Lab-1: Spam & Phishing

Digital Forensics
Spring 2005

Posted: February 2\textsuperscript{nd}
Due: February 11\textsuperscript{th}

This is a week long assignment to address one of the most important and annoying problems on the Internet—Spam! Most often we are not aware of how spammers send out emails or where they send spam from.

1 Tracking Spam

In this assignment, as a forensic analyst your task is to find out as much information as you can about 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 are free to select 5 distinct spam emails (at least 3 of which must be Phishing related emails) from the Great Spam Archive [1] or from your inbox. Based on this sample and the tools mentioned in the lectures (and of your own research) please answer the following questions.

1. 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. 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.).

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

3. List obfuscation techniques used in your sample to defeat spam filters.

4. List obfuscation techniques used to trick a user into a phishing scam.

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 on CANSPAM [2] legislation. Prepare a small report (at least 1 page, 2 pages maximum) advising the senator on the impact of CANSPAM on Spam. Please include the following information plus other appropriate information in your report and back them up with proper sources.

- What percentage of Spam originates outside of US?
- What is the likely effect of CANSPAM on the flow of spam?
- Are there any loop-holes in CANSPAM that Spammers can take advantage of?
References


