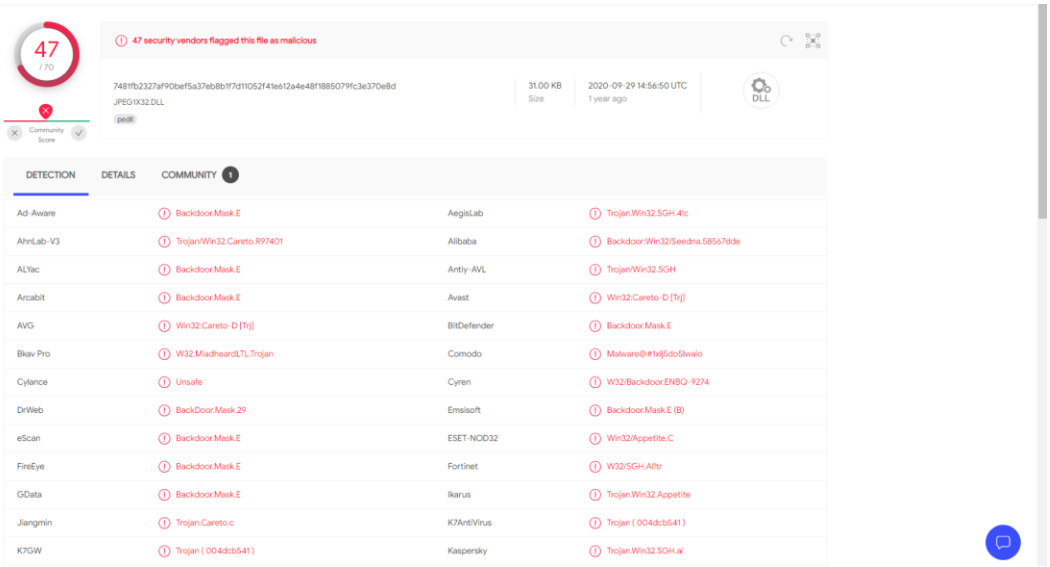
Trịnh Quốc Hiếu –Bi10-060-USTHCS

Malware Analysis Final Report

Contents

Check on virus total



- The virus can be detected in 47
- Its basic information

MD5	53908fb164e2e2053ceba4bdb6d09db9
SHA-1	3219ba119ac4a0b74b174debfbb645203e87f602
SHA-256	7481fb2327af90bef5a37eb8b1f7d11052f41e612a4e48f1885079fc3e370e8d
Vhash	1340466d15155078z3409lz45z46z1
Authentihash	cefe1dee528b78a316e0f0796afc4325e3d115771842f7cddc90461314357909
Imphash	52660550aa2ac90863c1cfb4fd3ab2f8
Rich PE header hash	0a2e9ab8745a908b3afef87526fd1c2c
SSDEEP	768:euqA0/5CDYnY/1rhbAxZXUYJlxqyd3azWQcPjcl:ebA0s/hhkfDxj+crcl
File type	Win32 DLL
Magic	PE32 executable for MS Windows (DLL) (GUI) Intel 80386 32-bit
TrID	Win16 NE executable (generic) (45%)
TrID	Win32 Dynamic Link Library (generic) (21.1%)
TrID	Win32 Executable (generic) (14.4%)
TrID	OS/2 Executable (generic) (6.5%)
TrID	Generic Win/DOS Executable (6.4%)
File size	31.00 KB (31744 bytes)
PEiD packer	Microsoft Visual C++ v7.0 DLL

+ Hashes type : MD5, SHA-1, SHA-256, Vhash, Authentihas, SSDEEP

+ File type : Win32 DLL

+ File size : 31.00 KB (31744 bytes)

