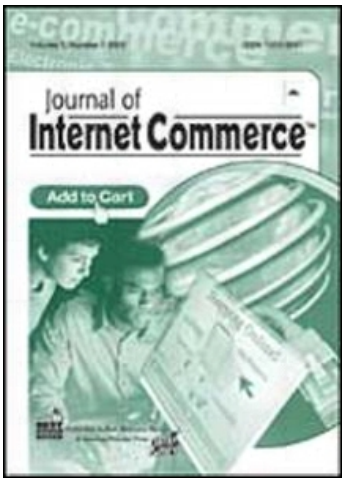

Journal of Internet Commerce
Publication details, including instructions for authors and subscription information:
http://www.informaworld.com/smpp/title~content=t792306872

Getting to the Root of the Problem

Allen C. Johnston [a]; Mark B. Schmidt [b]; Kirk P. Arnett [c]; Jeff Thomas [d]
[a] University of Louisiana Monroe, Monroe, LA [b] Business Computer Information Systems, St. Cloud State University, St. Cloud, MN [c] Mississippi State University, Mis State, MS [d] Computer Services, College of Veterinary Medicine, Mississippi State University, Mis State, MS

Online Publication Date: 08 October 2008

To cite this Article Johnston, Allen C., Schmidt, Mark B., Arnett, Kirk P. and Thomas, Jeff(2008)'Getting to the Root of the Problem',Journal of Internet Commerce,6:1,1 — 12
To link to this Article: DOI: 10.1300/J179v06n01_01
URL: http://dx.doi.org/10.1300/J179v06n01_01

Getting to the Root of the Problem

Allen C. Johnston, PhD
Mark B. Schmidt, PhD
Kirk P. Arnett, DBA
Jeff Thomas

ABSTRACT. Despite its maturity in certain computing environments, there appears to be a void in our awareness and understanding of the rootkit security menace. Rootkits are a form of malware that, once surreptitiously installed onto a victim's computer, allow a perpetrator to gain administrative-level access, monitor activities, open backdoor access portals, and hide all evidence of its activities. After describing the position of rootkits in the malware family and their prevalence in the Unix and Windows worlds, a practical question is posed. That is, what do information technology (IT) users know about rootkits? To answer that question, data collected from three geographically separated state institutions of higher learning is collated to provide a baseline of rootkit security knowledge. Today, rootkit knowledge is far below that of computer viruses or spyware. However, there is hope that users will not suffer the full brunt of rootkits, particularly if the security community can raise awareness of rootkits and their consequences. doi:10.1300/J179v06n01_01

Allen C. Johnston is Assistant Professor of CIS, University of Louisiana Monroe, 700 University Avenue, Monroe, LA 71209-0120 (E-mail: ajohnston@ulm.edu). Mark B. Schmidt is Assistant Professor, Business Computer Information Systems, St. Cloud State University, St. Cloud, MN 56301 (E-mail: mbschmidt@stcloudstate. edu). Kirk P. Arnett is Professor of Information Systems, Mississippi State University, PO Box 9581, Mis State MS 39762 (E-mail: Kpa1@msstate.edu). Jeff Thomas is Network Manager in Computer Services, College of Veterinary Medicine, Mississippi State University, Mis State MS 39762 (E-mail: Jeff@cvm.msstate.edu).

Journal of Internet Commerce, Vol. 6(1) 2007
Available online at http://jicom.haworthpress.com

doi:10.1300/J179v06n01_01

KEYWORDS. Rootkit, malware, security, threat, awareness

INTRODUCTION

According to the most recent Internet Security Threat Report (Symantec, 2005), threats to computer security continue to increase in frequency and sophistication. Based on statistics derived from Symantec's global detection and analysis resources, attacks targeting financial interests and confidential data are most prevalent, with malicious code representing a substantial component of both current and projected threats. According to the 2005 CSI/FBI report based on feedback from 697 computer security practitioners who represent a diverse slice of corporate America, 56% of the respondents reported some form of malicious attack within the past year, up from 54% the previous year (Gordon, Loeb, Lucyshyn, & Richardson, 2005). Considering the tendency for many organizations to either not report or under-report attacks due to investor confidence issues and in order to maintain a low profile, it is likely that the reported rate is low. For instance, iDefense reports monitoring more than 27,000 attacks last year, more than half of which were designed to covertly steal information or take over computers (Brenner, 2005). Symantec and other security conscious vendors, even with more sophisticated and proactive stances, will likely be unable to successfully handle the estimated 75 new threats a day.

