Lab 3: Malware and Network Analysis

1 Details

Aim: To provide a foundation in understanding malware, with a special focus on network analysis

This lab should only be run in a virtual image. Only connect to the network from the Windows XP when told to.

A demo of this lab is here: http://youtu.be/t_P7IkJn748

2 Analysing Malware

L1.1 We are going to investigate a variant of **Worm.Win32.Dorkbot.**

What are the key elements of the malware:

The malware is named DQ.EXE. Can you find any information on this malware?

L1.2 Run the Windows XP image. Now **DISCONNECT THE VM FROM THE NETWORK**. Go to your network adapter and define it with an address of 10.0.0.1 and a gateway of 10.0.0.1.

L1.3 Now try and connect from Windows XP to the Internet from a browser, and MAKE SURE YOU CANNOT CONNECT.

L1.4 Examine your IP address with IPCONFIG MAKE SURE YOUR ADDRESS IS 10.0.0.1 AND THAT YOU DO NOT HAVE ANY PUBLIC IP ADDRESSES.

Can you verify that you are not connect to the Internet?

L1.5 You will now be given DQ.EXE. Please ask you **tutor** for this.

L1.6 Download an MD5 and a SHA program and determine the fingerprint of the program (run **openssl md5 dq.exe**):

Outline the MD5 and SHA signature:

How many characters does MD5 signature have:

How many characters does SHA signature have:

L1.7 Start Wireshark and examine the basic flow of network traffic. There should be very little that is interesting in the traffic.

L1.8 Run the program from the command console.

What can you observe from running the program:

L1.9 Go to the c:\recycler folder. Can you find the malware:

What is the c:\recycler folder normally used for:

How did you find the malware?

Run the attrib *.* command, and determine the attributes on the malware files in c:\recycler folder:

Which command do you need to delete the files:

Make sure you have deleted them … check with dir /ah**. Are they gone?**

L1.10 Go to the registry with REGEDIT.EXE. Now go to:
HKCU\Software\Microsoft\Windows\CurrentVersion\Run

Where is the malware located within the Registry:

What does the registry entry do on the system:

L1.11 Examine the Wireshark trace.

What can you observe from the trace that the malware has done:

L1.12 Using HexWin, examine the memory. Can you determine anything that you could produce a fingerprint of the malware with:

Possible fingerprint signs:

L1.13 Now clean up the VM:

Did you manage to delete the files in c:\recyler:

Did you manage to delete the registry key:

After you clean up, reboot the VM, and check that malware is not present:

L1.14 Restore the VM to its original state using VM->Restore Snapshot.

4 Analysing the malware

Using the pfSense firewall, get the hosts on your DMZ online, using the addresses you were allocated in a previous lab (or with your own address). You can also run this part on any desktop with Wireshark installed, or insert a USB device into the virtual machine.

Demo: http://youtu.be/YJhqCOh4fLk

L1.15 It is too dangerous in the lab environment to enable the network adapter, so the following is a trace of it running on your desktop computer:

http://asecuritysite.com/log/dpexe.zip

Download and analyse it for:

Identify the basic signs of it when there is a connection to 10.0.0.1:

At which packet number does it manage to resolve the malicious domain:

What is the IP address it connects to:

Outline what it tries to do, and what the result is from the server it communicates with:

L1.16 On reflection, how would you create a detector on the network or on the host to detect this malware:

Outline methods that could be used:

5 Snort detector

L1.17 We can detect the presence of the malware agent using Snort as an IDS (Intrusion Detection System).

Now go to the c:\snort\bin folder and create a file (1.rules) with :

```
# Some additional pre-processor things
 preprocessor stream5_global: track_tcp yes, \
   track_udp yes, \
   track_icmp no, \
   max_tcp 262144, \
   max_udp 131072, \
   max_active_responses 2, \
   min_response_seconds 5
preprocessor stream5_tcp: policy windows, detect_anomalies, require_3whs 180, \
   overlap_limit 10, small_segments 3 bytes 150, timeout 180, \
    ports client 21 22 23 25 42 53 70 79 109 110 111 113 119 135 136 137 139 143 \
        161 445 513 514 587 593 691 1433 1521 1741 2100 3306 6070 6665 6666 6667 6668 6669 \
        7000 8181 32770 32771 32772 32773 32774 32775 32776 32777 32778 32779, \
    ports both 80 81 82 83 84 85 86 87 88 89 90 110 311 383 443 465 563 591 593 631 636 901 989 992 993 994 995 1220 1414 1830 2301 2381 2809 3037 3057 3128 3443 3702 4343 4848 5250 6080 6988
        7907 7000 7001 7144 7145 7510 7802 7777 7779 \
       7801 7900 7901 7902 7903 7904 7905 7906 7908 7909 7910 7911 7912 7913 7914 7915 7916 \
        7917 7918 7919 7920 8000 8008 8014 8028 8080 8085 8088 8090 8118 8123 8180 8222 8243 8280 8300 8500 8800 8888 8899 9000 9060 9080 9090 9091 9443 9999 10000 11371 34443 34444 41080 50000
        50002 55555
preprocessor stream5_udp: timeout 180
```

```
alert udp any any -> any 53 (content: "fjpark";sid:1111; msg: "DQ Malware";)
```

Download file here: https://dl.dropboxusercontent.com/u/40355863/1.zip

What does the last line of the rule detect:

Next run Snort off-line with:

snort -c 1.rules -r dqexe.pcap -l log

Outline the contents of the alert.ids file in the log folder:

Next add rules to perform the following:

Sending an email to the SMTP server:

Detect the IP address of FJPARK.COM:

Detect Net-BIOS request for FJPARK.COM:

6 Reverse TCP connection

This part of the lab can be done on any desktop.

A typical method that an intruder will do on an infected machine is to perform a dial-back TCP connection. In this part of the lab, we will create, analyse and detect a basic dial-back connection.

L1.18 On Kali, download the following file (or mount a USB drive onto your VM):

http://asecuritysite.com/log/meta_reverse_tcp.zip

Next add rules to perform the following:

Which TCP port is used for the dial-back from the infected host:

Which is the IP address which hosts the malware:

Which is the IP address which is the attacker:

By using, Following Stream in Wireless, what does the intruder do on the machine:

7 Android malware

In this part of the lab we will analyse a reverse connection which installs the Metasploit Meterpreter.

L1.19 On Kali, download the following file:

http://asecuritysite.com/log/and_malware.zip

Outline the following:

Which is the Android IP address:

Which is the attacking IP address:

Which TCP port is used as a dial-back:

What does the attacker do on the device: