Assignment 5 Report

Group Name: Aw, Snap!
Group Members: Weijia Sun, Xinyu Lyu, Mengmei Ye

Introduction on Snort:
It is an open source intrusion prevention system capable of real-time traffic analysis and packet logging. For this assignment, we are gonna use the Snort to analyze the Lab03-01.exe

Install snort on Ubuntu 16.04:
1. First we use the command lines below to get the source codes of snort.

```
$ wget https://www.snort.org/downloads/snort/daq-2.0.6.tar.gz
$ wget https://www.snort.org/downloads/snort/snort-2.9.13.tar.gz
```

2. Then we extract the source package with the codes below.

```
$ tar xvzf daq-2.0.6.tar.gz
$ tar xvzf snort-2.9.11.1.tar.gz
```

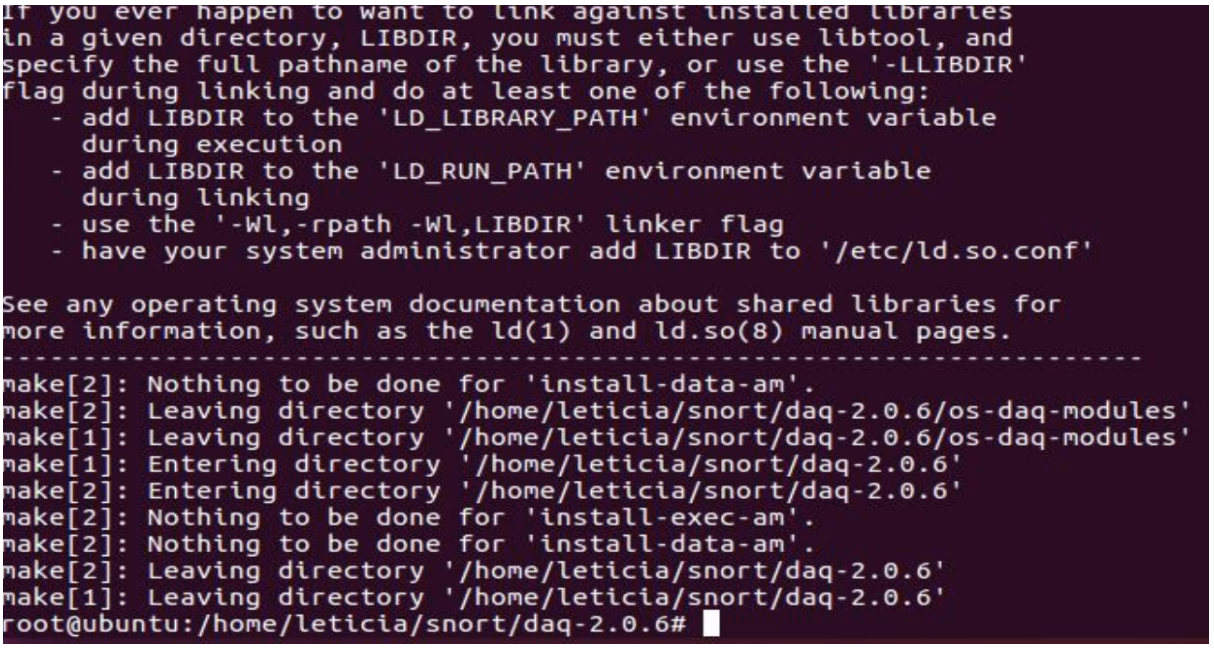
3. Before installing the packages, we need install some development packages that daq depends on with the command lines shown below.

```
$ sudo apt-get install flex
$ sudo apt-get install bison
$ sudo apt-get install libpcap-dev
```

4. Then enter the path of the daq, compile and install the package with the command lines below.

```
$ cd daq-2.0.6
$ ./configure && make && make install
```

And the figure below shows that daq has been installed successfully.



5. Then we need to install some development packages that snort depends on, otherwise the configuration script will report an error due to the lack of libpcre-dev, libdumbnet-dev.

```
$ sudo apt-get install libpcre3-dev
$ sudo apt-get install libdumbnet-dev
$ sudo apt-get install zlib1g-dev
```

6. Then we create a directory in local, then enter the extracted snort directory, compile and install snort with the command line below.

```
$ mkdir /usr/local/snort
$ ./configure --prefix=/usr/local/snort/ --enable-sourcefire && make &&
make install
```