+ Creation time: 2013-04-09 14:15:17

+ Target machine : PE32 executable for MS Windows (DLL) (GUI) Intel 80386 32-bit

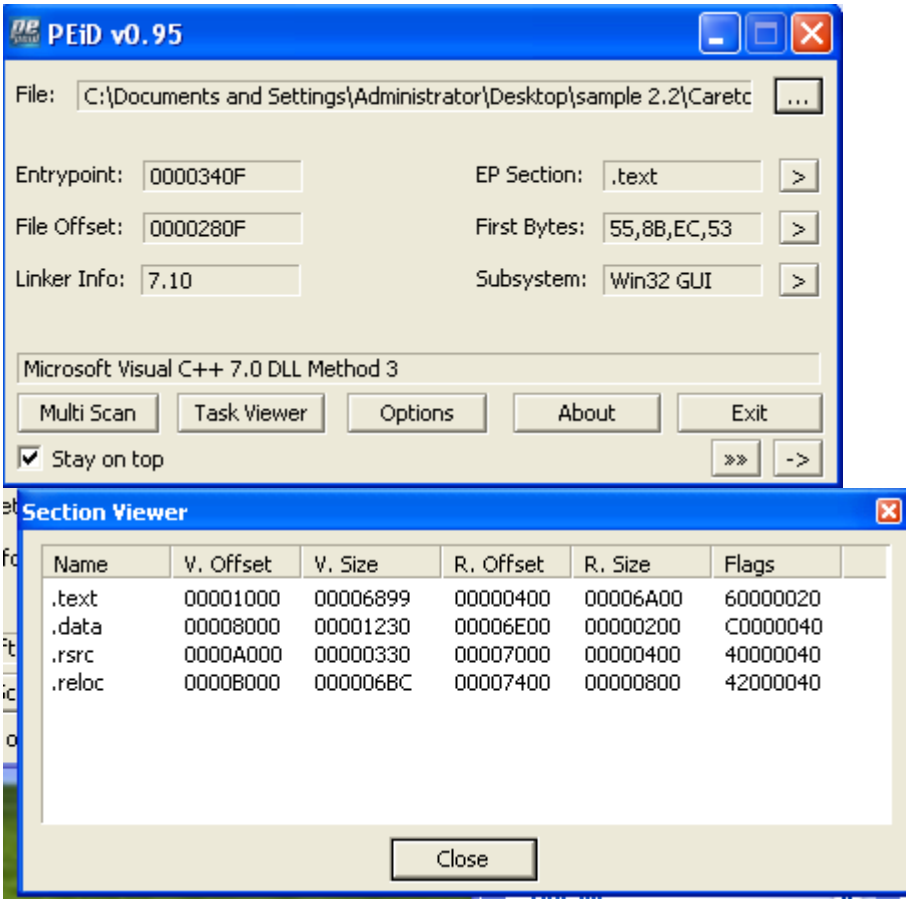
+ Imports :

ADVAPI32.dll

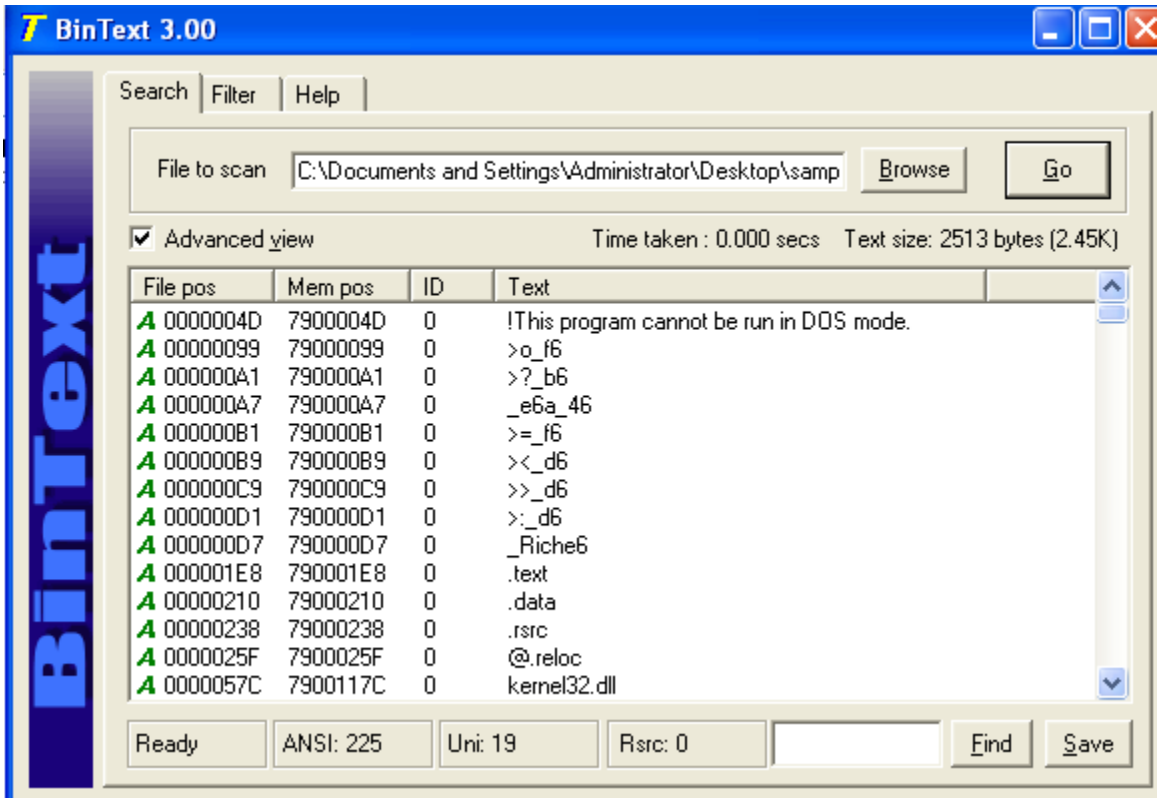
KERNEL32.dll
msvcrt.dll
WS2_32.dll
USER32.dll

