

2019.02.14. CodeEngn Basic RCE L09  
Tree to Tree

Basic RCE L09

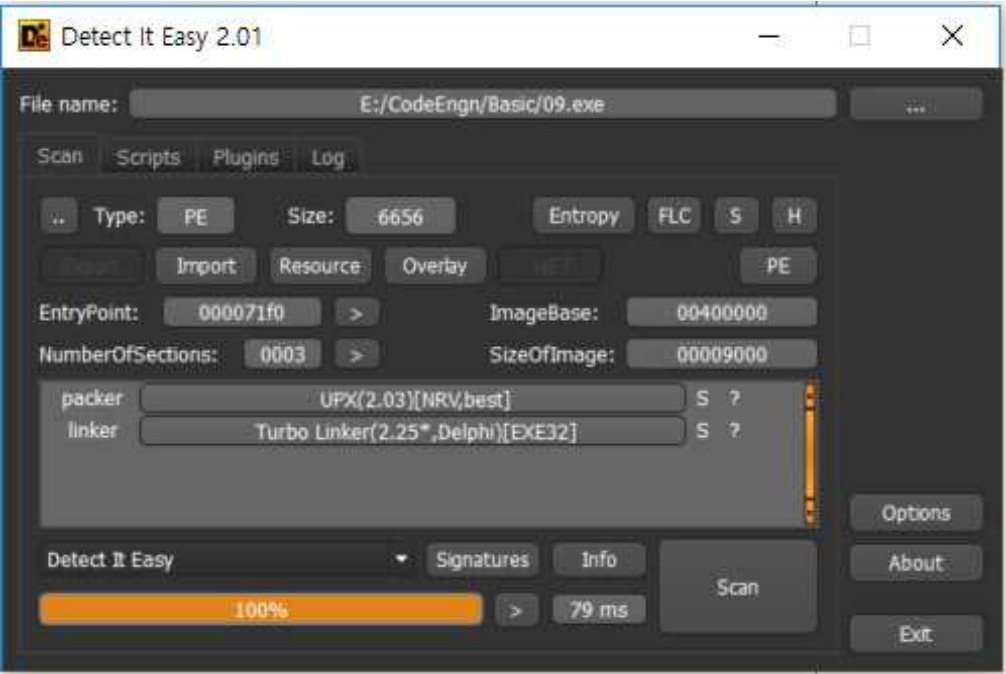
StolenByte를 구하시오 Ex) 75156A0068352040

— Author: abex

— File Password: codeengn



StolenByte가 뭔지 하고 한참 생각하다가 일단 돌려봤다.



이번에도 UPX패커!  
습관적으로 언패킹을 시작

유형	주소	Module/Label/Exception	상태	디스어셈블리	Hits	Summary
소프트웨어	004071f0	<09.exe.EntryPoint>	one-time	<a href="#">pushad</a>	0	<a href="#">진입점 중단점</a>

pushad와 popad를 찾은 순간 실행했을 때 나오는 문구들이 들어있다.  
일단 UPX OEP를 찾고 덤프했다.

0040736D	61	popad	
0040736E	6A 00	push 0	
00407370	68 00204000	push 09.402000	
00407375	68 12204000	push 09.402012	
0040737A	8D 4424 80	lea eax, dword ptr ss:[esp-80]	
0040737E	6A 00	push 0	
00407380	39C4	cmp esp, eax	
00407382	75 FA	jne 09.40737E	
00407384	83 EC 80	sub esp, FFFFFFF80	
00407387	E9 809CFFFF	jmp 09.40100C	

402000:"abex' 3rd crackme"  
 402012:"Click OK to check for the keyfile."