The figure below shows that the snort has been successfully.

```
make[3]: Entering directory '/home/leticia/snort/snort-2.9.11.1/tools/u2spewfoo
 /bin/mkdir -p '/usr/local/snort/bin'
  /bin/bash ../../libtool   --mode=install /usr/bin/install -c u2spewfoo '/usr/
ocal/snort/bin'
libtool: install: /usr/bin/install -c u2spewfoo /usr/local/snort/bin/u2spewfoo
make[3]: Nothing to be done for 'install-data-am'.
make[3]: Leaving directory '/home/leticia/snort/snort-2.9.11.1/tools/u2spewfoo'
make[2]: Leaving directory '/home/leticia/snort/snort-2.9.11.1/tools/u2spewfoo'
make[2]: Entering directory '/home/leticia/snort/snort-2.9.11.1/tools'
make[3]: Entering directory '/home/leticia/snort/snort-2.9.11.1/tools'
make[3]: Nothing to be done for 'install-data-am'.
make[3]: Leaving directory '/home/leticia/snort/snort-2.9.11.1/tools'
make[2]: Leaving directory '/home/leticia/snort/snort-2.9.11.1/tools'
make[1]: Leaving directory '/home/leticia/snort/snort-2.9.11.1/tools'
make[1]: Entering directory '/home/leticia/snort/snort-2.9.11.1'
make[2]: Entering directory '/home/leticia/snort/snort-2.9.11.1'
make[2]: Nothing to be done for 'install-exec-am'.
 /bin/mkdir -p '/usr/local/snort/share/man/man8'
 /usr/bin/install -c -m 644 snort.8 '/usr/local/snort/share/man/man8'
 /bin/mkdir -p '/usr/local/snort/lib/pkgconfig'
 /usr/bin/install -c -m 644 snort.pc '/usr/local/snort/lib/pkgconfig'
make[2]: Leaving directory '/home/leticia/snort/snort-2.9.11.1'
make[1]: Leaving directory '/home/leticia/snort/snort-2.9.11.1'
root@ubuntu:/home/leticia/snort/snort-2.9.11.1#
```

7. Before validating the configuration of the snort, we first find the IP address of the system.Then we use the commands line below to valid the configuration of the snort. And we can use the lo as the test environment since the we want to locally analyse the Lab03-01.exe.

```
yingyue@hkx-OptiPlex-5040:~/snort-2.9.13$ ifconfig
docker0   Link encap:Ethernet  HWaddr 02:42:9d:e0:1e:60
          inet addr:172.17.0.1  Bcast:172.17.255.255  Mask:255.255.0.0
          UP BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:0
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)

eno1      Link encap:Ethernet  HWaddr 34:17:eb:dc:4c:f4
          inet addr:172.16.79.45  Bcast:172.16.79.255  Mask:255.255.255.0
          inet6 addr: fe80::1830:1e47:6135:3ebb/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:29101 errors:0 dropped:0 overruns:0 frame:0
          TX packets:7352 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:16713539 (16.7 MB)  TX bytes:2392729 (2.3 MB)
          Interrupt:20 Memory:f7c00000-f7c20000

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:446 errors:0 dropped:0 overruns:0 frame:0
          TX packets:446 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:35841 (35.8 KB)  TX bytes:35841 (35.8 KB)
```

Configuration of the snort:

Then we use the command lines below to valid the configuration of the snort.

```
$ sudo snort -T -c /etc/snort/snort.conf -i lo
```

```
yingyue@hkx-OptiPlex-5040: ~
yingyue@hkx-OptiPlex-5040:~$ sudo snort -T -c /etc/snort/snort.conf -i lo
[sudo] password for yingyue:
Running in Test mode

        --== Initializing Snort ==--
Initializing Output Plugins!
Initializing Preprocessors!
Initializing Plug-ins!
Parsing Rules file "/etc/snort/snort.conf"
PortVar 'HTTP_PORTS' defined :  [ 36 80:90 311 383 555 591 593 631 801 808 818 9
01 972 1158 1220 1414 1533 1741 1830 1942 2231 2301 2381 2578 2809 2980 3029 303
7 3057 3128 3443 3702 4000 4343 4848 5000 5117 5250 5450 5600 5814 6080 6173 698
8 7000:7001 7005 7071 7144:7145 7510 7770 7777:7779 8000:8001 8008 8014:8015 802
0 8028 8040 8080:8082 8085 8088 8090 8118 8123 8180:8182 8222 8243 8280 8300 833
3 8344 8400 8443 8500 8509 8787 8800 8888 8899 8983 9000 9002 9060 9080 9090:909
1 9111 9290 9443 9447 9710 9788 9999:10000 11371 12601 13014 15489 19980 29991 3
3300 34412 34443:34444 40007 41080 44449 50000 50002 51423 53331 55252 55555 567
12 ]
PortVar 'SHELLCODE_PORTS' defined :  [ 0:79 81:65535 ]
PortVar 'ORACLE_PORTS' defined :  [ 1024:65535 ]
PortVar 'SSH_PORTS' defined :  [ 22 ]
PortVar 'FTP_PORTS' defined :  [ 21 2100 3535 ]
PortVar 'SIP_PORTS' defined :  [ 5060:5061 5600 ]
PortVar 'FILE_DATA_PORTS' defined :  [ 36 80:90 110 143 311 383 555 591 593 631
801 808 818 901 972 1158 1220 1414 1533 1741 1830 1942 2231 2301 2381 2578 2809
2980 3029 3037 3057 3128 3443 3702 4000 4343 4848 5000 5117 5250 5450 5600 5814
6080 6173 6988 7000:7001 7005 7071 7144:7145 7510 7770 7777:7779 8000:8001 8008
8014:8015 8020 8028 8040 8080:8082 8085 8088 8090 8118 8123 8180:8182 8222 8243
8280 8300 8333 8344 8400 8443 8500 8509 8787 8800 8888 8899 8983 9000 9002 9060
9080 9090:9091 9111 9290 9443 9447 9710 9788 9999:10000 11371 12601 13014 15489
19980 29991 33300 34412 34443:34444 40007 41080 44449 50000 50002 51423 53331 55
252 55555 56712 ]
PortVar 'GTP_PORTS' defined :  [ 2123 2152 3386 ]
Detection:
   Search-Method = AC-Full-Q
    Split Any/Any group = enabled
    Search-Method-Optimizations = enabled
    Maximum pattern length = 20
```

```
yingyue@hkx-OptiPlex-5040: ~
[ Number of patterns truncated to 20 bytes: 640 ]
pcap DAQ configured to passive.
Acquiring network traffic from "lo".

        --== Initialization Complete ==--

           -*> Snort! <*-
  ,,_      Version 2.9.13 GRE (Build 15013)
 o"  )~    By Martin Roesch & The Snort Team: http://www.snort.org/contact#team
   ''''    Copyright (C) 2014-2019 Cisco and/or its affiliates. All rights reser
ved.
           Copyright (C) 1998-2013 Sourcefire, Inc., et al.
           Using libpcap version 1.7.4
           Using PCRE version: 8.42 2018-03-20
           Using ZLIB version: 1.2.11

           Rules Engine: SF_SNORT_DETECTION_ENGINE  Version 3.1  <Build 1>
           Preprocessor Object: SF_IMAP  Version 1.0  <Build 1>
           Preprocessor Object: SF_DNS  Version 1.1  <Build 4>
           Preprocessor Object: SF_SMTP  Version 1.1  <Build 9>
           Preprocessor Object: SF_SDF  Version 1.1  <Build 1>
           Preprocessor Object: SF_MODBUS  Version 1.1  <Build 1>
           Preprocessor Object: SF_GTP  Version 1.1  <Build 1>
           Preprocessor Object: appid  Version 1.1  <Build 5>
           Preprocessor Object: SF_DNP3  Version 1.1  <Build 1>
           Preprocessor Object: SF_FTPTELNET  Version 1.2  <Build 13>
           Preprocessor Object: SF_DCERPC2  Version 1.0  <Build 3>
           Preprocessor Object: SF_REPUTATION  Version 1.1  <Build 1>
           Preprocessor Object: SF_SIP  Version 1.1  <Build 1>
           Preprocessor Object: SF_SSLPP  Version 1.1  <Build 4>
           Preprocessor Object: SF_POP  Version 1.0  <Build 1>
           Preprocessor Object: SF_SSH  Version 1.1  <Build 3>

Snort successfully validated the configuration!
Snort exiting
```

