Computer Science 491/691
Malware Analysis
Homework 2

Assigned: February 16, 2019
Due: February 25, 2019

Submitted by
Name: Sai Sasaank Srivatsa Pallerla
ID: HG13015

How to turn this in for grading: You can edit your answers right into this file. Email it to the TAs as (will be) described in class. Make sure your name appears in the body of the document. Send your document to us with a name of the form LastnameFirstname.HW1.docx. You are free to use Open Office or Word, as you see fit.

Download and extract hw2.7z on a virtual machine. The password to the zip file is "infected", without the quotes. The file contains hw2.infected, which is a live malware sample.

Once you have downloaded the malware, use the network settings in VirtualBox to disconnect your VM from the internet. **You should only run the malware while your VM is not attached to the network!**

Hint: Chapter 3 of your Practical Malware Analysis textbook is a great resource, and other parts of your textbook may be helpful as well!

Part 1: Basic Static Analysis

Analyze the file at rest and answer the following questions:

1) What is the MD5 of hw2.infected?
MD5: 99392a1a364703ac314a46c410184c84

2) Select five of the imports from hw2.infected that you believe may be suspicious. For each import, describe what it does and why you selected it.

a. VirtualAlloc: This a memory-allocation function that allots memory to a remote function. Malware uses this import function as a part of process injection, given the behavior of this import and other imports functions, this import is suspicious.

b. CreateToolhelp32Snapshot: Creates snapshot of processes, threads and heaps. Mostly used in code that iterates through processes and threads. This enables the malware to create a list processes and threads, referred as snapshot. This function with the help of Process32Next/Process32First

c. Process32Next/Process32First: This enumerates processes with the help of another import function CreateToolhelp32Snapshot to find a suitable process and inject itself into it. This import with the combination VirtualAlloc helps in process injection, thus suspicious.

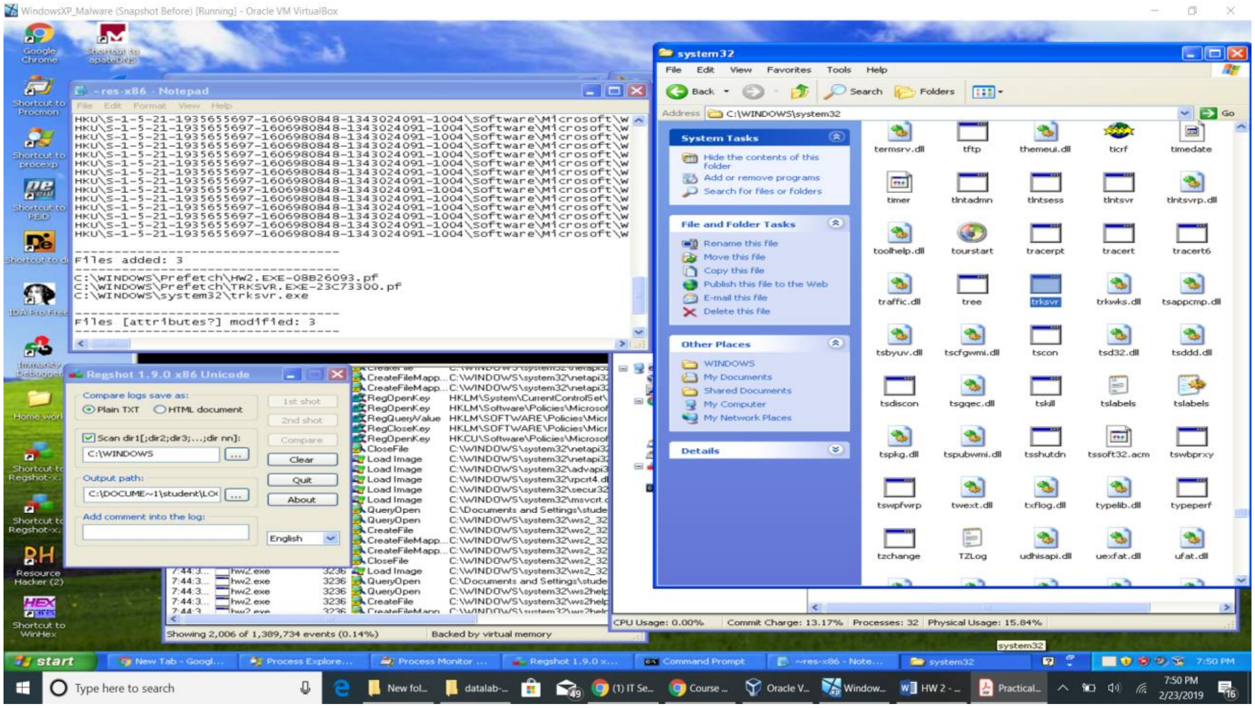
d. RegOpenKey: Opens a handle to a registry key so that it can be read and modified. Registry key contains operating system and application setting information, hence helps achieve persistence on host. All these features are required by a malware to find its way into the system, making this import function suspicious.

e. WSAStartup: Initializes low level network functionalities to make use of internet and avoid detection at the same time. And this malware makes use of network functionalities making this import function suspicious.

