악성코드 정적분석

김건희

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.

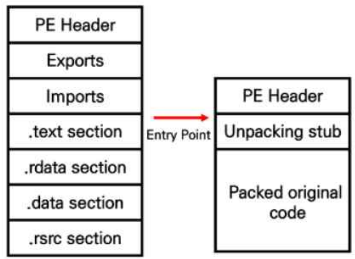
난독화 > 안티바이러스 프로그램 회피, 분석이 힘듬
패킹 > 악성코드 프로그램을 압축시키기 위해 사용

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);
}
```

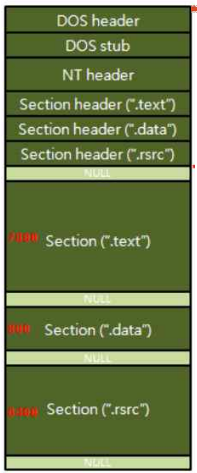
난독화 된 소스코드

```
Static void Fivo (char *PR2P_yYtK
Kqr4Juo7) { Int n = Int.parse (PR
2P_YtKKqr4Juo7[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

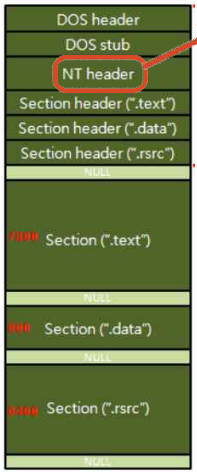


코드에 대한 정보,
애플리케이션 유형,
필요한 라이브러리 함수,
메모리 공간 요구 사항

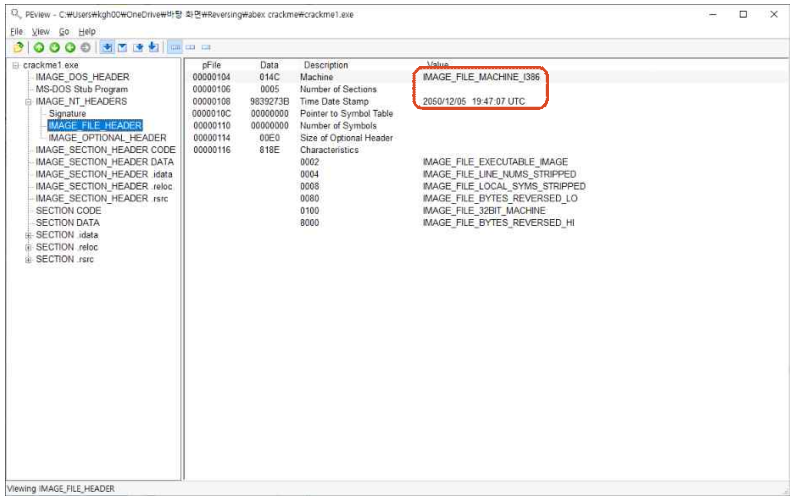
정적 링크 : 라이브러리 링크 방식에서 가장 적게 사용
런타임 링크 : 악성코드에서 패킹이나 난독화할 때 자주 사용
동적 링크 : 악성코드 분석가가 사용하는 가장 흔하고 대중적

