Practical Malware Analysis Lab 3-1

Questions

1. What are this malware's imports and strings?
2. What are the malware's host based indicators?
3. Are there any useful network-based signatures for this malware If so, what are they?

Question 1

When putting the exe Lab03-01.exe into Dependencies it only showed one import kernel32.dll and the function ExitProcess. The strings gave us more information about what this malware does.

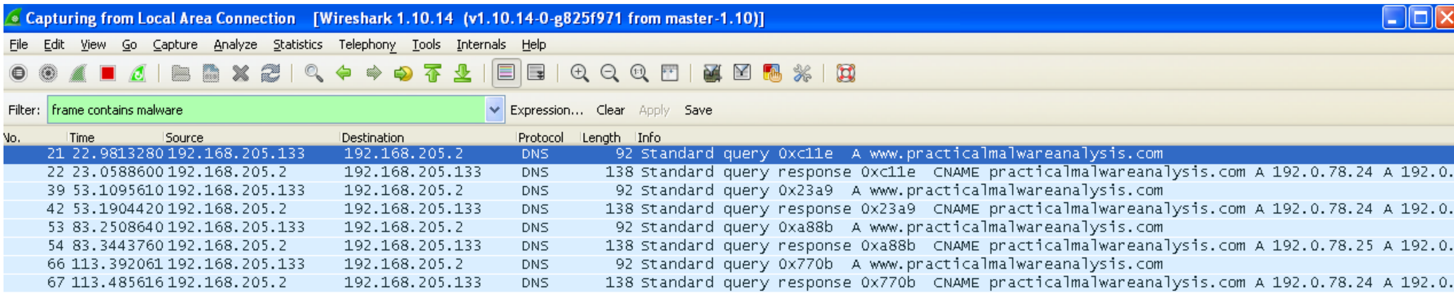
Results from using the program binText

StubPath
SOFTWARE\Classes\http\shell\open\commandV
Software\Microsoft\Active Setup\Installed Components\
test
www.practicalmalwareanalysis.com
Admin
?503
200
advpack
CONNECT %s:%i HTTP/1.0
VideoDriver
WinVMX32-
Vmx32to64.exe
SOFTWARE\Classes\http\shell\open\commandV
Software\Microsoft\Active Setup\Installed Components\
SOFTWARE\Microsoft\Windows\CurrentVersion\Run

Dynamic Analysis

Wireshark Results

There is a DNS request to the website www.practicalmalwareanalysis.com

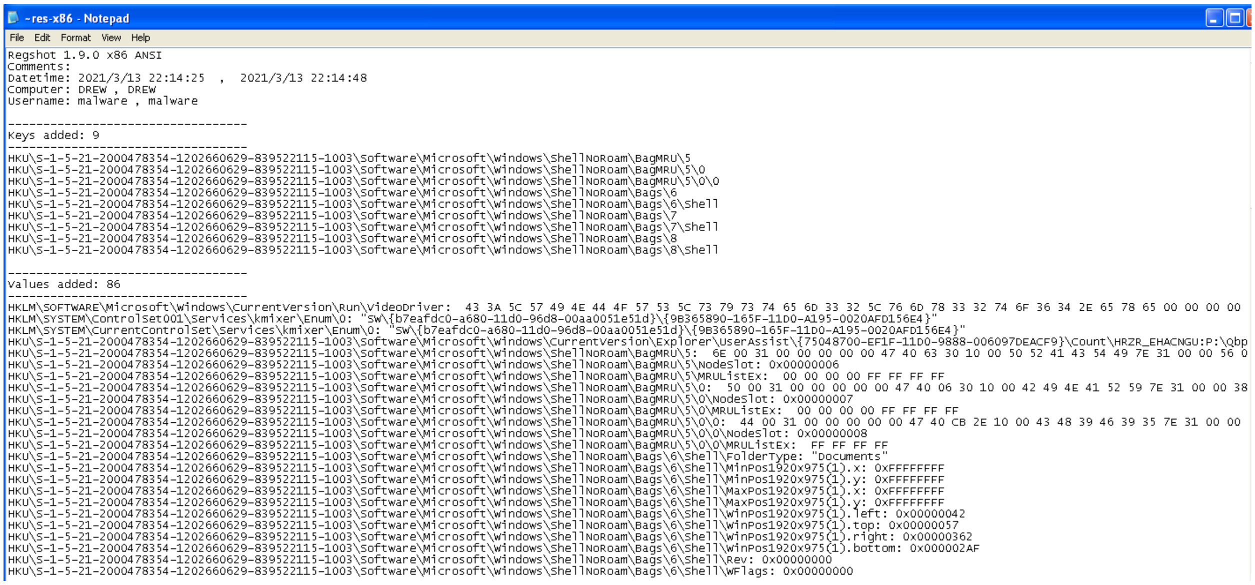

Capturing from Local Area Connection [Wireshark 1.10.14 (v1.10.14-0-g825f971 from master-1.10)]
File Edit View Go Capture Analyze Statistics Telephony Tools Internals Help
Expression... Clear Apply Save