Part 2: Basic Dynamic Analyis

Ensure that your VM is disconnected from the internet. Rename hw2.infected to hw2.exe and run it. Answer the following questions.

3) Where does the malware copy itself to? Describe how you got your answer.
The malware copies itself into C:\WINDOWS\System32
To get the location I ran Regshot and took shots before and after running the malware, while comparing it's clear that a file (malware has been added) and this can be seen in the “Files added” section.


WindowsXP_Malware (Snapshot Before) [Running] - Oracle VM VirtualBox
~res-x86 - Notepad
File Edit Format View Help
Regshot 1.9.0 x86 Unicode
system32
File Edit View Favorites Tools Help
Back Search Folders
Address C:\WINDOWS\system32
System Tasks
File and Folder Tasks
Other Places
Details
termsrv.dll
tftp
themeui.dll
ticrf
timedate
trkwks.dll
trksvr
tracert
tsshutdn
start

```
HKU\S-1-5-21-1935655697-1606980848-1343024091-1004\Software\Microsoft\W
HKU\S-1-5-21-1935655697-1606980848-1343024091-1004\Software\Microsoft\W
HKU\S-1-5-21-1935655697-1606980848-1343024091-1004\Software\Microsoft\W
HKU\S-1-5-21-1935655697-1606980848-1343024091-1004\Software\Microsoft\W
HKU\S-1-5-21-1935655697-1606980848-1343024091-1004\Software\Microsoft\W
HKU\S-1-5-21-1935655697-1606980848-1343024091-1004\Software\Microsoft\W
HKU\S-1-5-21-1935655697-1606980848-1343024091-1004\Software\Microsoft\W
HKU\S-1-5-21-1935655697-1606980848-1343024091-1004\Software\Microsoft\W
HKU\S-1-5-21-1935655697-1606980848-1343024091-1004\Software\Microsoft\W
HKU\S-1-5-21-1935655697-1606980848-1343024091-1004\Software\Microsoft\W
HKU\S-1-5-21-1935655697-1606980848-1343024091-1004\Software\Microsoft\W
HKU\S-1-5-21-1935655697-1606980848-1343024091-1004\Software\Microsoft\W
HKU\S-1-5-21-1935655697-1606980848-1343024091-1004\Software\Microsoft\W
HKU\S-1-5-21-1935655697-1606980848-1343024091-1004\Software\Microsoft\W

----------------------------------
Files added: 3
----------------------------------
C:\WINDOWS\Prefetch\HW2.EXE-08B26093.pf
C:\WINDOWS\Prefetch\TRKSVR.EXE-23C73300.pf
C:\WINDOWS\system32\trksvr.exe

----------------------------------
Files [attributes?] modified: 3
----------------------------------
```

Compare logs save as: ● Plain TXT ○ HTML document
☑ Scan dir1[;dir2;dir3;...;dir nn]: C:\WINDOWS
Output path: C:\DOCUME~1\student\LO
Add comment into the log:
English

```
CreateFileMapp... C:\WINDOWS\system32\netapi32
CreateFileMapp... C:\WINDOWS\system32\netapi32
RegOpenKey        HKLM\System\CurrentControlSet\
RegOpenKey        HKLM\Software\Policies\Microsof
RegQueryValue     HKLM\SOFTWARE\Policies\Micr
RegCloseKey       HKLM\SOFTWARE\Policies\Micr
RegOpenKey        HKCU\Software\Policies\Microsof
CloseFile         C:\WINDOWS\system32\netapi32
Load Image        C:\WINDOWS\system32\netapi32
Load Image        C:\WINDOWS\system32\advapi3
Load Image        C:\WINDOWS\system32\rpcrt4.dl
Load Image        C:\WINDOWS\system32\secur32
Load Image        C:\WINDOWS\system32\msvcrt.d
QueryOpen         C:\Documents and Settings\stude
QueryOpen         C:\WINDOWS\system32\ws2_32
CreateFile        C:\WINDOWS\system32\ws2_32
CreateFileMapp... C:\WINDOWS\system32\ws2_32
CreateFileMapp... C:\WINDOWS\system32\ws2_32
CloseFile         C:\WINDOWS\system32\ws2_32
7:44:3...  hw2.exe  3236  Load Image   C:\WINDOWS\system32\ws2_32
7:44:3...  hw2.exe  3236  QueryOpen    C:\Documents and Settings\stude
7:44:3...  hw2.exe  3236  QueryOpen    C:\WINDOWS\system32\ws2help
7:44:3...  hw2.exe  3236  CreateFile   C:\WINDOWS\system32\ws2help
Showing 2,006 of 1,389,734 events (0.14%)    Backed by virtual memory
```

