Song Yang (sea.yang@rutgers.edu)

Xin Yang (xin.yang@rutgers.edu)

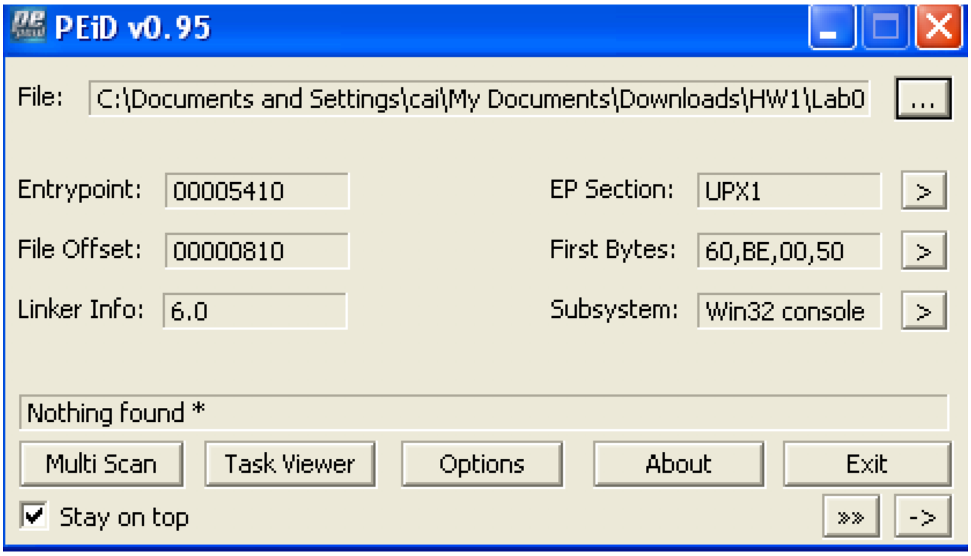
Zhuohang Li (zl299@scarletmaik.rutgers.edu)

Homework 1

Lab01-02.exe:

1. Yes. Detection ratio is 42/67. Mostly marked with Trojan generic downloader.

2. The file is packed with UPX and we are able to unpack it using UPX unpacker plugin.


PEiD v0.95

File: C:\Documents and Settings\cai\My Documents\Downloads\HW1\Lab0

Entrypoint: 00005410

EP Section: UPX1

File Offset: 00000810

First Bytes: 60,BE,00,50

Linker Info: 6.0

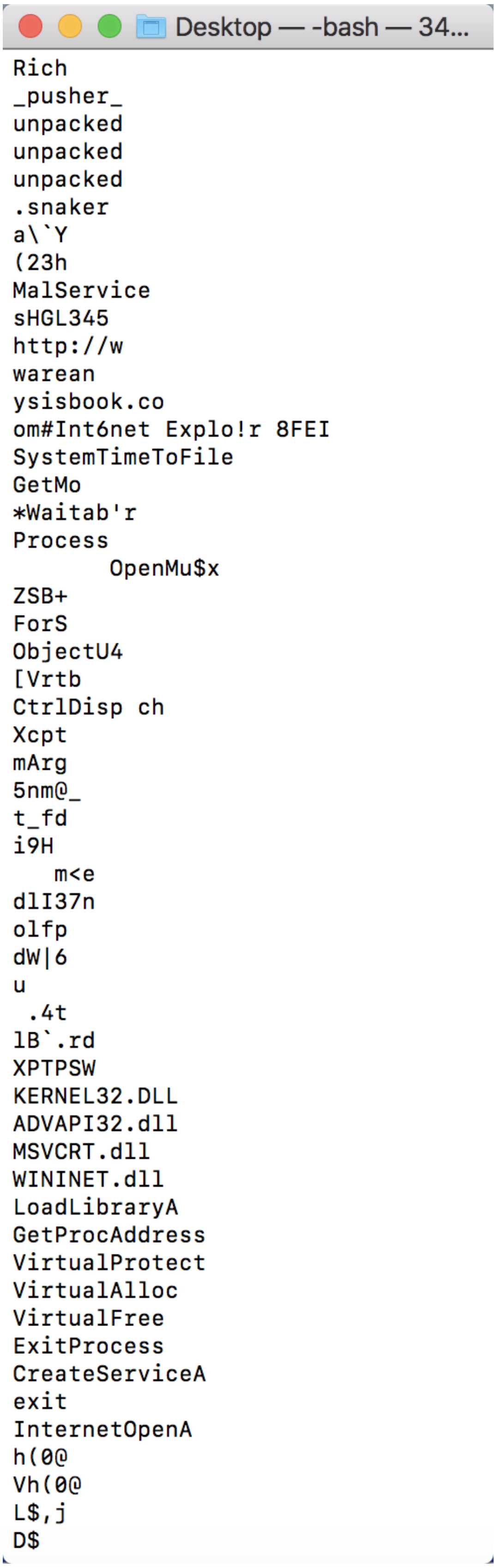
Subsystem: Win32 console

Nothing found *

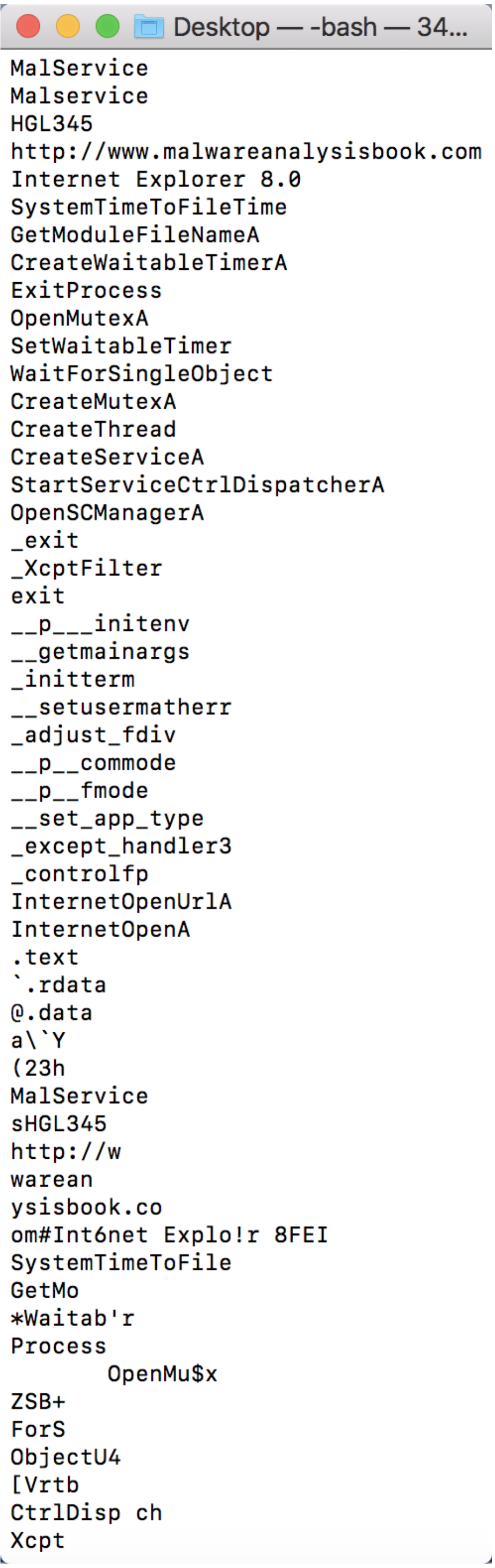
☑ Stay on top

3. Yes. Imports are ‘LoadLibraryA’, ‘GetProcAddress’, ‘CreateServiceA’ and ‘InternetOpenA’. These indicate that this program has something to do with creating service and connecting to the Internet.