Filter: frame contains malware

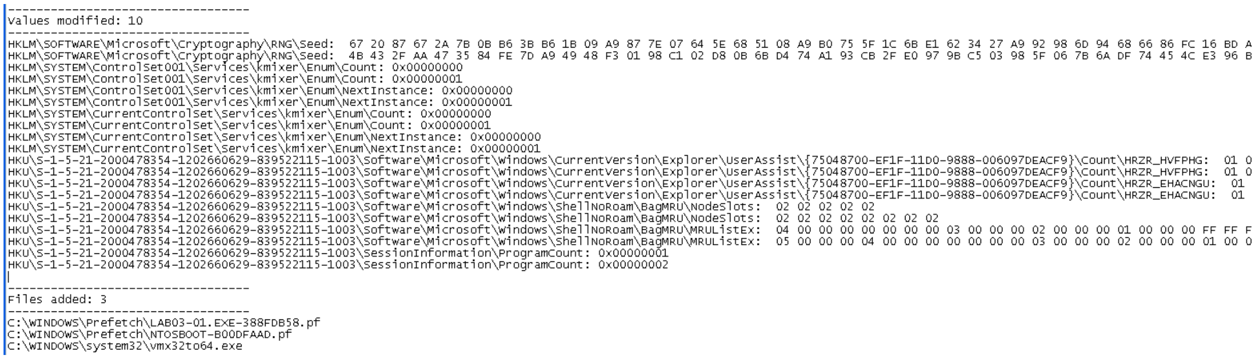
```
No.  Time        Source          Destination     Protocol Length Info
  21 22.9813280 192.168.205.133 192.168.205.2   DNS       92 Standard query 0xc11e  A www.practicalmalwareanalysis.com
  22 23.0588600 192.168.205.2   192.168.205.133 DNS      138 Standard query response 0xc11e  CNAME practicalmalwareanalysis.com A 192.0.78.24 A 192.0.
  39 53.1095610 192.168.205.133 192.168.205.2   DNS       92 Standard query 0x23a9  A www.practicalmalwareanalysis.com
  42 53.1904420 192.168.205.2   192.168.205.133 DNS      138 Standard query response 0x23a9  CNAME practicalmalwareanalysis.com A 192.0.78.24 A 192.0.
  53 83.2508640 192.168.205.133 192.168.205.2   DNS       92 Standard query 0xa88b  A www.practicalmalwareanalysis.com
  54 83.3443760 192.168.205.2   192.168.205.133 DNS      138 Standard query response 0xa88b  CNAME practicalmalwareanalysis.com A 192.0.78.25 A 192.0.
  66 113.392061 192.168.205.133 192.168.205.2   DNS       92 Standard query 0x770b  A www.practicalmalwareanalysis.com
  67 113.485616 192.168.205.2   192.168.205.133 DNS      138 Standard query response 0x770b  CNAME practicalmalwareanalysis.com A 192.0.78.24 A 192.0.
```

Regshot Results

The malware creates the file C:\WINDOWS\system32\vmx32to64.exe.