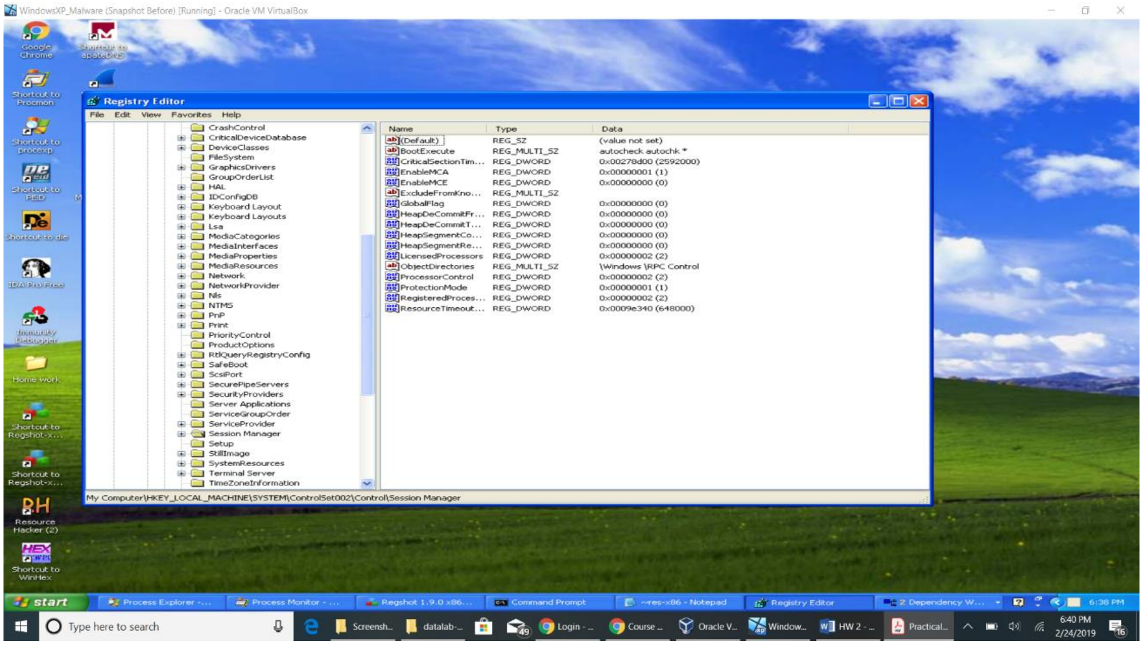
CPU Usage: 0.00% Commit Charge: 13.17% Processes: 32 Physical Usage: 15.84%

4) The malware installs itself as a service to gain persistence. What is the name of the service that it installs itself as? Provide both the <u>name</u> and <u>value</u> of the registry key that ensures that the malware is run as a service when the infected computer boots. Describe how you got your answer.

Name of the service that the malware installs itself as is Trksvr

This service can be found using the Registry key that have the keyword “service” in them. “HKEY_LOCAL_MACHINE/System/ControlSet001/Services/Trksvr”

For a service to start on boot it should have key which goes by the name “BootExecute” with value “autocheck autochk*” This can be found using the registry key “HKEY_LOCAL_MACHINE/System/ControlSet002/Control/SessionManager”


WindowsXP_Malware (Snapshot Before) [Running] - Oracle VM VirtualBox
Registry Editor
File
Edit
View
Favorites
Help

```
CrashControl
CriticalDeviceDatabase
DeviceClasses
FileSystem
GraphicsDrivers
GroupOrderList
HAL
IDConfigDB
Keyboard Layout
Keyboard Layouts
Lsa
MediaCategories
MediaInterfaces
MediaProperties
MediaResources
Network
NetworkProvider
Nls
NTMS
PnP
Print
PriorityControl
ProductOptions
RtlQueryRegistryConfig
SafeBoot
ScsiPort
SecurePipeServers
SecurityProviders
Server Applications
ServiceGroupOrder
ServiceProvider
Session Manager
Setup
StillImage
SystemResources
Terminal Server
TimeZoneInformation
```