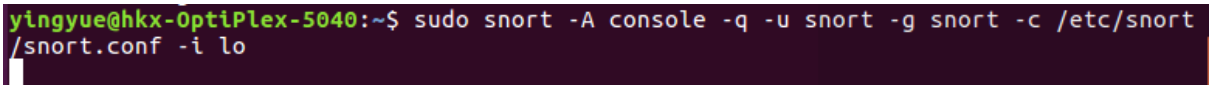
And the figures above shows that the we successfully validated the configuration of the snort.

Launch snort and monitor:

1. After validating the configuration of the snort, we want to launch the snort and monitor the loc IP address.

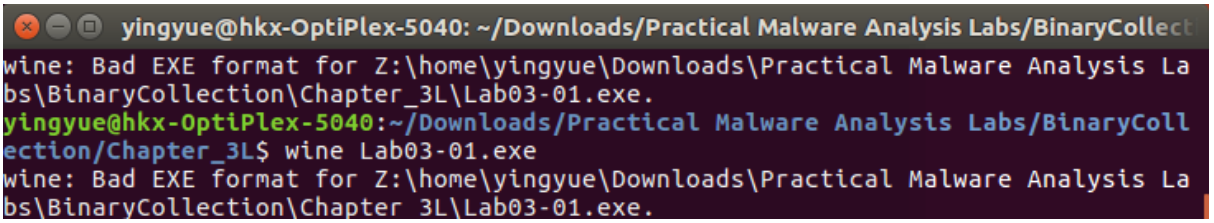
```
$ sudo snort -A console -q -u snort -g snort -c /etc/snort/snort.conf -i
lo
```

The figure below shows that we successfully launch the snort.



2. As we know, the Ubuntu system cannot execute exe file. Therefore, we install Wine on Ubuntu with the command lines below.

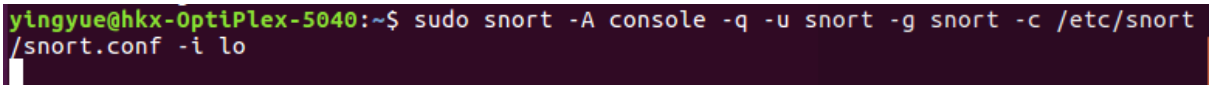
```
$ sudo add-apt-repository ppa:ubuntu-wine/ppa
$ sudo apt-get update
$ sudo apt-get install wine1.8
$ sudo apt-get install winetricks
```



