Lab 1 – Introduction to Incident Response

Sai Sasaank Srivatsa Pallerla

University of Maryland, Baltimore County

Presented to: Gina Scaldaferri

Date: 09/10/2019

About the Lab

In this lab we were supposed to examine a file that one of the employees downloaded from a website under the pretense of FOSS software to provide an SSH/Telnet client for Windows systems. Since the user has downloaded this software outside of IT's normal controls, we were tasked with reviewing this application and providing our assessment of whether it is okay to use, or if it poses a threat.

Part 1

There are lot of tools out in the internet that can be used to monitoring and analyzing application, traffic and behavior of a potential malicious executable. In this lab I have used the tools that I'm comfortable with. The question presented in the part one of the lab are as follows.

1. *What utility can be run on the Windows VM to monitor processes running on the system?*

Procmon: Also known as Processes monitor, is a part of SysInternals (tools package) developed my Microsoft that shows real-time file system, Registry and process/thread activity. It is an advanced monitoring tool that provides an extensive list of enhancements like rich and non-destructive filtering, comprehensive event properties such session IDs and user names, reliable process information, and details related to file and registry creation

2. *What utility can be run on the Windows VM to monitor network connections on the system?*

ApateDNS; This tools is used for monitoring network connections. When used in an virtual environment we just need to monitor the DNS loopback to get active connections.It is a tool for controlling DNS responses though an easy-to-use GUI. It spoofs DNS responses to a user-specified IP address by listening on the local machine. It also automatically sets the local DNS to localhost.

3. *What application could you run on Windows to capture network traffic from the system?*

Wireshark: It is one of the most famous tools that is used to monitor network traffic and protocols used. It lets us monitor the network at a microscopic level, both wired and wireless.

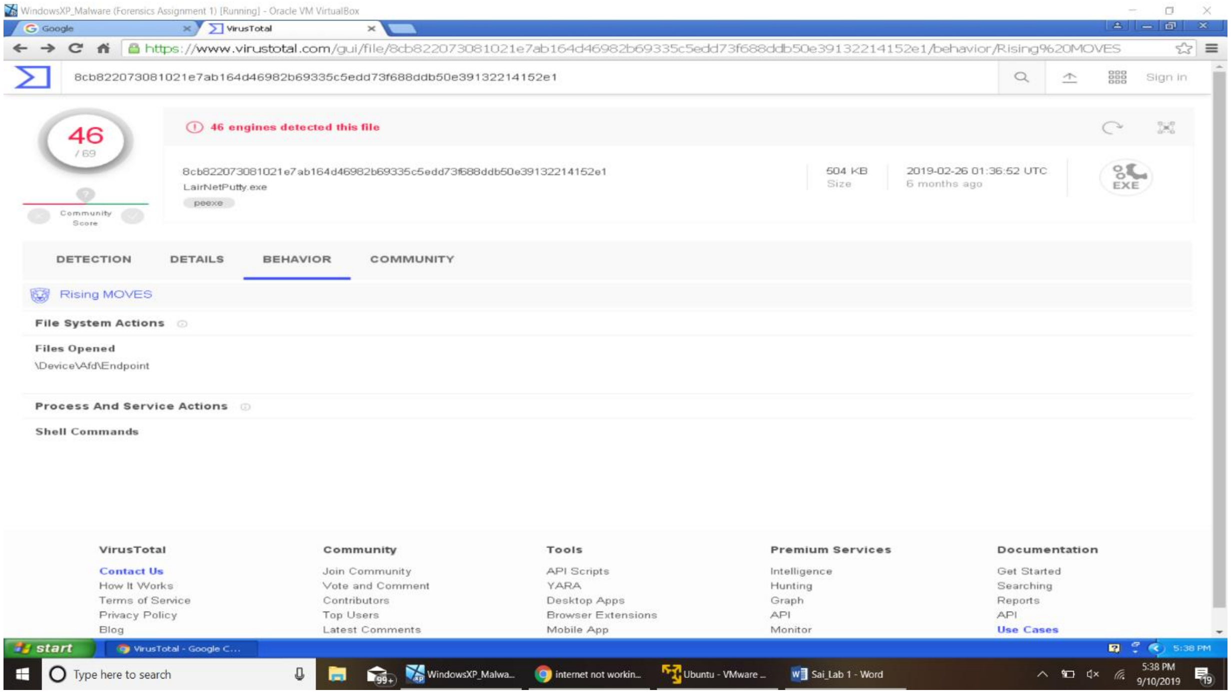
4. *What information can you gather about the application from reviewing it without any special tools?*

A simple method to gather information without reviewing it is by googling about it. In this case I uploaded the executable file to virus total just to verify it against existing malware database. If not virus total one can simply use the strings command against the executable and check if there are any suspicious strings in the .exe file. All these techniques come under static analysis.

Part 2

1. *What is your assessment of the application and why?*

For the initial assessment the executable was uploaded to virustotal.com which lead us to a preliminary decision that the file could be malicious. Upon further examining the file we found out that the executable has images which could act as executables, i.e., code hidden inside the images.



https://www.virustotal.com/gui/file/8cb822073081021e7ab164d46982b69335c5edd73f688ddb50e39132214152e1/behavior/Rising%20MOVES

8cb822073081021e7ab164d46982b69335c5edd73f688ddb50e39132214152e1

46 / 69

46 engines detected this file

8cb822073081021e7ab164d46982b69335c5edd73f688ddb50e39132214152e1
LairNetPutty.exe
peexe