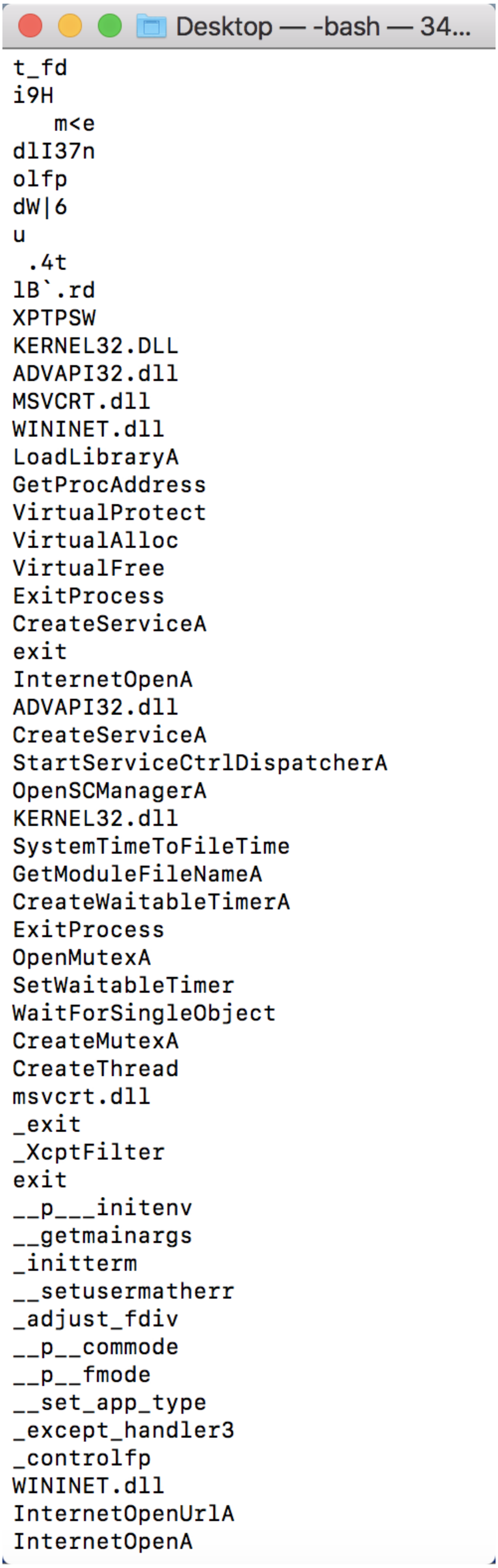
4. As is shown below, we can see an URL ‘http://www.malwareanalysisbook.com’ and a service named ‘MalService’ in the strings of the unpacked file. These could be used to identify the malware.



```
Rich
_pusher_
unpacked
unpacked
unpacked
.snaker
a\`Y
(23h
MalService
sHGL345
http://w
warean
ysisbook.co
om#Int6net Explo!r 8FEI
SystemTimeToFile
GetMo
*Waitab'r
Process
       OpenMu$x
ZSB+
ForS
ObjectU4
[Vrtb
CtrlDisp ch
Xcpt
mArg
5nm@_
t_fd
i9H
   m<e
dlI37n
olfp
dW|6
u
 .4t
lB`.rd
XPTPSW
KERNEL32.DLL
ADVAPI32.dll
MSVCRT.dll
WININET.dll
LoadLibraryA
GetProcAddress
VirtualProtect
VirtualAlloc
VirtualFree
ExitProcess
CreateServiceA
exit
InternetOpenA
h(0@
Vh(0@
L$,j
D$
```



```
MalService
Malservice
HGL345
http://www.malwareanalysisbook.com
Internet Explorer 8.0
SystemTimeToFileTime
GetModuleFileNameA
CreateWaitableTimerA
ExitProcess
OpenMutexA
SetWaitableTimer
WaitForSingleObject
CreateMutexA
CreateThread
CreateServiceA
StartServiceCtrlDispatcherA
OpenSCManagerA
_exit
_XcptFilter
exit
__p___initenv
__getmainargs
_initterm
__setusermatherr
_adjust_fdiv
__p__commode
__p__fmode
__set_app_type
_except_handler3
_controlfp
InternetOpenUrlA
InternetOpenA
.text
`.rdata
@.data
a\`Y
(23h
MalService
sHGL345
http://w
warean
ysisbook.co
om#Int6net Explo!r 8FEI
SystemTimeToFile
GetMo
*Waitab'r
Process
       OpenMu$x
ZSB+
ForS
ObjectU4
[Vrtb
CtrlDisp ch
Xcpt
```



