IGI PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.igi-global.com

ITJ4087

This paper appears in the publication, Journal of Global Information Management, Volume 16, Issue 2
edited by **Felix B. Tan**□□□□□□

RESEARCH NOTE

A Cross-Cultural Comparison of U.S. and Chinese Computer Security Awareness

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 article 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.

Keywords: *China; cross-cultural; data security; malware; rootkit; security management; spyware; virus*

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 697 computer security practitioners representing a diverse slice of corporate America, found that 56% of the respondents reported some form of malicious attack within the past year. This figure is up from 54% the previous year (Gordon, Loeb, Lucyshyn, & Richardson, 2005). 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 worlds 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, it is noted that more attention is afforded to security issues that effect 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 article 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 article 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.

MOTIVATION FOR U.S. AND CHINA COMPARISON

Recently, Chinese President Hu Jintao received a 21-gun salute, a visit to the White House, and a picture session with U.S. President George Bush. A day earlier he visited with Boeing, Microsoft, and Starbucks executives. This visit, especially with business leaders, may signal a change in what has been considerable software piracy in China and may represent a new effort to battle illegitimate copies of software and illicit use of software. Chinese government officials have pledged a crackdown on illegal software, which appears to be an effort to dismiss the notion of the Chinese as digital bandits and a combined government and business partnership to promote fair and safe software usage.

China, the world's fastest growing economy, has maintained an average 9.4% GDP growth rate for the last 27 years (Zheng, 2005). After a late start, Chinese business and public

computer usage has increased dramatically. The output of the computer hardware industry grew from RMB 5 billion in 1990 to RMB 124 billion (approximately $15.5B U.S.) in 1998 ("The Whole-View Scanning of the Electronic Information Industries in China," 1998). It is estimated that the GDP of information industries will be as high as RMB 6 trillion in 2010 ("China will become the biggest market for electronic information," 1998). As the economic reform continues, more and more Chinese businesses realize the crucial importance of using information technology and of protecting their information assets. Following the U.S., China has the world's second largest Internet user population with 110 million users (www.cnnic.net.cn). Almost one half of the users have broadband access and more than 70% of the Internet users are under 30 years old.

As more and more Chinese use computers and the Internet, computer security is becoming a serious concern. China is among the three most frequent security attack targets based on data collected during the first half of 2005 by IBM (IBM, 2005). The report noted one million attacks on Chinese government agencies and industries during that time. Outside firms doing business in China are not immune to the security attacks. As more U.S. businesses enter the Chinese market, a study of Chinese computer user's awareness of security threats should provide useful information to both U.S. and Chinese businesses alike.

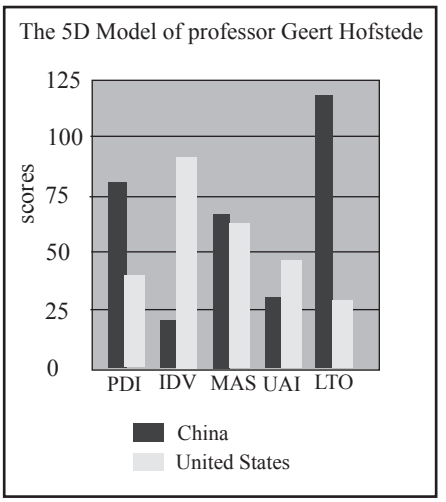
Another important reason to compare U.S. and China security awareness levels is the very different cultures of the two countries. Hofstede uses five indexes to measure culture differences: PDI (power distance index) measures the degree of equality between people in a society. IDV (individualism) measures the degree to which a society reinforces individual or collective achievement and interpersonal relationships. MAS (masculinity) focuses on the degree a society reinforces the traditional masculine work role model of male achievement, control, and power. UAI (uncertainty avoidance index) measures the level of tolerance for uncertainty and ambiguity within a society. LTO (long-term orientation) measures the degree a society embraces long term devotion to traditional, forward thinking values (Hofstede, 2003).