3. Then, we are able to execute the Lab03-01.exe with the command lines below.

```
wine Lab03-01.exe
```

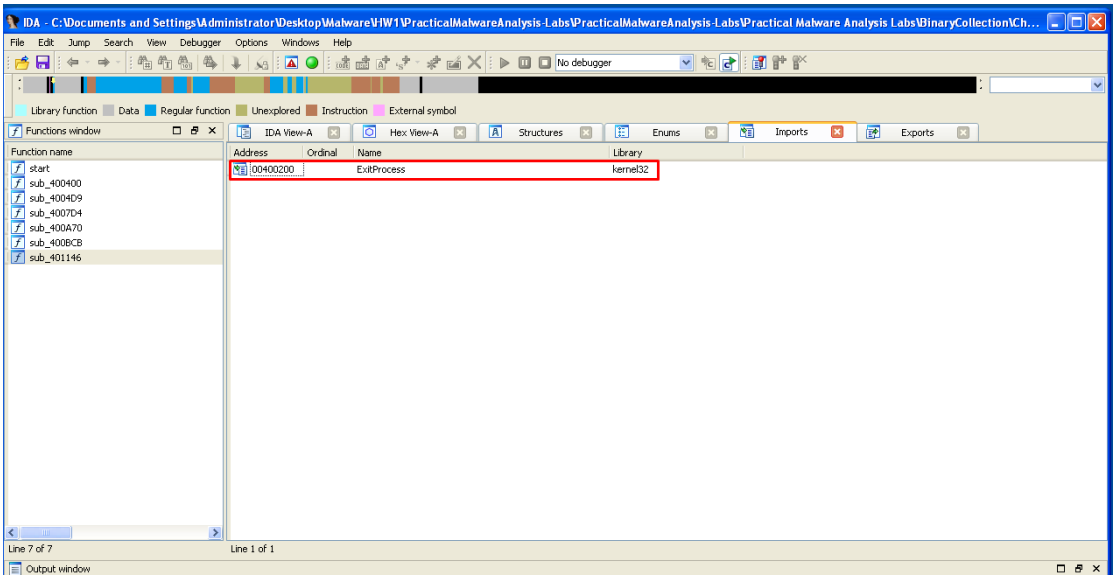
4. However, there are no log information at lo on snort detecting the call to http://www.practicalmalwareanalysis.com (DNS resolve) or the SSL connection or the TCP stream. We have tried our best to figure out the reason behind. However, we still can't find the solution. And we will continue to find the reason in the future.



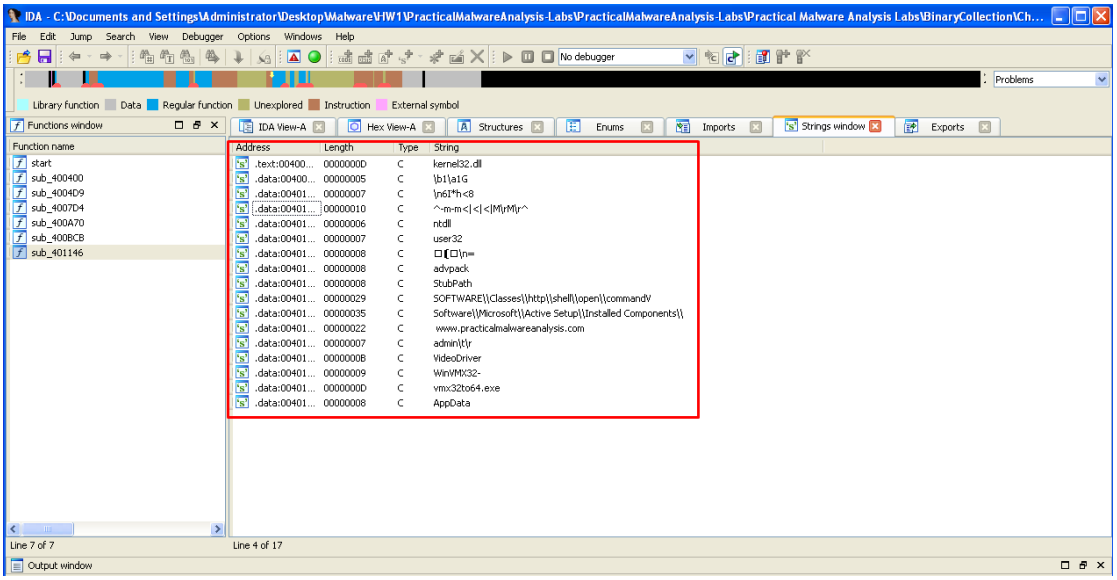
Analysis of Lab 03-01.exe

Since we cannot use the snort to analyze the malware, we tried to pick up the IDAPRO PEid Wireshark to analyze the malware, here is the result of analysis.

The import of the Lab 03-01.exe

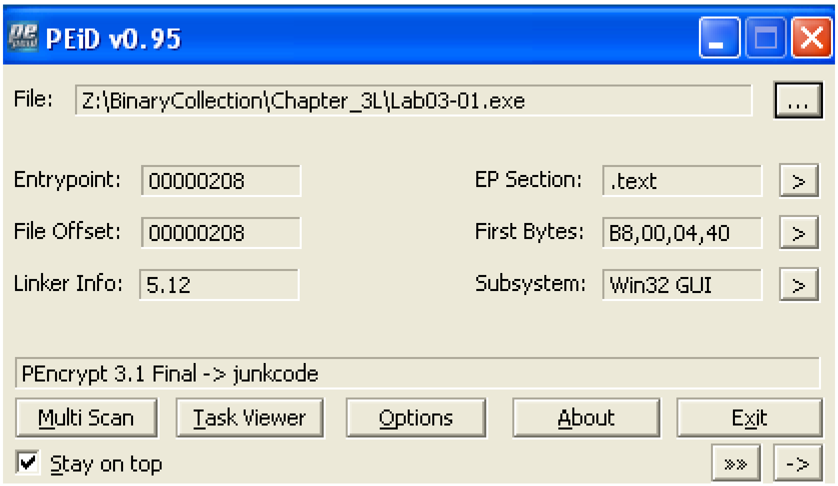


We use IDA pro for basic dynamic analysis of lab 3-1. And it reveals that the only import is ExitProcess from the kernel32 library.