504 KB
Size

2019-02-26 01:36:52 UTC
6 months ago

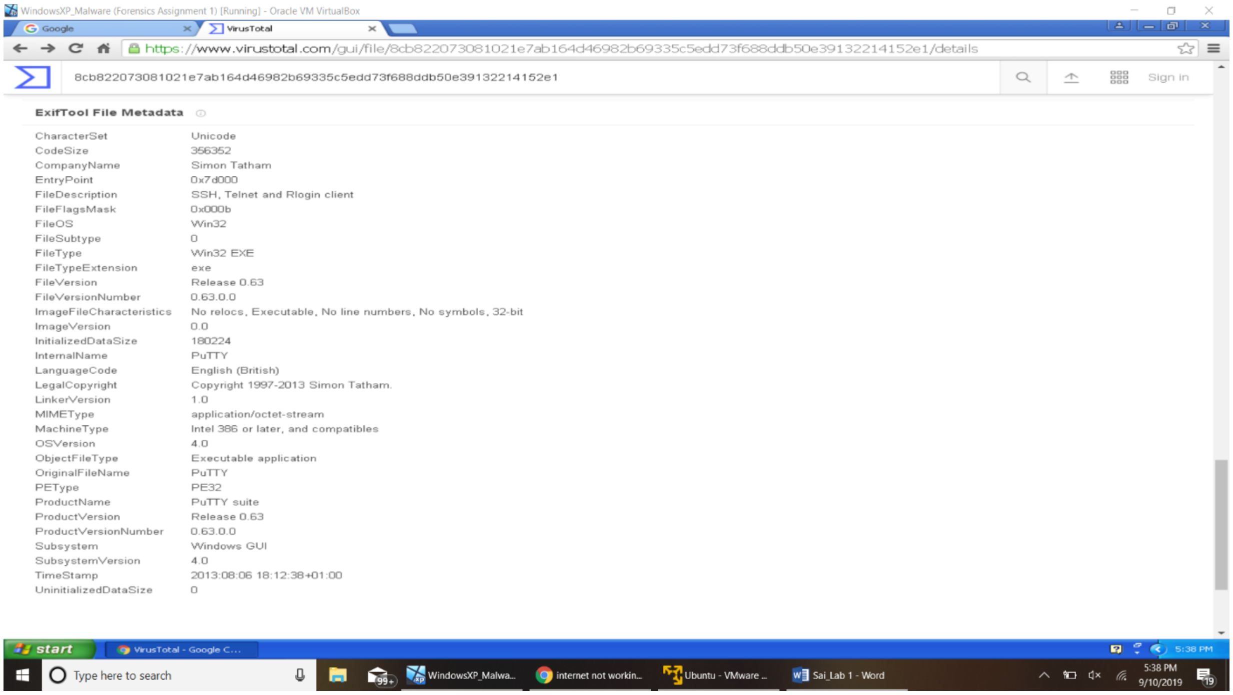
Rising MOVES

File System Actions

Files Opened
\Device\Afd\Endpoint

Process And Service Actions

Shell Commands



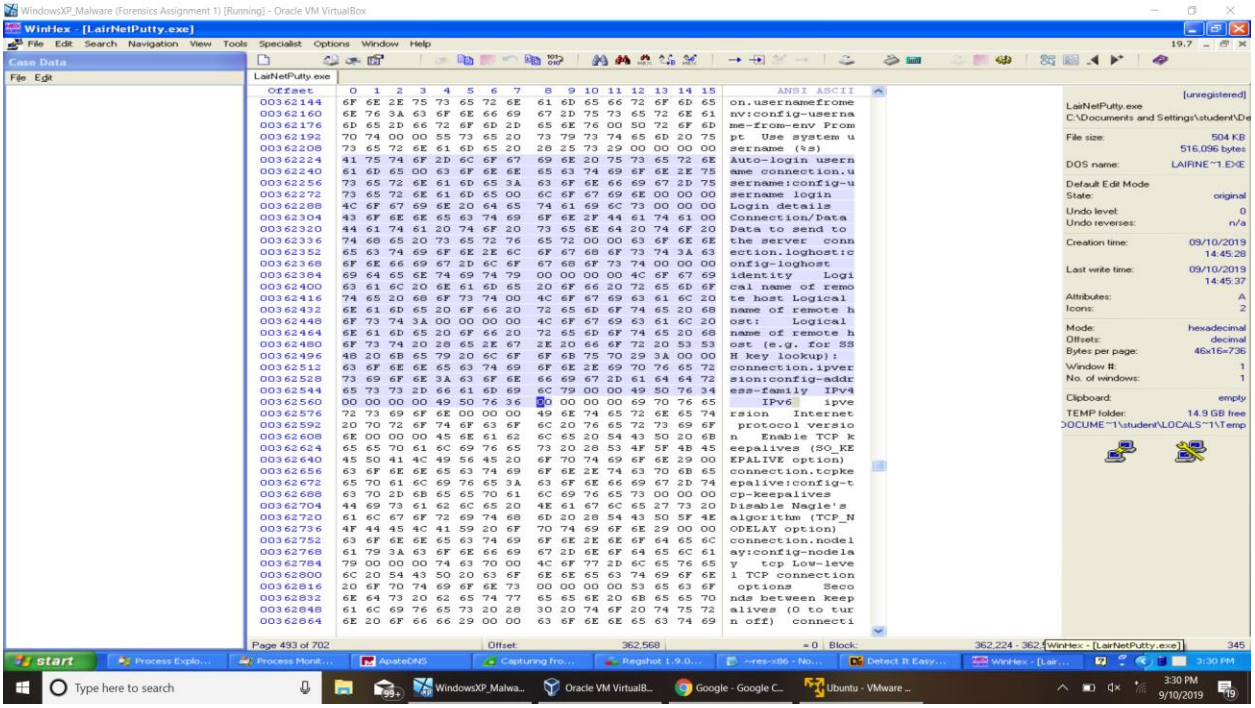
https://www.virustotal.com/gui/file/8cb822073081021e7ab164d46982b69335c5edd73f688ddb50e39132214152e1/details