Concurrent with the pervasiveness of modern security threats, recent research indicates that corporate IT officials are finally starting to embrace the need to dedicate an appropriate level of resources toward threat amelioration (Whitman, 2003). A recent survey of 301 IT executives places security and privacy third among their most urgent management concerns, with CIOs placing a greater emphasis on it then other executives (Luftman & McLean, 2004). Luftman and McLean (2004) contend the high ranking is a reflection of the post 9/11 reality as well as a growing trend among consumers and investors to demand improved protection against IT-related threats. Increases in the number of formal security audits, financial commitments to holistic security practices, and interest in security awareness training are indicative of the maturation of computer security measures (Gordon, Loeb, Lucyshyn, & Richardson, 2004).

Some security measures have become heavily engrained in the security practices of IT professionals. For instance, nearly all (96%) of the CSI/FBI respondents report using some form of anti-virus product (Gordon et al., 2004). Firewalls are also a prominent (97%) ingredient in most of the security management practices. A well-regarded survey (Whitman, 2003) of IS directors, managers, and supervisors from various organizations identify passwords, media backup, virus protection, and employee education as the four protection mechanisms with the highest adoption rates, with password use at 100%, media backup at 97.9%, virus protection software at 97.9%, and employee education at 89.6%. Indeed, advances have been made within the IT community in terms of generating awareness of proper security management methods and of the dangers posed by various threats to computing. Unfortunately, many IT security professionals may find their practices lacking in the face of an emerging, yet somewhat unfamiliar threat of rootkits.

The purpose of this paper is to establish a baseline from which to understand our current level of knowledge of the rootkit phenomenon and thereby gauge our progress in the struggle to effectively cope with the threat. Following a review of the current state of rootkit development and deployment strategies, a survey of IT users is described and the findings are analyzed and presented. The paper concludes with a discussion of strategies to ameliorate rootkit infestations.

ROOTKIT OVERVIEW

A rootkit is a "set of programs used to hack into a system and gain administrative-level access. Once a program has gained access, it can be used to monitor traffic and keystrokes; create a backdoor into the system for the hacker's use; alter log files; attack other machines on the network; and alter existing system tools to circumvent detection" (www.wetstonetech.com/page/page/1972572.htm). While rootkits are designed to infect individual systems, their stealth capabilities facilitate the combined use of highly pervasive malware to penetrate and infest numerous systems, and this infection leads to the armies of botnets or zombie nets that are being unleashed on unprotected resources.

One such clandestine rootkit known as "winlogon.exe" acts as a key logger as a user enters their system password, adding another layer of difficulty on the user, winlogon.exe will cause the system to crash if the

user attempts to kill the process (Brandt, 2006). Moreover, the presence of a rootkits can prove very detrimental to a user as they can keep certain files from being displayed and further they can cause inaccurate reporting of file counts and sizes to the user, while the rootkit keeps itself, other files, registry keys, and network connections hidden from detection (TechWeb, 2005). The Radicati Group estimates that threats to information security will cost $54 billion by 2006 (Licari, 2005). If hackers are able to employ the use of rootkits to gain total control of a user's machine while users remain unaware of the consequences, the current estimate of $54 billion could prove to be a mere pittance.

A form of malware once almost exclusively associated with Unix-based hosts, rootkits are gaining ubiquity among Windows-based PCs (Spanbauer, 2005), and IT security managers are scrambling to find new techniques to combat this menacing hazard. Windows-based IT managers have enjoyed a certain degree of amnesty from rootkit exploits. Now that rootkits are beginning to proliferate in the Windows- based computing community, the challenges are even more daunting. As Paul Robert's (2005a) article title states, "Microsoft on Rootkits: Be afraid, be very afraid!"

ROOTKITS IN CONTEXT

Rootkits were initially designed to infect Unix systems but have more recently been beleaguering Windows' systems. It would appear that hackers developing rootkits are now using the strategy of many other malware creators. Due to the popularity of the Windows operating system, not only do hackers have a larger number of machines available to attack but they also have found that many of the machines are unprotected thus allowing their handiwork to spread at a more rapid pace. It is clear that this trend to focus on Windows-based machines will continue (Seltzer, 2005).