Name	Type	Data
(Default)	REG_SZ	(value not set)
BootExecute	REG_MULTI_SZ	autocheck autochk *
CriticalSectionTim...	REG_DWORD	0x00278d00 (2592000)
EnableMCA	REG_DWORD	0x00000001 (1)
EnableMCE	REG_DWORD	0x00000000 (0)
ExcludeFromKno...	REG_MULTI_SZ	
GlobalFlag	REG_DWORD	0x00000000 (0)
HeapDeCommitFr...	REG_DWORD	0x00000000 (0)
HeapDeCommitT...	REG_DWORD	0x00000000 (0)
HeapSegmentCo...	REG_DWORD	0x00000000 (0)
HeapSegmentRe...	REG_DWORD	0x00000000 (0)
LicensedProcessors	REG_DWORD	0x00000002 (2)
ObjectDirectories	REG_MULTI_SZ	\Windows \RPC Control
ProcessorControl	REG_DWORD	0x00000002 (2)
ProtectionMode	REG_DWORD	0x00000001 (1)
RegisteredProces...	REG_DWORD	0x00000002 (2)
ResourceTimeout...	REG_DWORD	0x0009e340 (648000)

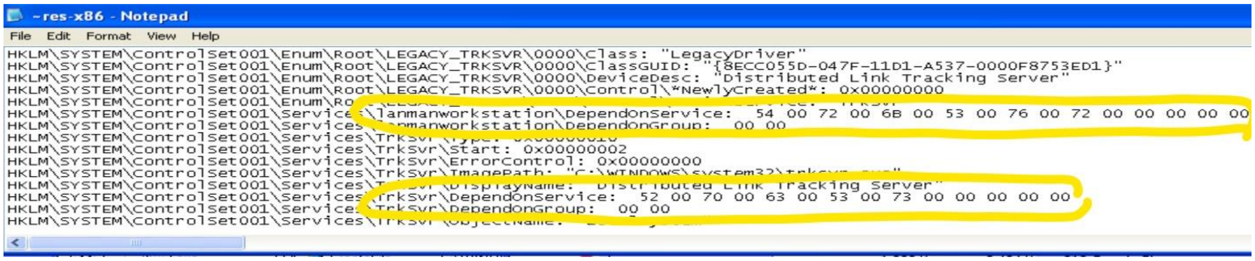
My Computer\HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Control\Session Manager

5) What is a Windows Service Dependency? Which service is the malware dependent upon? Which service depends upon the malware? Describe how you got your answers.

Windows Service Dependency: This allows apps to call into platform-specific functionality from shared code. This functionality enables apps to do anything that a native app can do. It is also a service locator. In practice, an interface is defined, and it finds the correct implementation of that interface from the various platform projects.

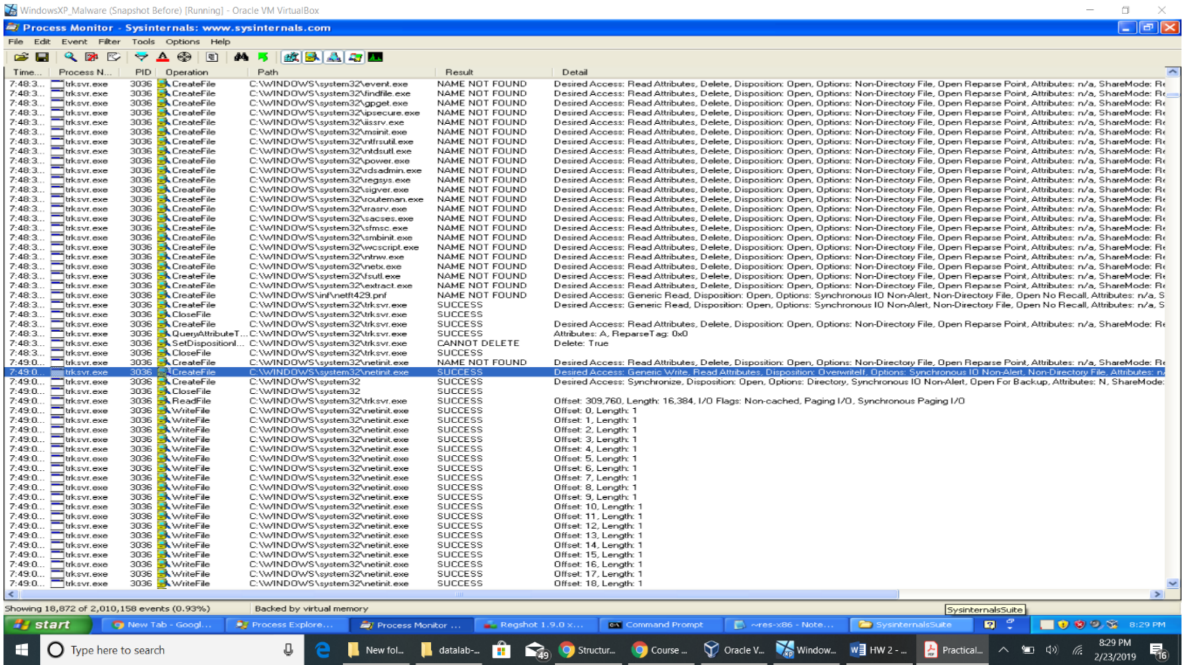
Malware is dependent on a service “RpcSs”, this can be found from the registry key “HKML\SYSTEM\ControlSet001\Services\Trksvr\DependOnService: 52 00 70 00 63 00 53 00 73 00 00 00 00 00”