Figure 1 shows the scores from Hofstede's studies between the USA and China on the five cultural dimensions. With the exception of the MAS index, China and U.S. scores depict two very different cultures. China has much higher scores on PDI and LTO, which indicates greater inequalities of power and wealth among its people. This is reflected by centralized decision making in Chinese society, where the rich and powerful dominate the country. The higher LTO indicates the people value long-term commitment and are less likely to adopt changes that may deviate from its tradition or normal practices. This explains why the Chinese have a high tolerance for injustice and inequality. They hope time will bring them justice. Meanwhile, China gets much lower scores on IDV and UAI, which indicate that Chinese culture values collective achievements and community effort. A low score on UAI is indicative of a culture where people are used to following many rules and instructions.

Culture influences how security policies are formulated and implemented. Culture also determines how a society will perceive computer security threats. It is the speculation that many Chinese organizations/businesses adopt centralized security measures which shield their users from viruses and spyware attack. For example, server-side software may block most malicious attacks, closely monitor a user's computing habits, and enforce stringent security rules on software downloading and installation. Chinese computer users may view these rules as perfectly acceptable and necessary, while in the U.S. such an environment may face opposition and cause privacy concerns among users. It is also speculated that when it comes to self reporting their knowledge of security threats, Chinese users may exhibit greater modesty in relation to their U.S. peers.

Although this study investigates awareness levels of three types of malware, including spyware, viruses, and rootkits, a more detailed description is presented of the rootkit concept,

Figure 1. China and U.S. scores on Hofstede's culture dimensions (Hofstede, 2003)



as it is a more recent phenomenon and hence less well known. A thorough discussion of rootkits and their potential effects follows this introduction. The following section provides a detailed description of the survey and both the American and Chinese respondents. Next, an analysis of the data is presented. Conclusions and a call to action are presented at the end of this manuscript.

ROOTKIT DETAIL

A rootkit is a "type of Trojan that keeps itself, other files, registry keys, and network connections hidden from detection. It runs at the lowest level of the machine and typically intercepts common API calls. For example, it can intercept requests to a file manager such as Explorer and cause it to keep certain files hidden from display, even reporting false file counts and sizes to the user" (TechWeb, 2005). A more concise definition can be found at rootkit.com, "a rootkit is a tool that is designed to hide itself and other processes, data, and/or activity on a system" (Hoglund, 2006). The origins of rootkits can be found in the Unix world, and because they allow access at the lowest (or root) level, the term rootkit was coined.

Originally targeting Unix machines, rootkits were developed circa 1995 and, until recently, have been relatively rare on Windows machines (Roberts, 2005). The first notable rootkit targeting Windows NT, was introduced in 1999 by Greg Hoglund who also maintains rootkit.com, a popular Web site for disseminating information about rootkit exploits (Dillard, 2005). More recently, computer criminals and even global multinational corporations such as Sony have developed rootkits to beleaguer systems running Microsoft Windows. It seems a certainty that malware developers will continue to develop Windows rootkits (Seltzer, 2005).

Rootkits can exert several effects on a computer system. They can hide files, processes, or registry data, most often in an attempt to mask intrusion and to surreptitiously gain administrative rights to a computer system. Further, rootkits can provide the mechanism by which various forms of malware, including viruses, spyware, and Trojans, attempt to conceal their existence from detection utilities such as anti-spyware and anti-virus applications. A blended threat refers to two of more malware programs, such as rootkits, spyware, viruses, and worms, acting in a symbiotic relationship in delivering a payload. A blended threat contains many advantageous features for the attacker. For instance, a spyware/rootkit blended threat would include the data gathering capabilities and performance degradation capacity of spyware (Arnett & Schmidt, 2005) with the stealth like nature and persistence of a rootkit. Not only is the resulting threat likely to cause more problems for the user, it is also more difficult to detect and remove than single threats.

Recently, rootkits have become progressively more prevalent in the networking world (Roberts, 2005). There have been companies such as Sony, which exploit rootkits for commercial purposes (Cass, 2006; Gibbs, 2005; Graham, 2005). Another recent use of rootkits was seen in a scheme at a university in California to obtain names and social security numbers of approximately 59,000 past, current, and potential faculty, staff, and students (Rosencrance &

Vijayan, 2005). Due to the nature of the rootkit threat, more academic study is warranted.

