
악성코드 정적분석

악성코드 분석 방법

악성코드 분석 정적분석 / 동적분석

동적분석 > 소프트웨어를 실행 o

정적분석 > 소프트웨어를 실행 x

정적분석의 특징

직관적, 신속히 분석이 가능

정교한 악성코드 분석에서 비효율적이고 중요한 행위를 놓칠 수 있음

악성코드 정적분석

악성코드 패킹 / 난독화 - 악성코드 파일의 탐지와 분석을 더 어렵게 함.

난독화 > 안티바이러스 프로그램 회피, 분석이 힘들

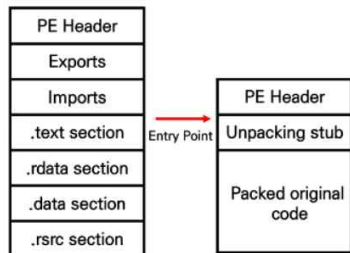
패킹 > 악성코드 프로그램을 압축시키기 위해 사용

원본 소스코드

```
Static void Fivo (char*args)
{
    Int n = Int.parse (args[0]);
    Int a = 0; Int b=1;
    For (int k=1;k<n;k++)
    {
        Int c=a+b;
        A=b;
        B=c;
    }
    Print ("Fib("+n+")="+b);
}
```

난독화 된 소스코드

```
Static void Fivo (char *PR2P_yYTK
Kqr4Juo7) { Int n = Int.parse (PR
2P_yYTKKqr4Juo7[0]; Int N3JZAB
9XBM1MX3Ec= 0; int xok3PcL9a
QFMKM_d=1; For (int SLX62RXq
cmVTAxPa=1;SLX62RXqcmVTAx
Pa<n;SLX62RXqcmVTAxPa++)I
nt c=N3JZAB9XBM1MX3Ec+xok3
PcL9aQFMKM_d; A=Xok3PcL9aQ
FMKM_d; B=c; } Print ("Fib ("+n+
")="+xok3PcL9aQFMKM_d); }
```



악성코드 정적분석

PE 파일 포맷



→ 코드에 대한 정보,
애플리케이션 유형,
필요한 라이브러리 함수,
메모리 공간 요구 사항

정적 링크 : 라이브러리 링크 방식에서 가장 적게 사용
런타임 링크 : 악성코드에서 패킹이나 난독화할 때 자주 사용
동적 링크 : 악성코드 분석가가 사용하는 가장 흔하고 대중적

악성코드 정적분석

PE 파일 포맷



IMAGE_FILE_HEADER

PEVIEW - C:\Users\high00\OneDrive\바탕 화면\Reversing\abex crackme\crackme1.exe

File View Go Help

	pFile	Data	Description	Value
crackme1.exe				
IMAGE_DOS_HEADER	00000104	014C	Machine	IMAGE_FILE_MACHINE_386
MS-DOS Stub Program	00000106	0005	Number of Sections	
IMAGE_NT_HEADERS	00000108	9839273B	Time Date Stamp	2060/12/05 19:47:07 UTC
Signature	0000010C	00000000	Pointer to Symbol Table	
IMAGE_OPTIONAL_HEADER	00000110	00000000	Number of Symbols	
IMAGE_SECTION_HEADER	00000114	00E0	Size of Optional Header	
IMAGE_SECTION_CODE	00000116	618E	Characteristics	
IMAGE_SECTION_HEADER DATA		0002		IMAGE_FILE_EXECUTABLE_IMAGE
IMAGE_SECTION_HEADER idata		0004		IMAGE_FILE_LINE_NUMS_STRIPPED
IMAGE_SECTION_HEADER reloc		0008		IMAGE_FILE_LOCAL_SYMS_STRIPPED
IMAGE_SECTION_HEADER rsrc		0080		IMAGE_FILE_BYTES_REVERSED_LO
SECTION CODE		0100		IMAGE_FILE_32BIT_MACHINE
SECTION DATA		8000		IMAGE_FILE_BYTES_REVERSED_HI
SECTION idata				
SECTION reloc				
SECTION rsrc				

Viewing IMAGE_FILE_HEADER

악성코드 정적분석

PE 파일 포맷



Virtual Size / Size of Raw Data

PEview - C:\Users\hgh00\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_11\Lab01-01.exe

File View Go Help

Lab01-01.exe

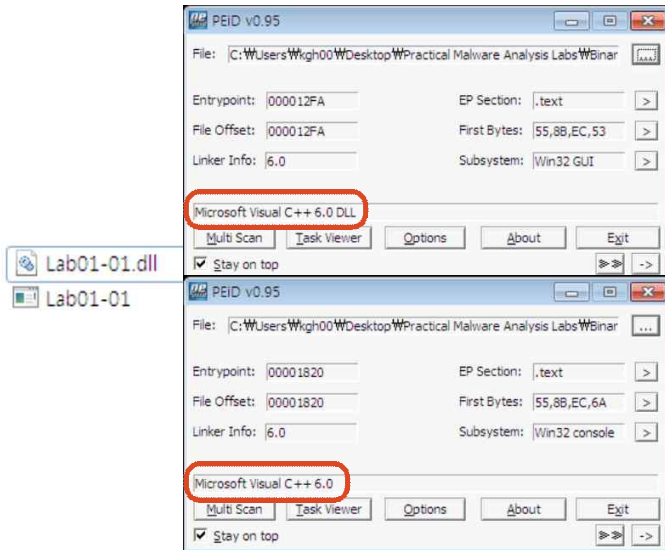
- IMAGE_DOS_HEADER
- MS-DOS Stub Program
- IMAGE_NT_HEADERS
 - IMAGE_SECTION_HEADER .text
 - IMAGE_SECTION_HEADER .rdata
 - IMAGE_SECTION_HEADER .data
- SECTION .text
- SECTION .rdata
- SECTION .data