Check in tool

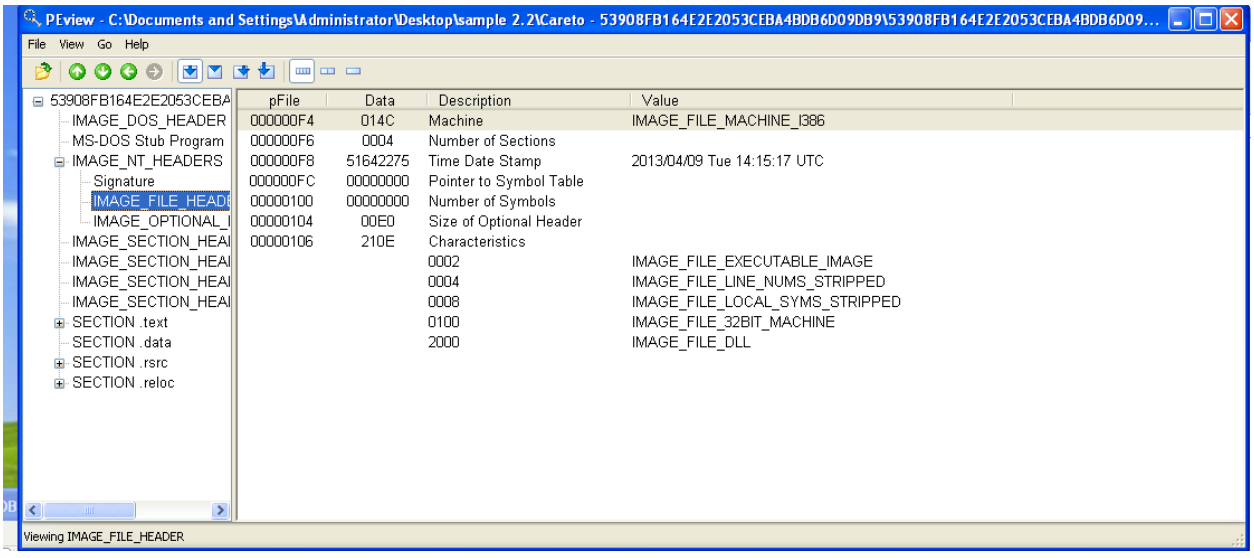
PeiD



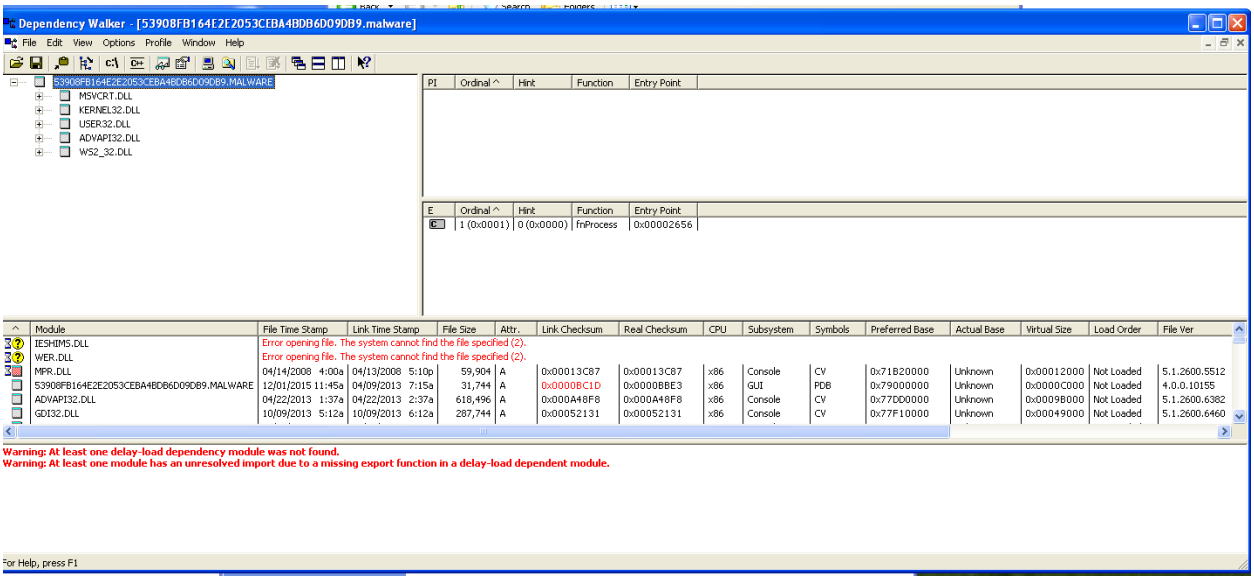
Bintext



PEview

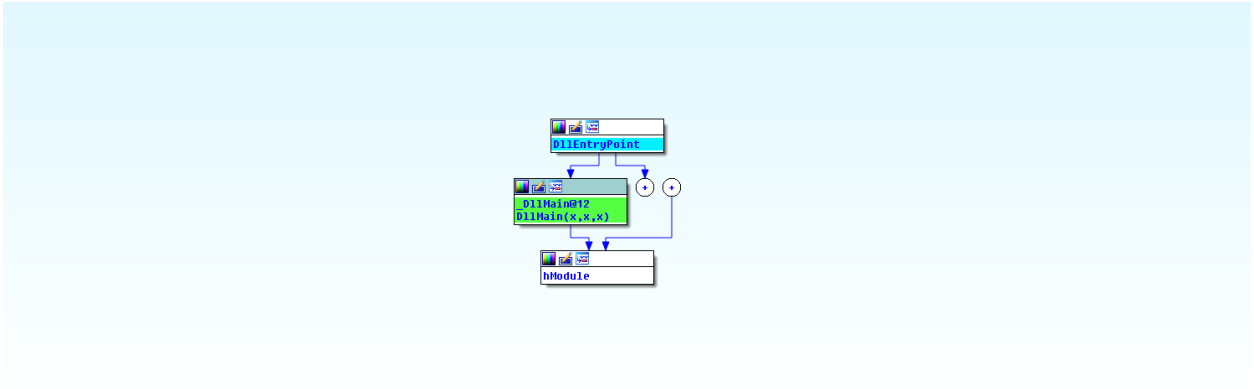


Dependecy Walker



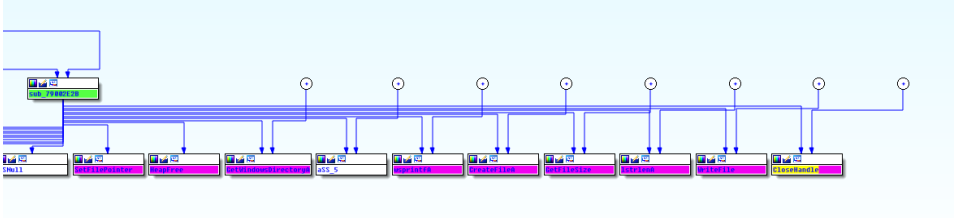
We check about import

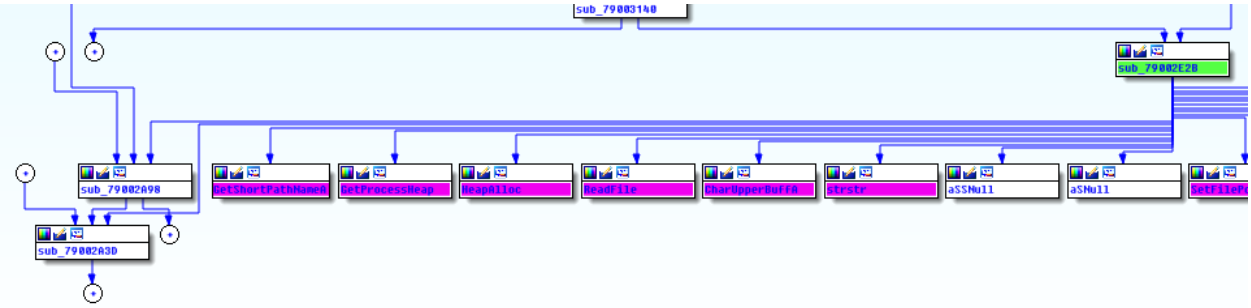