Interestingly, rootkits have maintained their family name since introduction. Consider that zombies have become botnets, man-in-the-middle attacks have become the "evil twin," DNS breaches have become Pharming, directed phishing attacks have become spear phishing, and so on. But rootkits were and are rootkits. Security reporters have come up with no better moniker. Rootkits have been linked to several attacks popularized by the media. For example, rootkits played a critical role in an attack against 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).

A rootkit refers to a piece of code that is intended to hide files, processes, or registry data, most often in an attempt to mask intrusion and to surreptitiously gain administrative rights to a computer system. Rootkits, when used in this malicious manner, can provide the mechanism by which various forms of malware–including viruses, spyware, and Trojans–attempt to hide their existence from detection utilities such as anti-spyware and anti-virus applications. So rootkits are not worms or viruses, but worms and viruses can deliver them. When embedded within the code of another malware program, such as spyware, the combined threat is referred to as a blended threat. For example, the product of a spyware/rootkit blended threat is software with the mobility and payload of spyware with the stealth-like nature and persistence of a rootkit to create a threat that is much more difficult to detect and remove.

As root is the highest level of administrative privilege on a Unix-based host, a rootkit is an attempt to establish and maintain this level of command on a compromised machine. In doing so, rootkits maintain their stealth posture by performing any number of functions, such as traffic monitoring, keystroke logging, log file altering, and system file modifying. Additionally, rootkits will usually create a backdoor into the compromised system to enable future access.

According to Dillard (2005b), a program manager for Microsoft Solutions for Security, the first public rootkit for Windows, NT rootkit, was introduced in 1999 by Greg Hoglund. Hoglund also maintains rootkit.com, a popular Website for disseminating information concerning the creation, detection, removal, and protection of computers from rootkit exploits. As Table 1 depicts, rootkits can be classified according to their volatility and execution mode. For instance, a rootkit that executes without user intervention each time the system boots is regarded as a persistent rootkit. This particular form of rootkit is maintained in a non-volatile location such as the system registry or is embedded within the file system. Conversely, memory-based rootkits are subject to removal upon reboot. Unfortunately, this form of rootkit is especially difficult to detect in that it does not leave file residue on the system after reboot. User-mode rootkits run in user mode with administrator privileges and typically avoid detection by intercepting and modifying system calls and filtering application programming interfaces (APIs). Finally, kernel-mode rootkits are established at the kernel level and are able to intercept native APIs as well as alter kernel-level data structures

TABLE 1. Classification of Rootkits Based on Volatility and Execution Mode

Volatility	Execution Mode
Persistent rootkit–rootkit code that resides in non-volatile location on the computer such as in the system registry or in the file system and executes without user intervention	*User mode*–rootkits run in user mode with administrator (root) privileges that mask detection by intercepting and modifying system calls and by filtering APIs
Memory-based rootkit–rootkit code that resides in volatile memory and is removed upon reboot	*Kernel mode*–rootkits that directly attack the system kernel and manipulate system calls by intercepting native APIs as well as by altering kernel level data structures or kernel execution paths

or kernel execution paths. This form of rootkit is the most difficult to implement and to detect.

AN EMERGING THREAT

Within the modern computer security paradigm, rootkits represent an under-reported, under-estimated threat to computer security. Over the past year, several higher education computing facilities across the United States have fallen victim to attacks involving rootkit installations. In April of 2004, Roberts and Weiss (2004) reported successful attempts by malicious hackers to compromise high-performance systems and install rootkit features to mask their presence. Although the attacks were successful in gaining access and installing rootkit code, they were quickly discovered and monitored before confidential data could be stolen. In March 2005, hackers installed rootkits on compromised systems at Boston College and California State University to hide remote attack activities against other systems (Rosencrance & Vijayan, 2004). Although forensic analysis led investigators to believe no confidential information was compromised, the mere presence of rootkit code underlines the sophistication intruders are incorporating in their attacks. In a similar incident involving a University of Connecticut server, a rootkit was apparently installed in October 2003, yet it was not discovered until June 2005 (T. News, 2005). A common thread in these stories is that the presence of a rootkit means that a security problem existed before the rootkit's installation; otherwise, the system would not have been compromised. Thus the defender of personal or corporate computers must not only remove the rootkit, but must also patch the vulnerability that initially allowed root access compromise.

