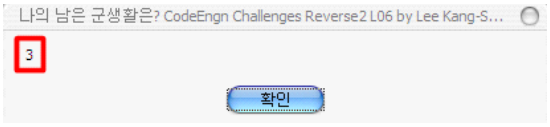
Advance RCE L06

2010년 9월 21일 화요일
오전 1:22

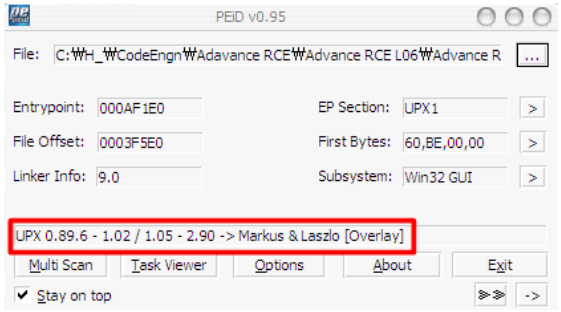
파일 확인

프로그램 실행



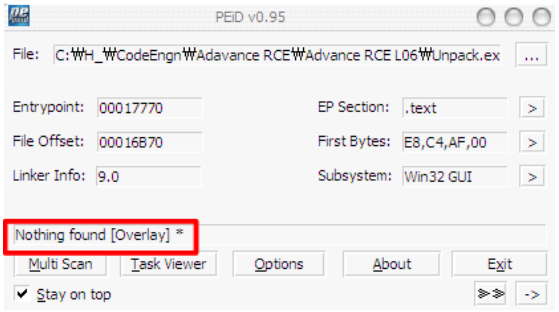
확인을 누르거나, 종료 아이콘을 누르거나 무조건 계속 해서 숫자가 Count 된다.

With PEID



UPX 로 Unpacking 이 된 파일이다.

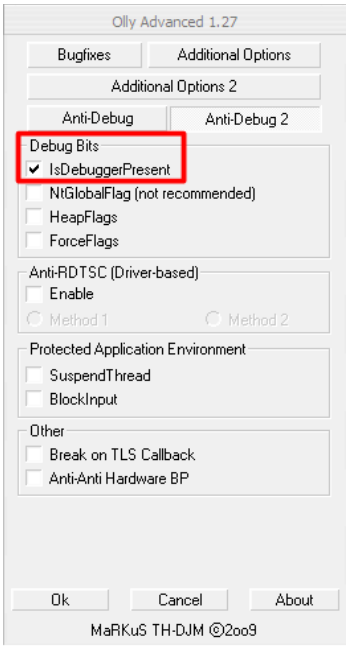
OllyDump 와 ImportREC 를 이용하여 Unpacking 을 수행한 후, 확인



With Ollydbg

프로그램을 Debugger 로 실행 시켜보면, IsDebuggerPresent 로 인해 Debugging 을 방지 하였다.

- **OllyAdvanced Plugin 을 통해 간단히 우회** 하였다.



Search For -> Name in current Module 을 통해 MessageBox 를 찾았다.

```
0045E06D   . 56            PUSH ESI                                 Style
0045E06E   . 51            PUSH ECX                                 Title
0045E06F   . 55            PUSH EBP                                 Text
0045E070   . 53            PUSH EBX                                 hOwner
0045E071   . FF15 9CD64700 CALL DWORD PTR DS:[<&USER32.MessageBoxW  MessageBoxW
0045E077   > 8B7424 4C     MOV ESI,DWORD PTR SS:[ESP+4C]
DS:[0047D69C]=77D46534 (USER32.MessageBoxW)

Address   Value      Comment
008AF8D8  00000000   hOwner = NULL
008AF8DC  015AF908   Text = "1"
008AF8E0  015AF540   Title = "나의 남은 군생활은? CodeEngn Challenges Reverse2 L06 by Lee Kang-Seok"
008AF8E4  00010000   Style = MB_OKIMB_APPLMODAL|10000
```

Stack 창을 보면, 우리가 본 **MessageBox 의 내용**이 들어있다.