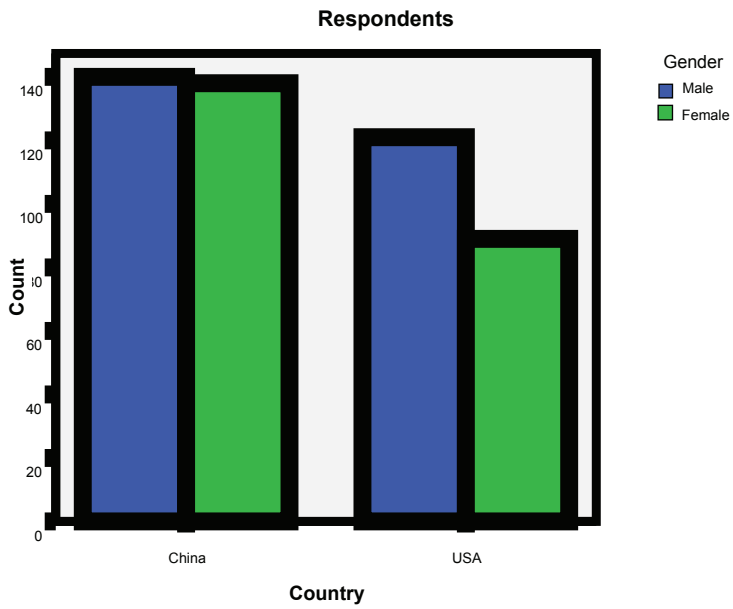
The following section describes the details of the survey. The survey was administered to IT users at three institutions of higher learning in the United States as well as users at an institution of higher learning in China. Data analysis and results are detailed in subsequent sections.

THE SURVEY

The survey used in this study is based on the survey used in two previous studies (Jones, Arnett, Tang, & Chen, 1993; Schmidt & Arnett, 2005). Both of these studies examined relatively new malware as it emerged on the computing landscape. The original study (Jones et al., 1993) focused on users perceptions of computer viruses. In the second study, Schmidt and Arnett (2005) utilized a similar instrument to assess users' perceptions of spyware. The study described herein was similar in that it investigated the relatively new phenomena of rootkits. Specifically, this study examined IT users' perceptions of rootkits, spyware, and viruses. It further compared the perceptions of users in the United States and China. The following section describes the survey, its subjects, and the analysis process that followed.

The survey used a five-point Likert scale (1 = Strongly Disagree, 3 = Neutral, 5 = Strongly Agree) for the research items and contained additional demographic items including gender, age, computer experience, education, and occupation. The subjects were college students who were enrolled in institutions during the 2005-2006 academic year. It is worth noting that, given the respondents are college students, they possibly posses a higher level of knowledge of technology than the average computer user. Previous studies have shown that majority of the computer users are young and with college backgrounds ("17th Statistical Survey Report on The Internet Development in China," 2006). A survey of such a major computer user group will provide a reasonably good understanding of the computer security awareness level. Further, these college students were readily accessible and their participation, while not required, was near 100% in both settings. This allows for currency in the reporting of the results.

Figure 2. Respondents by country and gender



In total, the U.S. survey was conducted with 210 subjects from three public institutes of higher learning from various geographical regions. To provide a basis for the cross cultural comparison, 278 college subjects in China completed the questionnaire. Figure 2 presents a summary of the respondents by gender and country.

The majority of the U.S. respondents were male (57%). Forty five (45%) of the respondents had 5-10 years of computer experience; while the Chinese respondents were evenly split in terms of gender and were somewhat less experienced with computers (53% had 2-5 years experience). A large number (94%) of U.S. respondents own at least one computer while fewer (63%) of Chinese respondents reported that they owned at least one computer. Table 1 presents selected demographics.

RESULTS AND ANALYSIS

Survey responses indicate that 83.7% of U.S. and 81.3% of Chinese users have not even heard of rootkits. Not surprisingly, user knowledge of viruses was much higher. In fact, every U.S. user (100%) and 98.2% of Chinese users have known of viruses for at least 1 year. Spyware appears to have a high level of awareness with 83.8% (U.S.) and 38.4% (Chinese) of users having known of spyware for more than 1 year. These findings indicate the relative newness of rootkits and lack of awareness from the user perspective. As one may suspect, this general lack of awareness of rootkits is reflected in security practices as only 2.5% (U.S.) and 3.2% (Chinese) of users report using Rootkit Revealer detection software.