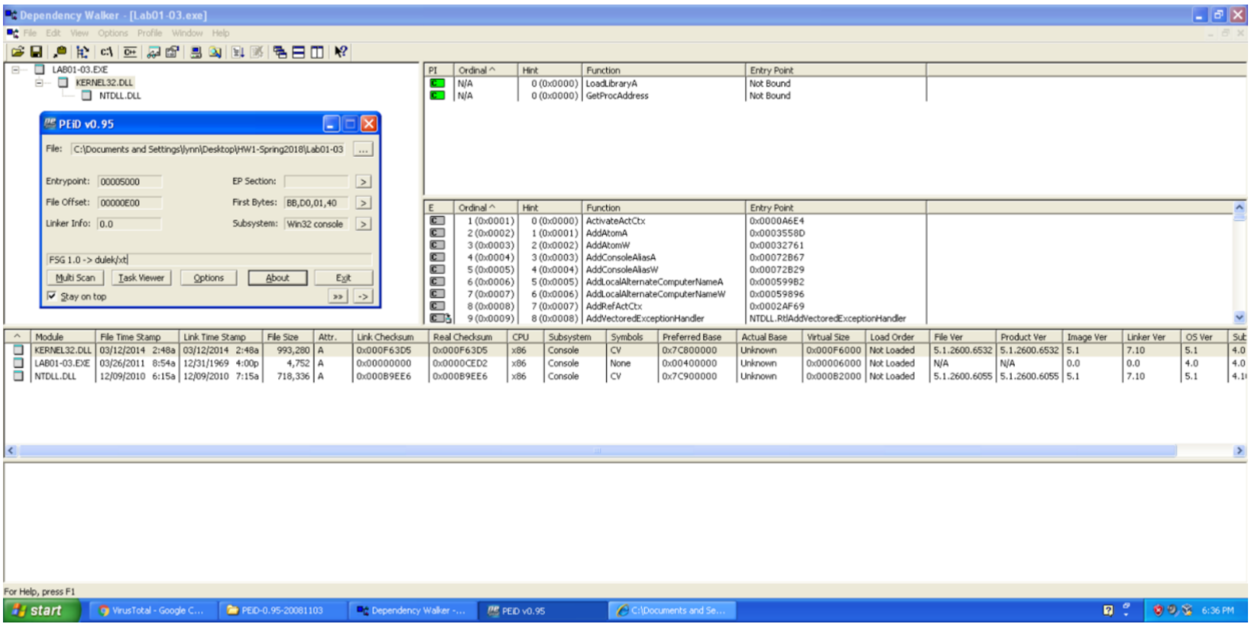
```
t_fd
i9H
   m<e
dlI37n
olfp
dW|6
u
 .4t
lB`.rd
XPTPSW
KERNEL32.DLL
ADVAPI32.dll
MSVCRT.dll
WININET.dll
LoadLibraryA
GetProcAddress
VirtualProtect
VirtualAlloc
VirtualFree
ExitProcess
CreateServiceA
exit
InternetOpenA
ADVAPI32.dll
CreateServiceA
StartServiceCtrlDispatcherA
OpenSCManagerA
KERNEL32.dll
SystemTimeToFileTime
GetModuleFileNameA
CreateWaitableTimerA
ExitProcess
OpenMutexA
SetWaitableTimer
WaitForSingleObject
CreateMutexA
CreateThread
msvcrt.dll
_exit
_XcptFilter
exit
__p___initenv
__getmainargs
_initterm
__setusermatherr
_adjust_fdiv
__p__commode
__p__fmode
__set_app_type
_except_handler3
_controlfp
WININET.dll
InternetOpenUrlA
InternetOpenA
```

Lab01-03.exe:

1. It could be Packer/Trojan/generic/Genome

2. The file is packed. as PEiD showed in the picture, it is packed with FSG 1.0 -> dulek/xt . PEiD cannot find the original entry point of this package so it still cannot be unpacked.

3. We saw 2 function called at first they are ‘LoadLibraryA’ and ‘GetProcaddress’, but they should be part of the package and not the origin program.



