Lab 2 Traffic analysis

Welcome to Lab 2

Using the tools you learned in lab 1, you will now analyze another pcap file that has known malware on it.
******Caution: The pcap file you use for this lab has malware, do not run this file on a Windows computer, only run it in your Security Onion VM******

Scenario

It was a morning ritual. Ms. Moneymany sipped her coffee as she quickly went through the email that arrived during the night. One of the messages caught her eye, because it was clearly spam that somehow got past the email filter. The message extolled the virtues of buying medicine on the web and contained a link to the on-line pharmacy. “Do people really fall for this stuff?” Ms. Moneymany thought. She was curious to know how the website would convince its visitors to make the purchase, so she clicked on the link.

The website was slow to load, and seemed to be broken. There was no content on the page. Disappointed, Ms. Moneymany closed the browser’s window and continued with her day.

She didn’t realize that her Windows XP computer just got infected.

You are the incident responder. You possess the network capture (PCAP) file that recorded Ms. Moneymany’s interactions with the website. Your mission is to understand what probably happened to Ms. Moneymany's system after she clicked the link. Your analysis will start with the PCAP file and will reveal a malicious executable.
Source: Network Forensic Puzzle Contest

Lab File

The file for this location is located at student > Downloads > Lab 2> infected.pcap

******Caution: The pcap file you use for this lab has malware, do not run this file on a Windows computer, only run it in your Security Onion VM******

Assignment

Using the tools from lab 1 analyze the infected.pcap file and answer the following questions:
1. As part of the infection process, Ms. Moneymany's browser downloaded two Java applets. What were the names of the two .jar files that implemented these applets? (6 points)
2. What was Ms. Moneymany's username on the infected Windows system? (6 points)
3. What was the starting URL of this incident? In other words, on which URL did Ms. Moneymany probably click? (6 points)
4. The malicious executable attempts to connect to an Internet host using an IP address which is hard-coded into it (there was no DNS lookup). What is the IP address of that Internet host? (6 points)

Analysis

The analysis will be worth 16 points and evaluated on the following criteria:
a. Clearly explained how the answer was determined
b. Conclusion supported with clear and easy to read screenshots
c. Written in your own words
d. Use of different tools to conduct the analysis and validate results

Total Points for lab: 40

Be ready to discuss this assignment in class or during an online session
Extra Credit (5 points)
1. As part of the infection, a malicious Windows executable file was downloaded onto Ms. Moneymany's system. What was the file's MD5 hash? Hint: It ends on "91ed".
2. What is the name of the packer used to protect the malicious Windows executable? Hint: This is one of the most popular freely-available packers seen in "mainstream" malware.
3. What is the MD5 hash of the unpacked version of the malicious Windows executable file?

Methodology

There are several ways to approach this assignment. Its importan that you decide your methodology before you start. Here are some suggestions:
1. Use tcprepaly to play the file and look for Sguil and Snorby alerts.
2. Open the file in Wireshark
3. Use Network Miner to analyze the file.
4. You will probably need more than one tool to solve the problem.

Additional File

If you want to practice with these tools, there is another file in the lab 2 directory "0826@19-snort.log. This is an old honeynet challenge. You can run all of the tools on this file. More info on this challenge can be found here:
http://old.honeynet.org/scans/scan23/
Note: This is for practice only, no credit is given for completing this