Depicted in Table 2, comparisons of responses provided by U.S. and Chinese users suggests that there are significant differences in how the two user groups report their familiarity of rootkits, spyware, and viruses in general. For example, U.S. and Chinese users report similar levels of familiarity with rootkits; while U.S. users report higher levels of familiarity with spyware and viruses than their Chinese coun-

Table 1. Selected profile of respondents

	Response category	USA respondents	Chinese respondents
Age	18 to 29 30 to 39 40 to 49 50 to 59 60 and over	82.6% 8.0% 8.5% 1.0% 0%	99.3% .4% 0% .4% 0%
Gender	Female Male	42.4% 57.6%	49.6% 50.4%
Computer experience	< 1 year > 1 year to 2 years > 2 years to 5 years > 5 years to 10 years > 10 years	2.5% 2.5% 20.6% 45.2% 29.1%	6.5% 14.7% 53.2% 24.5% 1.1%
Occupation	Full time student Part time student IT professional Other	81.5% 7.3% 6.8% 4.4%	96.0% 1.4% .7% 1.8%
How many personal computers (or laptops) do you own?	0 1 2 3 4 or more	6.2% 47.1% 31.4% 7.1% 8.1%	37.1% 50.4% 11.5% .7% .4%

terparts. Included in the analysis is a fictitious threat, "Trilobyte," which was introduced to the study simply as a means for ascertaining the quality of the survey responses. U.S. users report higher levels of familiarity than Chinese students with the "Trilobyte" virus, although neither group reports more than low to moderate familiarity. Interestingly, both groups believe their familiarity of the "Trilobyte" virus to be greater than that of rootkits. Also included in Table 2, perceptions of familiarity with the very real "Melissa" virus were similar among the user groups, with both groups reporting a moderate level of familiarity.

As depicted in Table 3 and interpreted in Table 4, ANOVA techniques were used to determine if the differences between U.S. and Chinese users regarding their awareness levels of viruses, spyware, and rootkits were in fact significant. The results indicate that there are significant differences between U.S. and Chinese users on four of the eight dimensions under consideration. Results indicate that for spyware and virus familiarity, U.S. and Chinese self-re-

Table 2. Respondent perception

Item		N	Mean	Std. Deviation
Familiar with rootkits	USA	209	1.44	0.950
	China	278	1.44	0.851
	Total	487	1.44	0.894
The "average" person at my institution is familiar with rootkits	USA	210	1.94	0.952
	China	278	1.96	0.985
	Total	488	1.95	0.970
Familiar with spyware	USA	210	4.13	1.034
	China	277	1.92	1.174
	Total	487	2.87	1.562
The "average" person at my institution is familiar with spyware	USA	210	3.85	0.903
	China	277	2.29	1.079
	Total	487	2.97	1.269
Familiar with viruses	USA	210	4.21	0.799
	China	275	2.40	1.244
	Total	485	3.19	1.400
The "average" person at my institution is familiar with viruses	USA	210	4.12	0.858
	China	277	2.62	1.092
	Total	487	3.27	1.242
Familiar with the fictitious "Trilobyte" virus	USA	208	1.95	1.107
	China	274	1.80	1.073
	Total	482	1.86	1.090
The "average" person at my institution is familiar with the fictitious "Trilobyte" virus	USA	209	2.31	0.957
	China	276	2.25	1.160
	Total	485	2.27	1.076

ported levels differ significantly (P<.001); yet for rootkits, the two groups' familiarity levels are similar.

Respondents from both countries were more familiar with spyware and viruses than they were with rootkits. It is believed that it takes some time for the awareness levels of new malware to reach a point where IT users are cognizant of the threats to such a level where they can and will adequately protect themselves. A historical view of viruses finds that 79.6% of respondents were aware of viruses for 1 or more years when viruses were approximately 10 years old (Jones et al., 1993). Schmidt and Arnett (2005) found that even though the concept of spyware was less than 10 years old, only 6% of respondents were aware of spyware for less than a year. It follows that as time progresses, users are more aware of malware in its early stages. It further appears that the time period from the introduction of a particular type of malware to widespread awareness of it is becoming compressed. Even the best prognosticative efforts reveal that only time will tell as to whether or not this pattern holds with rootkit awareness.