File: C:\Documents and Settings\lynn\Desktop\HW1-Spring2018\Lab01-03

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

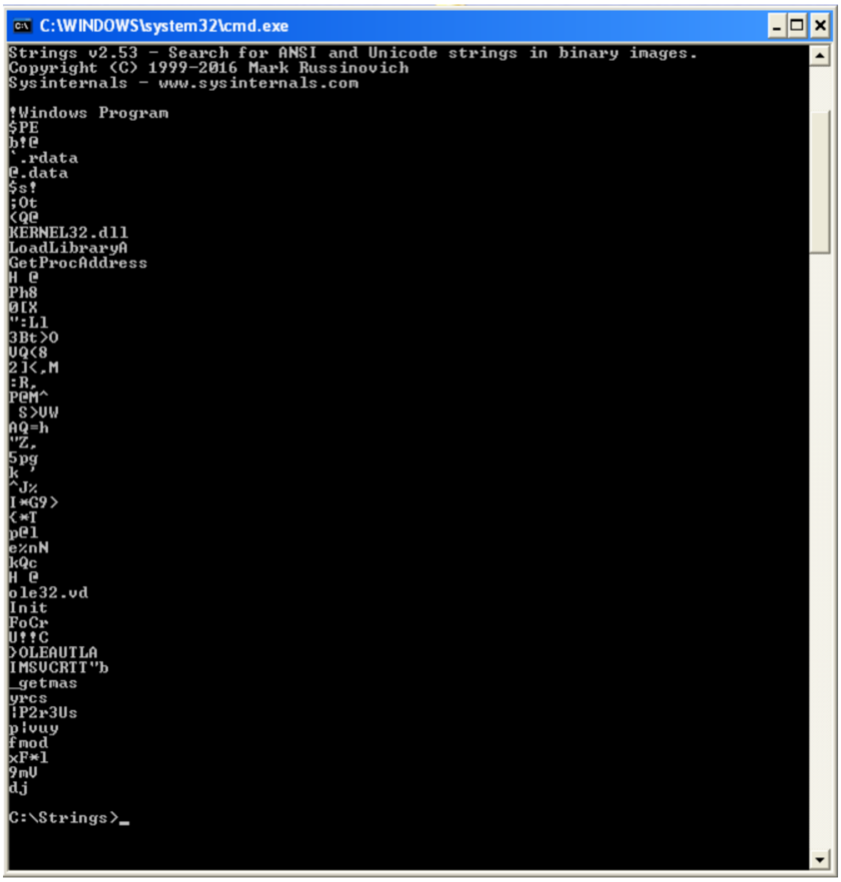
☑ Stay on top

PI	Ordinal ^	Hint	Function	Entry Point
C	N/A	0 (0x0000)	LoadLibraryA	Not Bound
C	N/A	0 (0x0000)	GetProcAddress	Not Bound

E	Ordinal ^	Hint	Function	Entry Point
C	1 (0x0001)	0 (0x0000)	ActivateActCtx	0x0000A6E4
C	2 (0x0002)	1 (0x0001)	AddAtomA	0x0003558D
C	3 (0x0003)	2 (0x0002)	AddAtomW	0x00032761
C	4 (0x0004)	3 (0x0003)	AddConsoleAliasA	0x00072B67
C	5 (0x0005)	4 (0x0004)	AddConsoleAliasW	0x00072B29
C	6 (0x0006)	5 (0x0005)	AddLocalAlternateComputerNameA	0x000599B2
C	7 (0x0007)	6 (0x0006)	AddLocalAlternateComputerNameW	0x00059896
C	8 (0x0008)	7 (0x0007)	AddRefActCtx	0x0002AF69
C	9 (0x0009)	8 (0x0008)	AddVectoredExceptionHandler	NTDLL.RtlAddVectoredExceptionHandler

^	Module	File Time Stamp	Link Time Stamp	File Size	Attr.	Link Checksum	Real Checksum	CPU	Subsystem	Symbols	Preferred Base	Actual Base	Virtual Size	Load Order	File Ver	Product Ver	Image Ver	Linker Ver	OS Ver	Sub
□	KERNEL32.DLL	03/12/2014 2:48a	03/12/2014 2:48a	993,280	A	0x000F63D5	0x000F63D5	x86	Console	CV	0x7C800000	Unknown	0x000F6000	Not Loaded	5.1.2600.6532	5.1.2600.6532	5.1	7.10	5.1	4.0
□	LAB01-03.EXE	03/26/2011 8:54a	12/31/1969 4:00p	4,752	A	0x00000000	0x0000CED2	x86	Console	None	0x00400000	Unknown	0x00006000	Not Loaded	N/A	N/A	0.0	0.0	4.0	4.0
□	NTDLL.DLL	12/09/2010 6:15a	12/09/2010 7:15a	718,336	A	0x000B9EE6	0x000B9EE6	x86	Console	CV	0x7C900000	Unknown	0x000B2000	Not Loaded	5.1.2600.6055	5.1.2600.6055	5.1	7.10	5.1	4.1

4. As is still packed, and Strings result below, the only message we know is the function mentioned above. No network hints, and we need to unpack.