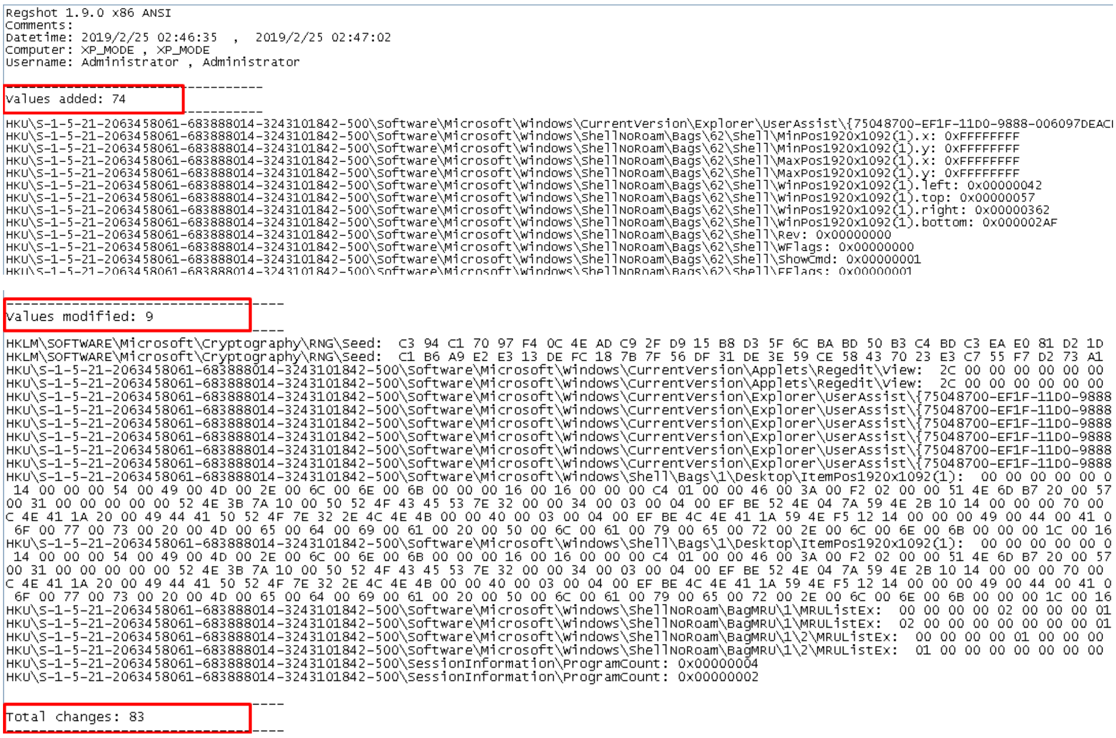
From the strings, we can obtain more information.
First, we monitor the registry of **SOFTWARE\\Classes\\http\\shell\\open \\commandV, Software\\Microsoft\\Active Setup\\Installed Components**. Then, we monitor the network traffic of http://www.practicalmalwarea nalysis.com.
Finally, we monitor the **vmx32to64.exe**, because it may hide somewhere in the infected machines.

We first run the lab 3-1.exe on PEiD to make sure that the malware has not been packed before.



We are sure that the malware has not been packed before.