Table 3. ANOVA results

Item		Sum of Squares	Df	Mean Square	F	Sig.
Familiar with rootkits	Between Groups	0.001	1	0.001	0.001	0.975
	Within Groups	388.196	485	0.800		
	Total	388.197	486			
The "average" person at my institution is familiar with rootkits	Between Groups	0.037	1	0.037	0.039	0.843
	Within Groups	457.879	486	0.942		
	Total	457.916	487			
Familiar with spyware	Between Groups	582.325	1	582.325	467.765	0.000
	Within Groups	603.781	485	1.245		
	Total	1,186.107	486			
The "average" person at my institution is familiar with spyware	Between Groups	290.669	1	290.669	286.686	0.000
	Within Groups	491.738	485	1.014		
	Total	782.407	486			
Familiar with viruses	Between Groups	391.942	1	391.942	339.653	0.000
	Within Groups	557.357	483	1.154		
	Total	949.299	484			
The "average" person at my institution is familiar with viruses	Between Groups	266.785	1	266.785	267.902	0.000
	Within Groups	482.977	485	0.996		
	Total	749.762	486			
Familiar with the fictitious "Trilobyte" virus	Between Groups	2.889	1	2.889	2.441	0.119
	Within Groups	568.074	480	1.183		
	Total	570.963	481			
The "average" person at my institution is familiar with the "Trilobyte" virus	Between Groups	0.376	1	0.376	0.324	0.569
	Within Groups	560.152	483	1.160		
	Total	560.528	484			

Table 4. Interpretation of differences

Item	U.S. Mean	Chinese Mean	Interpretation
I am familiar with how rootkits work	1.44	1.44	No significant difference. Amazingly both groups reported exactly the same, albeit low, awareness level with rootkits. Much work is needed to raise users' awareness in both countries in an effort to provide an adequate level of protection.
The "average" person at my institution is familiar with rootkits	1.94	1.96	No significant difference. Once again the groups reported a very similar awareness level. Interestingly, both groups envision that the average person in their organization is more aware of rootkits than there are themselves.
I am familiar with spyware	4.13	1.92	U.S. respondents have a self-reported "better" knowledge of spyware. This is possibly due to the recent coverage afforded spyware in the popular press.
The "average" person at my institution is familiar with spyware	3.85	2.29	U.S. respondents believe the average person in their organization is reasonably aware of spyware (but less aware then they themselves are). Chinese respondents believe their contemporaries are more informed than they regarding spyware.
I am familiar with computer viruses	4.21	2.40	U.S. respondents have a higher self-reported knowledge of viruses than do Chinese users. Because awareness is a critical step in prevention, it is somewhat discouraging to find the level so low among Chinese users.
The "average" person at my institution is familiar with computer viruses	4.12	2.62	U.S. respondents believe the average person to have a solid level of familiarity with viruses whereas, the Chinese report a lower awareness level. Again the U.S. respondents have indicated that their knowledge is above the average persons' knowledge whereas, Chinese users provide opposite findings.
I am familiar with the "Trilobyte" virus	1.95	1.80	No significant difference. It is encouraging to see that both groups reported a low to moderate awareness of the "Trilobyte" virus as this is a fictitious virus.
The "average" person at my institution is familiar with the "Trilobyte" virus	2.31	2.25	No significant difference. Interestingly, both groups envision that the average person at their institution knows more about this fictitious virus than they, themselves, do.

The U.S. respondents consider themselves more aware of spyware and viruses than do Chinese respondents. This is expected, given China's relatively lower score on Hofstede's IDV dimension of the cultural index. There are several possible explanations for the relatively low level of awareness among Chinese respondents. First, a relatively small percentage of the Chinese population owns and uses computers because computers and Internet access are still expensive for most Chinese. Even if people have computers, they do not use them regularly. Therefore, computer viruses and spyware are not as widely reported in China as they are in United States. Second, Chinese business and marketing firms use TV and paper media as their major advertising tools. Use of spyware for business advertising is limited due to the small computer user base. Third, computer security breaches are under-reported in China.