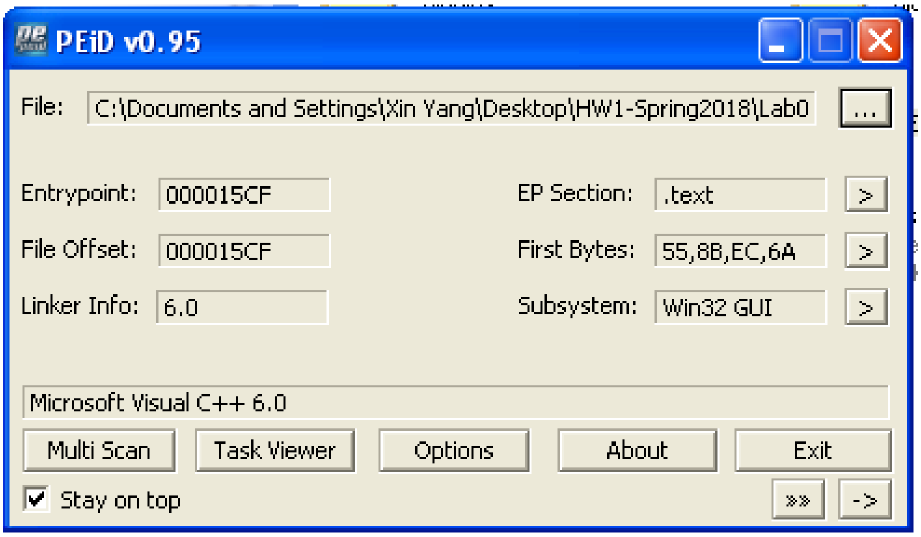
C:\WINDOWS\system32\cmd.exe

```
Strings v2.53 - Search for ANSI and Unicode strings in binary images.
Copyright (C) 1999-2016 Mark Russinovich
Sysinternals - www.sysinternals.com

!Windows Program
$PE
b!@
`.rdata
@.data
$s!
;Ot
<Q@
KERNEL32.dll
LoadLibraryA
GetProcAddress
H @
Ph8
0[X
":Ll
3Bt>O
VQ<8
2]<,M
:R,
P@M^
 S>VW
AQ=h
"Z,
5pg
k '
^J%
I*G9>
<*T
p@l
e%nN
kQc
H @
ole32.vd
Init
FoCr
U!!C
>OLEAUTLA
IMSVCRTT"b
_getmas
yrcs
¦P2r3Us
p¦vuy
fmod
xF*l
9mV
dj

C:\Strings>_
```

Lab01-04.exe:

1. Yes, 54/67 antivirus platforms in virustotal report this as a Trojan, keywords are generic, downloader.

2. The virtual size and raw size looks fine. Also from PEiD we can tell it's unpacked, and with dependency walker we can tell the imports clearly.