이 프로그램의 경우 계속 해서 실행 되는데 계속 누를순 없기 때문에, MessageBoxW 안으로 들어가서 약간의 Patch를 하였다.

```
77D3083D   6A 01           PUSH 1
77D3083F   FF75 18         PUSH DWORD PTR SS:[EBP+18]
77D30842   FF75 14         PUSH DWORD PTR SS:[EBP+14]
77D30845   FF75 10         PUSH DWORD PTR SS:[EBP+10]
77D30848   FF75 0C         PUSH DWORD PTR SS:[EBP+C]
77D3084B   FF75 08         PUSH DWORD PTR SS:[EBP+8]
77D3084E   E8 305B0100     CALL USER32.MessageBoxTimeoutW
```

MessageBoxTimeoutW 함수가 보이고, 마지막 인자인 dwMilliseconds 가 -1 로 설정되어 있던 것을 수정하였다.

- 이로 인해 **확인을 누르지 않아도 알아서 수행**이 된다.

프로그램이 종료되는 곳 확인

```
0043219E   . 6A 00         PUSH 0                                   hWnd = NULL
004321A0   . FF15 ECD64700 CALL DWORD PTR DS:[<&USER32.LockWindowU  LockWindowUpdate
004321A6   . 8B0D 08E94800 MOV ECX,DWORD PTR DS:[48E908]
004321AC   . 51            PUSH ECX                                 hWnd => 00260430 ('AutoIt v3',class='AutoIt v3')
004321AD   . FF15 DCD54700 CALL DWORD PTR DS:[<&USER32.DestroyWind  DestroyWindow
004321B3   . 8B35 E8D64700 MOV ESI,DWORD PTR DS:[<&USER32.GetMessa  USER32.GetMessageW
004321B9   . 6A 00         PUSH 0                                   MsgFilterMax = 0
004321BB   . 6A 00         PUSH 0                                   MsgFilterMin = 0
004321BD   . 6A 00         PUSH 0                                   hWnd = NULL
004321BF   . 8D9424 880100 LEA EDX,DWORD PTR SS:[ESP+188]
004321C6   . 52            PUSH EDX                                 pMsg
004321C7   . FFD6          CALL ESI                                 GetMessageW
```

그리고, Debugging 을 하다보면, 증가하는 값과 비교하는 값을 찾아볼 수 있다.

```
00408F11  > 8B06          MOV EAX,DWORD PTR DS:[ESI]      Cases 1,2,7 of switch 00408F08
00408F13  > 3BE8          CMP EBP,EAX
00408F15  .v7C 7E         JL SHORT Unpack.00408F95
00408F17  > 8B47 04       MOV EAX,DWORD PTR DS:[EDI+4]    Default case of switch 00408EF4
00408F1A  . 8B4C24 44     MOV ECX,DWORD PTR SS:[ESP+44]
00408F1E  . 40            INC EAX
00408F1F  . 8901          MOV DWORD PTR DS:[ECX],EAX
00408F21  > 8B4424 34     MOV EAX,DWORD PTR SS:[ESP+34]
00408F25  . 85C0          TEST EAX,EAX
00408F27  .v0F85 46690200 JNZ Unpack.0042F873
00408F2D  > 83FB 08       CMP EBX,8
00408F30  .v0F84 54690200 JE Unpack.0042F88A
00408F36  . 83FB 0A       CMP EBX,0A
00408F39  .v0F84 70690200 JE Unpack.0042F8AF
00408F3F  . 83FB 05       CMP EBX,5
00408F42  .v0F84 7E690200 JE Unpack.0042F8C6
00408F48  . 83FB 0B       CMP EBX,0B
00408F4B  .v0F84 83690200 JE Unpack.0042F8D4
00408F51  . 83FB 0C       CMP EBX,0C
EAX=00000002
EBP=00000316
```