악성코드 정적분석

PE 파일 포맷

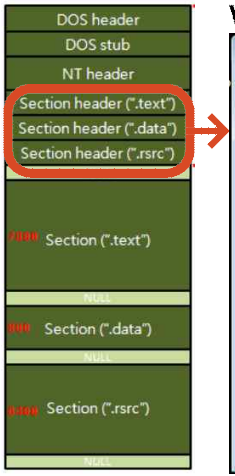


IMAGE_FILE_HEADER

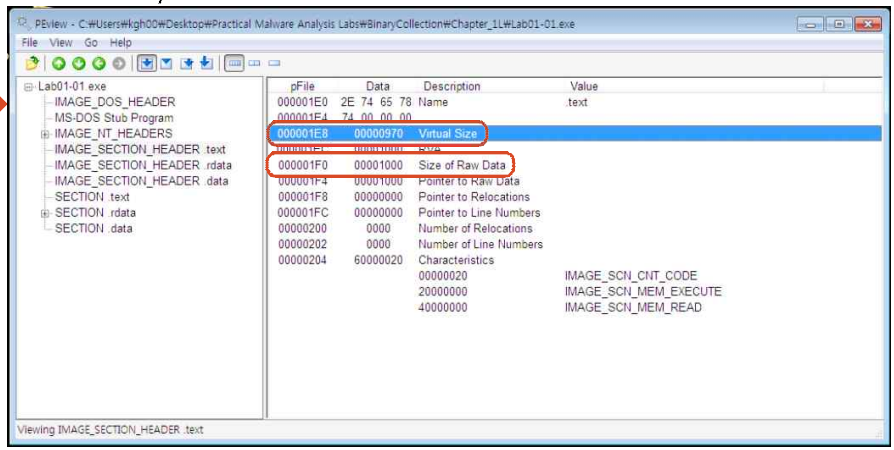


악성코드 정적분석

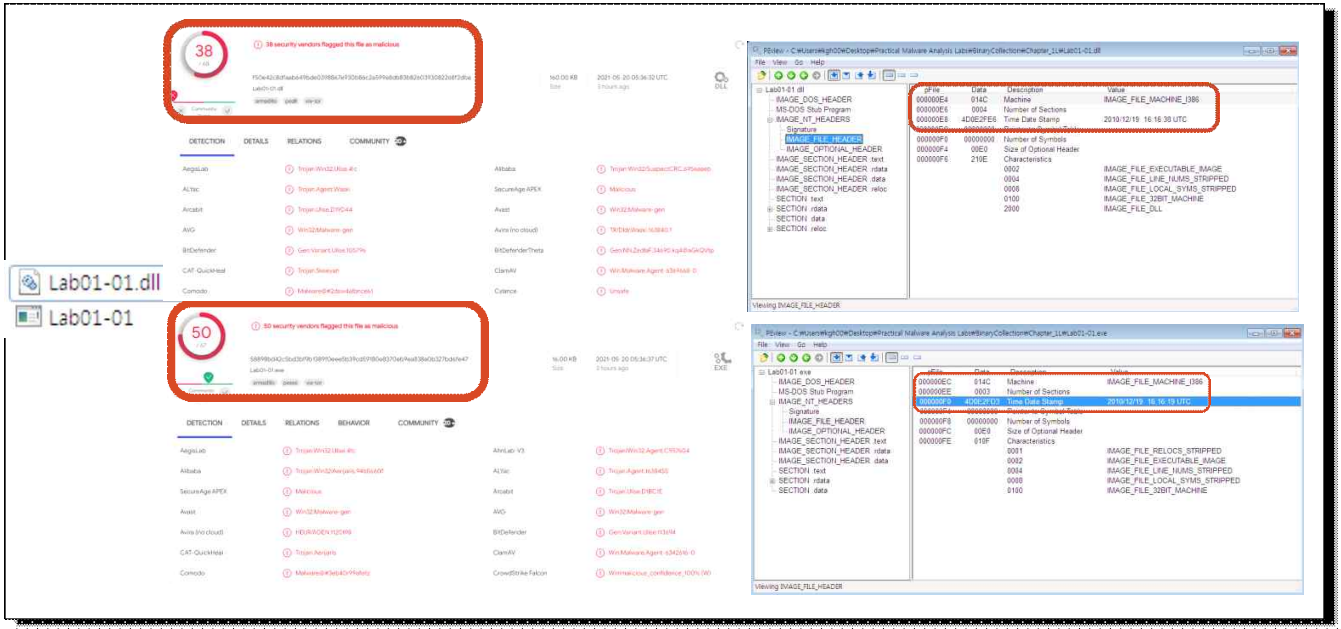
PE 파일 포맷



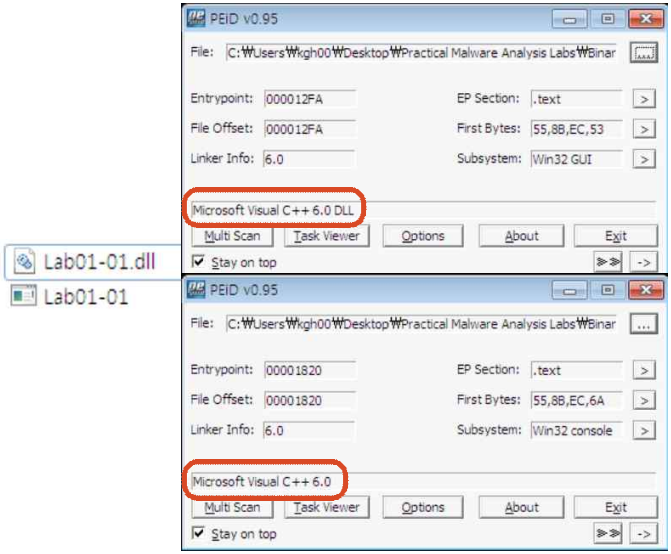
Virtual Size / Size of Raw Data



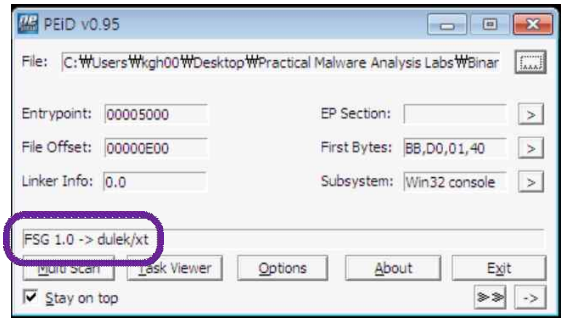
실습


Lab01-01.dll
Lab01-01
38
50
DETECTION
DETAILS
RELATIONS
BEHAVIOR
COMMUNITY

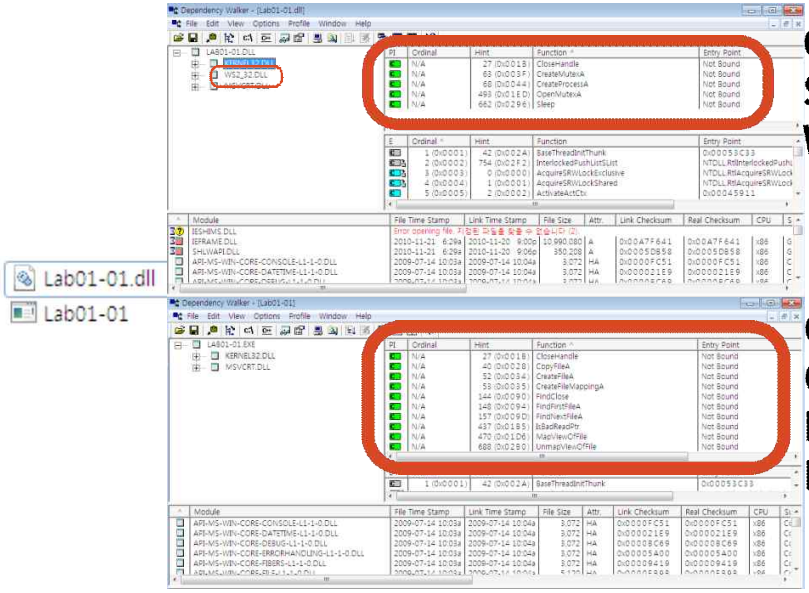
실습


Lab01-01.dll
Lab01-01
PEiD v0.95
File: C:₩Users₩kgh00₩Desktop₩Practical Malware Analysis Labs₩Binar
Entrypoint: 000012FA
EP Section: .text
File Offset: 000012FA
First Bytes: 55,8B,EC,53
Linker Info: 6.0
Subsystem: Win32 GUI
Microsoft Visual C++ 6.0 DLL
Multi Scan
Task Viewer
Options
About
Exit
Stay on top
PEiD v0.95
File: C:₩Users₩kgh00₩Desktop₩Practical Malware Analysis Labs₩Binar
Entrypoint: 00001820
EP Section: .text
File Offset: 00001820
First Bytes: 55,8B,EC,6A
Linker Info: 6.0
Subsystem: Win32 console
Microsoft Visual C++ 6.0
Multi Scan
Task Viewer
Options
About
Exit
Stay on top

패킹되었을 경우


PEiD v0.95
File: C:₩Users₩kgh00₩Desktop₩Practical Malware Analysis Labs₩Binar
Entrypoint: 00005000
EP Section:
File Offset: 00000E00
First Bytes: BB,D0,01,40
Linker Info: 0.0
Subsystem: Win32 console
FSG 1.0 -> dulek/xt
Task Viewer
Options
About
Exit