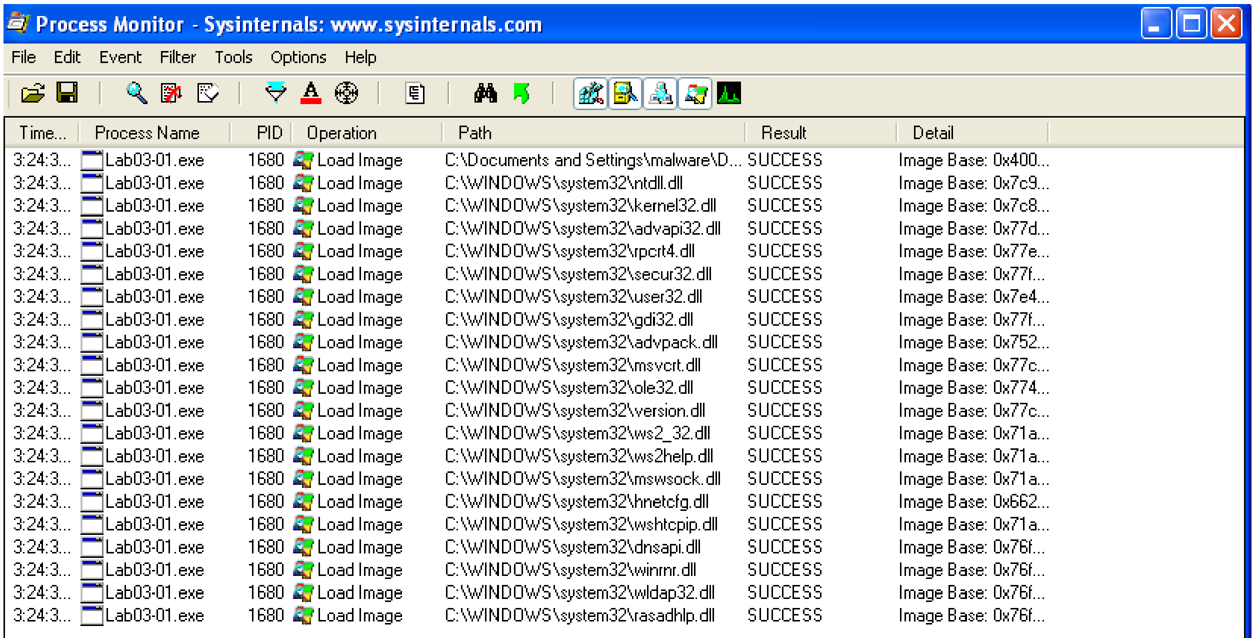
```
Regshot 1.9.0 x86 ANSI
Comments:
Datetime: 2021/3/13 22:14:25  ,  2021/3/13 22:14:48
Computer: DREW , DREW
Username: malware , malware

----------------------------------
Keys added: 9
----------------------------------
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\5
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\5\0
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\5\0\0
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\6
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\6\Shell
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\7
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\7\Shell
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\8
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\8\Shell

----------------------------------
Values added: 86
----------------------------------
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver:  43 3A 5C 57 49 4E 44 4F 57 53 5C 73 79 73 74 65 6D 33 32 5C 76 6D 78 33 32 74 6F 36 34 2E 65 78 65 00 00 00 00
HKLM\SYSTEM\ControlSet001\Services\kmixer\Enum\0: "SW\{b7eafdc0-a680-11d0-96d8-00aa0051e51d}\{9B365890-165F-11D0-A195-0020AFD156E4}"
HKLM\SYSTEM\CurrentControlSet\Services\kmixer\Enum\0: "SW\{b7eafdc0-a680-11d0-96d8-00aa0051e51d}\{9B365890-165F-11D0-A195-0020AFD156E4}"
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU:P:\Qbp
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\5:  6E 00 31 00 00 00 00 00 47 40 63 30 10 00 50 52 41 43 54 49 7E 31 00 00 56 0
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\5\NodeSlot: 0x00000006
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\5\MRUListEx:  00 00 00 00 FF FF FF FF
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\5\0:  50 00 31 00 00 00 00 00 47 40 06 30 10 00 42 49 4E 41 52 59 7E 31 00 00 38
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\5\0\NodeSlot: 0x00000007
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\5\0\MRUListEx:  00 00 00 00 FF FF FF FF
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\5\0\0:  44 00 31 00 00 00 00 00 47 40 CB 2E 10 00 43 48 39 46 39 35 7E 31 00 00
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\5\0\0\NodeSlot: 0x00000008
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\5\0\0\MRUListEx:  FF FF FF FF
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\6\Shell\FolderType: "Documents"
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\6\Shell\MinPos1920x975(1).x: 0xFFFFFFFF
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\6\Shell\MinPos1920x975(1).y: 0xFFFFFFFF
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\6\Shell\MaxPos1920x975(1).x: 0xFFFFFFFF
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\6\Shell\MaxPos1920x975(1).y: 0xFFFFFFFF
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\6\Shell\WinPos1920x975(1).left: 0x00000042
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\6\Shell\WinPos1920x975(1).top: 0x00000057
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\6\Shell\WinPos1920x975(1).right: 0x00000362
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\6\Shell\WinPos1920x975(1).bottom: 0x000002AF
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\6\Shell\Rev: 0x00000000
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\Bags\6\Shell\WFlags: 0x00000000
```



