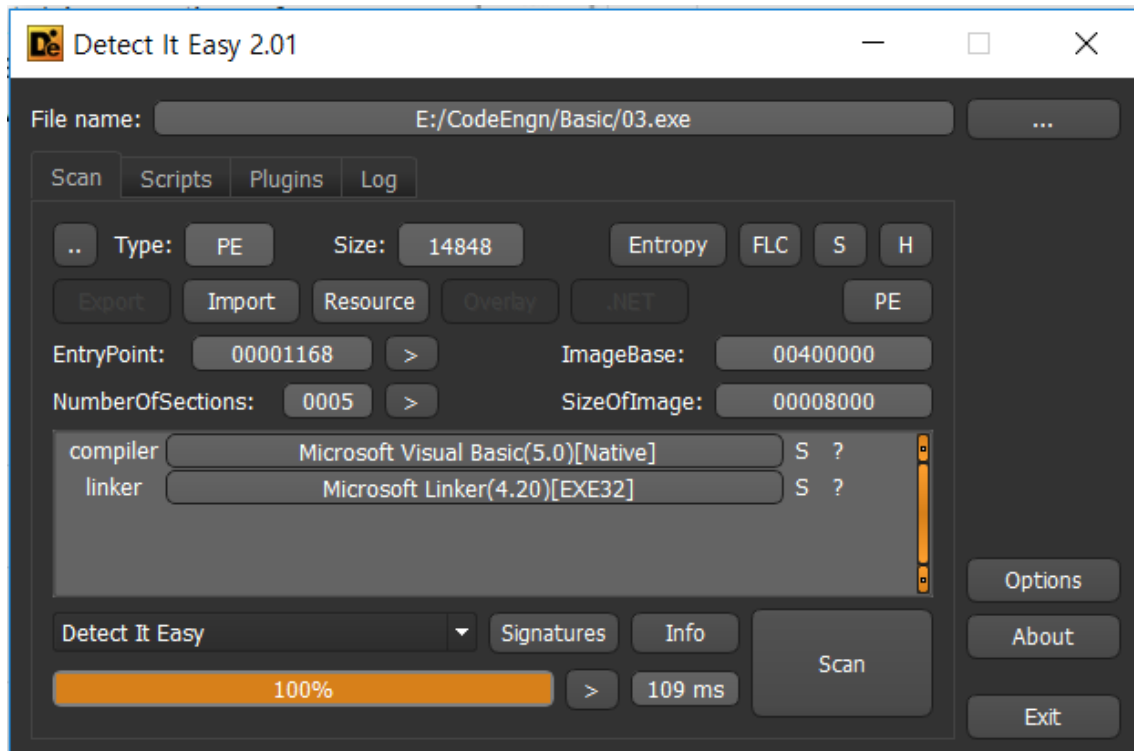


### 19.2.10 CodeEngn CrackMe3

Tree to Tree

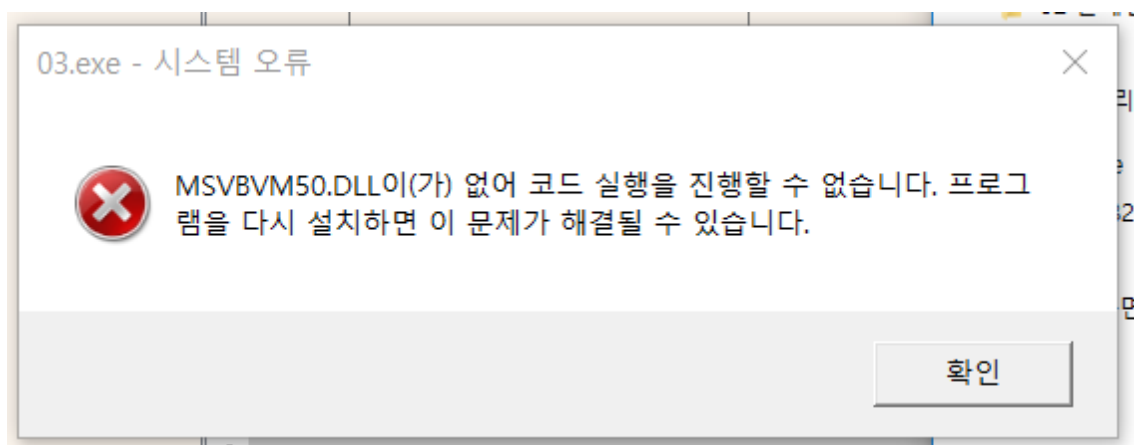
먼저 실행(PE)파일분석

Detect It Easy 툴사용



실행해보니 MSVBVM50.DLL이 없다.

