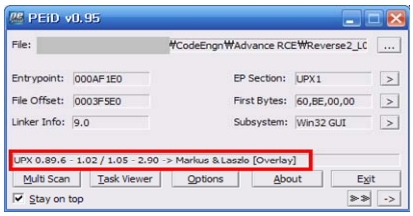
Reverse2 L01 Report by vivaman

1. Level1

- 이 프로그램은 몇 밀리세컨드 후에 종료 되는가
- 정답인증은 MD5 해쉬값(대문자) 변환 후 인증하시오



- UPX로 압축되어 있습니다.
- AutoIt v3는 기본적으로 UPX 압축을 씁니다.
- 압축을 풀 경우 해킹관련 프로그램으로 오해 받을 수 있다고 합니다.
- 사실 압축 풀고 디버깅을 해봤는데, 여러 번 삭제 당했습니다.
- OllyDbg에서 UPX는 이런 식으로 화면 조금 내려 오면...이런게 보입니다.(썰렁한 점프문)
- 브포 잡고, 실행(F9)한 후 F7 로 "Step into" 하면..OEP에 도착합니다.

```
004AF38D   .  39C4          CMP ESP,EAX
004AF38F   .^ 75 FA         JNZ SHORT Reverse2.004AF38B
004AF391   .  83EC 80       SUB ESP,-80
004AF394   .- E9 D783F6FF   JMP Reverse2.00417770
004AF399      00            DB 00
004AF39A      00            DB 00
004AF39B      00            DB 00
```

```
0041776A   E8 16190000      CALL Reverse2.00419085
0041776F   C3               RETN
00417770   E8 C4AF0000      CALL Reverse2.00422739                  This is the OEP!
00417775 ^ E9 79FEFFFF      JMP Reverse2.004175F3
0041777A   8BFF             MOV EDI,EDI
0041777C   55               PUSH EBP
0041777D   8BEC             MOV EBP,ESP
```

- 미리 저장된 시간을 불러 와서 milliseconds단위로 바꾸기 시작합니다.

```
0040DD4B   83F8 03          CMP EAX,3
0040DD4E   75 07            JNZ SHORT Reverse2.0040DD57
0040DD50   DD01             FLD QWORD PTR DS:[ECX]
0040DD52   5E               POP ESI
0040DD53   8BE5             MOV ESP,EBP
0040DD55   5D               POP EBP
0040DD56   C3               RETN
0040DD57   48               DEC EAX
DS:[01064E10]=13.17900000000000
```

```
0045E00D   E8 8C8AFDFF      CALL Reverse2.00436A9E
0045E012   84C0             TEST AL,AL
0045E014   75 53            JNZ SHORT Reverse2.0045E069
0045E016   E8 25FDFAFF      CALL Reverse2.0040DD40              시간계산 시작하는곳(시간 불러오고)
0045E01B   DD05 60724800    FLD QWORD PTR DS:[487260]
0045E021   D8D9             FCOMP ST(1)                         값:ST(1)=13.179000000000000000
0045E023   DFE0             FSTSW AX
0045E025   F6C4 41          TEST AH,41
0045E028   75 04            JNZ SHORT Reverse2.0045E02E
0045E02A   DDD8             FSTP ST
0045E02C   D9EE             FLDZ
0045E02E   DC0D 30724800    FMUL QWORD PTR DS:[487230]          값:13.179 * 1000=>milliseconds로 바꿈
0045E034   D97C24 48         FSTCW WORD PTR SS:[ESP+48]
0045E038   0FB74424 48       MOVZX EAX,WORD PTR SS:[ESP+48]
0045E03D   0D 000C0000       OR EAX,0C00
0045E042   894424 18         MOV DWORD PTR SS:[ESP+18],EAX
0045E046   8B4424 30         MOV EAX,DWORD PTR SS:[ESP+30]
0045E04A   D96C24 18         FLDCW WORD PTR SS:[ESP+18]
0045E04E   DF7C24 18         FISTP QWORD PTR SS:[ESP+18]         값:ST=13179.000000000000000
0045E052   8B5424 18         MOV EDX,DWORD PTR SS:[ESP+18]
0045E056   52                PUSH EDX
```

```
00444C3C   56               PUSH ESI
00444C3D   57               PUSH EDI
00444C3E   8B3D 58D74700    MOV EDI,DWORD PTR DS:[47D758]       WINMM.timeGetTime
00444C44   FFD7             CALL EDI                            timeGetTime 부름..
00444C46   803D D3E84800 0  CMP BYTE PTR DS:[48E8D3],0
00444C4D   8BF0             MOV ESI,EAX                         EAX:처음GetTime -> ESI
00444C4F   0F84 FF000000    JE Reverse2.00444D54
00444C55   8B5C24 14        MOV EBX,DWORD PTR SS:[ESP+14]
00444C59   8B2D 58D14700    MOV EBP,DWORD PTR DS:[47D158]       kernel32.Sleep
00444C5F   FFD7             CALL EDI
00444C61   3BC6             CMP EAX,ESI                         ESI:처음GetTime , EAX:지금GetTime
00444C63   0F83 CF000000    JNB Reverse2.00444D38               EAX가 크겠지,..점프~하겠지
00444C69   2BC6             SUB EAX,ESI
00444C6B   48               DEC EAX
00444C6C   E9 C9000000      JMP Reverse2.00444D3A
00444C71   8B03             MOV EAX,DWORD PTR DS:[EBX]          00444C71 에서 종료할려고 오는점프
00444C73   6A 00            PUSH 0
00444C75   68 FC864300      PUSH Reverse2.004386FC              ASCII "곱"
00444C7A   50               PUSH EAX
00444C7B   C705 28E94900 0  MOV DWORD PTR DS:[49E928],0
Jump is taken
00444D38=Reverse2.00444D38
```

-timeGetTime-

- 시스템이 부팅된 이후로 경과 시간을 milliseconds단위로 반환.

http://msdn.microsoft.com/en-us/library/aa912626.aspx

timeGetTime

Windows Mobile | Windows Embedded CE

8/28/2008

This function retrieves the system time, in milliseconds. The system time is the time elapsed since the system started.

