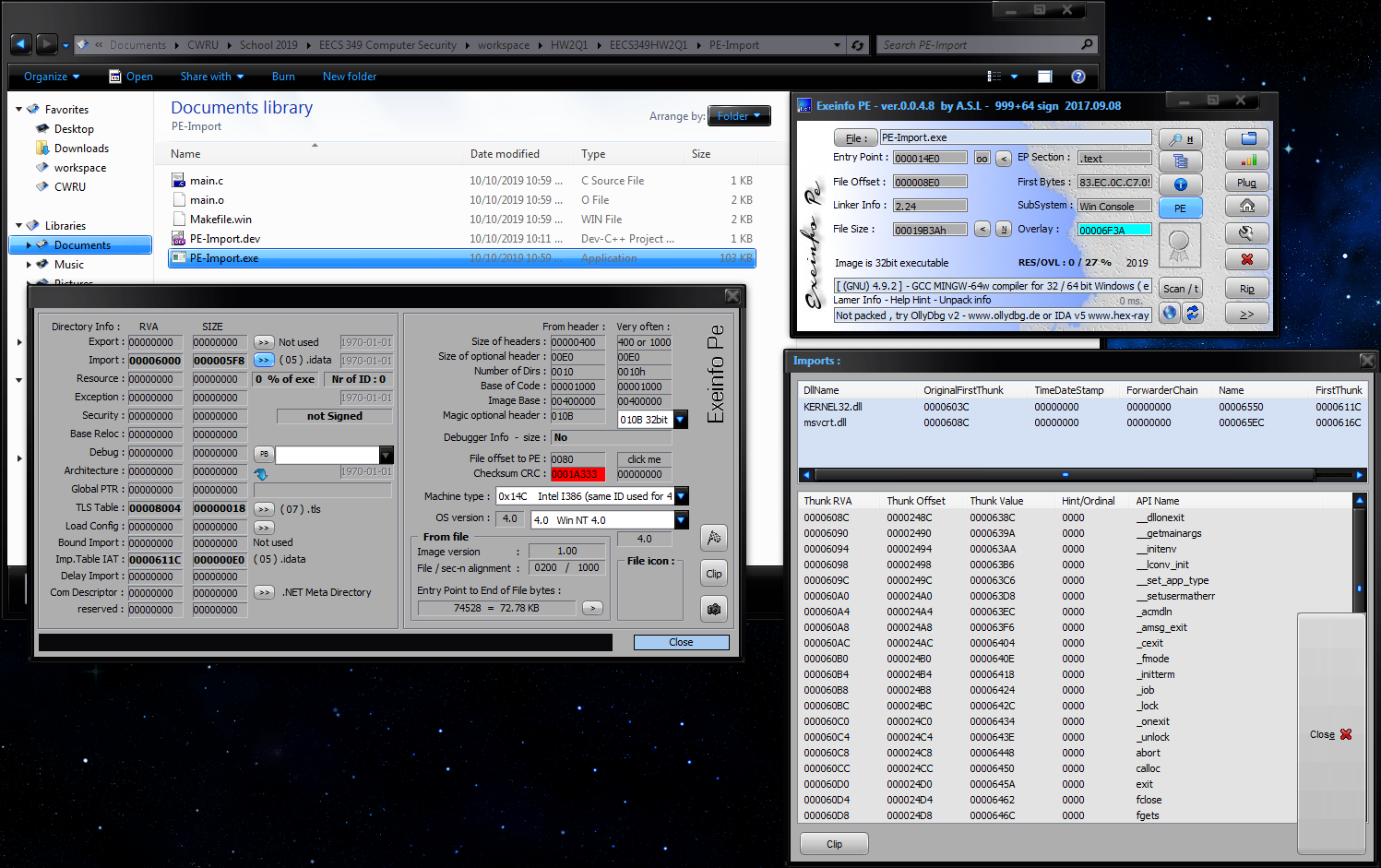
**Original PE-Import.exe**



Header info : PE-Import.exe

Export : 00000000 00000000

Import : 00006000 000005F8

Resource : 00000000 00000000

Exception : 00000000 00000000

Security : 00000000 00000000

Base Reloc : 00000000 00000000

Debug : 00000000 00000000

Architecture : 00000000 00000000

Global PTR : 00000000 00000000

TLS Table : 00008004 00000018

Load Config : 00000000 00000000

Bound Import : 00000000 00000000

Imp.Table IAT : 0000611C 000000E0

Com Descriptor : 00000000 00000000

reserved : 00000000 00000000

Size of headers : 00000400

Size of optional header : 00E0

Number of Dirs : 0010

Base of Code : 00001000

Image Base : 00400000

Magic optional header : 010B

Debugger Info - size : No

File offset to PE : 0080

Entry Point to End of File bytes : 00E0

Checksum CRC : 0001A333

Machine type : 0x14C Intel I386 (same ID used for 486 and 586)

OS version : 4.0 / 4.0 Win NT 4.0

1.00

Entry Point to End of File bytes : 74528 = 72.78 KB

DLL Name : KERNEL32.dll

---------

API Name :

---------

DeleteCriticalSection

EnterCriticalSection

GetCurrentProcess

GetCurrentProcessId

GetCurrentThreadId

GetLastError

GetStartupInfoA

GetSystemTimeAsFileTime

GetTickCount

InitializeCriticalSection

LeaveCriticalSection

QueryPerformanceCounter

SetUnhandledExceptionFilter

Sleep

TerminateProcess

TlsGetValue

UnhandledExceptionFilter

VirtualProtect

VirtualQuery

-=-=-=-=-=-

DLL Name : msvcrt.dll

---------

API Name :