PEiD v0.95

File: C:\Documents and Settings\Xin Yang\Desktop\HW1-Spring2018\Lab0

Entrypoint: 000015CF

EP Section: .text

File Offset: 000015CF

First Bytes: 55,8B,EC,6A

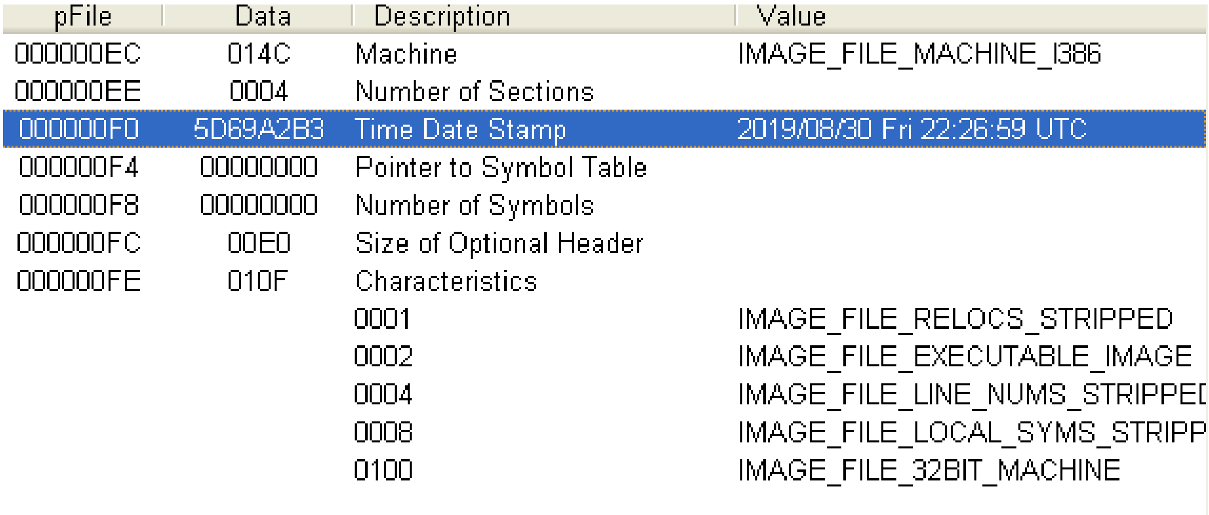
Linker Info: 6.0

Subsystem: Win32 GUI

Microsoft Visual C++ 6.0

☑ Stay on top

3. As PEview showed, it's compiled in 2019/08/30 Fri 22:26:59 UTC, it's in the future so the time is changed by the malware writer.