8cb822073081021e7ab164d46982b69335c5edd73f688ddb50e39132214152e1

ExifTool File Metadata

CharacterSet	Unicode
CodeSize	356352
CompanyName	Simon Tatham
EntryPoint	0x7d000
FileDescription	SSH, Telnet and Rlogin client
FileFlagsMask	0x000b
FileOS	Win32
FileSubtype	0
FileType	Win32 EXE
FileTypeExtension	exe
FileVersion	Release 0.63
FileVersionNumber	0.63.0.0
ImageFileCharacteristics	No relocs, Executable, No line numbers, No symbols, 32-bit
ImageVersion	0.0
InitializedDataSize	180224
InternalName	PuTTY
LanguageCode	English (British)
LegalCopyright	Copyright 1997-2013 Simon Tatham.
LinkerVersion	1.0
MIMEType	application/octet-stream
MachineType	Intel 386 or later, and compatibles
OSVersion	4.0
ObjectFileType	Executable application
OriginalFileName	PuTTY
PEType	PE32
ProductName	PuTTY suite
ProductVersion	Release 0.63
ProductVersionNumber	0.63.0.0
Subsystem	Windows GUI
SubsystemVersion	4.0
TimeStamp	2013:08:06 18:12:38+01:00
UninitializedDataSize	0

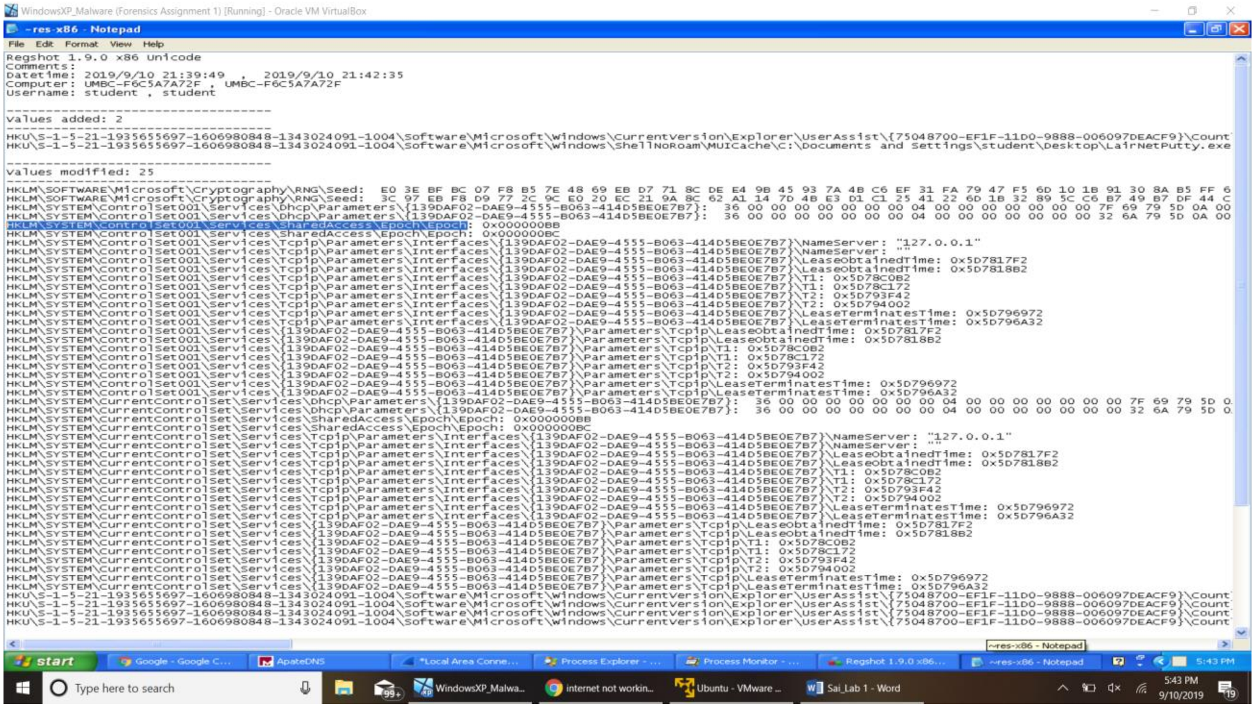
For later assessments we used ApateDNS, Promon, Process Explorer, Wireshark, WinHex and Regshot. This assessment led us to a conclusion that file was trying to connect to remote server and send data from the host computer to the server, for which wireshark and apate DNS were used. From preliminary assessment we can say that the code was stored inside an image. In later stages, using process explorer we found out more evidence to prove this point.



