PE 분석 보고서

2023 November 26 Sunday . 19시 27분 49초
작성자 : 홍길동

[DOS Header]

실제 변수명	값	의미
e_magic	MZ	DOS Signature
e_lfanew	0x100	NT header offset

[NT Header]

실제 변수명	값	의미
Signature	PE	NF Signature
Machine	0x14c	CPU 별 고유값 (x86 = 0x14c / x64 = 0x8664)
NumberOfSections	8	Section의 총 개수
SizeOfOptionalHeader	0xe0	OptionalHeader의 크기
Characteristics	0x818f	이 파일의 속성
Magic	0x10b	Optional header를 구분하는 Signature (32bit=10b / 64bit=20b)
SizeOfCode	0xfe00	IMAGE_SCN_CNT_CODE 속성을 갖는 섹션들의 총 사이즈 크기
AddressOfEntryPoint	0x113bc	PE 파일이 메모리 로드 후 처음 실행되어야 하는 코드 주소
ImageBase	0x400000	PE파일이 매핑되는 시작주소
SectionAlignment	4096	메모리 상에서의 최소 섹션 단위
FileAlignment	512	파일 상에서의 최소 섹션 단위

[Sections Header]

Name	Section 이름
VirtualAddress	섹션의 RAV(ImageBase + VA)를 위한 VA 값
SizeOfRawData	파일 상에서 섹션이 차지하는 크기
PointerToRawData	파일 상에서 섹션이 시작하는 위치
Characteristics	섹션의 특징을 나타냄

Name	Virtual Address	SizeOfRawData	PointerToRawData	Characteristics
.text	0x1000	0xf200	0x400	0x60000020
.itext	0x11000	0xc00	0xf600	0x60000020
.data	0x12000	0xe00	0x10200	0xc0000040
.bss	0x13000	0x0	0x11000	0xc0000000
.idata	0x19000	0xe00	0x11000	0xc0000040
.tls	0x1a000	0x0	0x11e00	0xc0000000
.rdata	0x1b000	0x200	0x11e00	0x40000040
.rsrc	0x1c000	0xb200	0x12000	0x40000040

[Details about Packed File]

Entry Point	0x113bc
Ep_Section	.itext
File Offset	0xf600
First 16 Bytes	b'₩x83'
Linker Info	0x14c
Subsystem	0x2
Compiler Info	0x14c

컴파일러 정보: intel 368/x86 = 0x14c , intel 64 = 0x0200 , AMD64 = 0x8664