

19.02.24 CodeEngn Advance 1

Tree to Tree

Advance RCE L01

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

— Author: CodeEngn

— File Password: codeengn



몇 밀리세컨드인지 해쉬값으로 바꾼뒤 인증하는 문제

CodeEngn Reverse2 L01

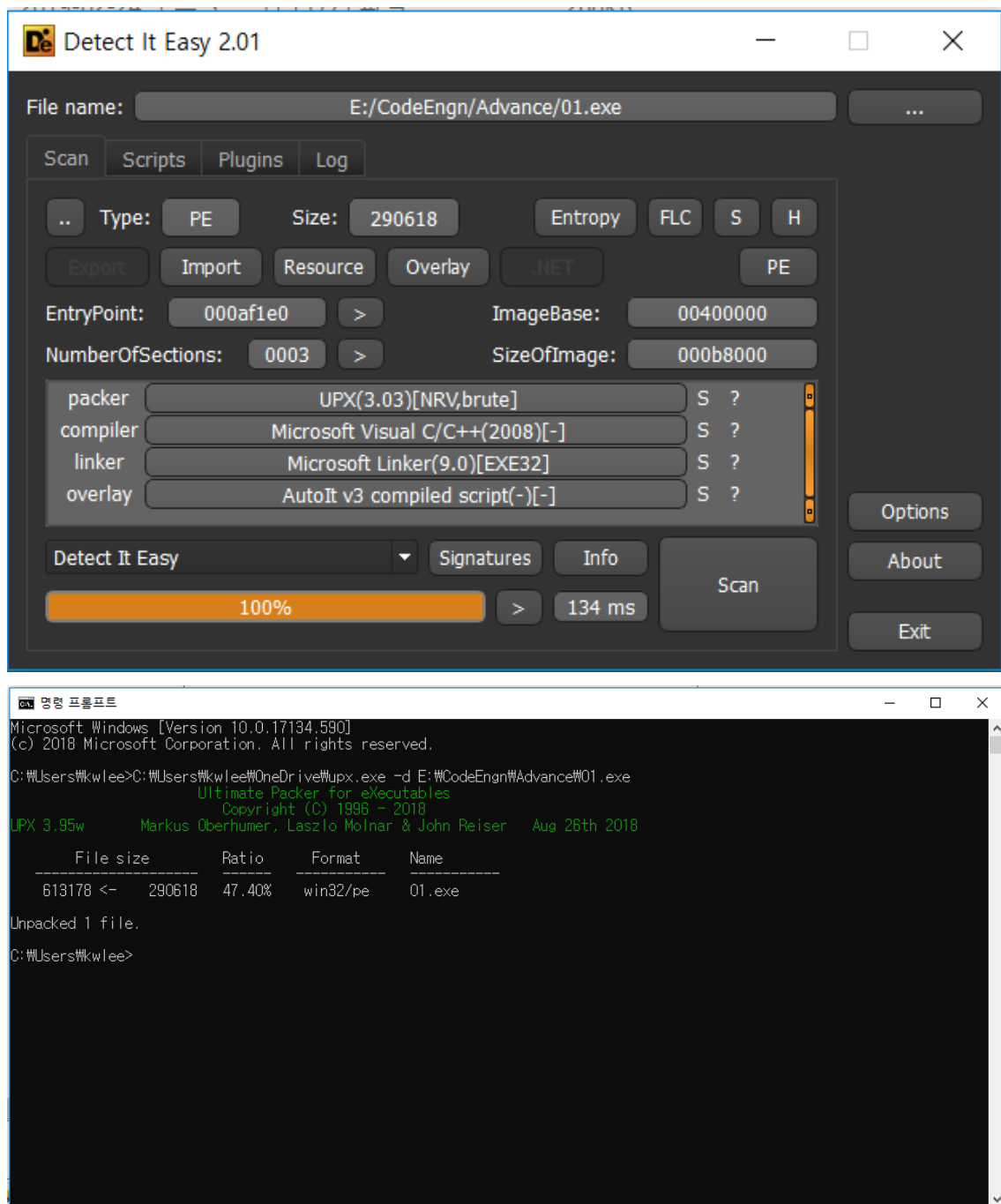
×

CodeEngn.com by Lee Kang-Seok

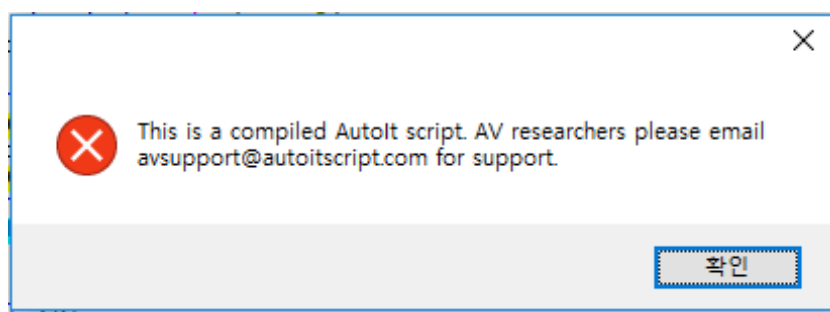
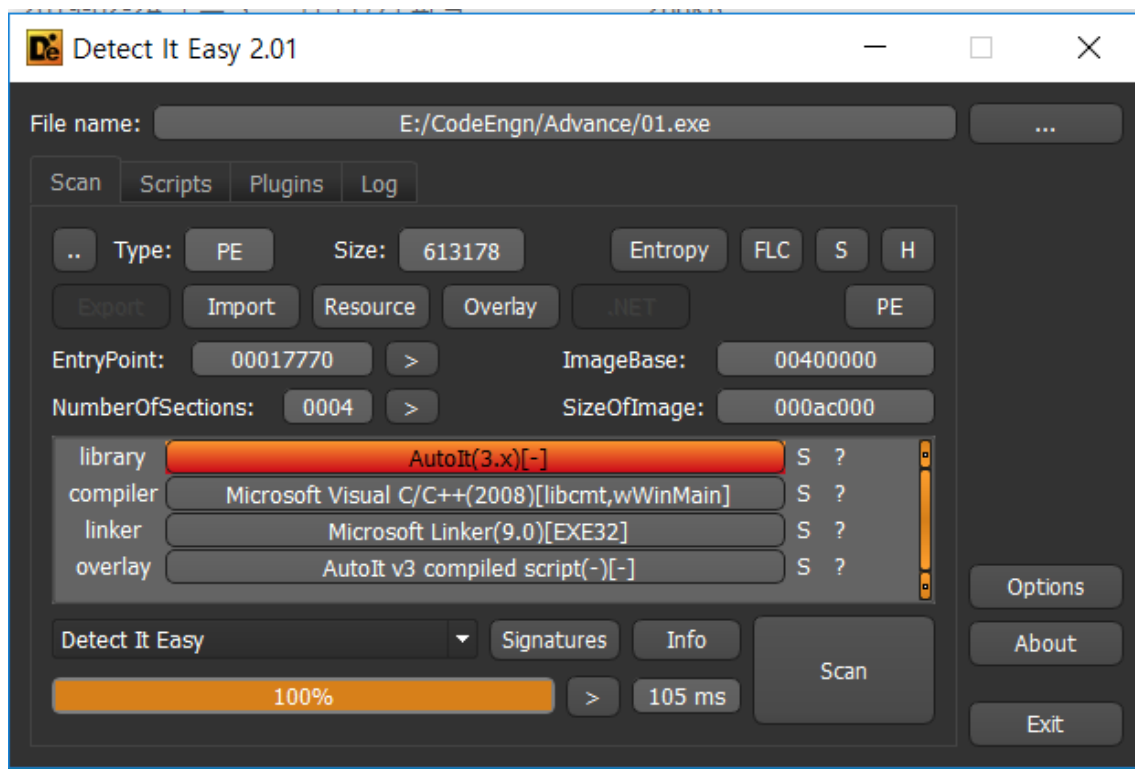
확인

Basic에서 봤던 실행모습 똑같아보임. basic 19

패킹과 Auto It 프로그램써서 만든것도 똑같음



Basic19와 동일하게 먼저 UPX unpack 시켜준다.



이것도 똑같이 안티디버깅 되어있음

basic19와 똑같다면 PEB 방식으로 되었을 것 IsDebuggerPresent 검색해봄

기존	보통	주소	유형	Ordinal	Symbol
00400000	01.exe	0047D1E8	가져오기		Output Debug Stringw
6D640000	comctl32.dll	0047D320	가져오기		<u>IsDebuggerPresent</u>
71680000	wsock32.dll				
71DE0000	winmmbase.dll				
721C0000	winmm.dll				