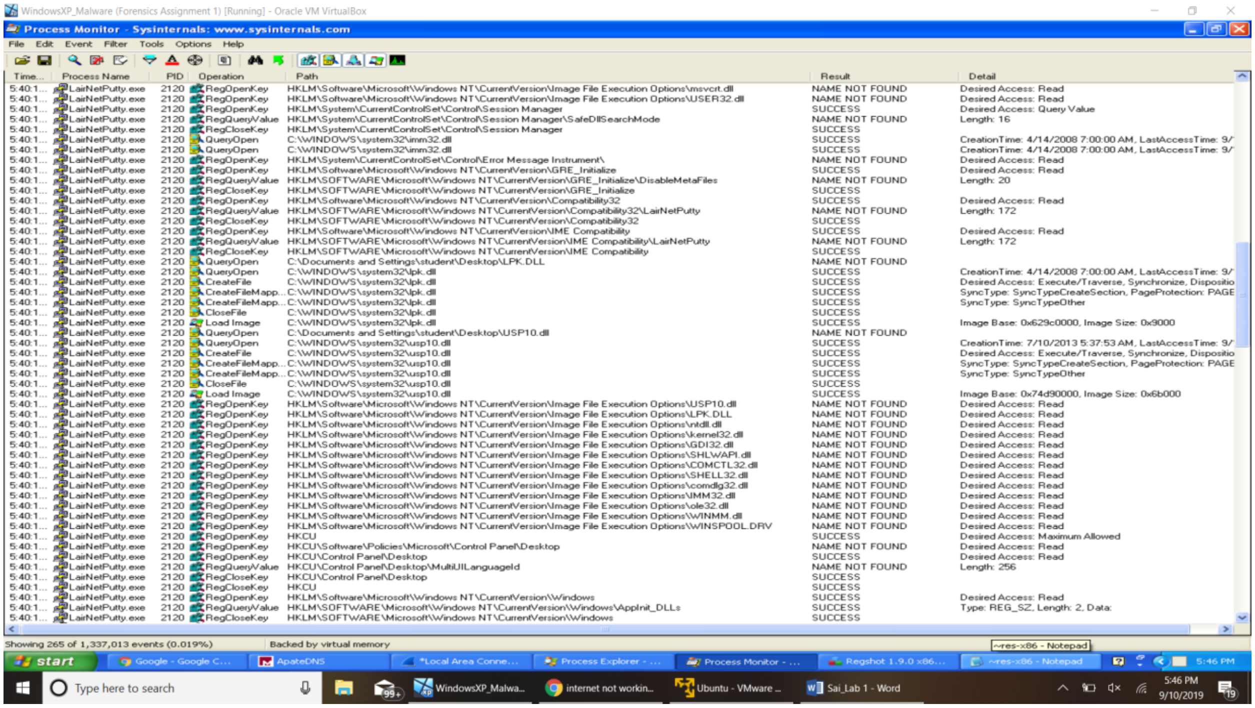
```
Offset      0  1  2  3  4  5  6  7   8  9 10 11 12 13 14 15     ANSI ASCII
00362144   6F 6E 2E 75 73 65 72 6E  61 6D 65 66 72 6F 6D 65   on.usernamefrome
00362160   6E 76 3A 63 6F 6E 66 69  67 2D 75 73 65 72 6E 61   nv:config-userna
00362176   6D 65 2D 66 72 6F 6D 2D  65 6E 76 00 50 72 6F 6D   me-from-env Prom
00362192   70 74 00 00 55 73 65 20  73 79 73 74 65 6D 20 75   pt  Use system u
00362208   73 65 72 6E 61 6D 65 20  28 25 73 29 00 00 00 00   sername (%s)
00362224   41 75 74 6F 2D 6C 6F 67  69 6E 20 75 73 65 72 6E   Auto-login usern
00362240   61 6D 65 00 63 6F 6E 6E  65 63 74 69 6F 6E 2E 75   ame connection.u
00362256   73 65 72 6E 61 6D 65 3A  63 6F 6E 66 69 67 2D 75   sername:config-u
00362272   73 65 72 6E 61 6D 65 00  6C 6F 67 69 6E 00 00 00   sername login
00362288   4C 6F 67 69 6E 20 64 65  74 61 69 6C 73 00 00 00   Login details
00362304   43 6F 6E 6E 65 63 74 69  6F 6E 2F 44 61 74 61 00   Connection/Data
00362320   44 61 74 61 20 74 6F 20  73 65 6E 64 20 74 6F 20   Data to send to
00362336   74 68 65 20 73 65 72 76  65 72 00 00 63 6F 6E 6E   the server  conn
00362352   65 63 74 69 6F 6E 2E 6C  6F 67 68 6F 73 74 3A 63   ection.loghost:c
00362368   6F 6E 66 69 67 2D 6C 6F  67 68 6F 73 74 00 00 00   onfig-loghost
00362384   69 64 65 6E 74 69 74 79  00 00 00 00 4C 6F 67 69   identity    Logi
00362400   63 61 6C 20 6E 61 6D 65  20 6F 66 20 72 65 6D 6F   cal name of remo
00362416   74 65 20 68 6F 73 74 00  4C 6F 67 69 63 61 6C 20   te host Logical
00362432   6E 61 6D 65 20 6F 66 20  72 65 6D 6F 74 65 20 68   name of remote h
00362448   6F 73 74 3A 00 00 00 00  4C 6F 67 69 63 61 6C 20   ost:    Logical
00362464   6E 61 6D 65 20 6F 66 20  72 65 6D 6F 74 65 20 68   name of remote h
00362480   6F 73 74 20 28 65 2E 67  2E 20 66 6F 72 20 53 53   ost (e.g. for SS
00362496   48 20 6B 65 79 20 6C 6F  6F 6B 75 70 29 3A 00 00   H key lookup):
00362512   63 6F 6E 6E 65 63 74 69  6F 6E 2E 69 70 76 65 72   connection.ipver
00362528   73 69 6F 6E 3A 63 6F 6E  66 69 67 2D 61 64 64 72   sion:config-addr
00362544   65 73 73 2D 66 61 6D 69  6C 79 00 00 49 50 76 34   ess-family  IPv4
00362560   00 00 00 00 49 50 76 36  00 00 00 00 69 70 76 65       IPv6    ipve
00362576   72 73 69 6F 6E 00 00 00  49 6E 74 65 72 6E 65 74   rsion   Internet
00362592   20 70 72 6F 74 6F 63 6F  6C 20 76 65 72 73 69 6F    protocol versio
00362608   6E 00 00 00 45 6E 61 62  6C 65 20 54 43 50 20 6B   n   Enable TCP k
00362624   65 65 70 61 6C 69 76 65  73 20 28 53 4F 5F 4B 45   eepalives (SO_KE
00362640   45 50 41 4C 49 56 45 20  6F 70 74 69 6F 6E 29 00   EPALIVE option)
00362656   63 6F 6E 6E 65 63 74 69  6F 6E 2E 74 63 70 6B 65   connection.tcpke
00362672   65 70 61 6C 69 76 65 3A  63 6F 6E 66 69 67 2D 74   epalive:config-t
00362688   63 70 2D 6B 65 65 70 61  6C 69 76 65 73 00 00 00   cp-keepalives
00362704   44 69 73 61 62 6C 65 20  4E 61 67 6C 65 27 73 20   Disable Nagle's
00362720   61 6C 67 6F 72 69 74 68  6D 20 28 54 43 50 5F 4E   algorithm (TCP_N
00362736   4F 44 45 4C 41 59 20 6F  70 74 69 6F 6E 29 00 00   ODELAY option)
00362752   63 6F 6E 6E 65 63 74 69  6F 6E 2E 6E 6F 64 65 6C   connection.nodel
00362768   61 79 3A 63 6F 6E 66 69  67 2D 6E 6F 64 65 6C 61   ay:config-nodela
00362784   79 00 00 00 74 63 70 00  4C 6F 77 2D 6C 65 76 65   y   tcp Low-leve
00362800   6C 20 54 43 50 20 63 6F  6E 6E 65 63 74 69 6F 6E   l TCP connection
00362816   20 6F 70 74 69 6F 6E 73  00 00 00 00 53 65 63 6F    options    Seco
00362832   6E 64 73 20 62 65 74 77  65 65 6E 20 6B 65 65 70   nds between keep
00362848   61 6C 69 76 65 73 20 28  30 20 74 6F 20 74 75 72   alives (0 to tur
00362864   6E 20 6F 66 66 29 00 00  63 6F 6E 6E 65 63 74 69   n off)  connecti
```