Service that depends upon malware is “lanmanworkstation”, this can be found from the registry key “HKML\SYSTEM\ControlSet001\Services\lanmanworkstation\DependOnService: 54 00 72 00 6B 00 53 00 76 00 72 00 00 00 00”
Convert from Hex to ASCII to view the names of services.



```
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_TRKSVR\0000\Class: "LegacyDriver"
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_TRKSVR\0000\ClassGUID: "{8ECC055D-047F-11D1-A537-0000F8753ED1}"
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_TRKSVR\0000\DeviceDesc: "Distributed Link Tracking Server"
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_TRKSVR\0000\Control\*NewlyCreated*: 0x00000000
HKLM\SYSTEM\ControlSet001\Enum\Ro
HKLM\SYSTEM\ControlSet001\Service\lanmanworkstation\DependOnService:   54 00 72 00 6B 00 53 00 76 00 72 00 00 00 00 00
HKLM\SYSTEM\ControlSet001\Services\lanmanworkstation\DependOnGroup:   00 00
HKLM\SYSTEM\ControlSet001\Services\TrkSvr\
HKLM\SYSTEM\ControlSet001\Services\TrkSvr\Start: 0x00000002
HKLM\SYSTEM\ControlSet001\Services\TrkSvr\ErrorControl: 0x00000000
HKLM\SYSTEM\ControlSet001\Services\TrkSvr\ImagePath: "C:\WINDOWS\system32\
HKLM\SYSTEM\ControlSet001\Services\TrkSvr\DisplayName: "Distributed Link Tracking Server"
HKLM\SYSTEM\ControlSet001\Services\TrkSvr\DependOnService:   52 00 70 00 63 00 53 00 73 00 00 00 00 00
HKLM\SYSTEM\ControlSet001\Service\TrkSvr\DependOnGroup:   00 00
HKLM\SYSTEM\ControlSet001\Services\TrkSvr\ObjectName:
```

6) After running for a few minutes, the malware calls CreateFile to create the file netinit.exe. Provide a screenshot of ProcMon showing this call to CreateFile.