One of the more prevalent rootkits is Hacker Defender, also known as hackdef, which was created by a hacker known as Holy Father. Beginning as a freely available software, Hacker Defender has drawn the ire of many rootkit detection developers in a continually evolving game of cat and mouse (Dillard, 2005a). Rootkit detection applications such as Strider Ghostbuster and Rootkit Revealer have proven effective in detecting the majority of rootkits, including Hacker Defender; however, for every release of detection software, an equally effective rootkit modification is released. Even Microsoft has engaged in the struggle with their release of the Malicious Software Removal Tool. Unfortunately, with proprietors of malicious endeavors such as identity theft, phishing, extortion, pay-per-machine spyware, and hacking-for-profit financing development, rootkits are becoming increasingly more sophisticated.

Given the veracity and voracity of the rootkit threat, it is critical that we establish a thread of consciousness of this threat among our IT user community. What is our current posture regarding rootkits? Specifically, what is the current knowledge level among IT users? The following section describes the method by which a survey of users was conducted concerning their perceptions of the rootkit threat. The results of this survey will provide a baseline from which to gauge progress toward amelioration of rootkits along a similar path to that of the computer virus and spyware threats.

Measuring User Perceptions of Rootkits

To understand where the education community stands in terms of rootkit awareness and knowledge, a survey was conducted involving 210 faculty, staff (including IT professionals), and students from three public institutes of higher learning from various geographical regions within the United States. We adopted a survey first used in a 1993 *Computers and Security* article (Jones, Arnett, Tang, & Chen, 1993) to gauge user knowledge of computer viruses and later used in a 2005 *Communications of the ACM* article (Schmidt & Arnett, 2005) to report user knowledge of spyware.

The survey respondents were predominantly male (57%), with 5 to 10 years of computer experience (43%). Most of the respondents operate in a Microsoft Windows environment with 69% having at least five years of experience. Conversely, less than 3% of the users have at least five years of experience with the Unix platform from which the rootkit threat evolved.

Survey responses indicate that only 16.2% of users have even heard of rootkits, and of those, only 10.6% have known of them beyond one year. Contrasting this is the fact that 99.5% of users have known of viruses for more than one year, and 83.8% of users have known of spyware for more than one year. These findings echo the relative newness of rootkits within the Microsoft Windows user domain. As could be expected, this general lack of awareness of rootkits is reflected in coping practices as only 9.5% of users run rootkit detection software.

Familiarity with rootkits is indeed low. In fact, only 6.19% of users self-report themselves as familiar with rootkits. In fact, users reported more familiarity with a fictitious virus, Trilobyte (7.14%), than with rootkits (See Table 2).

Even with the increase in the popular press of reports of incidents involving rootkits, awareness within the user community of the pervasiveness and dangers of rootkits remains low. Of those survey respondents that reported a familiarity with rootkits, slightly more than half were able to accurately report a rootkit's ability to manipulate logs (59%), to provide false feedback to detection utilities (56%), and to provide hackers with administrative rights (62%). Furthermore, only 53% of respondents reporting familiarity with rootkits recognized the presence of backdoor utilities within rootkits.

The limited awareness and knowledge of rootkits is especially alarming considering the recent "call to arms" against spyware and other forms of malicious malware. In August 2005, *Communications of the ACM* devoted a special edition to the emergence and proliferation of the threat of spyware (Stafford, 2005). However, within these articles no mention was made as to the presence of rootkit technology within spyware and their combined emergence as a new form of blended threat. What must occur next is an intelligence and preparedness ramp-up by the IT community consistent with that which is occurring in the fight against spyware. Certainly, we are on the brink of another battle for control of personal computers.

