Assignment 2 -Network services emulation for malware analysis

In this assignment, you will be exploring tools for emulating network services within our virtual malware analysis setup. Malware is often designed to communicate with external servers after infecting victim computers, in order to receive further command and control instructions, update itself, download further components, exfiltrate data etc. Because we are interested in exercising the malware to reveal as much of its network behavior as possible, it is necessary to provide the malware with emulated network services in a controlled environment.

For this assignment, a file containing three malware samples is provided on Cactus1 server. The file is named samples.7z. During your analysis, copy the file to the Windows XP virtual machine and unzip it. The password for unzipping the file is 'infected'.

A manual to set up an isolated network with a Windows XP VM and a REMnux ® VM is provided with this assignment. Now, you will be using ApateDNS on the XP VM and INetSim on the REMnux VM.

ApateDNS on Windows XP

Copy the ApateDNS source file from the assignment folder on Cactus to the XP machine and then unzip it. Alternatively, you can download ApateDNS from the URL given at the end of this instructions guide. Use the readme file enclosed in the ApateDNS folder to guide you on the tool's usage.

Next, configure an isolated network with the following settings:
REMnux VM: IP = 192.168.10.2
WinXP VM: IP = 192.168.10.1

Default gateway: 192.168.10.2
Preferred DNS: 127.0.0.1

Confirm connectivity between the two VMs and then on the REMnux machine, start INetSim by typing at a terminal:

```
$ inetsim
```

Press the 'Start server' button to start the ApateDNS listening on the localhost port 53. Make sure that the right network interface is selected from the 'Selected Interface' drop down menu. You can configure # of NXDOMAINS =0 in the first instance and then repeat the tasks with:

# of NXDOMAINS =3.

Start up Wireshark as well on the REMnux machine to capture packets on the network interface.

With ApateDNS, Wireshark and INetSim running, carry out the activities below and note/record any network behavior observed and tools have captured or logged. The INetSim logs can be found at:

```
$/var/log/inetsim/
```

The generated activity report for what has occurred during the iNetSim session is located at:

```
$/var/log/inetsim/report/
```

The report is saved in a file named in the format 'report.process_id.txt', after the session is closed. You may have to change file permissions in order to read it with your text editor.

Activities

1. Open a browser on the XP machine. Send a request for an image file from a hypothetical (or real) HTTP server. What happens when you do this?
2. Send another request for a web page through HTTPS. What do you notice?

3. Try downloading an executable (either .com or .exe file) from any website. What happens when you make this request?
4. Unzip the file containing the three malware samples (password: infected). Execute each of them and note/record their network behaviour as observed by you and/or logged with the tools.

    - Which domains are the samples trying to contact?
    - What http requests (if any) are being made and when do these requests occur?
    - From the logs, traffic capture and tool outputs, can you establish the sequenc of events in the malware samples' network activities?

2nd part: Network services with FakeNet

In this second part of this assignment you will be using FakeNet instead of ApateDNS and INetSim, and therefore will not require the REMnux VM.

Close ApateDNS and revert your XP VM to a clean snapshot (before any malware was executed).

Locate FakeNet in the 'Tools' folder on the XP VM and run it (with administrative privileges). With FakeNet now launched and listening for DNS request on port 53, repeat all the activities your carried out with INetSim previously. Note all your observations (take screenshots).

Execute each of the malware samples between snapshots and note down all your observations.

After executing each malware and observing its network behaviour as recorded by FakeNet, close the tool.

When you close the tool, a PCAP file containing captured network traffic will be saved in the FakeNet folder.

Open the saved PCAP file in Wireshark to examine it.

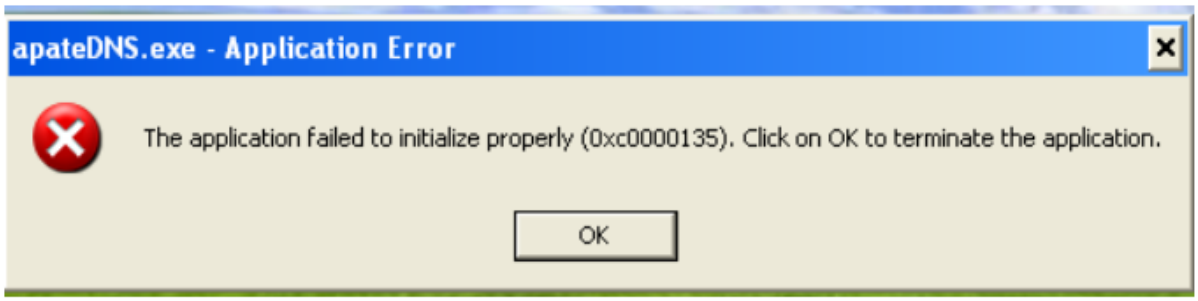
Do your observations of the malware network behaviour with FakeNet match those of INetSim?

Compare and contrast the outputs that you have obtained from both tools.

Installing ApateDNS

ApateDNS can be downloaded from here:
https://www.fireeye.com/content/dam/fireeye-www/services/freeware/sdl-apatedns.zip

Note: if you get the following error message when you attempt to run it on the Windows XP, you will get the following error message.



This is because ApateDNS would not run without the .NET framework 3.5 which is absent from the XP machine. To resolve this issue, download and install the .NET framework 3.5.

You can obtain a copy of the framework from the link below:
https://www.microsoft.com/en-us/download/details.aspx?id=21