pFile	Data	Description	Value
000001E0	2E 74 65 78	Name	.text
000001E4	74 00 00 00		
000001E8	00000970	Virtual Size	
000001F0	00001000	Size of Raw Data	
000001F4	00001000	Pointer to Raw Data	
000001F8	00000000	Pointer to Relocations	
000001FC	00000000	Pointer to Line Numbers	
00000200	0000	Number of Relocations	
00000202	0000	Number of Line Numbers	
00000204	60000020	Characteristics	
	00000020	IMAGE_SCN_CNT_CODE	
	20000000	IMAGE_SCN_MEM_EXECUTE	
	40000000	IMAGE_SCN_MEM_READ	

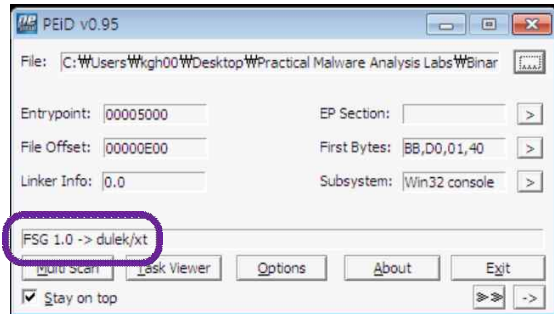
Viewing IMAGE_SECTION_HEADER .text

Lab01-01

실습



패킹되었을 경우



실습

The image shows two screenshots of the Dependency Walker tool. The top screenshot displays the function list for Lab01-01.dll, with a red box highlighting the following functions:

P#	Ordinal	Hint	Function	Entry Point
	N/A	27 (0x0018)	CloseHandle	Not Bound
	N/A	63 (0x003F)	CreateFileA	Not Bound
	N/A	68 (0x0044)	CreateProcessA	Not Bound
	N/A	493 (0x01ED)	OpenFileA	Not Bound
	N/A	662 (0x0296)	Sleep	Not Bound

The bottom screenshot displays the function list for Lab01-01.exe, with a red box highlighting the following functions:

P#	Ordinal	Hint	Function	Entry Point
	N/A	27 (0x0018)	CloseHandle	Not Bound
	N/A	40 (0x0028)	CopyFileA	Not Bound
	N/A	53 (0x0035)	CreateFileA	Not Bound
	N/A	144 (0x0090)	FindClose	Not Bound
	N/A	145 (0x0091)	FindFirstFileA	Not Bound
	N/A	157 (0x009D)	FindNextFileA	Not Bound
	N/A	437 (0x01B5)	IsBadReadFile	Not Bound
	N/A	470 (0x01D6)	MapViewOfFile	Not Bound
	N/A	688 (0x02B0)	UnmapViewOfFile	Not Bound

Additional text on the right side of the image lists the functions being analyzed:

- CreateProcessA
- Sleep
- WS2_32.DLL
- CreateFileA
- CopyFileA
- FindFirstFileA
- FindNextFileA

실습

```

1 D:\DATA\...\Chapter_11>strings Lab01-01.exe
2
3 Strings v2.51
4 Copyright (C) 1999-2013 Mark Russinovich
5 Sysinternals - www.sysinternals.com
6
7 !This program cannot be run in DOS mode.
8 Rich
9
10 CloseHandle
11 UnmapViewOfFile
12 IsBadReadPtr
13 MapViewOfFile
14 CreateFileMappingA
15 CreateFileA
16 FindClose
17 FindNextFileA
18 FindFirstFileA
19 CopyFileA
20 KERNEL32.dll
21 malloc
22 exit
23 MSVCRT.dll
24 _exit
25 _NcvtFilter
26 __p__initenv
27 __getmainargs
28 _initterm
29 __setusermatherr
30 _adjust_fdiv
31 __p__commode
32 __p__fmode
33 __set_app_type
34 _except_handler3
35 _controlfp
36 _wrtctrl
37 kernel32.dll
38 kernel32.dll
39 exe
40 C:\
41 C:\windows\system32\kernel32.dll
42 Kernel32
43 Lab01-01.dll
44 C:\Windows\System32\Kernel32.dll
45 WARNING_THIS_WILL_DESTROY_YOUR_MACHINE
46
47 D:\DATA\...\Chapter_11>

```

```

1 D:\DATA\...\Chapter_11>strings Lab01-01.dll
2
3 Strings v2.51
4 Copyright (C) 1999-2013 Mark Russinovich
5 Sysinternals - www.sysinternals.com
6
7 !This program cannot be run in DOS mode.
8
9 Rich
10 ...
11 CloseHandle
12 Sleep
13 CreateProcessA
14 CreateMutexA
15 OpenMutexA
16 KERNEL32.dll
17 WS2_32.dll
18 strcmp
19 MSVCRT.dll
20 free
21 _initterm
22 malloc
23 _adjust_fdiv
24 exec
25 sleep
26 hello
27 127.26.152.13
28 SAUFHUP
29 /0I0[0h0p0
30 14161[111
31 1Y2a2g2r2
32 3133
33
34 D:\DATA\...\Chapter_11>

```

End