Stay on top

실습


Lab01-01.dll
Lab01-01
CreateProcessA
Sleep
WS2_32.DLL
CreateFileA
CopyFileA
FindFirstFileA
FindNextFileA

실습


Lab01-01.dll
Lab01-01
D:\DATA\...\Chapter_1L>strings Lab01-01.exe
Strings v2.51
Copyright (C) 1999-2013 Mark Russinovich
Sysinternals - www.sysinternals.com
!This program cannot be run in DOS mode.
Richm
.rdata
CloseHandle
UnmapViewOfFile
IsBadReadPtr
MapViewOfFile
CreateFileMappingA
CreateFileA
FindClose
FindNextFileA
FindFirstFileA
CopyFileA
KERNEL32.dll
malloc
exit
MSVCRT.dll
_exit
_XcptFilter
__p___initenv
__getmainargs
_initterm
__setusermatherr
_adjust_fdiv
__p__commode
__p__fmode
__set_app_type
_except_handler3
_controlfp
_stricmp
kernel32.dll
kernel32.dll
.exe
C:*
C:\windows\system32\kernel32.dll
Kernel32.
Lab01-01.dll
C:\Windows\System32\Kernel32.dll
WARNING_THIS_WILL_DESTROY_YOUR_MACHINE
D:\DATA\...\Chapter_1L>
D:\DATA\...\Chapter_1L>strings Lab01-01.dll
Strings v2.51
Copyright (C) 1999-2013 Mark Russinovich
Sysinternals - www.sysinternals.com
!This program cannot be run in DOS mode.
Rich
.rdata
CloseHandle
Sleep
CreateProcessA
CreateMutexA
OpenMutexA
KERNEL32.dll
WS2_32.dll
strncmp
MSVCRT.dll
free
_initterm
malloc
_adjust_fdiv
exec
sleep
hello
127.26.152.13
SADFHUHF
/010[0h0p0
1416[lll
1Y2a2g2r2
3!3]3
D:\DATA\...\Chapter_1L>

End