WindowsXP_Malware (Snapshot Before) [Running] - Oracle VM VirtualBox
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

```
Time...   Process N...  PID   Operation          Path                                     Result            Detail
7:48:3... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32\event.exe            NAME NOT FOUND    Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Point, Attributes: n/a, ShareMode: Re
7:48:3... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32\findfile.exe         NAME NOT FOUND    Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Point, Attributes: n/a, ShareMode: Re
7:48:3... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32\gpget.exe            NAME NOT FOUND    Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Point, Attributes: n/a, ShareMode: Re
7:48:3... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32\ipsecure.exe         NAME NOT FOUND    Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Point, Attributes: n/a, ShareMode: Re
7:48:3... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32\iissrv.exe           NAME NOT FOUND    Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Point, Attributes: n/a, ShareMode: Re
7:48:3... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32\msinit.exe           NAME NOT FOUND    Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Point, Attributes: n/a, ShareMode: Re
7:48:3... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32\ntfrsutil.exe        NAME NOT FOUND    Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Point, Attributes: n/a, ShareMode: Re
7:48:3... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32\ntdsutl.exe          NAME NOT FOUND    Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Point, Attributes: n/a, ShareMode: Re
7:48:3... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32\power.exe            NAME NOT FOUND    Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Point, Attributes: n/a, ShareMode: Re
7:48:3... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32\rdsadmin.exe         NAME NOT FOUND    Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Point, Attributes: n/a, ShareMode: Re
7:48:3... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32\regsys.exe           NAME NOT FOUND    Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Point, Attributes: n/a, ShareMode: Re
7:48:3... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32\sigver.exe           NAME NOT FOUND    Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Point, Attributes: n/a, ShareMode: Re
7:48:3... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32\routeman.exe         NAME NOT FOUND    Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Point, Attributes: n/a, ShareMode: Re
7:48:3... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32\rrasrv.exe           NAME NOT FOUND    Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Point, Attributes: n/a, ShareMode: Re
7:48:3... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32\sacses.exe           NAME NOT FOUND    Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Point, Attributes: n/a, ShareMode: Re
7:48:3... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32\sfmsc.exe            NAME NOT FOUND    Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Point, Attributes: n/a, ShareMode: Re
7:48:3... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32\smbinit.exe          NAME NOT FOUND    Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Point, Attributes: n/a, ShareMode: Re
7:48:3... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32\wcscript.exe         NAME NOT FOUND    Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Point, Attributes: n/a, ShareMode: Re
7:48:3... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32\ntnw.exe             NAME NOT FOUND    Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Point, Attributes: n/a, ShareMode: Re
7:48:3... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32\netx.exe             NAME NOT FOUND    Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Point, Attributes: n/a, ShareMode: Re
7:48:3... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32\fsutl.exe            NAME NOT FOUND    Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Point, Attributes: n/a, ShareMode: Re
7:48:3... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32\extract.exe          NAME NOT FOUND    Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Point, Attributes: n/a, ShareMode: Re
7:48:3... trksvr.exe    3036  CreateFile         C:\WINDOWS\inf\netft429.pnf              NAME NOT FOUND    Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Open No Recall, Attributes: n/a, S
7:48:3... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32\trksvr.exe           SUCCESS           Desired Access: Generic Read, Disposition: Open, Options: Synchronous IO Non-Alert, Non-Directory File, Open No Recall, Attributes: n/a, S
7:48:3... trksvr.exe    3036  CloseFile          C:\WINDOWS\system32\trksvr.exe           SUCCESS
7:48:3... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32\trksvr.exe           SUCCESS           Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Point, Attributes: n/a, ShareMode: Re
7:48:3... trksvr.exe    3036  QueryAttributeT... C:\WINDOWS\system32\trksvr.exe           SUCCESS           Attributes: A, ReparseTag: 0x0
7:48:3... trksvr.exe    3036  SetDispositionI... C:\WINDOWS\system32\trksvr.exe           CANNOT DELETE     Delete: True
7:48:3... trksvr.exe    3036  CloseFile          C:\WINDOWS\system32\trksvr.exe           SUCCESS
7:49:0... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32\netinit.exe          NAME NOT FOUND    Desired Access: Read Attributes, Delete, Disposition: Open, Options: Non-Directory File, Open Reparse Point, Attributes: n/a, ShareMode: Re
7:49:0... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32\netinit.exe          SUCCESS           Desired Access: Generic Write, Read Attributes, Disposition: OverwriteIf, Options: Synchronous IO Non-Alert, Non-Directory File, Attributes: n/
7:49:0... trksvr.exe    3036  CreateFile         C:\WINDOWS\system32                      SUCCESS           Desired Access: Synchronize, Disposition: Open, Options: Directory, Synchronous IO Non-Alert, Open For Backup, Attributes: N, ShareMode:
7:49:0... trksvr.exe    3036  CloseFile          C:\WINDOWS\system32                      SUCCESS
7:49:0... trksvr.exe    3036  ReadFile           C:\WINDOWS\system32\trksvr.exe           SUCCESS           Offset: 309,760, Length: 16,384, I/O Flags: Non-cached, Paging I/O, Synchronous Paging I/O
7:49:0... trksvr.exe    3036  WriteFile          C:\WINDOWS\system32\netinit.exe          SUCCESS           Offset: 0, Length: 1
7:49:0... trksvr.exe    3036  WriteFile          C:\WINDOWS\system32\netinit.exe          SUCCESS           Offset: 1, Length: 1
7:49:0... trksvr.exe    3036  WriteFile          C:\WINDOWS\system32\netinit.exe          SUCCESS           Offset: 2, Length: 1
7:49:0... trksvr.exe    3036  WriteFile          C:\WINDOWS\system32\netinit.exe          SUCCESS           Offset: 3, Length: 1
7:49:0... trksvr.exe    3036  WriteFile          C:\WINDOWS\system32\netinit.exe          SUCCESS           Offset: 4, Length: 1
7:49:0... trksvr.exe    3036  WriteFile          C:\WINDOWS\system32\netinit.exe          SUCCESS           Offset: 5, Length: 1
7:49:0... trksvr.exe    3036  WriteFile          C:\WINDOWS\system32\netinit.exe          SUCCESS           Offset: 6, Length: 1
7:49:0... trksvr.exe    3036  WriteFile          C:\WINDOWS\system32\netinit.exe          SUCCESS           Offset: 7, Length: 1
7:49:0... trksvr.exe    3036  WriteFile          C:\WINDOWS\system32\netinit.exe          SUCCESS           Offset: 8, Length: 1
7:49:0... trksvr.exe    3036  WriteFile          C:\WINDOWS\system32\netinit.exe          SUCCESS           Offset: 9, Length: 1
7:49:0... trksvr.exe    3036  WriteFile          C:\WINDOWS\system32\netinit.exe          SUCCESS           Offset: 10, Length: 1
7:49:0... trksvr.exe    3036  WriteFile          C:\WINDOWS\system32\netinit.exe          SUCCESS           Offset: 11, Length: 1
7:49:0... trksvr.exe    3036  WriteFile          C:\WINDOWS\system32\netinit.exe          SUCCESS           Offset: 12, Length: 1
7:49:0... trksvr.exe    3036  WriteFile          C:\WINDOWS\system32\netinit.exe          SUCCESS           Offset: 13, Length: 1
7:49:0... trksvr.exe    3036  WriteFile          C:\WINDOWS\system32\netinit.exe          SUCCESS           Offset: 14, Length: 1
7:49:0... trksvr.exe    3036  WriteFile          C:\WINDOWS\system32\netinit.exe          SUCCESS           Offset: 15, Length: 1
7:49:0... trksvr.exe    3036  WriteFile          C:\WINDOWS\system32\netinit.exe          SUCCESS           Offset: 16, Length: 1
7:49:0... trksvr.exe    3036  WriteFile          C:\WINDOWS\system32\netinit.exe          SUCCESS           Offset: 17, Length: 1
7:49:0... trksvr.exe    3036  WriteFile          C:\WINDOWS\system32\netinit.exe          SUCCESS           Offset: 18, Length: 1

Showing 18,872 of 2,010,158 events (0.93%)          Backed by virtual memory
```

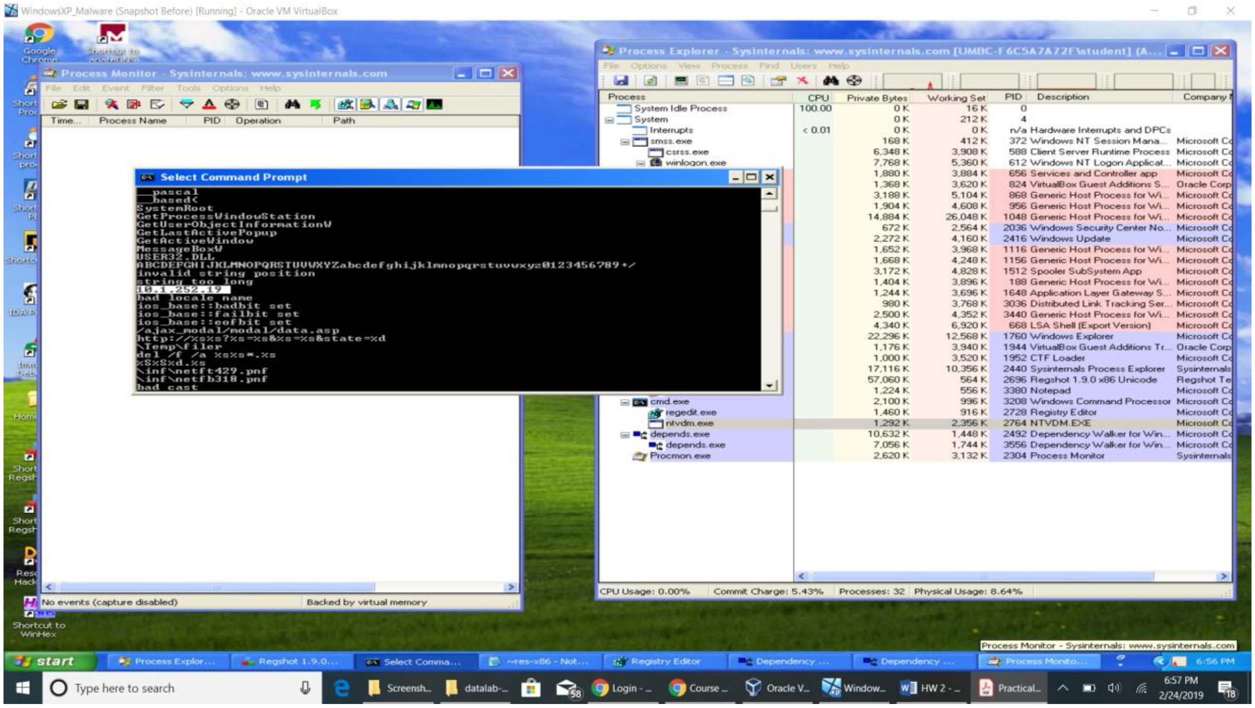
7) What is the full file path of netinit.exe? What is the MD5 of netinit.exe?

Full file path: C:/WINDOWS/System32

MD5: 43e9f09868c0471ab2a42678b8d3c686

8) Investigate the strings of netinit.exe. What IP address is hard-coded into the file?