Page 493 of 702   Offset: 362,568   = 0   Block: 362,224 - 362,5   345

[unregistered]
LairNetPutty.exe
C:\Documents and Settings\student\De
File size: 504 KB
516,096 bytes
DOS name: LAIRNE~1.EXE
Default Edit Mode
State: original
Undo level: 0
Undo reverses: n/a
Creation time: 09/10/2019 14:45:28
Last write time: 09/10/2019 14:45:37
Attributes: A
Icons: 2
Mode: hexadecimal
Offsets: decimal
Bytes per page: 46x16=736
Window #: 1
No. of windows: 1
Clipboard: empty
TEMP folder: 14.9 GB free
DOCUME~1\student\LOCALS~1\Temp

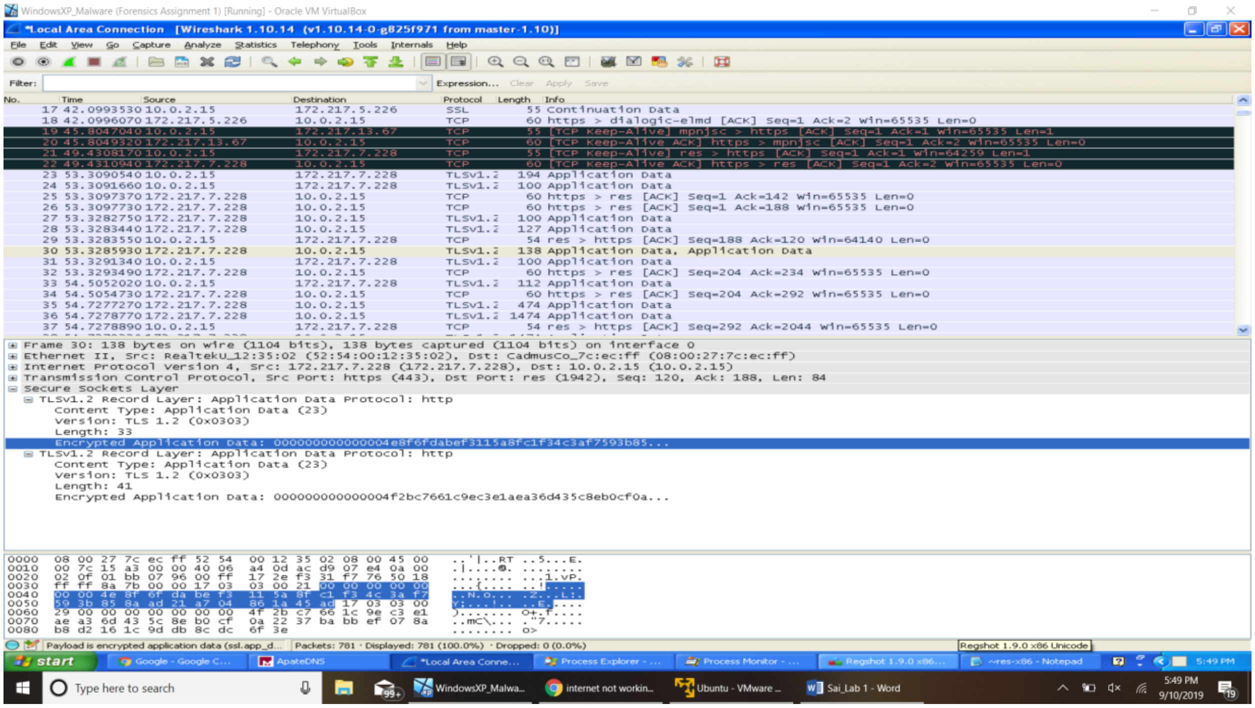


```
Regshot 1.9.0 x86 Unicode
Comments:
Datetime: 2019/9/10 21:39:49  ,  2019/9/10 21:42:35
Computer: UMBC-F6C5A7A72F , UMBC-F6C5A7A72F
Username: student , student

----------------------------------
Values added: 2
----------------------------------
HKU\S-1-5-21-1935655697-1606980848-1343024091-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKU\S-1-5-21-1935655697-1606980848-1343024091-1004\Software\Microsoft\Windows\ShellNoRoam\MUICache\C:\Documents and Settings\student\Desktop\LairNetPutty.exe

----------------------------------
Values modified: 25
----------------------------------
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  E0 3E BF BC 07 F8 B5 7E 48 69 EB D7 71 8C DE E4 9B 45 93 7A 4B C6 EF 31 FA 79 47 F5 6D 10 1B 91 30 8A B5 FF 6
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  3C 97 EB F8 D9 77 2C 9C E0 20 EC 21 9A 8C 62 A1 14 7D 4B E3 D1 C1 25 41 22 6D 1B 32 89 5C C6 B7 49 B7 DF 44 C
HKLM\SYSTEM\ControlSet001\Services\Dhcp\Parameters\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}:  36 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 7F 69 79 5D 0A 00
HKLM\SYSTEM\ControlSet001\Services\Dhcp\Parameters\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}:  36 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 32 6A 79 5D 0A 00
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Epoch\Epoch: 0x000000BB
HKLM\SYSTEM\ControlSet001\Services\SharedAccess\Epoch\Epoch: 0x000000BC
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\NameServer: "127.0.0.1"
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\NameServer: ""
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\LeaseObtainedTime: 0x5D7817F2
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\LeaseObtainedTime: 0x5D7818B2
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\T1: 0x5D78C0B2
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\T1: 0x5D78C172
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\T2: 0x5D793F42
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\T2: 0x5D794002
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\LeaseTerminatesTime: 0x5D796972
HKLM\SYSTEM\ControlSet001\Services\Tcpip\Parameters\Interfaces\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\LeaseTerminatesTime: 0x5D796A32
HKLM\SYSTEM\ControlSet001\Services\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\Parameters\Tcpip\LeaseObtainedTime: 0x5D7817F2
HKLM\SYSTEM\ControlSet001\Services\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\Parameters\Tcpip\LeaseObtainedTime: 0x5D7818B2
HKLM\SYSTEM\ControlSet001\Services\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\Parameters\Tcpip\T1: 0x5D78C0B2
HKLM\SYSTEM\ControlSet001\Services\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\Parameters\Tcpip\T1: 0x5D78C172