오류가 난다. 저 위에 문구 때문이라고 생각하고 StolenByte를 검색해봤더니  
언팩을 막기 위해 코드 일부분을 숨겨놓는 행위

2019-02-12 오후 3:06

2019-02-12 오후 3:06

2018-12-17 오전 2:27

2019-02-14 오후 3:03

2019-02-14 오후 3:03

2019-02-03 오후 10:56

2019-02-03 오후 10:56

응용 프로그램

응용 프로그램

압축(7Z) 파일

응용 프로그램

응용 프로그램

응용 프로그램

압축(7Z) 파일

응용 프로그램

압축(7Z) 파일

응용 프로그램

응용 프로그램

응용 프로그램

압축(7Z) 파일

응용 프로그램

오류

Up

확인

Error

Hmmmmm, I can't find the file!

확인

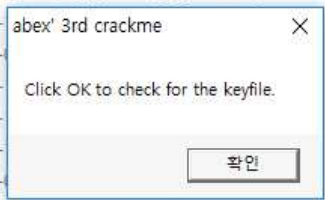
이번에는 문자열이 push되는 부분에 breakpoint를 걸고

The image shows a debugger window titled "Scylla x86 v0.9.8" with a menu bar (File, Imports, Trace, Misc, Help). The main window is divided into several sections:

- Attach to an active process:** A dropdown menu shows "4260 - 09.exe - E:\CodeEngn\Basic\09.exe". A "Pick DLL" button is next to it.
- Imports:** A list of imported DLLs: "kernel32.dll (3) FThunk: 00003054" and "user32.dll (1) FThunk: 00003064". Below this are buttons for "Show Invalid", "Show Suspect", and "Clear".
- IAT Info:** Fields for "OEP" (0040736E), "VA" (00403054), and "Size" (00000014). Buttons for "IAT Autosearch" and "Get Imports" are present.
- Actions:** A button labeled "Autotrace".
- Dump:** Buttons for "Dump", "PE Rebuild", and "Fix Dump".
- Log:** A text area showing the following log entries:
  - IAT Search Adv: IAT VA 00403054 RVA 00003054 Size 0x0014 (20)
  - IAT Search Nor: IAT VA 00403050 RVA 00003050 Size 0x0018 (24)
  - IAT parsing finished, found 4 valid APIs, missed 0 APIs
  - DIRECT IMPORTS - Found 0 possible direct imports with 0 unique APIs!
  - Dump success E:\CodeEngn\Basic\09\_dump.exe
  - Import Rebuild success E:\CodeEngn\Basic\09\_dump\_SCY.exe
- Footer:** A status bar showing "Imports: 4", "Invalid: 0", "Imagebase: 00400000", and "09.exe".

덤프해서 실행해봤다.

05_dump.exe	2019-02-12 오후 3:06	응용 프로그램	346KB
05_dump_SCY.exe	2019-02-12 오후 3:06	abex' 3rd crackme	353KB
06.7z	2019-02-12 오후 3:06		24KB
06.exe	2018-12-17 오전 2:27		26KB
06_dump.exe	2019-02-12 오후 3:06		163KB
06_dump_SCY.exe	2019-02-12 오후 3:06		164KB
07.7z	2019-02-12 오후 3:06		2KB
07.exe	2018-12-17 오전 2:27	응용 프로그램	8KB
08.7z	2019-02-03 오후 10:56	압축(7Z) 파일	39KB
08.exe	2018-12-17 오전 2:27	응용 프로그램	55KB
08_dump.exe	2019-02-14 오후 3:03	응용 프로그램	141KB
08_dump_SCY.exe	2019-02-14 오후 3:03	응용 프로그램	144KB
09.7z	2019-02-03 오후 10:56	압축(7Z) 파일	2KB
09.exe	2018-12-17 오전 2:31	응용 프로그램	7KB
09_dump.exe	2019-02-14 오후 11:12	응용 프로그램	24KB
09_dump_SCY.exe	2019-02-14 오후 11:12	응용 프로그램	25KB
10.7z	2019-02-03 오후 10:56	압축(7Z) 파일	131KB



잘된다. StolenByte는 12byte  
6A0068002040006812204000