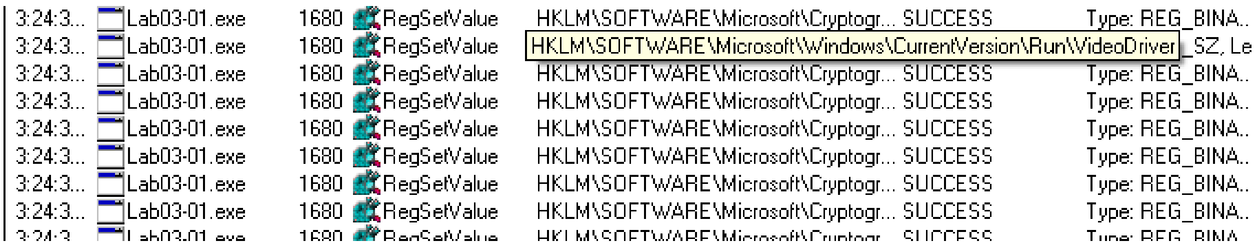
```
----------------------------------
Values modified: 10
----------------------------------
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  67 20 87 67 2A 7B 0B B6 3B B6 1B 09 A9 87 7E 07 64 5E 68 51 08 A9 B0 75 5F 1C 6B E1 62 34 27 A9 92 98 6D 94 68 66 86 FC 16 BD A
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  4B 43 2F AA 47 35 84 FE 7D A9 49 48 F3 01 98 C1 02 D8 0B 6B D4 74 A1 93 CB 2F E0 97 9B C5 03 98 5F 06 7B 6A DF 74 45 4C E3 96 B
HKLM\SYSTEM\ControlSet001\Services\kmixer\Enum\Count: 0x00000000
HKLM\SYSTEM\ControlSet001\Services\kmixer\Enum\Count: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\kmixer\Enum\NextInstance: 0x00000000
HKLM\SYSTEM\ControlSet001\Services\kmixer\Enum\NextInstance: 0x00000001
HKLM\SYSTEM\CurrentControlSet\Services\kmixer\Enum\Count: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Services\kmixer\Enum\Count: 0x00000001
HKLM\SYSTEM\CurrentControlSet\Services\kmixer\Enum\NextInstance: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Services\kmixer\Enum\NextInstance: 0x00000001
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_HVFPHG:  01 0
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_HVFPHG:  01 0
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU:  01
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR_EHACNGU:  01
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\NodeSlots:  02 02 02 02 02
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\NodeSlots:  02 02 02 02 02 02 02 02
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\MRUListEx:  04 00 00 00 00 00 00 00 03 00 00 00 02 00 00 00 01 00 00 00 FF FF F
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\Software\Microsoft\Windows\ShellNoRoam\BagMRU\MRUListEx:  05 00 00 00 04 00 00 00 00 00 00 00 03 00 00 00 02 00 00 00 01 00 0
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\SessionInformation\ProgramCount: 0x00000001
HKU\S-1-5-21-2000478354-1202660629-839522115-1003\SessionInformation\ProgramCount: 0x00000002

----------------------------------
Files added: 3
----------------------------------
C:\WINDOWS\Prefetch\LAB03-01.EXE-388FDB58.pf
C:\WINDOWS\Prefetch\NTOSBOOT-B00DFAAD.pf
C:\WINDOWS\system32\vmx32to64.exe
```

Process Monitor Results

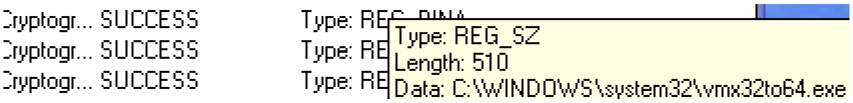
By filtering Process Monitor to the operation “Load Image” we can see what dlls the malware imports. It also creates the registry entry of VideoDriver.


Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time...	Process Name	PID	Operation	Path	Result	Detail
3:24:3...	Lab03-01.exe	1680	Load Image	C:\Documents and Settings\malware\D...	SUCCESS	Image Base: 0x400...
3:24:3...	Lab03-01.exe	1680	Load Image	C:\WINDOWS\system32\ntdll.dll	SUCCESS	Image Base: 0x7c9...
3:24:3...	Lab03-01.exe	1680	Load Image	C:\WINDOWS\system32\kernel32.dll	SUCCESS	Image Base: 0x7c8...
3:24:3...	Lab03-01.exe	1680	Load Image	C:\WINDOWS\system32\advapi32.dll	SUCCESS	Image Base: 0x77d...
3:24:3...	Lab03-01.exe	1680	Load Image	C:\WINDOWS\system32\rpcrt4.dll	SUCCESS	Image Base: 0x77e...
3:24:3...	Lab03-01.exe	1680	Load Image	C:\WINDOWS\system32\secur32.dll	SUCCESS	Image Base: 0x77f...
3:24:3...	Lab03-01.exe	1680	Load Image	C:\WINDOWS\system32\user32.dll	SUCCESS	Image Base: 0x7e4...
3:24:3...	Lab03-01.exe	1680	Load Image	C:\WINDOWS\system32\gdi32.dll	SUCCESS	Image Base: 0x77f...
3:24:3...	Lab03-01.exe	1680	Load Image	C:\WINDOWS\system32\advpack.dll	SUCCESS	Image Base: 0x752...
3:24:3...	Lab03-01.exe	1680	Load Image	C:\WINDOWS\system32\msvcrt.dll	SUCCESS	Image Base: 0x77c...
3:24:3...	Lab03-01.exe	1680	Load Image	C:\WINDOWS\system32\ole32.dll	SUCCESS	Image Base: 0x774...
3:24:3...	Lab03-01.exe	1680	Load Image	C:\WINDOWS\system32\version.dll	SUCCESS	Image Base: 0x77c...
3:24:3...	Lab03-01.exe	1680	Load Image	C:\WINDOWS\system32\ws2_32.dll	SUCCESS	Image Base: 0x71a...
3:24:3...	Lab03-01.exe	1680	Load Image	C:\WINDOWS\system32\ws2help.dll	SUCCESS	Image Base: 0x71a...
3:24:3...	Lab03-01.exe	1680	Load Image	C:\WINDOWS\system32\mswsock.dll	SUCCESS	Image Base: 0x71a...
3:24:3...	Lab03-01.exe	1680	Load Image	C:\WINDOWS\system32\hnetcfg.dll	SUCCESS	Image Base: 0x662...
3:24:3...	Lab03-01.exe	1680	Load Image	C:\WINDOWS\system32\wshtcpip.dll	SUCCESS	Image Base: 0x71a...
3:24:3...	Lab03-01.exe	1680	Load Image	C:\WINDOWS\system32\dnsapi.dll	SUCCESS	Image Base: 0x76f...
3:24:3...	Lab03-01.exe	1680	Load Image	C:\WINDOWS\system32\winrnr.dll	SUCCESS	Image Base: 0x76f...
3:24:3...	Lab03-01.exe	1680	Load Image	C:\WINDOWS\system32\wldap32.dll	SUCCESS	Image Base: 0x76f...
3:24:3...	Lab03-01.exe	1680	Load Image	C:\WINDOWS\system32\rasadhlp.dll	SUCCESS	Image Base: 0x76f...



```
3:24:3...  Lab03-01.exe  1680  RegSetValue  HKLM\SOFTWARE\Microsoft\Cryptogr... SUCCESS      Type: REG_BINA...
3:24:3...  Lab03-01.exe  1680  RegSetValue  HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run\VideoDriver _SZ, Le
3:24:3...  Lab03-01.exe  1680  RegSetValue  HKLM\SOFTWARE\Microsoft\Cryptogr... SUCCESS      Type: REG_BINA...
3:24:3...  Lab03-01.exe  1680  RegSetValue  HKLM\SOFTWARE\Microsoft\Cryptogr... SUCCESS      Type: REG_BINA...
3:24:3...  Lab03-01.exe  1680  RegSetValue  HKLM\SOFTWARE\Microsoft\Cryptogr... SUCCESS      Type: REG_BINA...
3:24:3...  Lab03-01.exe  1680  RegSetValue  HKLM\SOFTWARE\Microsoft\Cryptogr... SUCCESS      Type: REG_BINA...
3:24:3...  Lab03-01.exe  1680  RegSetValue  HKLM\SOFTWARE\Microsoft\Cryptogr... SUCCESS      Type: REG_BINA...
3:24:3...  Lab03-01.exe  1680  RegSetValue  HKLM\SOFTWARE\Microsoft\Cryptogr... SUCCESS      Type: REG_BINA...
3:24:3...  Lab03-01.exe  1680  RegSetValue  HKLM\SOFTWARE\Microsoft\Cryptogr... SUCCESS      Type: REG_BINA...
```



```
Cryptogr... SUCCESS          Type: REG_BINA...
Cryptogr... SUCCESS          Type: RE
Cryptogr... SUCCESS          Type: RE

Type: REG_SZ
Length: 510
Data: C:\WINDOWS\system32\vmx32to64.exe
```

Question 1

When putting the exe Lab03-01.exe into Dependencies it only showed one import kernel32.dll and the function ExitProcess, but by running the malware and using procmon we can see it imports various dlls.

Question 2

Some host based indicators include the exe C:\Windows\system32\Vmx32to64.exe , and the registry entry of VideoDriver.

Question 3

Traffic to the website www.practicalmalwareanalysis.com