아예 똑 같다 밀리세컨드 재는것도 똑같은 방식일 듯

0040E940	81 EC 38 04 00 00	sub esp, 438
0040E946	53	push ebx
0040E947	56	push esi
0040E948	57	push edi
0040E949	8B F8	mov edi, eax
0040E94B	8D 44 24 20	lea eax, dword ptr ss:[esp+20]
0040E94F	50	push eax
0040E950	68 04 01 00 00	push 104
0040E955	FF 15 24 D3 47 00	call dword ptr ds:[<&GetCurrentDirectoryw>]
0040E958	57	push edi
0040E95C	E8 1F DF FF FF	call 01.40C880
0040E961	FF 15 20 D3 47 00	call dword ptr ds:[<&IsDebuggerPresent>]
0040E967	85 C0	test eax, eax
0040E969	0F 85 6F 4F 02 00	jne 01.4338DE
0040E96F	8B 44 24 0F	mov byte ptr ss:[esp+F], al
0040E973	BE 30 04 4A 00	mov esi, 01.4A0430
0040E978	39 05 3C F4 49 00	cmp dword ptr ds:[49F43C], eax
0040E97E	0F 84 73 4F 02 00	je 01.4338F7
0040E984	68 3C F4 49 00	push 01.49F43C
0040E989	8D 4C 24 13	lea ecx, dword ptr ss:[esp+13]
0040E98D	B8 54 F4 49 00	mov eax, 01.49F454
0040E992	E8 39 15 00 00	call 01.40FED0
0040E997	84 C0	test al, al
0040E999	0F 84 78 4F 02 00	je 01.43391A
0040E99F	8A 0D 30 04 4A 00	mov cl, byte ptr ds:[4A0430]
0040E9A5	8A 1D 31 04 4A 00	mov bl, byte ptr ds:[4A0431]
0040E9AB	68 38 F4 49 00	push 01.49F438
0040E9B0	8D 94 24 34 02 00 00	lea edx, dword ptr ss:[esp+234]
0040E9B7	52	push edx
0040E9B8	68 04 01 00 00	push 104
0040E9BD	68 54 F4 49 00	push 01.49F454
0040E9C2	88 0D 40 F4 49 00	mov byte ptr ds:[49F440], cl
0040E9C8	FF 15 F4 D2 47 00	call dword ptr ds:[<&GetFullPathNameW>]
0040E9CE	A1 3C F4 49 00	mov eax, dword ptr ds:[49F43C]
0040E9D2	50	push eax

우선 매번 값바꿔주기 귀찮으니까 IsDebuggerPresent리턴값 비교문을 바꿈
test eax, eax -> xor eax, eax

0040E95C	E8 1F DF FF FF	call 01.40C880
0040E961	FF 15 20 D3 47 00	call dword ptr ds:[<&IsDebuggerPresent>]
0040E967	85 C0	test eax, eax
0040E969	0F 85 6F 4F 02 00	jne 01.4338DE
0040E96F	8B 44 24 0F	mov byte ptr ss:[esp+F], al

0040E967 어셈블

xor eax, eax

☐ 크기 유지(S)
 ☐ 잔존 바이트를 NOP로 채우기(F)
 ☐ XEDParse
 ☒ asmjit

명령어가 성공적으로 인코딩되었습니다!



정상적으로 실행됨

J: 26E0 - 모듈: 01patch.exe - Thread: 수 스레드 208 - x32dbg

디버그(D) Trace 플러그인(P) 플러그인(I) 설정(O) 도움말(H) Jan 20 2019

Assembly code snippet:

```

00417770  E8 C4AF0000  call 01patch.422739
00417771  E9 79FEFFFF  jmp 01patch.4175F3
00417772  8B FF        mov edi,edi
00417773  55          push ebp
00417774  8B EC        mov ebp,esp
00417775  8B C1        mov ecx,eax
00417776  8B 4D 08     mov ecx,dword ptr ss:[ebp+8]
00417777  C7 00 88DA4700 mov dword ptr ds:[eax],01patch.47DA88
00417778  8B 09        mov ecx,dword ptr ds:[ecx]
00417779  83 60 08 00  and dword ptr ds:[eax+8],0
0041777A  89 48 04     mov dword ptr ds:[eax+8],ecx
0041777B  5D          pop ebp
0041777C  C2 0800     ret 8
0041777D  8B FF        mov edi,edi
0041777E  55          push ebp
0041777F  8B EC        mov ebp,esp
00417780  53          push ebx
00417781  8B 5D 08     mov ebx,dword ptr ss:[ebp+8]
00417782  56          push esi
00417783  8B F1        mov esi,ecx
00417784  C7 06 88DA4700 mov dword ptr ds:[esi],01patch.47DA88
00417785  8B 43 08     mov eax,dword ptr ds:[ebx+8]
00417786  89 46 08     mov dword ptr ds:[esi+8],eax
00417787  85 C0        test eax,eax
00417788  8B 43 04     mov eax,dword ptr ds:[ebx+4]
00417789  57          push edi
0041778A  74 31        jle 01patch.4177E8
  