IP Address: 10.1.252.19


WindowsXP_Malware (Snapshot Before) [Running] - Oracle VM VirtualBox
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help
Time... Process Name PID Operation Path
No events (capture disabled)
Backed by virtual memory
Select Command Prompt
Process Explorer - Sysinternals: www.sysinternals.com [UMBC-F6C5A7A72F\student] (A...
File Options View Process Find Users Help
start
Process Explor...
Regshot 1.9.0...
Select Comma...
~res-x86 - Not...
Registry Editor
Dependency ...
Dependency ...
Process Monito...
6:56 PM
Type here to search
Screensh...
datalab-...
Login - ...
Course ...
Oracle V...
Window...
HW 2 - ...
Practical...
6:57 PM
2/24/2019

```
__pascal
__based(
SystemRoot
GetProcessWindowStation
GetUserObjectInformationW
GetLastActivePopup
GetActiveWindow
MessageBoxW
USER32.DLL
ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz0123456789+/
invalid string position
string too long
10.1.252.19
bad locale name
ios_base::badbit set
ios_base::failbit set
ios_base::eofbit set
/ajax_modal/modal/data.asp
http://%s%s?%s=%s&%s=%s&state=%d
\Temp\filer
del /f /a %s%s*.%s
%S%S%d.%s
\inf\netft429.pnf
\inf\netfb318.pnf
bad cast
```

Process	CPU	Private Bytes	Working Set	PID	Description	Company N
System Idle Process	100.00	0 K	16 K	0		
System		0 K	212 K	4		
Interrupts	< 0.01	0 K	0 K	n/a	Hardware Interrupts and DPCs	
smss.exe		168 K	412 K	372	Windows NT Session Mana...	Microsoft Co
csrss.exe		6,348 K	3,908 K	588	Client Server Runtime Process	Microsoft Co
winlogon.exe		7,768 K	5,360 K	612	Windows NT Logon Applicat...	Microsoft Co
		1,880 K	3,884 K	656	Services and Controller app	Microsoft Co
		1,368 K	3,620 K	824	VirtualBox Guest Additions S...	Oracle Corp
		3,188 K	5,104 K	868	Generic Host Process for Wi...	Microsoft Co
		1,904 K	4,608 K	956	Generic Host Process for Wi...	Microsoft Co
		14,884 K	26,048 K	1048	Generic Host Process for Wi...	Microsoft Co
		672 K	2,564 K	2036	Windows Security Center No...	Microsoft Co
		2,272 K	4,160 K	2416	Windows Update	Microsoft Co
		1,652 K	3,968 K	1116	Generic Host Process for Wi...	Microsoft Co
		1,668 K	4,248 K	1156	Generic Host Process for Wi...	Microsoft Co
		3,172 K	4,828 K	1512	Spooler SubSystem App	Microsoft Co
		1,404 K	3,896 K	188	Generic Host Process for Wi...	Microsoft Co
		1,244 K	3,696 K	1648	Application Layer Gateway S...	Microsoft Co
		980 K	3,768 K	3036	Distributed Link Tracking Ser...	Microsoft Co
		2,500 K	4,352 K	3440	Generic Host Process for Wi...	Microsoft Co
		4,340 K	6,920 K	668	LSA Shell (Export Version)	Microsoft Co
		22,296 K	12,568 K	1760	Windows Explorer	Microsoft Co
		1,176 K	3,940 K	1944	VirtualBox Guest Additions Tr...	Oracle Corp
		1,000 K	3,520 K	1952	CTF Loader	Microsoft Co
		17,116 K	10,356 K	2440	Sysinternals Process Explorer	Sysinternals
		57,060 K	564 K	2696	Regshot 1.9.0 x86 Unicode	Regshot Te
		1,224 K	556 K	3380	Notepad	Microsoft Co
cmd.exe		2,100 K	996 K	3208	Windows Command Processor	Microsoft Co
regedit.exe		1,460 K	916 K	2728	Registry Editor	Microsoft Co
ntvdm.exe		1,292 K	2,356 K	2764	NTVDM.EXE	Microsoft Co
depends.exe		10,632 K	1,448 K	2492	Dependency Walker for Win...	Microsoft Co
depends.exe		7,056 K	1,744 K	3556	Dependency Walker for Win...	Microsoft Co
Procmon.exe		2,620 K	3,132 K	2304	Process Monitor	Sysinternals

CPU Usage: 0.00% Commit Charge: 5.43% Processes: 32 Physical Usage: 8.64%

9) EXTRA CREDIT What network shares does the malware try to access? Describe how you got your answer.

Network shares can usually be found in the registry key that have the word “Explorer” in them. Example of such registry key is “HKEY_CURRENT_USER\Software\Windows\CurrentVersion\Explorer\....\”.

In this case, after running the malware hw2.exe, use Regshot to capture snaps before and after running malware, then in values added you can see one registry keys that is added(containing the keyword Explorer) which give the network shares accessed by the malware.

Here the registry keys are: “HKEY_USER\S-1-5-21-1935655697-1606980848-1343024091-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF(}\Count\HRZR_EHACNGU:P:\\Qbphzragf naq Frggvatf\fgghqrag\Qrfxbbc\uj2.rkr: 05 00 00 00 06 00 00 00 D0 00 C5 A2 D6 Ce D4 01:”