Practical Malware Analysis Lab 3-2

Questions

1. How can you get this malware to install itself?
2. How would you get this malware to run after installation?
3. How could you find the process under which this malware is running?
4. What are the malware's host based indicators?
5. Are there any useful network-based signatures for this malware?

Static Analysis

File: Lab03-02.dll
Imports: Kernel32.dll, ADVAPI32.dll, WS2_32.dll, WININET.dll, MSVCRT.dll

Kernel32.dll → CreateProcessA, CreateThread, GetModuleFileName. GetCurrentDirectoryA, Sleep, LoadLibraryA, ReadFile, GetTempPathA, GetSystemTime, GetStartupInfo

ADVAPI32.dll → CreateServiceA, DeleteService. OpenServiceA, RegCloseKey, RegOpenKeyExA, RegCreateKey, RegQueryValueExA, RegSetValueExA, SetServiceStatus

WS2_32.dll → closesocket,connect,htons, ioctlsocket, inet_addr, recv, select, send, shutdown, gethostname, WSASocketA, WSAStartup, WSACleanup, __WSAFDIsSet.

WININET.dll → HttpOpenRequestA, HttpQueryInfoA, HttpSendRequestA, InternetCloseHandle, InternetConnectA, InternetOpenA, InternetReadFile.

MSVCRT.dll → Basic C++ functions

Results for checking strings.

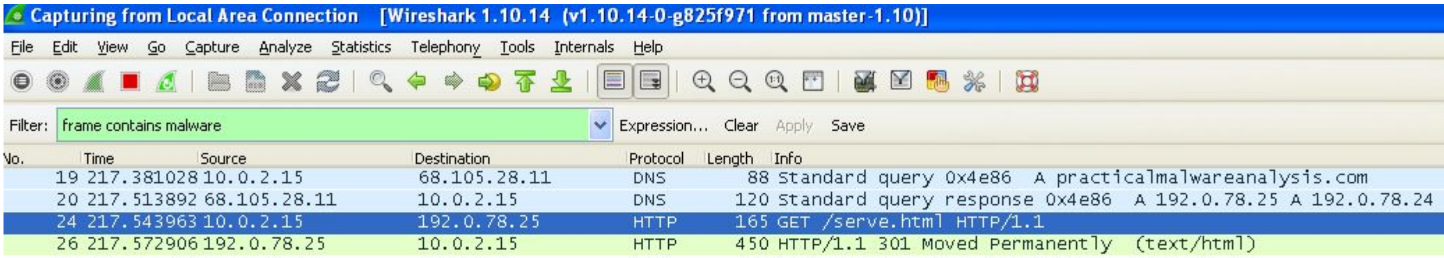
```
000000004D78  000010005978   0  ServiceMain
000000004E28  000010006028   0  practicalmalwareanalysis.com
000000004F7C  00001000617C   0  cmd.exe /c
000000004F74  000010006174   0  getfile
000000004F38  000010006138   0  HTTP/1.1
000000005048  000010006248   0  Parameters
00000000505C  00001000625C   0  Start
000000004E68  000010006068   0  serve.html
000000005018  000010006218   0  ServiceDll
000000004D95  000010005995   0  installA
0000000050A4  0000100062A4   0  Depends INA+, Collects and stores network
configuration and location information, and notifies applications when this information changes.
```

```
00000000513C   00001000633C      0   %SystemRoot%\System32\svchost.exe -k
000000005254   000010006454      0   RegQueryValueEx(Svchost\netsvcs)
0000000052D8   0000100064D8      0   SOFTWARE\Microsoft\Windows
NT\CurrentVersion\Svchost
0000000051A4   0000100063A4      0   Intranet Network Awareness (INA+)
000000005164   000010006364      0   SYSTEM\CurrentControlSet\Services\
```

Dynamic Analysis

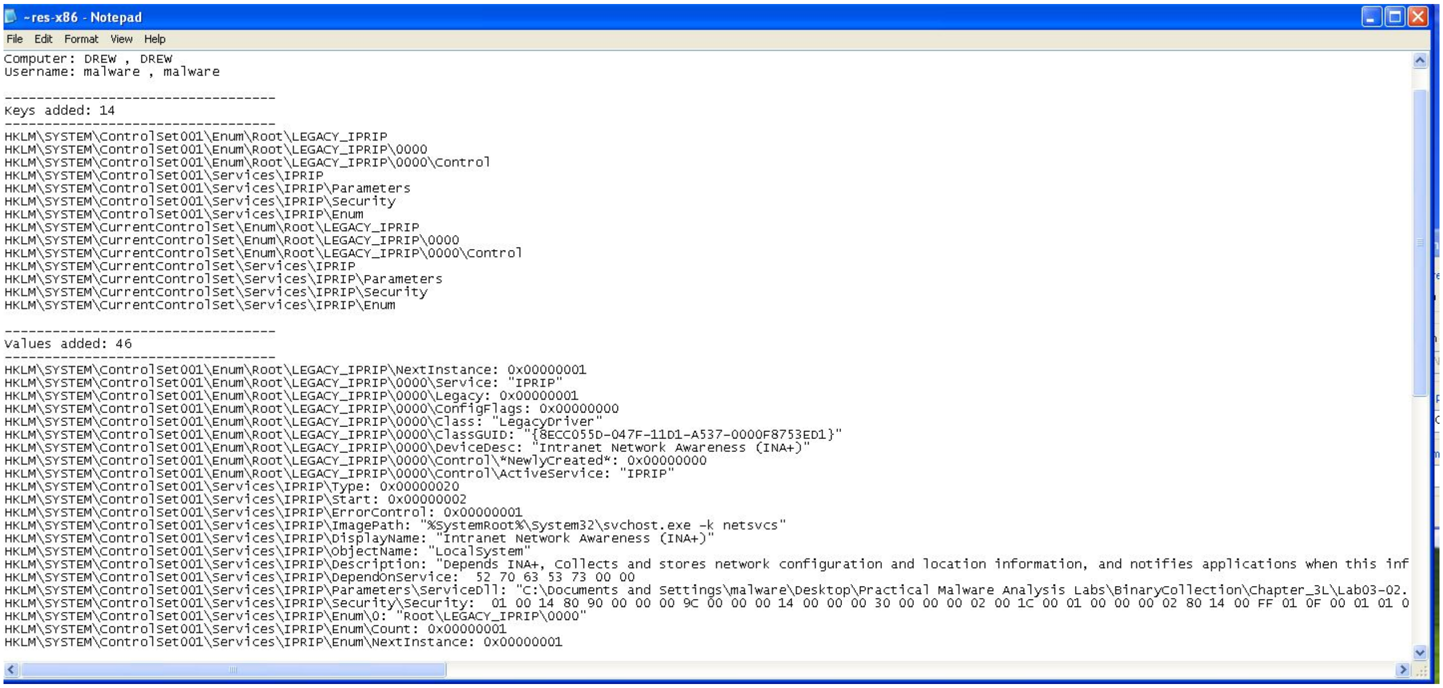
To install the malware you would use
rundll32.exe Lab03-02.dll installA
Then to start the service the malware service you use