Check on ida



This is main malware

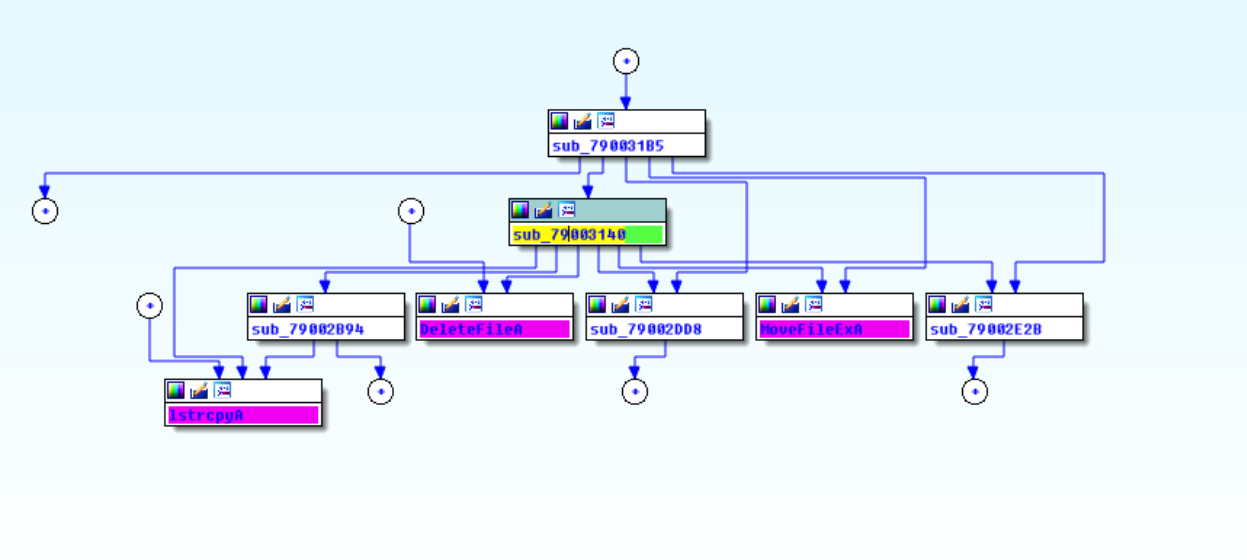
Check sub_79002E2B



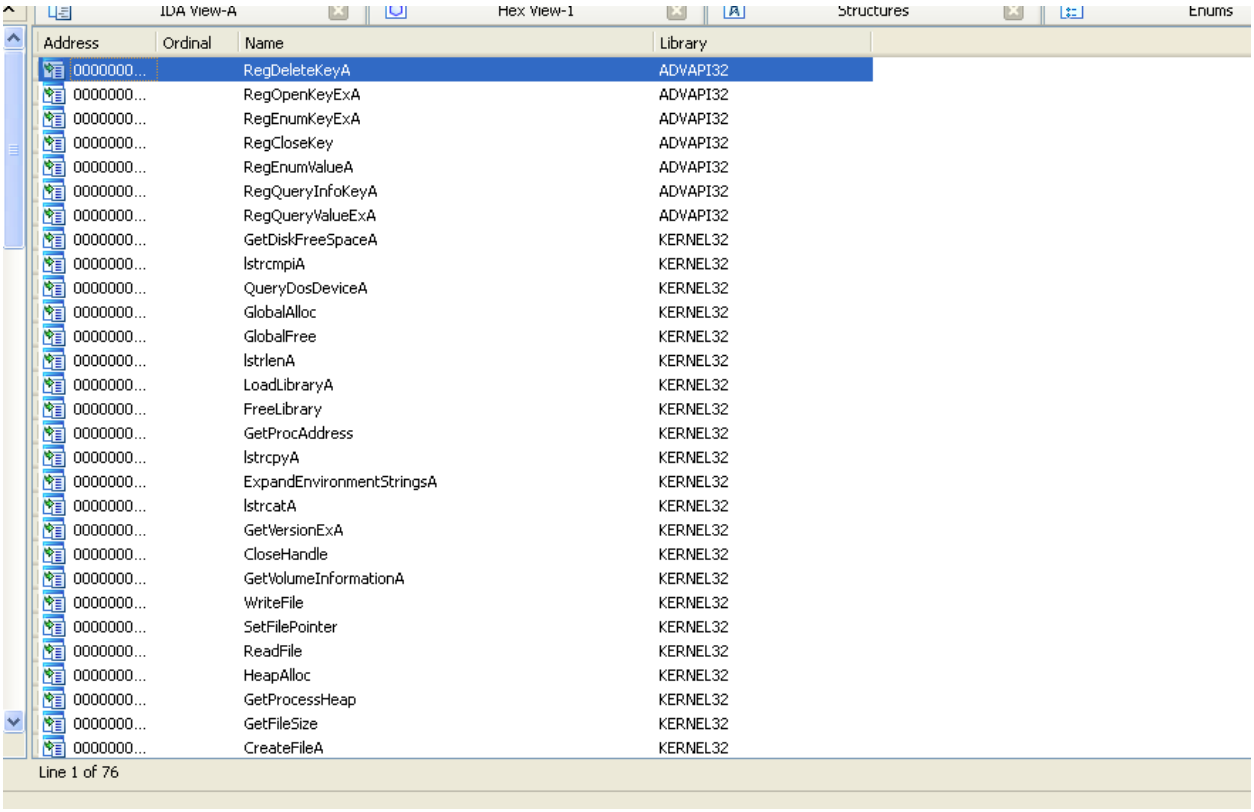


Important function

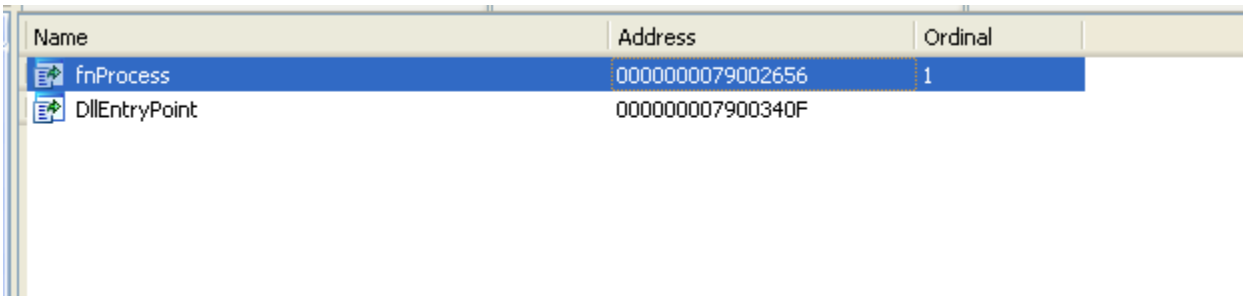
Check sub_79003104



Imports


IDA View-A
Hex View-1
Structures
Enums
Address
Ordinal
Name
Library
00000000...
RegDeleteKeyA
ADVAPI32
RegOpenKeyExA
RegEnumKeyExA
RegCloseKey
RegEnumValueA
RegQueryInfoKeyA
RegQueryValueExA
GetDiskFreeSpaceA
KERNEL32
lstrcmpiA
QueryDosDeviceA
GlobalAlloc
GlobalFree
lstrlenA
LoadLibraryA
FreeLibrary
GetProcAddress
lstrcpyA
ExpandEnvironmentStringsA
lstrcatA
GetVersionExA
CloseHandle
GetVolumeInformationA
WriteFile
SetFilePointer
ReadFile
HeapAlloc
GetProcessHeap
GetFileSize
CreateFileA
Line 1 of 76

Export


Name
Address
Ordinal
fnProcess
0000000079002656
1
DllEntryPoint
000000007900340F