Chapter 5
Discovering Computer Security Awareness Levels Among U.S. and Chinese Computer Users

Mark B. Schmidt
St. Cloud State University, USA

Allen C. Johnston
University of Alabama at Birmingham, USA

Kirk P. Arnett
Mississippi State University, USA

Jim Q. Chen
St. Cloud State University, USA

Suicheng Li
Xi'an University of Technology, China

ABSTRACT

Despite the recent increased attention afforded malware by the popular press, there appears to be a dearth in user awareness and understanding of certain aspects of the security paradigm. This chapter presents a comparison of user awareness levels of rootkits, spyware, and viruses between U.S. and Chinese users. The results of a survey of 210 U.S. respondents and 278 Chinese respondents indicate that respondents' awareness and knowledge of rootkits is well below that of spyware and viruses. Data analysis further reveals that there are significant differences in Chinese and U.S. user perceptions with regard to spyware and computer viruses. However, there is no difference in cross-cultural awareness with regard to rootkits. Due to the ubiquitous nature of the Internet, rootkits and other malware do not yield at transnational borders. An important step to mitigate the threats posed by malware such as rootkits is to raise awareness levels of users worldwide.

DOI: 10.4018/978-1-60566-920-5.ch005

INTRODUCTION

In order to increase efficiency and effectiveness, organizations are increasingly reliant on computer based information systems. Paradoxically, this increased use and reliance on information systems has lead to increased incidents of computer abuse (see Dhillon & Backhouse, 2000). In fact, the most recent CSI/FBI report, which was based on feedback from 522 computer security practitioners representing a diverse slice of corporate America, found that 43% of the respondents reported some form of malicious attack within the past year. This figure is down from 46% the previous year (Richardson, 2008). Yet another metric that attempts to enumerate the number of attacks comes from iDefense where they report monitoring more than 27,000 attacks last year, of which more than half were designed to covertly steal information or take over computers (Brenner, 2005). The under reporting of computer attacks is prevalent for many reasons, and most of these reasons center on a desire to avoid negative press. Given the corporate world's propensity to under report, other efforts and strategies are needed to examine threats and continue to raise awareness of these threats. Before such efforts can begin, a baseline of awareness levels can be used to establish an appropriate starting place.

Primarily because of today's reliance on computer networks and the Internet we note that more attention is afforded to security issues that affect computer networks and the Internet. This coverage is apparent in the popular press as well as academic literature. Many journals include security articles or have special issues devoted to security and malware. For example, the August 2005, Communications of the ACM was devoted to spyware (Stafford, 2005).

Despite the recent increase in attention given to the information systems security milieu, there is a puzzling dearth of scholarly research regarding rootkits. It is possible that this shortage has more to do with publication delay than a lack of interest among security researchers. Although rootkits have been around for 10 plus years, they have only recently appeared in the news. This is due to their invasion of the Windows world and recent high profile events such as the SONY rootkits and the early discovery of attack vector used to slip unsigned drivers past Windows Vista release candidate security.

A recent survey of 301 IT executives found that security concerns are increasing on the ranking of managements' most important concerns (Luftman & McLean, 2004). In efforts to mitigate the threats posed to information systems security concerns, IT officials are finally beginning to devote an increasing amount of resources to threat detection and amelioration (Whitman, 2003). The appropriate steps that may be taken to counteract security threats include increasing the number of formal security audits, providing financial commitments to holistic security practices, and increasing interest in security awareness training (Gordon, Loeb, Lucyshyn, & Richardson, 2004).

PURPOSE

The purpose of this paper is twofold. The first purpose is to provide an understanding of the concept and potential damage of rootkits. In doing so, it is hoped that users will become cognizant of the rootkit phenomenon, thereby taking a first step in the struggle to effectively cope with the threat. The second purpose of this paper is to present a cross-cultural comparison of rootkit awareness levels among end users in the United States and China. The data representing the level of awareness among users in the United States was initially published in 2006 (see Schmidt, Johnston, & Arnett, 2006), whereas the data from Chinese users was obtained specifically for this study. The insights derived from this study will provide a baseline awareness level of rootkits and will empirically test the self-reported familiarity levels of rootkits.