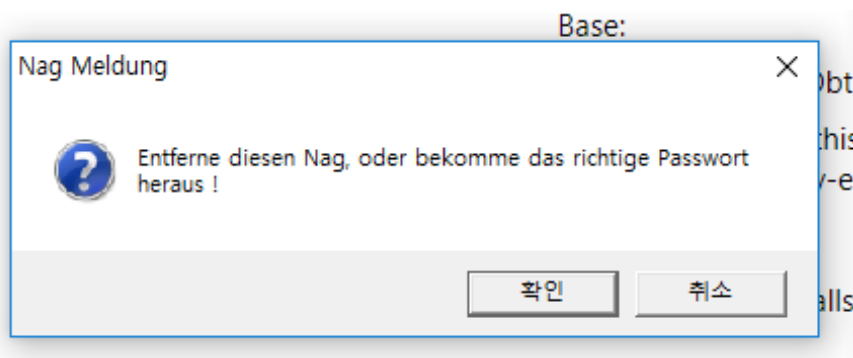
VisualBasic을 실행하기위한 ,dll파일필요



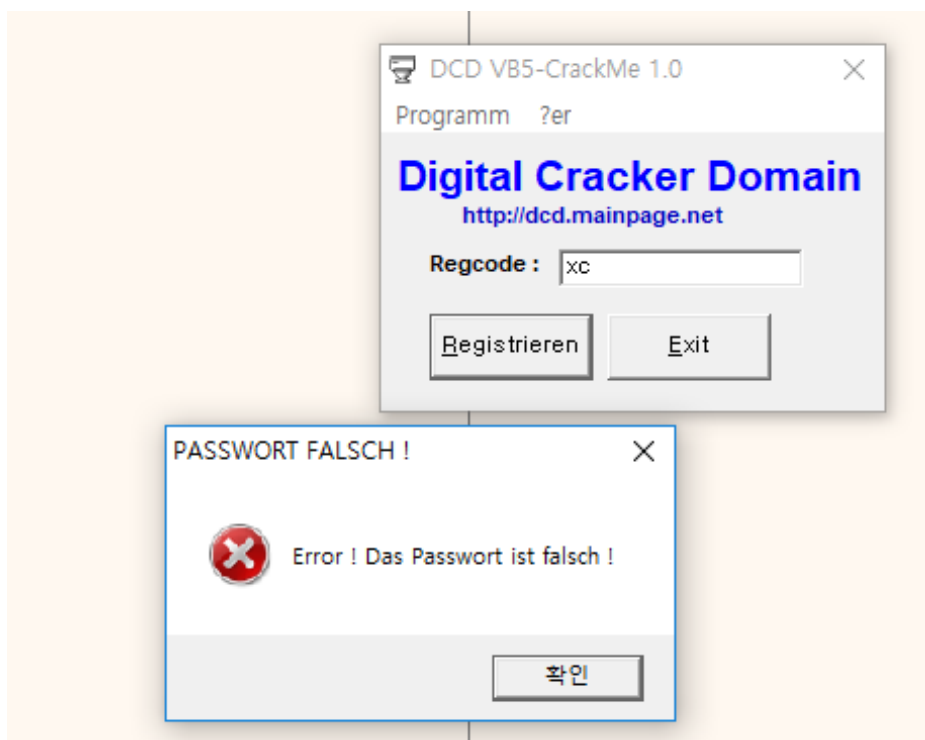
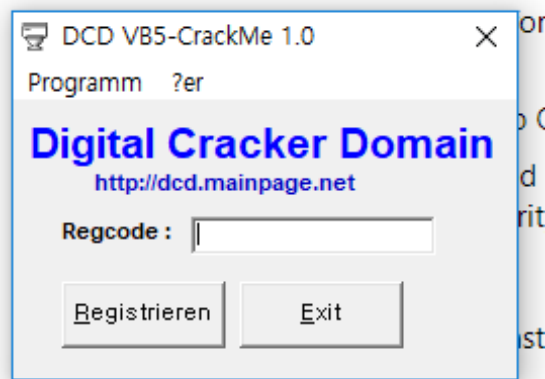
<https://support.microsoft.com/en-us/help/180071/file-msvbvm50-exe-installs-visual-basic-5-0-run-time-files>

이경로에서 받았다.

실행하면 나오는 notice



확인 누르면 나오는 화면



아무글자나 친 후에 확인

CODE가 있는 섹션으로 가서

함수명들을 보니 문자열을 비교하는 함수 발견

\_\_vbaStrCmp

0040113E	FF 25 FC504000	jmp dword ptr ds:[<&__vbaHresultCheckObj>]	JMP.<&__vbaHresultCheckObj
00401144	FF 25 08514000	jmp dword ptr ds:[<&__vbaObjSet>]	JMP.<&__vbaObjSet
0040114A	FF 25 34514000	jmp dword ptr ds:[<&__vbaStrCmp>]	JMP.<&__vbaStrCmp
00401150	FF 25 3C514000	jmp dword ptr ds:[<&EVENT_SINK_QueryInterface>]	JMP.<&EVENT_SINK_QueryInterface
00401156	FF 25 20514000	jmp dword ptr ds:[<&EVENT_SINK_AddRef>]	JMP.<&EVENT_SINK_AddRef
0040115C	FF 25 34514000	jmp dword ptr ds:[<&EVENT_SINK_Release>]	JMP.<&EVENT_SINK_Release

\_\_vbaStrCmp함수를 파고들어보니 내가 입력한 패스워드 xc가 보인다.