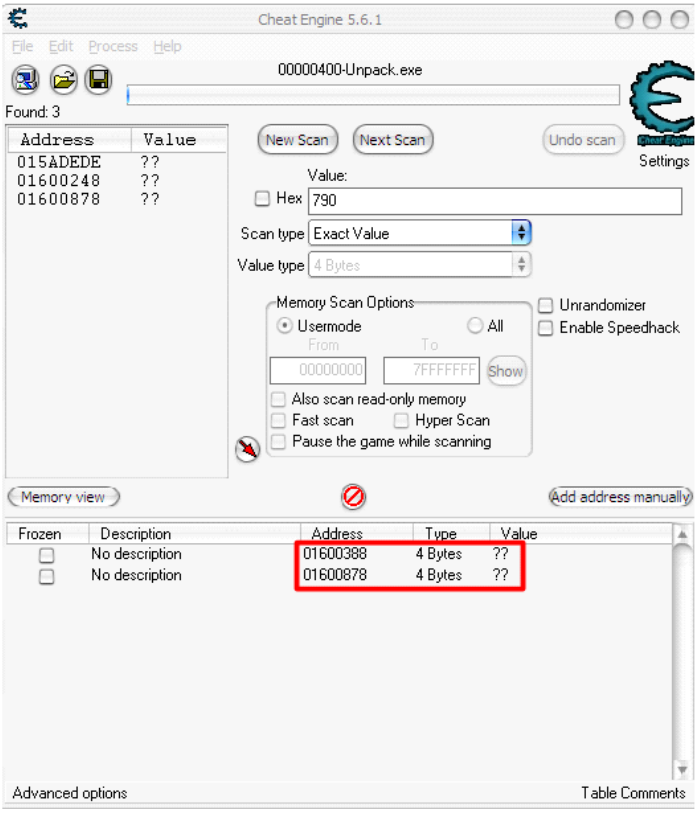
EBP 에 있는 값이 최종 군생활 날짜이고, EAX 값은 현재 카운트 되고 있는 날짜 이다.

- **0x316 = 790 이므로 최종 군생활 날짜는 790일**이다.

문제 해결

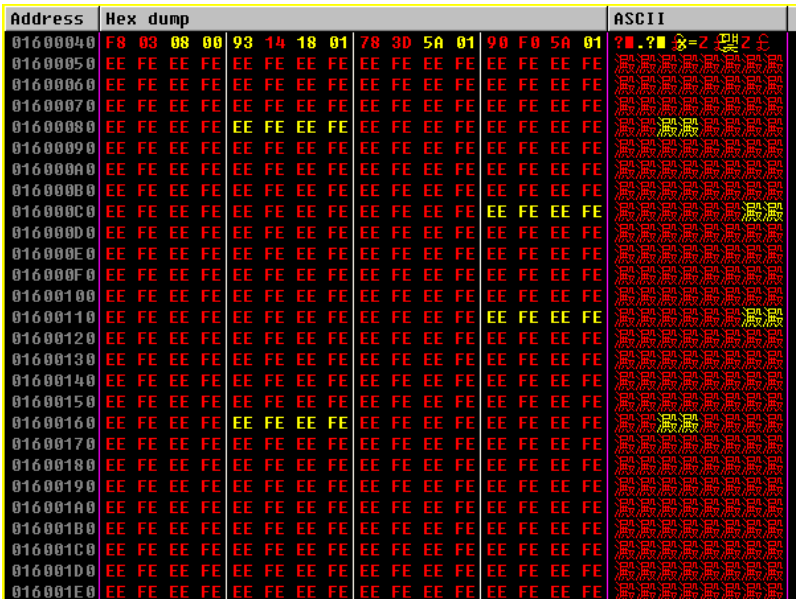
요즘 아는 동생 덕에 새로 알게된 **Cheat Engine 이라는 툴을 써서 790일이 맞는지 확인**해 보았다.

- 우선 1을 넣고 Scan, 2를 넣고 Scan 이런식으로 **증가하는 값이 있는 Address 를 찾아서 790으로 설정**
- 그리고, **790으로 설정되어 있는 Address 를 찾아서 고정 후 확인**



- 확인 결과 **Value 값이 해제 되었고, 프로그램도 종료** 되었다.

실제 프로그램 종료 후에 Count 와 관련된 **Dump 창이 모두 초기화 되는것을 확인** 하였다.



보충 설명

MessageBoxTimeoutW(HWND hWnd, LPCWSTR lpText, LPCWSTR lpCaption,
UNIT uType, WORD wLanguageId, DWORD dwMilliseconds)

답

790(MD5 Hash) = 2DACE78F80BC92E6D7493423D729448E