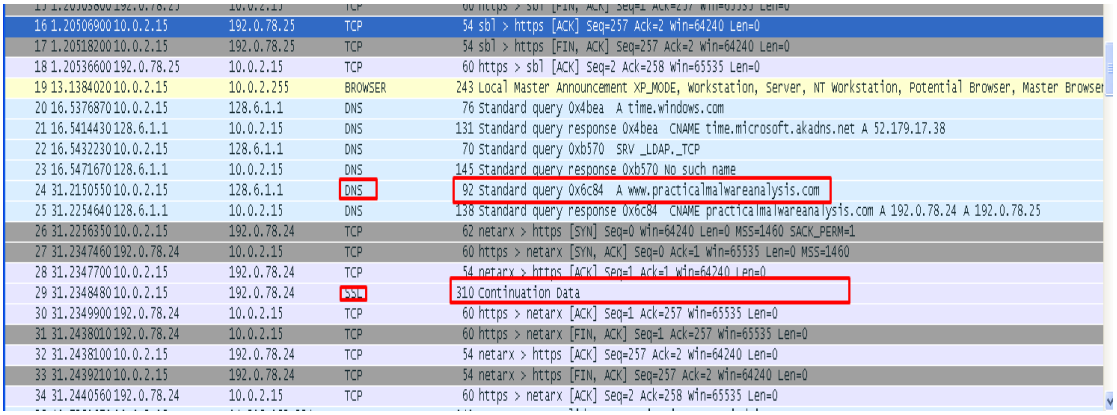
Regshot



```
Regshot 1.9.0 x86 ANSI
Comments:
Datetime: 2019/2/25 02:46:35  ,  2019/2/25 02:47:02
Computer: XP_MODE , XP_MODE
Username: Administrator , Administrator

----------------------------------------
Values added: 74
----------------------------------------
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACI
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\MinPos1920x1092(1).x: 0xFFFFFFFF
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\MinPos1920x1092(1).y: 0xFFFFFFFF
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\MaxPos1920x1092(1).x: 0xFFFFFFFF
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\MaxPos1920x1092(1).y: 0xFFFFFFFF
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\WinPos1920x1092(1).left: 0x00000042
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\WinPos1920x1092(1).top: 0x00000057
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\WinPos1920x1092(1).right: 0x00000362
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\WinPos1920x1092(1).bottom: 0x000002AF
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\Rev: 0x00000000
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\WFlags: 0x00000000
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\ShowCmd: 0x00000001
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\ShellNoRoam\Bags\62\Shell\FFlags: 0x00000001

----------------------------------------
Values modified: 9
----------------------------------------
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  C3 94 C1 70 97 F4 0C 4E AD C9 2F D9 15 B8 D3 5F 6C BA BD 50 B3 C4 BD C3 EA E0 81 D2 1D
HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed:  C1 B6 A9 E2 E3 13 DE FC 18 7B 7F 56 DF 31 DE 3E 59 CE 58 43 70 23 E3 C7 55 F7 D2 73 A1
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit\View:  2C 00 00 00 00 00 00
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\CurrentVersion\Applets\Regedit\View:  2C 00 00 00 00 00 00
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\Shell\Bags\1\Desktop\ItemPos1920x1092(1):  00 00 00 00 00 0
 14 00 00 00 54 00 49 00 4D 00 2E 00 6C 00 6E 00 6B 00 00 00 16 00 16 00 00 00 C4 01 00 00 46 00 3A 00 F2 02 00 00 51 4E 6D B7 20 00 57
00 31 00 00 00 00 00 52 4E 3B 7A 10 00 50 52 4F 43 45 53 7E 32 00 00 34 00 03 00 04 00 EF BE 52 4E 04 7A 59 4E 2B 10 14 00 00 00 70 00
C 4E 41 1A 20 00 49 44 41 50 52 4F 7E 32 2E 4C 4E 4B 00 00 40 00 03 00 04 00 EF BE 4C 4E 41 1A 59 4E F5 12 14 00 00 00 49 00 44 00 41 0
 6F 00 77 00 73 00 20 00 4D 00 65 00 64 00 69 00 61 00 20 00 50 00 6C 00 61 00 79 00 65 00 72 00 2E 00 6C 00 6E 00 6B 00 00 00 1C 00 16
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\Shell\Bags\1\Desktop\ItemPos1920x1092(1):  00 00 00 00 00 0
 14 00 00 00 54 00 49 00 4D 00 2E 00 6C 00 6E 00 6B 00 00 00 16 00 16 00 00 00 C4 01 00 00 46 00 3A 00 F2 02 00 00 51 4E 6D B7 20 00 57
00 31 00 00 00 00 00 52 4E 3B 7A 10 00 50 52 4F 43 45 53 7E 32 00 00 34 00 03 00 04 00 EF BE 52 4E 04 7A 59 4E 2B 10 14 00 00 00 70 00
C 4E 41 1A 20 00 49 44 41 50 52 4F 7E 32 2E 4C 4E 4B 00 00 40 00 03 00 04 00 EF BE 4C 4E 41 1A 59 4E F5 12 14 00 00 00 49 00 44 00 41 0
 6F 00 77 00 73 00 20 00 4D 00 65 00 64 00 69 00 61 00 20 00 50 00 6C 00 61 00 79 00 65 00 72 00 2E 00 6C 00 6E 00 6B 00 00 00 1C 00 16
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\1\MRUListEx:  00 00 00 00 02 00 00 00 01
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\1\MRUListEx:  02 00 00 00 00 00 00 00 01
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\1\2\MRUListEx:  00 00 00 00 01 00 00 00
HKU\S-1-5-21-2063458061-683888014-3243101842-500\Software\Microsoft\Windows\ShellNoRoam\BagMRU\1\2\MRUListEx:  01 00 00 00 00 00 00 00
HKU\S-1-5-21-2063458061-683888014-3243101842-500\SessionInformation\ProgramCount: 0x00000004
HKU\S-1-5-21-2063458061-683888014-3243101842-500\SessionInformation\ProgramCount: 0x00000002

----------------------------------------
Total changes: 83
----------------------------------------
```