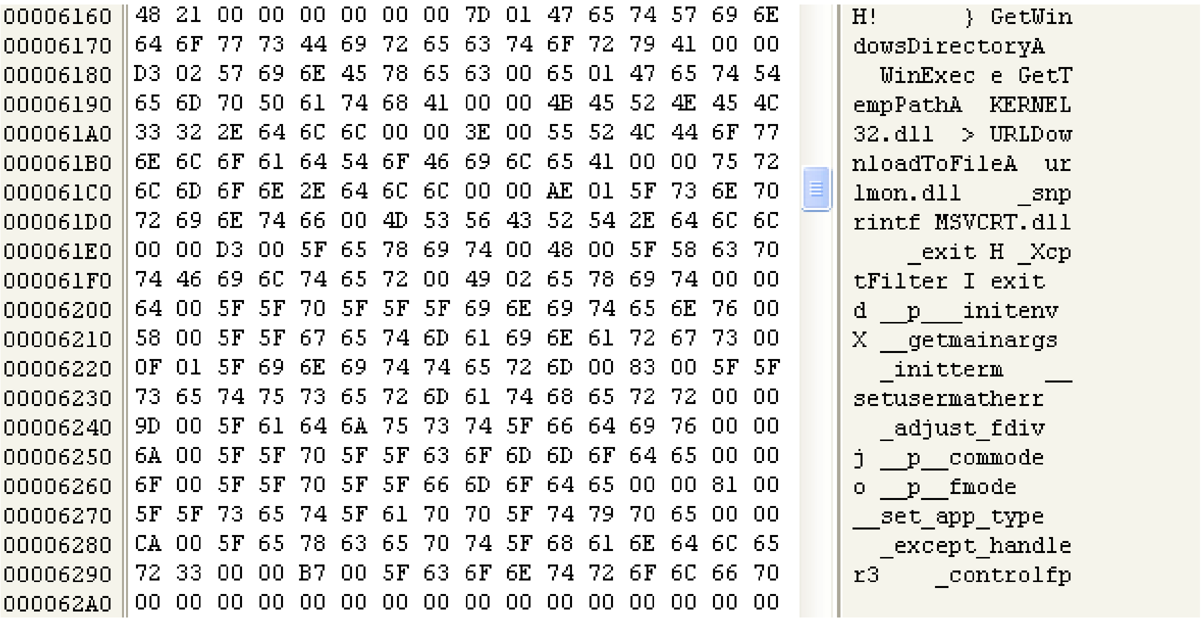


pFile	Data	Description	Value
000000EC	014C	Machine	IMAGE_FILE_MACHINE_I386
000000EE	0004	Number of Sections	
000000F0	5D69A2B3	Time Date Stamp	2019/08/30 Fri 22:26:59 UTC
000000F4	00000000	Pointer to Symbol Table	
000000F8	00000000	Number of Symbols	
000000FC	00E0	Size of Optional Header	
000000FE	010F	Characteristics	
		0001	IMAGE_FILE_RELOCS_STRIPPED
		0002	IMAGE_FILE_EXECUTABLE_IMAGE
		0004	IMAGE_FILE_LINE_NUMS_STRIPPEI
		0008	IMAGE_FILE_LOCAL_SYMS_STRIPP
		0100	IMAGE_FILE_32BIT_MACHINE

4. There’re LoadLibraryA, CreateFileA, FindResourceA, GetModuleHandleA, GetWindowsDirectoryA, MoveFileA, GetTempPathA in kernel32.dll, and LookupPrivilegeValueA, AdjustTokenPrivileges in advapi32.dll. We can infer that this malware is going to import some wierd libraries and change or download some files, also it would change the permission.

5. By running ‘strings’ command, there’re words like \system32\wupdmgr.exe and \winup.exe and URLDownloadToFileA, this might hint this malware will download or change files in the above directories. Also there’s a URL “http://www.practicalmalwareanalysis.com/updater.exe”, this should be the server which this malware tries to connect to.

6. Using Resource Hacker, the only resource in BIN is 101:1033, and the contents are all hex. With the hex reader at the right part, we can see there are contents about the library and imported functions such as KERNEL32.dll, MSVCRT.dll, urlmon.dll and suspicious functions GetWindowsDirectoryA, WinExec, URLDownloadToFileA, which make us think this malware is going to download some files and execute, also it may replace some dll files.



```
00006160  48 21 00 00 00 00 00 00 7D 01 47 65 74 57 69 6E   H!      } GetWin
00006170  64 6F 77 73 44 69 72 65 63 74 6F 72 79 41 00 00   dowsDirectoryA
00006180  D3 02 57 69 6E 45 78 65 63 00 65 01 47 65 74 54     WinExec e GetT
00006190  65 6D 70 50 61 74 68 41 00 00 4B 45 52 4E 45 4C   empPathA  KERNEL
000061A0  33 32 2E 64 6C 6C 00 00 3E 00 55 52 4C 44 6F 77   32.dll  > URLDow
000061B0  6E 6C 6F 61 64 54 6F 46 69 6C 65 41 00 00 75 72   nloadToFileA  ur
000061C0  6C 6D 6F 6E 2E 64 6C 6C 00 00 AE 01 5F 73 6E 70   lmon.dll    _snp
000061D0  72 69 6E 74 66 00 4D 53 56 43 52 54 2E 64 6C 6C   rintf MSVCRT.dll
000061E0  00 00 D3 00 5F 65 78 69 74 00 48 00 5F 58 63 70       _exit H _Xcp
000061F0  74 46 69 6C 74 65 72 00 49 02 65 78 69 74 00 00   tFilter I exit
00006200  64 00 5F 5F 70 5F 5F 5F 69 6E 69 74 65 6E 76 00   d __p___initenv
00006210  58 00 5F 5F 67 65 74 6D 61 69 6E 61 72 67 73 00   X __getmainargs
00006220  0F 01 5F 69 6E 69 74 74 65 72 6D 00 83 00 5F 5F     _initterm   __
00006230  73 65 74 75 73 65 72 6D 61 74 68 65 72 72 00 00   setusermatherr
00006240  9D 00 5F 61 64 6A 75 73 74 5F 66 64 69 76 00 00     _adjust_fdiv
00006250  6A 00 5F 5F 70 5F 5F 63 6F 6D 6D 6F 64 65 00 00   j __p__commode
00006260  6F 00 5F 5F 70 5F 5F 66 6D 6F 64 65 00 00 81 00   o __p__fmode
00006270  5F 5F 73 65 74 5F 61 70 70 5F 74 79 70 65 00 00   __set_app_type
00006280  CA 00 5F 65 78 63 65 70 74 5F 68 61 6E 64 6C 65     _except_handle
00006290  72 33 00 00 B7 00 5F 63 6F 6E 74 72 6F 6C 66 70   r3    _controlfp
000062A0  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```