Lab 10: Malware Analysis (Host)

Aim

The aim of this lab is to provide a foundation in understanding of the threats that occur within malware (host) and how to detect and analyse it.

Outline

Malware analysis is the study or process of determining the functionality, origin and potential impact of a given malware sample such as a virus, worm, trojan horse, rootkit, or backdoor.

The Win32/Dorkbot family of worms (with an alert level of ***Severe***) can steal user names and passwords and can also perform spamming and Denial of Service (DoS) attacks. In this lab, we are going to investigate a variant of **Worm.Win32.Dorkbot.**

Activities:

Complete Lab 6:	Malware Analysis (Host).
Time to Complete:	up to 1 hour

Learning activities:

At the end of this lab, you should understand:

- How to analyse for key threats.
- How to detect threats.

Attention:

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

Lab Overview

We only use Windows XP Private in this lab.

Don't put any of your allocated IP addresses on your Windows XP Private. Only connect to the network from the Windows XP when told to.

Demonstrations can be found 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 Private** image. Make sure that your Windows XP Private is **DISCONNECTED FROM THE NETWORK**. For this, go to your network adapter and define it with: IP address of 10.0.0.1, subnet mask of: 255.0.0.0, default gateway of: 10.0.0.2 and preferred DNS server of 10.0.0.3.

L1.3 Now try and connect from Windows XP to the Internet from a browser, and **MAKE SURE YOU CANNOT CONNECT e.g. type: www.bbc.co.uk.**

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 connected to the Internet?

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

L1.6 Using an MD5 and a SHA program and determine the fingerprint of the program:

Outline the MD5 signature:

MD5:

How many characters does MD5 signature have? (**hint** use: md5sum in command prompt)

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 Go to the **c:\recycler** folder using command prompt and list the files. Can you see any files/folder there?

L1.9 Now run the program from the command console (**hint:** type: ***dq.exe***)

What can you observe on Wireshark after running the program?

L1.10 Now go to the **c:\recycler** folder using command prompt again and list the files.

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

Can you see any new directories in recycler? If so, enter to it and list all the files. Can you see any files there? How about when you use "/ah" attributes of "dir"?

How many files you can see in the directory after using "/ah" attributes of "dir"?

Now try to remove all the files there. (Hint: use "erase" command).

Now check if the malware is still there. If so, how can you erase it? (Hint: Run "attrib" command, and determine the attributes of the malware files)

What are the attributes of the malware?

Use "attrib -s -h -r" command and check if you can reset the attributes of the malware?

Now, use "attrib" command again and make sure you reset all the attributes of the malware.

Now try to remove all the files again by using "erase" command.

Check with "dir /ah". Are they gone?

L1.9 Go to the registry by typing "regedit". Now go to:
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run

Where is the malware located within the Registry? Can you spot the name?

What does the registry entry do on the system?

L1.10 Examine the Wireshark trace.

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

L1.11 Open HexWin and then the malware to examine the memory.

Can you determine anything that you could produce a fingerprint of the malware with? If so, what are the possible fingerprint signs?

L1.12 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.

L1.15 Restore the VM to its original state using VM->Restore Snapshot.

L1.13 It is too dangerous in the lab environment to enable the network adapter, so the following is a trace of it running in a real environment:

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?

L1.14 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.

Malware Analysis (Host Analysis)

Reflective statements (end-of-exercise):

You should reflect on these questions:

- What methods does the malware writer use to hide the file from the user, and how does it stop them from deleting it?
- What method can a malware writer use to make sure that the malware is loaded ever time that the computer is restarted?
- Without a connection to the Internet, what would you look for, for the malware connecting to a remote server?
- How might an intruder hide their malware from a virus scanner?
- How might a browser search engine redirect be used in a malicious way?