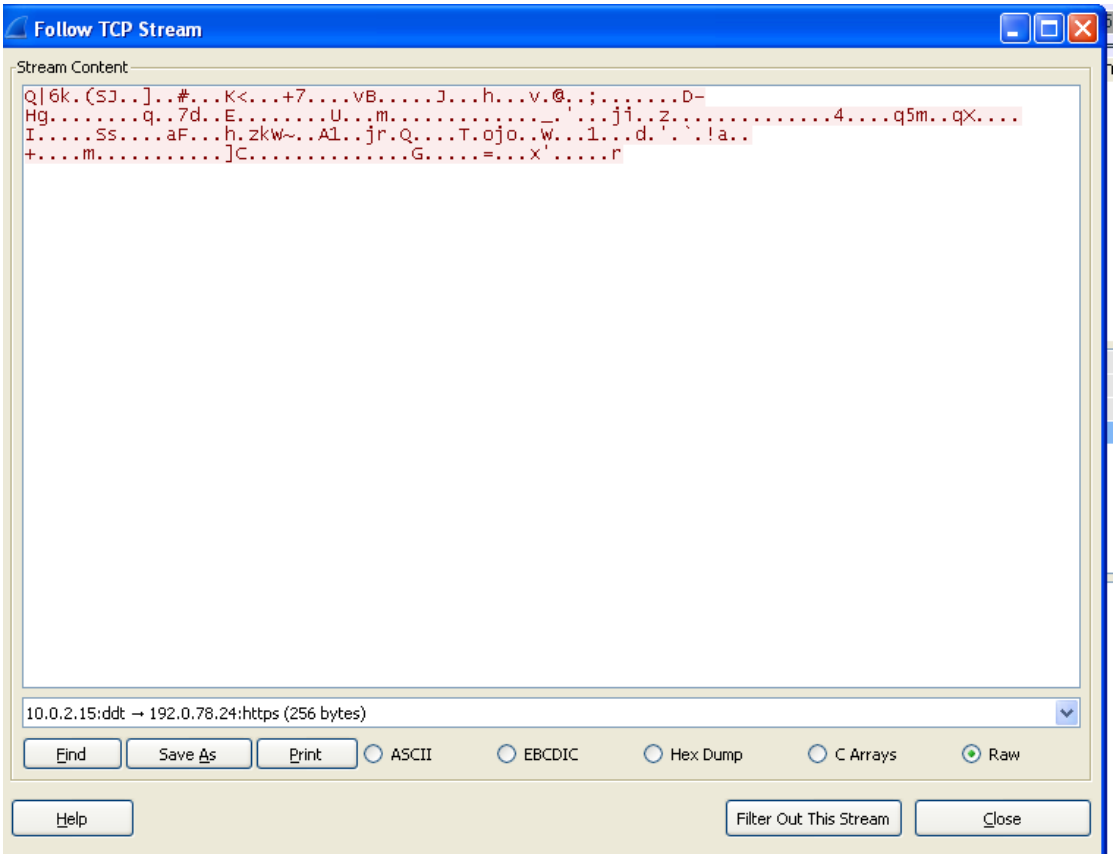
After using Regshot, we compare the registry and found out that the malware is trying to execute c:\windows\system32\vmx32to64.exe.

Wireshark



16 1.20506900	10.0.2.15	192.0.78.25	TCP	54 sbl > https [ACK] Seq=257 Ack=2 Win=64240 Len=0
17 1.20518200	10.0.2.15	192.0.78.25	TCP	54 sbl > https [FIN, ACK] Seq=257 Ack=2 Win=64240 Len=0
18 1.20536600	192.0.78.25	10.0.2.15	TCP	60 https > sbl [ACK] Seq=2 Ack=258 Win=65535 Len=0
19 13.1384020	10.0.2.15	10.0.2.255	BROWSER	243 Local Master Announcement XP_MODE, Workstation, Server, NT Workstation, Potential Browser, Master Browse
20 16.5376870	10.0.2.15	128.6.1.1	DNS	76 Standard query 0x4bea A time.windows.com
21 16.5414430	128.6.1.1	10.0.2.15	DNS	131 Standard query response 0x4bea CNAME time.microsoft.akadns.net A 52.179.17.38
22 16.5432230	10.0.2.15	128.6.1.1	DNS	70 Standard query 0xb570 SRV _LDAP._TCP
23 16.5471670	128.6.1.1	10.0.2.15	DNS	145 Standard query response 0xb570 No such name
24 31.2150550	10.0.2.15	128.6.1.1	DNS	92 Standard query 0x6c84 A www.practicalmalwareanalysis.com
25 31.2254640	128.6.1.1	10.0.2.15	DNS	138 Standard query response 0x6c84 CNAME practicalmalwareanalysis.com A 192.0.78.24 A 192.0.78.25
26 31.2256350	10.0.2.15	192.0.78.24	TCP	62 netarx > https [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
27 31.2347460	192.0.78.24	10.0.2.15	TCP	60 https > netarx [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460
28 31.2347700	10.0.2.15	192.0.78.24	TCP	54 netarx > https [ACK] Seq=1 Ack=1 Win=64240 Len=0
29 31.2348480	10.0.2.15	192.0.78.24	SSL	310 Continuation Data
30 31.2349900	192.0.78.24	10.0.2.15	TCP	60 https > netarx [ACK] Seq=1 Ack=257 Win=65535 Len=0
31 31.2438010	192.0.78.24	10.0.2.15	TCP	60 https > netarx [FIN, ACK] Seq=1 Ack=257 Win=65535 Len=0
32 31.2438100	10.0.2.15	192.0.78.24	TCP	54 netarx > https [ACK] Seq=257 Ack=2 Win=64240 Len=0
33 31.2439210	10.0.2.15	192.0.78.24	TCP	54 netarx > https [FIN, ACK] Seq=257 Ack=2 Win=64240 Len=0
34 31.2440560	192.0.78.24	10.0.2.15	TCP	60 https > netarx [ACK] Seq=2 Ack=258 Win=65535 Len=0

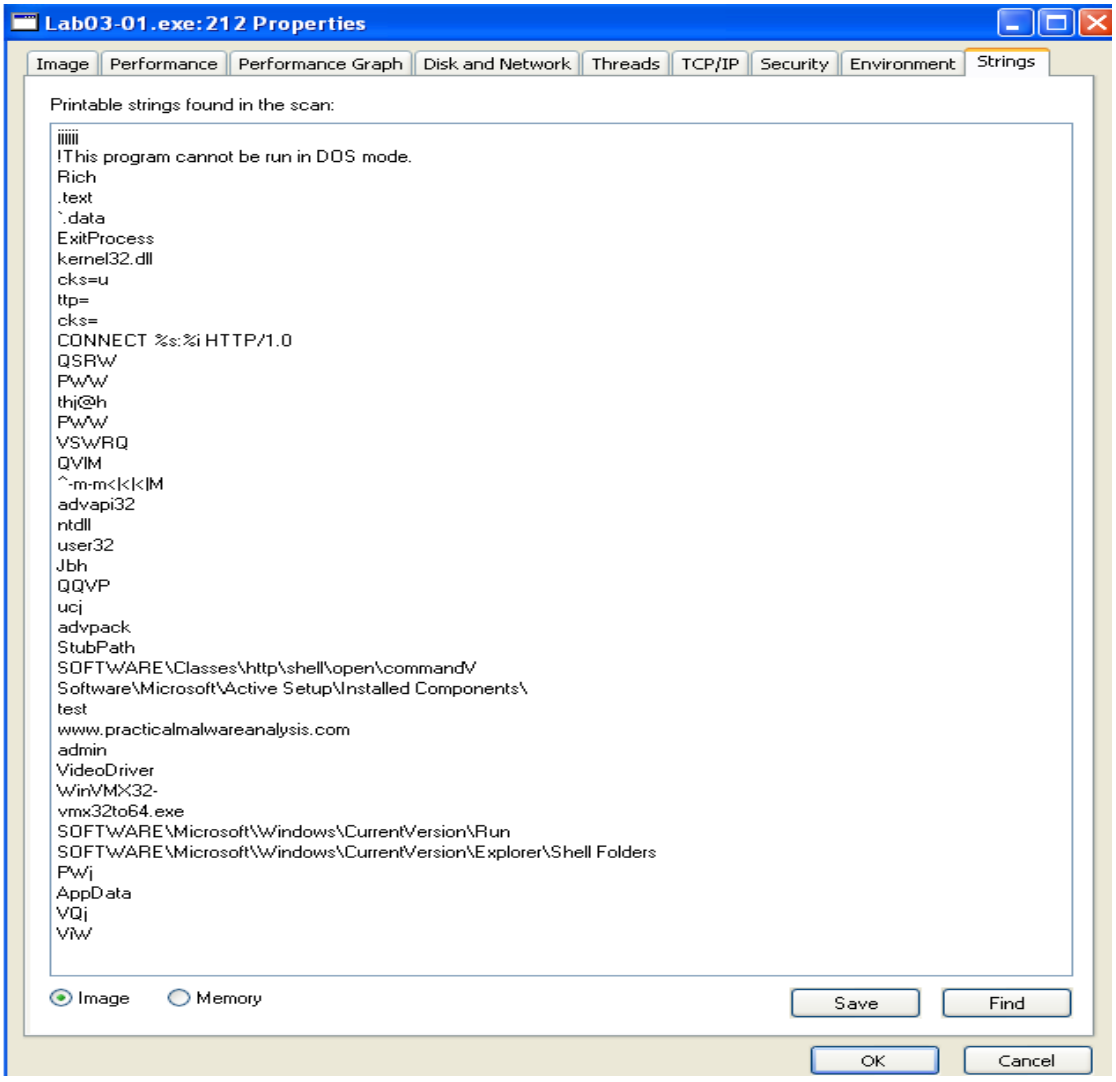
From the track history of Wireshark, we find that a call was made to www.practicalmalwareanalysis.com (DNS as a protocol). Then, an SSL connection has been made.



At last, we can see that some random 256 bytes being sent following the TCP data stream.

Process Explorer

Type	Name
Directory	\KnownDlls
Directory	\Windows
Directory	\BaseNamedObjects
File	C:\Documents and Settings\Administrator\Desktop
File	\Device\KsecDD
Key	HKLM
Key	HKLM\SYSTEM\ControlSet001\Services\WinSock2\Parameters\Protocol_Catalog9
Key	HKLM\SYSTEM\ControlSet001\Services\WinSock2\Parameters\NameSpace_Catalog5
KeyedEvent	\KernelObjects\CritSecOutOfMemoryEvent
Mutant	\BaseNamedObjects\WinVMX32
Semaphore	\BaseNamedObjects\shell.{A48F1A32-A340-11D1-BC6B-00A0C90312E1}
Thread	Lab03-01.exe(4000): 4004
Thread	Lab03-01.exe(4000): 4004
WindowStation	\Windows\WindowStations\WinSta0
WindowStation	\Windows\WindowStations\WinSta0



With the analysis from Process Explorer, we can see more strings and the mutex handle.

The basic signature is **http://www.practicalmalwareanalysis.com**. And they are the 256 random bytes being sent via port 443 following the TCP data stream.