TABLE 2. Perceptions of Threat (%)

Familiarity with Viruses	Familiarity with Spyware	Familiarity with Rootkits
88.57	82.38	6.19

STRATEGIES FOR SUCCESS

Given the signature of a rootkit is to conceal its presence and activities, anti-virus applications are largely ineffective in that they cannot detect what they cannot see. Additionally, the manner in which rootkits are installed on systems further complicates their detection by traditional anti-malware software. Rootkits are often installed through tactics such as social engineering or through exploits of operating system vulnerabilities. Traditional symptoms of malware infestation, such as replication activities, are simply absent from rootkit manifestations. Jamie Butler, director of engineering for HBGary Incorporated, and Sherri Sparks, a PhD student at the University of Central Florida, reinforced the concept of rootkit obfuscation at the 2005 Black Hat conference in Las Vegas (Naraine, 2005). Their demonstration of the proof-of-concept rootkit, Shadow Walker, in which the code was able to hide in memory with virtually no impact on performance, further advanced the notion that current rootkit detection mechanisms are inadequate.

Conventional malware detection mechanisms such as anti-virus and anti-spyware software, now firmly established in the security practices of IT management, must be revisited as to their ability to address rootkit exploits. Embedded within spyware, viruses, or worms, rootkits provide stealth capabilities to malware making them almost impossible to detect and even more difficult to remove (Roberts, 2005b). For example, new variants of Rbot, a malicious remote control program, are now complete with the open-source rootkit FU (Roberts, 2005b). With the embedded rootkit code, this new blended threat is able to better hide from task management utilities that in the past were able to detect Rbot's processes. While Roberts (2005b) points out that this particular threat is fairly clumsy, it does represent a growing evolution among malicious-code purveyors to integrate rootkit logic into their programs. For instance, Roberts (2005c) reports new variants of the prevalent Cool Web Search spyware have rootkit code embedded within the malware in an effort to conceal its presence on compromised systems. Once a fairly simple program to detect and remove, Cool Web Search has now become a nightmare for those responsible for the security of infected machines.

With the emergence of these blended threats, computer security managers must take actions above and beyond traditional anti-malware techniques and employ methods consistent with the requirements of advanced rootkit detection and removal. Computer security measures such as network firewalls, e-mail scanning, anti-malware utilities,

intrusion detection applications, and intrusion prevention applications are synonymous with a holistic approach to IT security and should be regarded as a necessary first line of defense against rootkit infestation. Additionally, all computers should be updated frequently with any available software updates. There are far too many stories of infected machines where patches to block the infection were available, but simply not installed, long before the infection took place. In addition to the technical controls, behavioral controls should be implemented. Users should be educated about the dangers of malware, file sharing, and the potential for social engineering tactics. Users should also be made aware of the dangers associated with malicious Websites.

However, even the most well-protected networks are vulnerable to attack and, as such, detection and remediation techniques should be employed. Unfortunately, due to their nature and diversity, rootkits provide very little evidence of their presence. Certainly, typical malware-associated symptoms such as performance loss and file meta- data changes such as file size and time and date should be examined; however, the best detection results are found using rootkit-specific detection utilities. Many of these programs incorporate behavior detection, integrity detection, and signature-based analysis to detect stealthy programs (Naraine, 2005). Rootkit defense technologies, such as Microsoft's Strider Ghostbuster, FSecure's Blacklight, and SysInternal's Rootkit Revealer seek out registry and file-system API discrepancies that may point to a user-mode or kernel-mode rootkit (Naraine, 2005).

To effectively cope with the emerging rootkit threat, a deliberate approach to rootkit protection is required. Organizations and users must integrate rootkit-specific controls into their existing protection mechanisms. These controls, both technical and behavioral, must complement the security, thereby promoting a consistent and effective approach to malware deterrence, prevention, detection, and remediation. Fortunately, it now appears that anti-virus vendors are also beginning to seriously consider detection and removal of rootkit infestations as a part of their responsibilities. An additional sign of the prevalent nature of the rootkit milieu can be found in the fact that developers are also working on no-cost detection tools (Brandt, 2006).

CONCLUSION

The 1990s were the decade of the network-layer attacks (Tiller, 2005). If rootkits continue unabated, the next decade could very well be

an era characterized by hackers gaining control at all layers. Clearly rootkits pose a significant threat to computer security. Given the current levels of awareness and knowledge within the user community, this threat should continue to emerge much as virus and spyware threats did in their early stages. It should also be expected that our response to this threat would encounter many of the same challenges we face in our efforts against viruses and spyware. Awareness is a critical first step in securing against malware of any sort (Peltier, 2005). Currently, it appears as though we have a long road ahead.