net start “Intranet Network Awareness (INA+)”


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
 19  217.381028  10.0.2.15     68.105.28.11  DNS          88   Standard query 0x4e86  A practicalmalwareanalysis.com
 20  217.513892  68.105.28.11  10.0.2.15     DNS         120   Standard query response 0x4e86  A 192.0.78.25 A 192.0.78.24
 24  217.543963  10.0.2.15     192.0.78.25   HTTP        165   GET /serve.html HTTP/1.1
 26  217.572906  192.0.78.25   10.0.2.15     HTTP        450   HTTP/1.1 301 Moved Permanently  (text/html)
```



```
Computer: DREW , DREW
Username: malware , malware

----------------------------------
Keys added: 14
----------------------------------
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_IPRIP
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_IPRIP\0000
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_IPRIP\0000\Control
HKLM\SYSTEM\ControlSet001\Services\IPRIP
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Security
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Enum
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_IPRIP
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_IPRIP\0000
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_IPRIP\0000\Control
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Parameters
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Security
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Enum

----------------------------------
Values added: 46
----------------------------------
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_IPRIP\NextInstance: 0x00000001
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_IPRIP\0000\Service: "IPRIP"
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_IPRIP\0000\Legacy: 0x00000001
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_IPRIP\0000\ConfigFlags: 0x00000000
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_IPRIP\0000\Class: "LegacyDriver"
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_IPRIP\0000\ClassGUID: "{8ECC055D-047F-11D1-A537-0000F8753ED1}"
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_IPRIP\0000\DeviceDesc: "Intranet Network Awareness (INA+)"
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_IPRIP\0000\Control\*NewlyCreated*: 0x00000000
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_IPRIP\0000\Control\ActiveService: "IPRIP"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Type: 0x00000020
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Start: 0x00000002
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ErrorControl: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ImagePath: "%SystemRoot%\System32\svchost.exe -k netsvcs"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\DisplayName: "Intranet Network Awareness (INA+)"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\ObjectName: "LocalSystem"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Description: "Depends INA+, Collects and stores network configuration and location information, and notifies applications when this inf
HKLM\SYSTEM\ControlSet001\Services\IPRIP\DependOnService:  52 70 63 53 73 00 00
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Parameters\ServiceDll: "C:\Documents and Settings\malware\Desktop\Practical Malware Analysis Labs\BinaryCollection\Chapter_3L\Lab03-02.
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Security\Security:  01 00 14 80 90 00 00 00 9C 00 00 00 14 00 00 00 30 00 00 00 02 00 1C 00 01 00 00 00 02 80 14 00 FF 01 0F 00 01 01 0
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Enum\0: "Root\LEGACY_IPRIP\0000"
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Enum\Count: 0x00000001
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Enum\NextInstance: 0x00000001
```

Question 1

rundll32.exe Lab03-02.dll installA

Question 2

Then to start the malware service you use net start “Intranet Network Awareness (INA+)”.

Question 3

By using the command net start without any arguments I was able to list all services on the uninfected computer. When installing the malware I ran the same command and saw the extra service “Intranet Network Awareness (INA+)”. This had to be the service the malware installed.

Question 4

Some host based indicators include

Values Added

HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_IPRIP\0000\Service: "IPRIP"
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_IPRIP\0000\DeviceDesc: "Intranet Network Awareness (INA+)"
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_IPRIP\0000\Control\*NewlyCreated*: 0x00000000
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_IPRIP\0000\Control\ActiveService: "IPRIP"
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Enum\0: "Root\LEGACY_IPRIP\0000"

Keys added

HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_IPRIP
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_IPRIP\0000
HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY_IPRIP\0000\Control
HKLM\SYSTEM\ControlSet001\Services\IPRIP\Enum
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_IPRIP
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_IPRIP\0000
HKLM\SYSTEM\CurrentControlSet\Enum\Root\LEGACY_IPRIP\0000\Control
HKLM\SYSTEM\CurrentControlSet\Services\IPRIP\Enum

Question 5

Traffic to the website practicalmalwareanalysis.com and a request to serve.html