Syntax

```
DWORD  timeGetTime(void);
```

Parameters

None.

Return Value

Returns the system time, in milliseconds.

Remarks

The only difference between this function and the timeGetSystemTime function is that **timeGetSystemTime** uses the MMTIME structure to return the system time. The **timeGetTime** function has less overhead than **timeGetSystemTime**.

The value returned by the **timeGetTime** function is a **DWORD** value.

The return value resets to zero every 2^32 milliseconds, which is about 49.71 days. This can cause problems in code that directly uses the **timeGetTime** return value in computations, particularly when the value is used to control code execution. Depending on how you are using the hardware timer, you may need to handle the timer reset condition.

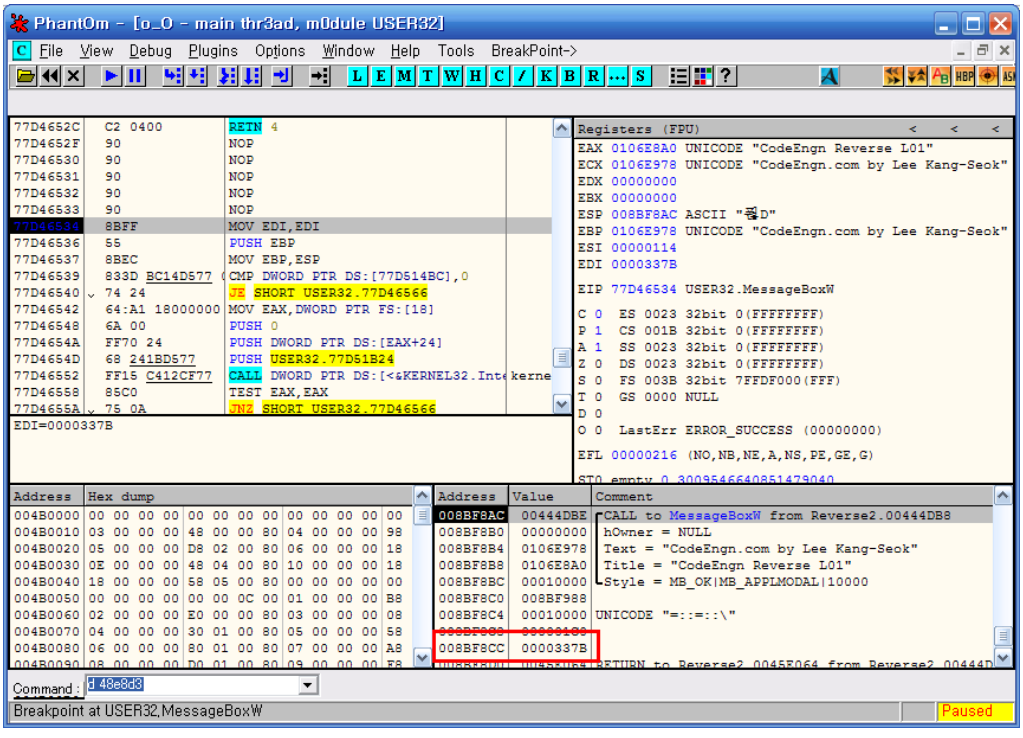
Always use the difference between two **timeGetTime** return values in computations.

Requirements

Header	mmsystem.h
Library	Mmtimer.lib
Windows Embedded CE	Windows CE .NET 4.2 and later

```
00444D32   33C0            XOR EAX,EAX
00444D34   5B              POP EBX
00444D35   C2 0400         RETN 4
00444D38   2BC6            SUB EAX,ESI                  나중시간(EAX)-처음시간(ESI)=시간차이(EAX)
00444D3A   3B43 04         CMP EAX,DWORD PTR DS:[EBX+4] 지정된시간:Stack DS:[008BF8CC]=0000337B
00444D3D ^ 0F83 2EFFFFFF   JNB Reverse2.00444C71        시간차이(EAX)가 337B 보다 작으면 노점프
00444D43   6A 0A           PUSH 0A                      좋은건노점프/종료는점프
00444D45   FFD5            CALL EBP
00444D47   803D D3E84800 ( CMP BYTE PTR DS:[48E8D3],0
00444D4E ^ 0F85 0BFFFFFF   JNZ Reverse2.00444C5F        시간차이가 작아서 다시 시간계산하러 고고싱~
00444D54   5F              POP EDI
00444D55   5E              POP ESI
00444D56   5D              POP EBP
Jump is NOT taken
00444C71=Reverse2.00444C71
```

- MessageBoxW에 브포 걸린 화면.



- 13179 = 337Bh
- MD5 = DB59260CCE0B871C7B2BB780EEE305DB -끝-