 68 00
0F85 DE000000
8B43 18
     0040116E
     00401178
                                             8378 OC 02
0F85 D1000000
     0040117B
0040117F
                                             8378 10 00
0F85 C7000000
                                              8D35 9A104000
B0 47
     0040118F
                                                                                                                                                                                           esi:EntryPoint
                                                                                             mov al,47
add al,byte ptr ds:[403209]
                                              0205 09324000
```

- => return khác 0 => jne True khi chạy debug.
  - 0x401256: exit process
- => jmp or nop it



#### 4. ZwQueryInformationProcess

- Trả về thông tin về process

```
• 0040120D
                        C705 14374000 000 mov dword ptr ds: [403714],0
                                                 push 0
push 4
                        6A 00
                        6A 04
.
   00401219
                        68 14374000
   0040121B
                                                 push antidebug. 403714
   00401220
                        6A 07
                                                 push 7
                                                 push /
push FFFFFFFF

call <JMP. &ZwQueryInformationProces

test eax,eax
ine antidebug. 401256
lea esi,dword ptr ds:[4010A4]
                        6A FF
   00401222
                        E8 FD050000
00401229
                        85C0
                        75 29
                        8D35 A4104000
• 0040122D
                                                                                                  esi:EntryPoint
```

- => return khác 0, là port dùng để dubug
- => ine True => exit
- => nop or jump

```
A3 0C3/4000 mov dword ptr ds:[403/0C], e. C705 14374000 000 mov dword ptr ds:[403/14], 0
   00401208
0040120D
                      6A 00
                                            push 0
                      6A 04
                                            push 4
                      68 14374000
                                            push anti6.403714
   0040121B
   00401220
                      6A 07
                                            push
    0040122
                      6A 00
                                            push 0
                      E8 FD050000
                                                  <JMP.&ZwQueryInformationProce</pre>
→ 00401229
                                            test eax, eax
                      85CO
                      EB 00
                                             imp anti6.40122D
                      8D35 A4104000
                                            lea esi, dword ptr ds:[4010A4]
 0
   00401233
                      BO 4F
                                            mov al,4F
add al,byte ptr ds:[403714]
                                                                                        4F: '0'
                      0205 14374000
```

#### 5. ZwSetInformationThread

Ở debug, thread được tạo ra dừng gửi thông báo về các debug event

```
●II 00401529
                                                       pusnta
                           6A 00
                                                       push 0
.
    0040152C
                           6A 00
                                                       push 0
   0040152E
.
                           6A 11
                                                       push 11
                                                       push FFFFFFE
                           6A FE
.
                                                      call <JMP.&ZwSetInformationThread>
push dword ptr ss:[ebp+8]
call <JMP.&Istrlen>
mov dword ptr ds:[403710] eax
                           E8 F5020000
FF75 08
8
   0040153
                          E8 6B030000
   0040153A
0
```

=> imp bỏ qua lệnh này

```
00401528
                                60
                                                                 pushad
00401529
                                90
                                                                  pushfd
                                                                  jmp anti6.401537
                                EB OB
                                6A 00
0
   0040152E
                                6A 11
                                                                 push 11
                                                                push ff
push FFFFFFFE

call <JMP.&ZwsetInformationThread>
push dword ptr ss:[ebp+8]

call <JMP.&Istrlen>
mov dword ptr ds:[403710],eax
mov ecx,dword ptr ss:[ebp+10]
   00401530
                                6A FE
.
                               E8 F5020000
FF75 08
                               E8 6B030000
A3 10374000
   0040153A
0040153F
.
.
00401544
                                8B4D 10
```

## 6. CheckRemoteDebuggerPresent

- return 0, nếu không ở debug
- return khác 0, nếu ở debug

```
add byte ptr ds:[eax],al
push antidebug.403714
                                                                                                ecx.EntryPoint
   0040135E
                       0000
.
                       68 14374000
                                                push FFFFFFF
                                                call <JMP.&CheckRemoteDebuggerPrese
cmp dword ptr ds:[403714],0
jne antidebug.401256</pre>
                       E8 C6040000
  0040136C
                       833D 14374000 00
-
                       OF85 DDFEFFFF
00401379
00401378
                       0BC0
0E9405 0A324000
                                               or eax, eax
```

=> jmp or nop lệnh jne

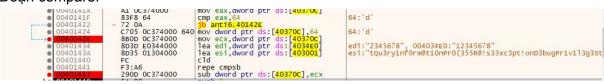
```
Ids eax,fword ptr ds:[ecx]
add byte ptr ds:[eax],al
push anti6.403714
push FFFFFFFF
● 0040135C
                        C501
   0040135E
                         0000
                         68 14374000
6A FF
00401365
                                                  call <JMP.&CheckRemoteDebuggerPres
cmp dword ptr ds:[403714],0</pre>
                         E8 C6040000
                         833D 14374000 00
● 0040136C
                         90
                                                   nop
  00401375
00401376
                         90
90
0
                                                   nop
.
                                                   nop
   00401377
                         90
                                                   nop
.
                                                  nop
or eax,eax
   00401378
                         90
   00401379
.
                         OBC O
                                                  sete byte ptr ds:[40320A]
   0040137B
                        OF9405 OA324000
```

## 7. bug (from GetTickCount)



## Tìm flag:

- Đoạn compare:



- => ecx = value[0x40370C] = len(input) edi point to [0x4034E0] = input esi point to [0x403001] = "flag"
- => output: number of compared character in input (until end of input or not equal)
- => flag:

"NtQu3ry1nf0rm@t10nPr0(355R@!s33xc3pt!onD3bugPr1v1l3g3St@ckT1m3CCS3lf-P3BF1ndW1nd0wH1d1ng@nt1-R3v3rs3"