HKLM\SYSTEM\ControlSet001\Services\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\Parameters\Tcpip\T2: 0x5D793F42
HKLM\SYSTEM\ControlSet001\Services\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\Parameters\Tcpip\T2: 0x5D794002
HKLM\SYSTEM\ControlSet001\Services\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\Parameters\Tcpip\LeaseTerminatesTime: 0x5D796972
HKLM\SYSTEM\ControlSet001\Services\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\Parameters\Tcpip\LeaseTerminatesTime: 0x5D796A32
HKLM\SYSTEM\CurrentControlSet\Services\Dhcp\Parameters\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}:  36 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 7F 69 79 5D 0.
HKLM\SYSTEM\CurrentControlSet\Services\Dhcp\Parameters\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}:  36 00 00 00 00 00 00 00 04 00 00 00 00 00 00 00 32 6A 79 5D 0.
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Epoch\Epoch: 0x000000BB
HKLM\SYSTEM\CurrentControlSet\Services\SharedAccess\Epoch\Epoch: 0x000000BC
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\NameServer: "127.0.0.1"
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\NameServer: ""
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\LeaseObtainedTime: 0x5D7817F2
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\LeaseObtainedTime: 0x5D7818B2
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\T1: 0x5D78C0B2
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\T1: 0x5D78C172
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\T2: 0x5D793F42
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\T2: 0x5D794002
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\LeaseTerminatesTime: 0x5D796972
HKLM\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\LeaseTerminatesTime: 0x5D796A32
HKLM\SYSTEM\CurrentControlSet\Services\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\Parameters\Tcpip\LeaseObtainedTime: 0x5D7817F2
HKLM\SYSTEM\CurrentControlSet\Services\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\Parameters\Tcpip\LeaseObtainedTime: 0x5D7818B2
HKLM\SYSTEM\CurrentControlSet\Services\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\Parameters\Tcpip\T1: 0x5D78C0B2
HKLM\SYSTEM\CurrentControlSet\Services\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\Parameters\Tcpip\T1: 0x5D78C172
HKLM\SYSTEM\CurrentControlSet\Services\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\Parameters\Tcpip\T2: 0x5D793F42
HKLM\SYSTEM\CurrentControlSet\Services\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\Parameters\Tcpip\T2: 0x5D794002
HKLM\SYSTEM\CurrentControlSet\Services\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\Parameters\Tcpip\LeaseTerminatesTime: 0x5D796972
HKLM\SYSTEM\CurrentControlSet\Services\{139DAF02-DAE9-4555-B063-414D5BE0E7B7}\Parameters\Tcpip\LeaseTerminatesTime: 0x5D796A32
HKU\S-1-5-21-1935655697-1606980848-1343024091-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKU\S-1-5-21-1935655697-1606980848-1343024091-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKU\S-1-5-21-1935655697-1606980848-1343024091-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
HKU\S-1-5-21-1935655697-1606980848-1343024091-1004\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count
```