---------

\_\_dllonexit

\_\_getmainargs

\_\_initenv

\_\_lconv\_init

\_\_set\_app\_type

\_\_setusermatherr

\_acmdln

\_amsg\_exit

\_cexit

\_fmode

\_initterm

\_iob

\_lock

\_onexit

\_unlock

abort

calloc

exit

fclose

fgets

fopen

fprintf

fputs

free

fwrite

getchar

malloc

memcpy

puts

signal

strcspn

strlen

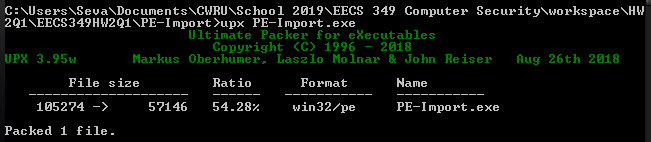
strncmp

strstr

vfprintf

-=-=-=-=-=-

**Packed PE-Import.exe**



Header info : PE-Import.exe

Export : 00000000 00000000

Import : 0001F000 000000B4

Resource : 00000000 00000000

Exception : 00000000 00000000

Security : 00000000 00000000

Base Reloc : 00000000 00000000

Debug : 00000000 00000000

Architecture : 00000000 00000000

Global PTR : 00000000 00000000

TLS Table : 0001EA28 00000018

Load Config : 00000000 00000000

Bound Import : 00000000 00000000

Imp.Table IAT : 00000000 00000000

Com Descriptor : 00000000 00000000

reserved : 00000000 00000000

Size of headers : 00001000

Size of optional header : 00E0

Number of Dirs : 0010

Base of Code : 00018000

Image Base : 00400000

Magic optional header : 010B

Debugger Info - size : No

File offset to PE : 0080

Entry Point to End of File bytes : 00E0

Checksum CRC : 00000000

Machine type : 0x14C Intel I386 (same ID used for 486 and 586)

OS version : 4.0 / 4.0 Win NT 4.0

1.00

Entry Point to End of File bytes : 1440 = 1.41 KB

DLL Name : KERNEL32.DLL

---------

API Name :

---------

LoadLibraryA

ExitProcess

GetProcAddress

VirtualProtect

-=-=-=-=-=-

DLL Name : msvcrt.dll

---------

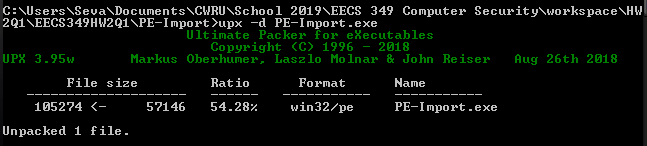
API Name :

---------

\_iob

-=-=-=-=-=-

**Unpacked PE-Import.exe**



Header info : PE-Import.exe

Export : 00000000 00000000

Import : 00006000 000005F8

Resource : 00000000 00000000

Exception : 00000000 00000000

Security : 00000000 00000000

Base Reloc : 00000000 00000000

Debug : 00000000 00000000

Architecture : 00000000 00000000

Global PTR : 00000000 00000000

TLS Table : 00008004 00000018

Load Config : 00000000 00000000

Bound Import : 00000000 00000000

Imp.Table IAT : 00000000 00000000

Com Descriptor : 00000000 00000000

reserved : 00000000 00000000

Size of headers : 00001000

Size of optional header : 00E0

Number of Dirs : 0010

Base of Code : 00001000

Image Base : 00400000

Magic optional header : 010B

Debugger Info - size : No

File offset to PE : 0080

Entry Point to End of File bytes : 00E0

Checksum CRC : 00000000

Machine type : 0x14C Intel I386 (same ID used for 486 and 586)

OS version : 4.0 / 4.0 Win NT 4.0

1.00

Entry Point to End of File bytes : 74528 = 72.78 KB

DLL Name : KERNEL32.DLL

---------

API Name :

---------

DeleteCriticalSection

EnterCriticalSection

GetCurrentProcess

GetCurrentProcessId

GetCurrentThreadId

GetLastError

GetStartupInfoA

GetSystemTimeAsFileTime

GetTickCount

InitializeCriticalSection

LeaveCriticalSection

QueryPerformanceCounter

SetUnhandledExceptionFilter

Sleep

TerminateProcess

TlsGetValue

UnhandledExceptionFilter

VirtualProtect

VirtualQuery

-=-=-=-=-=-

DLL Name : msvcrt.dll

---------

API Name :

---------

\_\_dllonexit

\_\_getmainargs

\_\_initenv

\_\_lconv\_init

\_\_set\_app\_type

\_\_setusermatherr

\_acmdln

\_amsg\_exit

\_cexit

\_fmode

\_initterm

\_iob

\_lock

\_onexit

\_unlock

abort

calloc

exit

fclose

fgets

fopen

fprintf

fputs

free

fwrite

getchar

malloc

memcpy

puts

signal

strcspn

strlen

strncmp

strstr

vfprintf

-=-=-=-=-=-

**FOOLING MALWARE DETECTION**

By obfuscating the code, I was able to make only 1 of 68 programs detect the exe as malware:

<https://www.virustotal.com/gui/file/dc7c28b16ea4163299a3e64598824d08cba7047de3c42bd52083f9e81f938b80/detection>

the obfuscated file is obfuscated-main.c (compiled into obfuscated-main.exe)  
Interestingly, packing the file made 5 programs detect the same file as malware.