On Spam Susceptibility and Browser Updating

Eric Luong, University of Alberta, Canada
Toan Huynh, University of Alberta, Canada
James Miller, University of Alberta, Canada

ABSTRACT

This study examines the intersection between the group of users susceptible to spam and users who continue to use out-dated browsers. Specifically, it empirically determines if an association between unsafe user behaviour and the use of an out-dated browser exists. A case study is conducted wherein spam-like emails are sent to 25,000 random email users. The emails each contain a link to a webpage that records information on any visitors. The collected data is parsed and analyzed. Information was recorded on 90 distinct visitors. Analysis showed that approximately 66% of visitors were using out-dated browsers. The work implies that future research on the problem of spam should include browser version information (as a dichotomous variable) as a covariant in their analysis. The results suggest that greater effort must be put into educating the public about safe online behaviour and best practices, including the importance of updating software.

Keywords: Email, Security, Social Engineering, Spam, Web Browser

INTRODUCTION

Susceptibility to Spam

A great deal of research has been conducted regarding the number of users browsing with out-dated—and thus vulnerable—web browsers (Frei, Duebendorfer, Ollmann, & May, 2008), and separate research has been conducted regarding the success of spam (Kanich et al., 2009). However, the intersection has not yet been explored. We are interested in the number of users who interact with spam while using an out-dated browser. Specifically, our study seeks to address the question of whether there is an association between users who click on suspicious links in an email and whether or not the web browser that they use is out-dated. Note that there is certainly spam in circulation that advertises actual products or services, but we are specifically concerned with spam that is more malicious in nature. A link from a spam message may lead to a legitimate commerce website, but it is still risky for a user to click through. The target website may be a phishing page, or it may attempt to download and install a program to the user’s computer without their knowledge or consent (Hinde, 2003).

The results of this study may help to answer questions concerning past and present efforts to
improve online security. For example, if many users of up-to-date browsers exhibit unsafe behaviour, it suggests that further education and awareness is necessary for all; in the meantime, continued updates and improvements are helpful and effective. On the other hand, if unsafe behaviour is only seen among users of out-dated browsers, more effort should be put into ensuring that these users upgrade and patch their software as new versions become available. Security will always depend on the user as security programs and other safeguards can only do so much (Hazari, 2001, 2010; Orgill, Romney, Bailey, & Orgill, 2004; Werner, 2005). It is arguable that a user with good habits and knowledge of safe practices, even on an unprotected, out-dated system, is better off than a reckless user on an up-to-date and “secured” machine. Updates and patches are not as important if they only serve to protect those who can already protect themselves.

Insecure Browsers

Despite the best efforts of the computer security industry, many users continue to practice unsafe habits in their online activity (Messaging Anti-Abuse Working Group [MAAWG], 2010). In general, it is considered best practice to use the latest version of any software. Failure to update and apply patches can leave user systems vulnerable to flaws and exploitations. This advice is especially applicable to web browsers and browser plugins, as they are used to access potentially dangerous content from unknown servers. However, a recent study found that over 40% of Internet users – 576 million users – were navigating the Internet with out-dated web browsers (Frei et al., 2008) and are thus at risk from rogue websites and other malicious attacks.

There are numerous reasons why a user may not update their software. Users may not be aware that an update is available, or they may not think that the benefits outweigh the hassle. Some users may choose to refrain from installing the latest updates because they have come to trust the older version and imagine that the patch may actually open up new security holes. Of course, aside from ignorance or laziness, there are various other reasons why some users are unable to upgrade, e.g., businesses that require certain browsers for compatibility with required applications. Nonetheless, the use of out-dated browsers is risky and puts users in danger.

Spam Messages

Although attacks may come from many directions, including popular websites that have been hijacked to carry malicious content, users also fall victim to social engineering (Orgill et al., 2004). A webpage can be set up to exploit a security flaw within a targeted browser, but it is only effective if users visit the page. Besides carrying dangerous executables as attachments, emails may also be used to direct users to malicious websites through innocuous-looking links. To this end, unsolicited emails are sent in bulk to potential targets. These unwanted messages are known as spam.

Anyone with experience using email should be familiar with spam messages, though some users may not realize how dangerous spam can be. According to a recent survey by MAAWG (2010), many users have interacted with spam, with “tens of millions of consumers [having taken] action like clicking on links or opening attachments”. Surprisingly, 46% of users who accessed spam did so intentionally, with 18% reporting that they wanted “to see what would happen.” According to the survey, this cavalier attitude towards spam and suspicious emails seems to be more prevalent among the younger demographic. MAAWG also found that young people consider themselves more experienced than older users in Internet security.

The persistent problem of spam has fuelled a large body of research. Even as academic and industrial research aims to develop new measures to fight spam, spammers continue to react, adapt, and evolve to overcome anti-spam techniques. Goodman, Cormack, and Heckerman (2007) give a brief overview of the technology that has been implemented on both
Related Content

On Spam Susceptibility and Browser Updating
Eric Luong, Toan Huynh and James Miller (2012). *International Journal of Systems and Service-Oriented Engineering* (pp. 44-57).
[www.igi-global.com/article/spam-susceptibility-browser-updating/64198?camid=4v1](www.igi-global.com/article/spam-susceptibility-browser-updating/64198?camid=4v1)

Performance Evaluation of Secure Key Deployment and Exchange Protocol for MANETs
[www.igi-global.com/article/performance-evaluation-secure-key-deployment/52593?camid=4v1a](www.igi-global.com/article/performance-evaluation-secure-key-deployment/52593?camid=4v1a)

Extraction of an Architectural Model for Least Privilege Analysis
[www.igi-global.com/article/extraction-architectural-model-least-privilege/74843?camid=4v1a](www.igi-global.com/article/extraction-architectural-model-least-privilege/74843?camid=4v1a)
Agile Software Development: The Straight and Narrow Path to Secure Software?
*International Journal of Secure Software Engineering* (pp. 71-85).
[www.igi-global.com/article/agile-software-development/46153?camid=4v1a](www.igi-global.com/article/agile-software-development/46153?camid=4v1a)