740C3563	55	push ebp	__vbaStrCmp
740C3564	8B EC	mov ebp, esp	
740C3566	53	push ebx	
740C3567	56	push esi	
740C3568	57	push edi	
740C3569	83 7D 10 00	cmp dword ptr ss:[ebp+10], 0	[ebp+10]:L"xc"
740C356D	BE 00000000	mov esi, 0	
740C3572	74 06	jbe msvbvm50.740C357A	
740C3574	8B 45 10	mov eax, dword ptr ss:[ebp+10]	[ebp+10]:L"xc"
740C3577	8B 70 FC	mov esi, dword ptr ds:[eax-4]	
740C357A	83 7D 0C 00	cmp dword ptr ss:[ebp+C], 0	[ebp+C]:L"2G83G35Hs2"
740C357E	BF 00000000	mov edi, 0	
740C3583	74 06	jbe msvbvm50.740C358B	
740C3585	8B 40 0C	mov ecx, dword ptr ss:[ebp+C]	[ebp+C]:L"2G83G35Hs2"
740C3588	8B 79 FC	mov edi, dword ptr ds:[ecx-4]	
740C358B	3B FE	cmp edi, esi	
740C358D	8B DF	mov ebx, edi	
740C358F	73 25	jbe msvbvm50.740C35B6	
740C3591	83 7D 08 00	cmp dword ptr ss:[ebp+8], 0	
740C3595	75 36	jne msvbvm50.740C35CD	
740C3597	85 DB	test ebx, ebx	
740C3599	74 28	jbe msvbvm50.740C35C3	
740C359B	8B C3	mov eax, ebx	
740C359D	D1 E8	shr eax, 1	
740C359F	50	push eax	
740C35A0	FF 75 0C	push dword ptr ss:[ebp+C]	[ebp+C]:L"2G83G35Hs2"
740C35A3	FF 75 10	push dword ptr ss:[ebp+10]	[ebp+10]:L"xc"
740C35A6	E8 3FA40000	call msvbvm50.740CD9EA	
740C35AB	85 C0	test eax, eax	
740C35AD	74 0B	jbe msvbvm50.740C35BA	
740C35AF	5F	pop edi	
740C35B0	5E	pop esi	
740C35B1	5B	pop ebx	
740C35B2	5D	pop ebp	
740C35B3	C2 0C 00	ret 4	

또 xc와 비교하는 문자열 2G83G35Hs2을 발견

740DF8FA	FF 74 24 08	push dword ptr ds:[esp+8]	[esp+8]:L"xc"
740DF8FE	6A 00	push 0	[esp+0]:L"xc"
740DF900	E8 5E3CFE FF	call msvbvm50.740DF908	
740DF905	0F 8F C0	movsx eax, ax	
740DF908	C2 08 00	ret 8	
740DF90B	51	push ecx	__vbaChkstk
740DF90C	57	push edi	
740DF90D	50	push eax	
740DF90E	3D 00100000	cmp eax, 1000	
740DF913	8D 4C 24 10	lea ecx, dword ptr ss:[esp+10]	[esp+10]:L"HI["
740DF917	0F 83 89E10400	jbe msvbvm50.7412DA86	
740DF91D	2B C8	sub ecx, eax	
740DF91F	8B C4	mov eax, esp	
740DF921	85 01	test dword ptr ds:[ecx], eax	
740DF923	8D 61 F0	lea esp, dword ptr ds:[ecx-10]	
740DF926	8B 08	mov ecx, dword ptr ds:[eax]	
740DF928	89 0C 24	mov dword ptr ss:[esp], ecx	
740DF92B	8B 48 04	mov ecx, dword ptr ds:[eax+4]	
740DF92E	89 4C 24 04	mov dword ptr ss:[esp+4], ecx	[esp+4]:L"2G83G35Hs2"
740DF932	8B 48 08	mov ecx, dword ptr ds:[eax+8]	
740DF935	89 4C 24 08	mov dword ptr ss:[esp+8], ecx	[esp+8]:L"xc"
740DF939	8B 48 0C	mov ecx, dword ptr ds:[eax+C]	
740DF93C	89 4C 24 0C	mov dword ptr ss:[esp+C], ecx	
740DF940	59	pop ecx	
740DF941	8D 7C 24 0C	lea edi, dword ptr ss:[esp+C]	
740DF945	C1 E9 02	shr ecx, 2	
740DF948	B8 00000000	mov eax, 0	
740DF94D	F3 AB	rep stosl	
740DF94F	5F	pop edi	
740DF950	59	pop ecx	
740DF951	C3	ret	
740DF952	55	push ebp	__vbaOnError
740DF953	8B EC	mov ebp, esp	
740DF955	83 EC 04	sub esp, 4	
740DF958	83 2D 64F01C74	cmp dword ptr ds:[741CF064], 0	
740DF95F	75 39	jne msvbvm50.740DF99A	
740DF961	A1 6CF01C74	mov eax, dword ptr ds:[741CF06C]	

그대로 입력하니 암호가 나온다.

