Rootkits and What We Know: Assessing US and Korean Knowledge and Perceptions

Kirk P. Arnett, Mississippi State University, USA
Mark B. Schmidt, St. Cloud State University, USA
Allen C. Johnston, University of Alabama Birmingham, USA
Jongki Kim, Pusan National University, Korea
Hajin Hwang, Catholic University of Daegu, Korea

ABSTRACT

Respondents from eight Korean and US higher education institutions were surveyed as to their knowledge and experience with various forms of computer malware. The surveys provide insight into knowledge of rootkits that have become coffee lounge discussion following the once secretive Sony rootkit news break in late 2005 and then the rash of accusations and acknowledgments of other rootkits that followed. The surveys provide an empirical assessment of perceptions between students in the two countries with regard to various forms of malware. The two groups are similar in many respects, but they exhibit significant differences in self-reported perceptions of rootkit familiarity. US respondents report higher levels of familiarity for all assessed malware types, including the fictional “Trilobyte” virus. A timeline-based comparison between virus and rootkit knowledge reveals that relatively little is known about rootkits today. This highlights dangers related to existing knowledge levels but presents hope for solutions and an accelerated rootkit awareness curve to improve worldwide malware protection.

Keywords: cross-culture; malware; spyware; rootkit; virus

INTRODUCTION

Korea and the US, along with the rest of the Internet-enabled world, continually battle a growing number of computer attacks. The source of these attacks may be domestic or foreign. The attacks may be from government or terrorist-sponsored organizations for intelligence gathering or they may be from criminal groups or individuals intent on financial gains. The attacks may be against personal, business, education, or governmental computer assets. Regardless of the source or target, each country must prepare for current attacks as well as attacks that will surely occur in the future. For maximum effect, the preparation must be to protect personal, business, and governmental assets, and the preparation must span the globe.

Countries around the globe need skilled persons to battle against attacks, and these countries certainly have attackers who are on
the opposite side of the battlefield. Each country houses hackers who create malware, and each country trains computer hackers for offensive as well as defensive cyber attacks. Despite its lack of sophisticated digital infrastructure, North Korea has attacked both South Korean and US governmental computer installations. The capabilities of graduates from Kim il Sung’s North Korean hacker training academy, where students undergo five years of specialty courses for hacking careers, are said to be comparable to the best US CIA trained hackers (Digital Chosunilbo, 2005).

During this decade, US soldiers have been indicted for breaking into South Korean computer systems (Stars and Stripes, 2001). We do not know whether or not this was government sponsored, but we do know that attacks are not only one-to-many or many-to-one events. Rather, cyber attacks are characterized as events in which many sources are involved in attacking many targets. South Korea’s Ministry of National Defense said a 5% budget increase was allocated mainly for projects such as “the buildup of the core capability needed for coping with advanced scientific and information warfare.” The report also revealed that South Korea’s military has 177 computer training facilities and had trained more than 200,000 “information technicians” (Kramarento, 2003). Training efforts such as these are a necessary strategy for any country that is a part of today’s malware-infested landscape.

A relatively new form of malware is a rootkit. Although well known in the Unix arena, rootkits are now rapidly expanding in Windows environments. Even the newest software developments may not be immune to rootkits, as Polish security researcher Joanna Rutkowska demonstrated blue pill—a proof of concept rootkit to circumvent prerelease Microsoft Vista security. A rootkit is a piece of software that allows its user to gain top level (root) privileges where the rootkit is installed. A rootkit is not a virus or a worm, but it may deliver a virus or worm. Once installed, if a backdoor mechanism is made available to the attacker, the rootkit will allow the attacker to “own” the machine. Co-author of the now famous rootkit.com Web site, Jamie Butler says that it is this stealth nature of a rootkit that is the real danger as a “rootkit is software used to hide other software from the user and security tools, to evade detection” (Williamson, 2007). The result is, because they are unknown, rootkit infections may last longer and therefore do more damage for longer periods than could a single worm or virus.

Our belief is that rootkit threat levels are not understood, and our purpose is to describe the findings from a cross-cultural study. The research goal is to assess the knowledge levels and perceptions of Korean and US college students regarding rootkits and more traditional malware with an eye toward identifying possible problems or solutions that might surface. The organization is to first examine selected relevant literature regarding Korea and the US in today’s digital world. Rootkits are then examined as to their current status and potential threat level. The study methodology is briefly described and the data comparisons are presented and discussed. Finally, the limitations that should be considered in interpreting the results are suggested and courses of action for these and other countries are recommended.

RELEVANT LITERATURE

F-Secure reports the Winevar e-mail worm was found in-the-wild in Korea at the end of November 2002 (Hulme, 2002). Apparently it was intentionally released by the virus writer during South Korea’s Anti-Virus Researcher’s Asian Conference. The Korean-born W32/Buchon@mm mass mailer also delivers a keylogger. The Slammer virus that affected Windows machines running SQL Server was especially destructive in Korea, resulting in a massive DoS attack. At its time, the Code Red Worm, which was originally designed to attack White House computers (Lemos, 2001), infected at least 225,000 computers elsewhere and shut down Internet services in Korea for several hours in 2001. Korea and the US have well known security firms to combat malware; they each have virus writers who release viruses in
Privacy and Online Data Collection
www.igi-global.com/chapter/privacy-online-data-collection/13523?camid=4v1a