The under-reporting is largely due to the limited free flow of information and the lack of efficient business news reporting channels. Most news media in China are state owned. Strict rules are imposed on news media. The government uses the media as propaganda tools to publicize government policy. Unless a security breach is sufficiently severe, it is difficult to obtain news media's attention.

Given the relative maturity of the computer virus concept, the belief was that awareness levels would be higher. Even with the increase in popular press reports of incidents involving rootkits, awareness regarding the pervasiveness and threats posed by rootkits remains low in both groups.

The limited awareness and knowledge of rootkits is especially alarming considering recent high-profile viruses, the Sony rootkit debacle, spyware, and other forms of malicious software in the headlines. IS journals are affording more and more coverage to computer security issues. For instance, the August 2005 issue of *Communications of the ACM* was devoted to the topic of spyware (Stafford, 2005). To adequately prepare for the future of secure computing, the first step is to make users aware of the challenges that they face. Given the nature of rootkits, spyware, viruses, blended threats, and yet to be developed computer malware, we may be just beginning what will prove to be a constant battle for control of the modern computing paradigm.

CONCLUSION

It takes time for the level of awareness to reach a critical mass in respect to any malware. Until this point is reached, it is unlikely that users will take the proper precautions to protect themselves from this type of malware. Users in the U.S. appear to be reasonably aware of viruses and spyware. However, there is much to be done in terms of achieving that level of awareness for rootkits in both the U.S. and China. Rootkits are particularly threatening as they have the potential to cause a great deal of harm because they are designed not only to conceal themselves but also to conceal other symbiotic malware such as viruses and spyware (Seltzer, 2005). Because of the Chinese culture's position on Hofstede's cultural dimensions index, (i.e., relatively high in PDI and LTO and simultaneously low in IDV and UAI), Chinese organizations may be very successful in implementing centralized prevention, detection, and remediation procedures. Comparatively, home users in China need to become more aware of security threats in today's rapidly changing computer security paradigm. MAS appears to be similar for both countries, thus minimal differences in security policy development is necessary based on this dimension. Considering the large discrepancy in LTO between countries, it might be necessary to exert more effort to convince Chinese uses of the long term benefits of a rigorous security policy. Given China's relatively high score in PDI, it is possible that there will be many in that culture that do not have access to computing resources. Therefore, it would be important to consider the implications of the digital divide when developing security policies and conducting computer security policies.

In many cases, awareness is the first step to providing security (Goodhue & Straub, 1989; Im & Baskerville, 2005; Siponen, 2000; Straub & Welke, 1998). Unfortunately, consumers are not demanding rootkit detection and removal methods and antivirus software developers have been slow to add rootkit features to their protection tools. There are, however, some notable exceptions. For instance, F-Secure (http://www.f-secure.com) now includes "BlackLight," a rootkit detection tool with its "F-Secure Internet Security 2006" security suite. It seems obvious that as awareness increases, perhaps due to recent high profile rootkit abuses such as the Sony debacle, that user awareness of rootkits will increase. When the knowledge levels increase, it is then logical to assume consumers will demand more adequate protection tools and that those demands will be met by security and other vendors.

The 2005 Global Information Security Survey, conducted by Accenture, found that Chinese organizations suffer more than U.S. organizations from the effects of malware

(D'Antoni, 2005). Consequently, there is no surprise that Chinese users indicated less awareness regarding spyware and viruses relative to the U.S. users. Perhaps because fewer Chinese respondents (62.9%) compared to 93.8% of U.S. respondents own one or more computers, their exposure to threat may be limited because the owner rather than the user is responsible for computer security of the machines in question. It should be expected that these levels will increase over the next few years as malware becomes more prevalent in the computing milieu.

It is evident to many that malware poses significant threats to computer security. Given the current levels of awareness and knowledge within the user community, there are steps to be taken to increase awareness of rootkits in both the U.S. and China as well as both spyware and viruses in China. Unfortunately, it is likely that security professionals' attempts to mitigate the threats posed by malware will encounter many challenges. The first of these challenges appears to be the awareness levels among users. Unfortunately, a lack of knowledge of malware negatively effects an organization's ability to counter the effects that malware is likely to cause (Straub & Welke, 1998). Given the aforementioned findings, it is with great anticipation that effective widespread malware amelioration will be common in the computing environment.