REFERENCES

Brandt, A. (2006). New Rootkit Detectors Help Protect You and Your PC. *PC World*, Vol. 24, No. 8, p. 36.

Brenner, B. (2005). *Botnets are More Menacing Than Ever*. Retrieved September, 2005, from http://searchsecurity.techtarget.com/originalContent/0,289142,sid14_gci1068871,00.html

Dillard, K. (2005a). *Rootkit Battle: Rootkit Revealer vs. Hacker Defender*. From SearchWindowsSecurity.com

Dillard, K. (2005b). *What is a rootkit?* From SearchWindowsSecurity.com

Glossary, W. T. (2005). Retrieved 10-29-05, from http://www.wetstonetech.com/page/page/1972572.html

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2004). In *2004 CSI/FBI Computer Crime and Security Survey* (pp. 1-16): Computer Security Institute.

Gordon, L. A., Loeb, M. P., Lucyshyn, W., & Richardson, R. (2005). In *2005 CSI/FBI Computer Crime and Security Survey* (pp. 1-16): Computer Security Institute.

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*, Vol. 12, pp. 191-197.

Licari, J. (2005). Securing the Information Workplace: Managing Threats to Enterprise E-Mail, IM, and Document Sharing Environments. *Information Systems Security*, Vol. 14, No. 4, pp. 45-50.

Luftman, J. & McLean, E. R. (2004). Key Issues for IT Executives. *MIS Quarterly Executive*, Vol. 3, No. 2, pp. 89-104.

Naraine, R. (2005, July 28). "*Shadow Walker" Pushes Envelope for Stealth Rootkits*, from http://www.eweek.com/article2/0,1759,1841266,00.asp

News, C. H. (2005). *Rootkit Report*.

News, T. (2005). *University Discovers Rootkit on Compromised Server*. Retrieved June, 2005, from http://www.techweb.com/wire/164903436

Peltier, T. R. (2005). Implementing an Information Security Awareness Program. *Information Systems Security*, Vol. 14, No. 2, pp. 37-48.

Roberts, P. F. (2005a). *Microsoft on "Rootkits": Be Afraid, Be Very Afraid.* Retrieved September 8, 2005, from http://www.computerworld.com/securitytopics/security/story/0,10801,99843,00.html

Roberts, P. F. (2005b, May 23). Rootkits Spawn New Malware. *eWeek*.
Roberts, P. F. (2005c, June 20). Spyware Danger Meets Rootkit Stealth. *eWeek*.
Roberts, P. F. & Weiss, T. R. (2004, April 19). Hackers Breach Research Systems, But Data Kept Safe. *Computerworld*, Vol. 38, pp. 8-10.
Rosencrance, L. & Vijayan, J. (2004, March 21). University Computers Hacked on Each Coast. *ComputerWorld*.
Rosencrance, L. & Vijayan, J. (2005, March 21). University Computers Hacked on Each Coast. *ComputerWorld*, Vol. 39, pp. 57.
Schmidt, M. B. & Arnett, K. P. (2005). Spyware: A Little Knowledge is a Wonderful Thing. *Communications of the ACM*, Vol. 48, No. 8, pp. 67-70.
Seltzer, L. (2005). Rootkits: The Ultimate Stealth Attack. *PC Magazine*, Vol. 24, p. 76.
Spanbauer, S. (2005, June). Rootkits: Invisible Assault on Windows. *PC World*.
Stafford, T. F. (2005). Spyware. *Communications of the ACM*, Vol. 48, No. 8, pp. 34-35.
Symantec. (2005). *Symantec Internet Security Threat Report Highlights Rise in Threats to Confidential Information*. Cupertino, CA.
TechWeb. (2005). Retrieved 10/29/05, from http://www.techweb.com/encyclopedia/
Tiller, J. (2005). Digging Trenches. *Information Systems Security*, Vol. 14, No. 4, pp. 2-4.
Whitman, M. E. (2003). Enemy at the Gate: Threat to Information Security. *Communications of the ACM*, Vol. 46, No. 8, pp. 91-95.

RECEIVED: June 15, 2006
ACCEPTED: September 20, 2006

doi:10.1300/J179v06n01_01