```

메시지 창 띄워주는 곳까지 트레이싱하면 프로세스가 갑자기 1개 증가하는 함수가 있다

여기선 그게 MessageBoxA

mov edi, edi하는순간 바로 프로세스 증가함

edi가 밀리세컨드로 예상

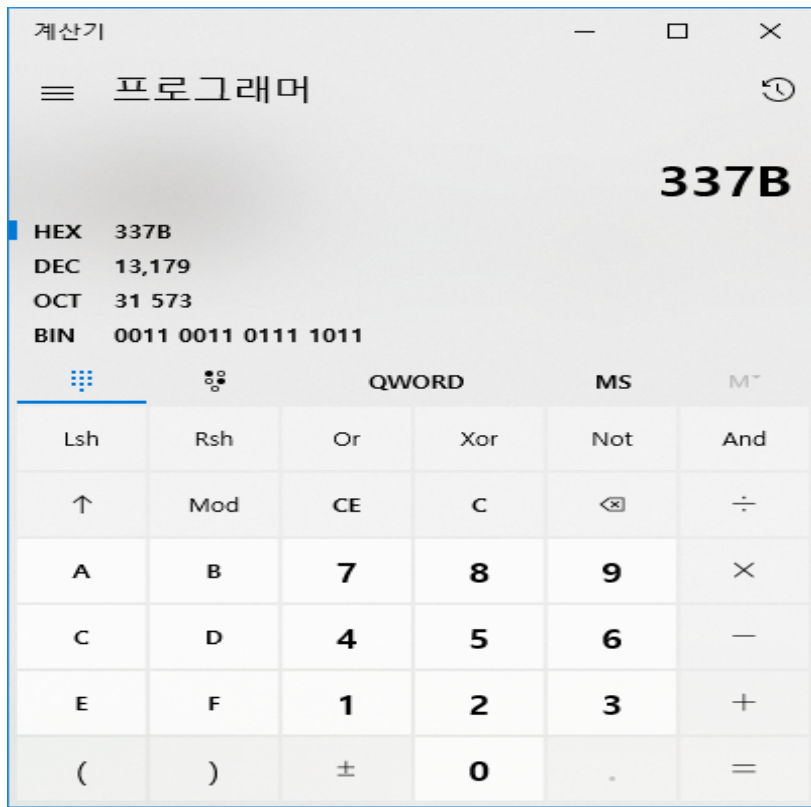
Assembly code snippet:

```

76408290  8B FF        mov edi,edi
76408291  55          push ebp
76408292  8B EC        mov ebp,esp
76408293  6A FF        push 0
76408294  6A 00        push 0
76408295  FF 75 14     push dword ptr ss:[ebp+14]
76408296  FF 75 10     push dword ptr ss:[ebp+10]
76408297  FF 75 0C     push dword ptr ss:[ebp+8]
76408298  FF 75 08     push dword ptr ss:[ebp+4]
76408299  E8 56FEFFFF  call user32.MessageBoxTimeoutW
7640829A  5D          pop ebp
7640829B  C2 1000     ret 10
7640829C  CC          int3
7640829D  CC          int3
7640829E  CC          int3
7640829F  CC          int3
764082A0  CC          int3
764082A1  CC          int3
764082A2  CC          int3
764082A3  CC          int3
764082A4  CC          int3
764082A5  CC          int3
764082A6  CC          int3
764082A7  CC          int3
764082A8  CC          int3
764082A9  CC          int3
764082AA  CC          int3
764082AB  CC          int3
764082AC  CC          int3
764082AD  CC          int3
764082AE  CC          int3
764082AF  CC          int3
764082B0  CC          int3
764082B1  CC          int3
764082B2  CC          int3
764082B3  CC          int3
764082B4  CC          int3
764082B5  CC          int3
764082B6  CC          int3
764082B7  CC          int3
764082B8  CC          int3
764082B9  CC          int3
764082BA  CC          int3
764082BB  CC          int3
764082BC  CC          int3
764082BD  CC          int3
764082BE  CC          int3
764082BF  CC          int3
764082C0  8B FF        mov edi,edi
764082C1  55          push ebp
764082C2  8B EC        mov ebp,esp
764082C3  CC          int3
  
```

스레드 (Thread) window:

ID	진입점	TE8	EIP	일시중지 횟수	우선 순위	대기시간
10C	00416243	00286000	770ACE30	0	보통	Susp
40C8	77091440	00283000	770AC58C	0	보통	Susp
5188	77091440	002AD000	770AC58C	0	보통	Susp
D00	77091440	002A4000	770AC58C	0	보통	Susp
4580	00417770	002A4000	76408292	0	보통	Exec
5288	77091440	002A7000	770AC58C	0	보통	Susp
2104	77091440	00286000	770AC58C	0	보통	Susp



10진수 변환시 13179

md5 Hash Generator

This simple tool computes the MD5 hash of a string. Also available: [SHA-1 hash generator](#) and

String:

13179

md5

☐ Treat multiple lines as separate strings

MD5 Hash:

db59260cce0b871c7b2bb780eee305db

13179 MD5 하면 db59260cce0b871c7b2bb780eee305db

Clear