All malware including rootkits, spyware, viruses, and blended threats are potentially very dangerous to the computing environment. Fortunately, users need not suffer the full effect of malware if the security community can raise awareness to the point where end users will utilize appropriate detection and removal tools as part of their overall computing protection paradigm. The first step in this call to action is to use the baseline awareness levels described herein in the development of a program to increase awareness levels of malware in both countries to the appropriate level so users are prepared to understand, detect, and remove malware. It has been suggested that solid policy formulation to mitigate security risk from malware such as spyware needs to be a global effort (Warkentin, Luo, & Templeton, 2005). In order for such a global effort to be successful, global awareness levels need to by measured and, in many cases, be raised. This article provides a baseline measurement of specific malware awareness levels for users in two prominent countries.

REFERENCES

17th Statistical Survey Report on The Internet Development in China. (2006). [Electronic Version]. Retrieved April, 19, 2006 from www.cnnic.net.cn

Arnett, K. P., & Schmidt, M. B. (2005). Busting the ghost in the machine. *Communications of the ACM, 48*(8), 92-95.

Brenner, B. (2005). Botnets are more menacing than ever. Retrieved September, 2005, from http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1068871,00.html

Cass, S. (2006). Antipiracy software ppens door to electronic intruders. *IEEE Spectrum, 43*(1), 12-13.

China Will Become the Biggest Market for Electronic Information. (1998). *People's Daily,* May 11, 1998.

D'Antoni, H. (2005, October 31). IT security in China shows cracks. *InformationWeek,* 47-51.

Dhillon, G., & Backhouse, J. (2000). Information system security management in the new millennium. *Communications of the ACM, 43*(7), 125-128.

Dillard, K. (2005). *Rootkit battle: Rootkit revealer vs. hacker defender*. SearchWindowsSecurity.com

Gibbs, M. (2005, November 14). More on Sony's rootkit. *Network World, 22,* 82.

Goodhue, D. L., & Straub, D. W. (1989). *Security concerns of system users: A proposed study of user perceptions of the adequacy of security measures.* Paper presented at the Twenty-Second Annual Hawaii International Conference on System Science (HICSS), Kailua-Kona, HI.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2004). *2004 CSI/FBI computer crime and security survey*.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). *2005 CSI/FBI computer crime and*

security survey. Retrieved from http://www.gocsi.com/forms/fbi/csi_fbi_survey.jhtml;jsessionid=CREWIZUTIPCCSQSNDBCCKHSCJUMEKJVN

Graham, J. (2005, November 16). Copy-protected-CD flap raises questions. *USA Today*.

Hofstede, G. (2003). *Cultural dimensions*. Retrieved August, 12, 2006, from http://www.geert-hofstede.com/geert_hofstede_resources.shtml

Hoglund, G. (2006). *The definition of a rootkit*. Retrieved February, 17, 2006, from http://www.rootkit.com/blog.php?newsid=440

IBM. (2005). *Government, financial services and manufacturing sectors top targets of security attacks in first half of 2005*.

Im, G. P., & Baskerville, R. L. (2005). A longitudinal study of information system threat categories: The enduring problem of human error. *The DATA BASE for Advances in Information Systems, 36*(4), 68-79.

Jones, M. C., Arnett, K. P., Tang, J. T. E., & Chen, N. S. (1993). Perceptions of computer viruses a cross-cultural assessment. *Computers and Security, 12*, 191-197.

Luftman, J., & McLean, E. R. (2004). Key issues for IT executives. *MIS Quarterly Executive, 3*(2), 89-104.

Roberts, P. F. (2005, October 17). Rootkits sprout on networks. *eWeek, 22,* 25.

Rosencrance, L., & Vijayan, J. (2005, March 21). University computers hacked on each coast. *ComputerWorld, 39,* 57.

Schmidt, M. B., & Arnett, K. P. (2005). Spyware: A little knowledge is a wonderful thing. *Communications of the ACM, 48*(8), 67-70.