WindowsXP_Malware (Forensics Assignment 1) [Running] - Oracle VM VirtualBox
Process Monitor - Sysinternals: www.sysinternals.com
File Edit Event Filter Tools Options Help

Time...	Process Name	PID	Operation	Path	Result	Detail
5:40:1...	LairNetPutty.exe	2120	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\msvcrt.dll	NAME NOT FOUND	Desired Access: Read
5:40:1...	LairNetPutty.exe	2120	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\USER32.dll	NAME NOT FOUND	Desired Access: Read
5:40:1...	LairNetPutty.exe	2120	RegOpenKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	Desired Access: Query Value
5:40:1...	LairNetPutty.exe	2120	RegQueryValue	HKLM\System\CurrentControlSet\Control\Session Manager\SafeDllSearchMode	NAME NOT FOUND	Length: 16
5:40:1...	LairNetPutty.exe	2120	RegCloseKey	HKLM\System\CurrentControlSet\Control\Session Manager	SUCCESS	
5:40:1...	LairNetPutty.exe	2120	QueryOpen	C:\WINDOWS\system32\imm32.dll	SUCCESS	CreationTime: 4/14/2008 7:00:00 AM, LastAccessTime: 9/
5:40:1...	LairNetPutty.exe	2120	QueryOpen	C:\WINDOWS\system32\imm32.dll	SUCCESS	CreationTime: 4/14/2008 7:00:00 AM, LastAccessTime: 9/
5:40:1...	LairNetPutty.exe	2120	RegOpenKey	HKLM\System\CurrentControlSet\Control\Error Message Instrument\	NAME NOT FOUND	Desired Access: Read
5:40:1...	LairNetPutty.exe	2120	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS	Desired Access: Read
5:40:1...	LairNetPutty.exe	2120	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize\DisableMetaFiles	NAME NOT FOUND	Length: 20
5:40:1...	LairNetPutty.exe	2120	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\GRE_Initialize	SUCCESS	
5:40:1...	LairNetPutty.exe	2120	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Compatibility32	SUCCESS	Desired Access: Read
5:40:1...	LairNetPutty.exe	2120	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility32\LairNetPutty	NAME NOT FOUND	Length: 172
5:40:1...	LairNetPutty.exe	2120	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Compatibility32	SUCCESS	
5:40:1...	LairNetPutty.exe	2120	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\IME Compatibility	SUCCESS	Desired Access: Read
5:40:1...	LairNetPutty.exe	2120	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\IME Compatibility\LairNetPutty	NAME NOT FOUND	Length: 172
5:40:1...	LairNetPutty.exe	2120	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\IME Compatibility	SUCCESS	
5:40:1...	LairNetPutty.exe	2120	QueryOpen	C:\Documents and Settings\student\Desktop\LPK.DLL	NAME NOT FOUND	
5:40:1...	LairNetPutty.exe	2120	QueryOpen	C:\WINDOWS\system32\lpk.dll	SUCCESS	CreationTime: 4/14/2008 7:00:00 AM, LastAccessTime: 9/
5:40:1...	LairNetPutty.exe	2120	CreateFile	C:\WINDOWS\system32\lpk.dll	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Dispositio
5:40:1...	LairNetPutty.exe	2120	CreateFileMapp...	C:\WINDOWS\system32\lpk.dll	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE
5:40:1...	LairNetPutty.exe	2120	CreateFileMapp...	C:\WINDOWS\system32\lpk.dll	SUCCESS	SyncType: SyncTypeOther
5:40:1...	LairNetPutty.exe	2120	CloseFile	C:\WINDOWS\system32\lpk.dll	SUCCESS	
5:40:1...	LairNetPutty.exe	2120	Load Image	C:\WINDOWS\system32\lpk.dll	SUCCESS	Image Base: 0x629c0000, Image Size: 0x9000
5:40:1...	LairNetPutty.exe	2120	QueryOpen	C:\Documents and Settings\student\Desktop\USP10.dll	NAME NOT FOUND	
5:40:1...	LairNetPutty.exe	2120	QueryOpen	C:\WINDOWS\system32\usp10.dll	SUCCESS	CreationTime: 7/10/2013 5:37:53 AM, LastAccessTime: 9/
5:40:1...	LairNetPutty.exe	2120	CreateFile	C:\WINDOWS\system32\usp10.dll	SUCCESS	Desired Access: Execute/Traverse, Synchronize, Dispositio
5:40:1...	LairNetPutty.exe	2120	CreateFileMapp...	C:\WINDOWS\system32\usp10.dll	SUCCESS	SyncType: SyncTypeCreateSection, PageProtection: PAGE
5:40:1...	LairNetPutty.exe	2120	CreateFileMapp...	C:\WINDOWS\system32\usp10.dll	SUCCESS	SyncType: SyncTypeOther
5:40:1...	LairNetPutty.exe	2120	CloseFile	C:\WINDOWS\system32\usp10.dll	SUCCESS	
5:40:1...	LairNetPutty.exe	2120	Load Image	C:\WINDOWS\system32\usp10.dll	SUCCESS	Image Base: 0x74d90000, Image Size: 0x6b000
5:40:1...	LairNetPutty.exe	2120	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\USP10.dll	NAME NOT FOUND	Desired Access: Read
5:40:1...	LairNetPutty.exe	2120	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\LPK.DLL	NAME NOT FOUND	Desired Access: Read
5:40:1...	LairNetPutty.exe	2120	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ntdll.dll	NAME NOT FOUND	Desired Access: Read
5:40:1...	LairNetPutty.exe	2120	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\kernel32.dll	NAME NOT FOUND	Desired Access: Read
5:40:1...	LairNetPutty.exe	2120	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\GDI32.dll	NAME NOT FOUND	Desired Access: Read
5:40:1...	LairNetPutty.exe	2120	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SHLWAPI.dll	NAME NOT FOUND	Desired Access: Read
5:40:1...	LairNetPutty.exe	2120	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\COMCTL32.dll	NAME NOT FOUND	Desired Access: Read
5:40:1...	LairNetPutty.exe	2120	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\SHELL32.dll	NAME NOT FOUND	Desired Access: Read
5:40:1...	LairNetPutty.exe	2120	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\comdlg32.dll	NAME NOT FOUND	Desired Access: Read
5:40:1...	LairNetPutty.exe	2120	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\IMM32.dll	NAME NOT FOUND	Desired Access: Read
5:40:1...	LairNetPutty.exe	2120	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\ole32.dll	NAME NOT FOUND	Desired Access: Read
5:40:1...	LairNetPutty.exe	2120	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\WINMM.dll	NAME NOT FOUND	Desired Access: Read
5:40:1...	LairNetPutty.exe	2120	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Image File Execution Options\WINSPOOL.DRV	NAME NOT FOUND	Desired Access: Read
5:40:1...	LairNetPutty.exe	2120	RegOpenKey	HKCU	SUCCESS	Desired Access: Maximum Allowed
5:40:1...	LairNetPutty.exe	2120	RegOpenKey	HKCU\Software\Policies\Microsoft\Control Panel\Desktop	NAME NOT FOUND	Desired Access: Read
5:40:1...	LairNetPutty.exe	2120	RegOpenKey	HKCU\Control Panel\Desktop	SUCCESS	Desired Access: Read
5:40:1...	LairNetPutty.exe	2120	RegQueryValue	HKCU\Control Panel\Desktop\MultiUILanguageId	NAME NOT FOUND	Length: 256
5:40:1...	LairNetPutty.exe	2120	RegCloseKey	HKCU\Control Panel\Desktop	SUCCESS	
5:40:1...	LairNetPutty.exe	2120	RegCloseKey	HKCU	SUCCESS	
5:40:1...	LairNetPutty.exe	2120	RegOpenKey	HKLM\Software\Microsoft\Windows NT\CurrentVersion\Windows	SUCCESS	Desired Access: Read
5:40:1...	LairNetPutty.exe	2120	RegQueryValue	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows\AppInit_DLLs	SUCCESS	Type: REG_SZ, Length: 2, Data:
5:40:1...	LairNetPutty.exe	2120	RegCloseKey	HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Windows	SUCCESS	

