Lab-0: Tracking Spam

Digital Forensics
Spring 2004

Posted: February 3rd
Due: February 16th

This is a two-week long assignment to address one of the most important and annoying problems on the Internet today—spam! Most often we are not aware of how the spammers send out spam and where they send spam from in the first place.

1 Tracking Spam

In this assignment, as a forensic analyst your task is to find out as much information as you can about some spam. In order to track spam you should be familiar with the inner-workings of email protocols, most importantly SMTP [3] and mail-headers. Please review appropriate class lecture [4] before you begin. For this lab you’re free to select 15 distinct spam emails from the Great Spam Archive [1] or from your own inbox. Based on this sample and the tools mentioned in the lectures answer the following questions.

- For each of the spam email do a hop-by-hop analysis to find out the (real) origin of the spam. Indicate headers that are forged, if any. Please justify your conclusion beyond a reasonable doubt. That is, explain why we should believe your conclusion about the origin of the spam especially in the presence of forged information. Your report should include detailed information on how you arrived at your conclusion (tools used, information gathered, sources of information, trust-worthiness of your sources etc.).

- List some of the most useful mail-headers in your analysis above.

- List obfuscation techniques used in your sample. Also, list the goal of each obfuscation technique. For example, “to defeat a spam filter,” “to trick a user into clicking on a link” etc.

2 Spam Legislation

As a forensic analyst you must be aware of legislation as well as provide feedback to the legislators to improve the legislation. In this section you are to advise New York Senator Schumer who is trying to assess the CANSPAM [2] legislation and whether further legislation will be needed. The question on the table is: what percentage of the spam is coming from outside the US and therefore not subject to US courts? What is the likely effect of CANSPAM on the flow of spam? You may use additional samples from the Great Spam Archive to quantify your results.
3 Playing Sherlock Holmes

Here is your chance to play the famous detective Sherlock Holmes. The following is a real incident which took place last semester right here at Polytechnic University. Name of the characters have been withheld for no particular reason. Following email exchange occurred between a student and one of the instructors of a class:

First, following “anonymous” email was sent out to the class list in reply to a previous email from Professor Memon.

The question is how did the instructor find out **IP address of Jon Doe’s host**? Could she have done the same had Jon Doe sent the email from Yahoo? Why? Why not? **Hint**: Note that the email was sent using a Hotmail account via the web interface hence “Received: ” headers may not have **IP address of Jon Doe’s host**.

If you were to send an anonymous email what precautions would you take? Which web service would you use?

References