Schmidt, M. B., Johnston, A. C., & Arnett, K. P. (2006). An empirical investigation of rootkit awareness. *Business Research Yearbook: Global Business Perspectives, 13*, 153-158.

Seltzer, L. (2005). Rootkits: The ultimate stealth attack. *PC Magazine, 24,* 76.

Siponen, M. T. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security, 8*(1), 31-41.

Stafford, T. F. (2005). Spyware. *Communications of the ACM, 48*(8), 34-35.

Straub, D. W., & Welke, R. J. (1998). Coping with systems risk: Security planning models for management decision making. *MIS Quarterly, 22*(4), 441-469.

Warkentin, M., Luo, X., & Templeton, G. F. (2005). A framework for spyware assessment. *Communications of the ACM, 48*(8), 79-84.

Whitman, M. E. (2003). Enemy at the gate: Threat to information security. *Communications of the ACM, 46*(8), 91-95.

The Whole-View Scanning of the Electronic Information Industries in China. (1998, August 10, 1998). *People's Daily*.

Zheng, J. (2005). China's GDP grows 9.5% in first half [Electronic Version]. *National Bureau of Statistics (NBS)*. Retrieved May 1, 2006, from http://www.china-embassy.org/eng/gyzg/t204319.htm

Mark B. Schmidt is an associate professor of IS in the G.R. Herberger College of Business at St. Cloud State University. He has a BS degree in business administration and agri-business from Southwest State University, a master's degree in business administration from St. Cloud State University, and master's and PhD degrees in business information systems from Mississippi State University. He has works published in the Communications of the ACM, Journal of Computer Information Systems, Journal of Global Information Management, Journal of End User Computing, Mountain Plains Journal of Business and Economics, Business Research Yearbook, Mississippi Business Journal, Proceedings of the National Decision Sciences Institute, Proceedings of the Americas Conference on Information Systems, Proceedings of the Information

Resources Management Association, Proceedings of the Security Conference, *and in the* Proceedings of the ISOneWorld International Conference. *His research focuses on information security, end-user computing, and innovative information technologies.*

Allen C. Johnston an assistant professor in the school of business at the University of Alabama at Birmingham. He holds a BS from Louisiana State University in electrical engineering as well as an MSIS and PhD in information systems from Mississippi State University. His works can be found in such outlets as Communications of the ACM, Journal of Information Privacy and Security, International Journal of Information Security and Privacy, *and* Journal of Internet Commerce. *The primary focus of his research has been in the area of information assurance and security, with a specific concentration on the behavioral aspects of information security and privacy.*

Kirk P. Arnett is professor of management information systems at Mississippi State University. He was previously the College of Business and Industry Outstanding Faculty Member and the National Association of Academic Advisors Outstanding Academic Advisor. He has been a member of the academic community for more than 20 years and has multiple publications in the Communications of the ACM, Information and Management, the Journal of Computer Information Systems, Man-Machine Studies *and other journals. More than 80 doctoral students have worked with Dr. Arnett for their dissertations. Prior to his full time academic career, Dr. Arnett worked with several US companies for more than 15 years in the information systems arena. In addition to academic credentials Dr. Arnett is a certified computing professional (CCP) from the Institute for Certification of Computing Professionals and holds a Global Information Assurance Certificate from SANS Institute.*

Jim Q. Chen is chairperson and professor of business computer information systems at St. Cloud State University. He received his PhD in management information systems in 1995 from University of Nebraska-Lincoln. His current research interests include Web application development methodologies, E-commerce, and computer database security. His recent publications appeared in Information Systems Management, Communications of the ACM, Decision Support Systems, Journal of Internet Commerce, Journal of Computer Information Systems, Systems Development Management, *among other journals.*

Suicheng Li is vice dean and professor of School of Business Administration at Xi'an University of Technology in China. He received his PhD in management science and engineering in 2005 from Northwestern Polytechnical University in China. His current research interests include supply chain management and strategic management. His recent publications appeared in Journal of Industrial Engineering and Engineering Management *(in Chinese),* Science Research Management *(in Chinese),* Industrial Engineering Journal *(in Chinese), among other journals.*