Showing 265 of 1,337,013 events (0.019%) Backed by virtual memory


WindowsXP_Malware (Forensics Assignment 1) [Running] - Oracle VM VirtualBox
*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
Filter:
Expression... Clear Apply Save

```
No.     Time        Source          Destination     Protocol Length Info
     17 42.0993530 10.0.2.15        172.217.5.226   SSL        55 Continuation Data
     18 42.0996070 172.217.5.226    10.0.2.15       TCP        60 https > dialogic-elmd [ACK] Seq=1 Ack=2 Win=65535 Len=0
     19 45.8047040 10.0.2.15        172.217.13.67   TCP        55 [TCP Keep-Alive] mpnjsc > https [ACK] Seq=1 Ack=1 Win=65535 Len=1
     20 45.8049320 172.217.13.67    10.0.2.15       TCP        60 [TCP Keep-Alive ACK] https > mpnjsc [ACK] Seq=1 Ack=2 Win=65535 Len=0
     21 49.4308170 10.0.2.15        172.217.7.228   TCP        55 [TCP Keep-Alive] res > https [ACK] Seq=1 Ack=1 Win=64259 Len=1
     22 49.4310940 172.217.7.228    10.0.2.15       TCP        60 [TCP Keep-Alive ACK] https > res [ACK] Seq=1 Ack=2 Win=65535 Len=0
     23 53.3090540 10.0.2.15        172.217.7.228   TLSv1.2   194 Application Data
     24 53.3091660 10.0.2.15        172.217.7.228   TLSv1.2   100 Application Data
     25 53.3097370 172.217.7.228    10.0.2.15       TCP        60 https > res [ACK] Seq=1 Ack=142 Win=65535 Len=0
     26 53.3097730 172.217.7.228    10.0.2.15       TCP        60 https > res [ACK] Seq=1 Ack=188 Win=65535 Len=0
     27 53.3282750 172.217.7.228    10.0.2.15       TLSv1.2   100 Application Data
     28 53.3283440 172.217.7.228    10.0.2.15       TLSv1.2   127 Application Data
     29 53.3283550 10.0.2.15        172.217.7.228   TCP        54 res > https [ACK] Seq=188 Ack=120 Win=64140 Len=0
     30 53.3285930 172.217.7.228    10.0.2.15       TLSv1.2   138 Application Data, Application Data
     31 53.3291340 10.0.2.15        172.217.7.228   TLSv1.2   100 Application Data
     32 53.3293490 172.217.7.228    10.0.2.15       TCP        60 https > res [ACK] Seq=204 Ack=234 Win=65535 Len=0
     33 54.5052020 10.0.2.15        172.217.7.228   TLSv1.2   112 Application Data
     34 54.5054730 172.217.7.228    10.0.2.15       TCP        60 https > res [ACK] Seq=204 Ack=292 Win=65535 Len=0
     35 54.7277270 172.217.7.228    10.0.2.15       TLSv1.2   474 Application Data
     36 54.7278770 172.217.7.228    10.0.2.15       TLSv1.2  1474 Application Data
     37 54.7278890 10.0.2.15        172.217.7.228   TCP        54 res > https [ACK] Seq=292 Ack=2044 Win=65535 Len=0
```

```
⊞ Frame 30: 138 bytes on wire (1104 bits), 138 bytes captured (1104 bits) on interface 0
⊞ Ethernet II, Src: RealtekU_12:35:02 (52:54:00:12:35:02), Dst: CadmusCo_7c:ec:ff (08:00:27:7c:ec:ff)
⊞ Internet Protocol Version 4, Src: 172.217.7.228 (172.217.7.228), Dst: 10.0.2.15 (10.0.2.15)
⊞ Transmission Control Protocol, Src Port: https (443), Dst Port: res (1942), Seq: 120, Ack: 188, Len: 84
⊟ Secure Sockets Layer
  ⊟ TLSv1.2 Record Layer: Application Data Protocol: http
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 33
      Encrypted Application Data: 000000000000004e8f6fdabef3115a8fc1f34c3af7593b85...
  ⊟ TLSv1.2 Record Layer: Application Data Protocol: http
      Content Type: Application Data (23)
      Version: TLS 1.2 (0x0303)
      Length: 41
      Encrypted Application Data: 000000000000004f2bc7661c9ec3e1aea36d435c8eb0cf0a...
```

```
0000   08 00 27 7c ec ff 52 54  00 12 35 02 08 00 45 00   ..'|..RT ..5...E.
0010   00 7c 15 a3 00 00 40 06  a4 0d ac d9 07 e4 0a 00   .|....@. ........
0020   02 0f 01 bb 07 96 00 ff  17 2e f3 31 f7 76 50 18   ........ ...1.vP.
0030   ff ff 8a 7b 00 00 17 03  03 00 21 00 00 00 00 00   ...{.... ..!.....
0040   00 00 4e 8f 6f da be f3  11 5a 8f c1 f3 4c 3a f7   ..N.o... .Z...L:.
0050   59 3b 85 8a ad 21 a7 04  86 1a 45 ad 17 03 03 00   Y;...!.. ..E.....
0060   29 00 00 00 00 00 00 00  4f 2b c7 66 1c 9e c3 e1   )....... O+.f....
0070   ae a3 6d 43 5c 8e b0 cf  0a 22 37 ba bb ef 07 8a   ..mC\... ."7.....
0080   b8 d2 16 1c 9d db 8c dc  6f 3e                     ........ o>
```

Payload is encrypted application data (ssl.app_d... Packets: 781 · Displayed: 781 (100.0%) · Dropped: 0 (0.0%)

Conclusion

In conclusion this executable has been classified as a malicious trojan. Immediate and necessary action have been scheduled to remove this file from the infected system and the network is also being monitored for any traces of this trojan.

From this lab I learned that one should not download any executables/ files from outside IT norms and even if someone did it has to be immediately reported so that the incident response team can take immediate action before severe damage is done.