Rootkits:

A hidden issue in security

Bryan Crawford
Olimhon Malikov
Matthew Miller

MBA605
Demorest, GA

20 February, 2006

Abstract:

Rootkit: A rookit is a collection of programs used by a hacker to evade detection while trying to gain unauthorized access to a computer. This is done either by replacing system files or libraries, or by installing a kernel module. The hacker installs the rootkit after obtaining user-level access.[1]

In this era of business threats to company security come in all forms, many of which are electronic threats that affect information systems and databases, often times these systems are critical to operations or contain important information that needs to be protected. Rootkits are quickly becoming a buzz word in computer security as they provide protection to malicious mal-ware and trojan ware programs that may affect a user's computer system. It is important to remember that in and of itself a rootkit is not always malicious or harmful, many computer security programs use this technology to operate. However the passages that rootkits provide for hackers to access a system are what make them dangerous. This writing reflects out research into what rootkits are capable of, how they affect a system, and one major example of how a major company attempted to use this technology to protect itself, only to run into negative publicity and a great financial burden.

"2006 will be the year of the rootkit. It's no longer just about getting on machines, it's how to stay on machines"[2] *Vincent Weafer, Senior Director, Symantec Security Response*

As the computer technology around the world continues to develop at a very steady speed the problems also keep a similar pace. Specifically within the personal computer and server technology areas security still remains as one of the primary and hard to tackle concerns. The battle between the software makers and virus authors has been active and computer attackers are posing newer weapons as means of intrusion.

One of these means of intrusion, known as rootkit, has recently become quite popular among hackers.

According to a recent report on rootkits by Kaspersky Lab[3], a developer of secure content management solutions aiming to protect against viruses, spyware, Trojans, hacker attacks and spam, rootkits are described as a set of programs enabling a hacker to maintain access to a computer after cracking it, while preventing the hacker from being detected. Kaspersky Lab's[4] report looks at how rootkits are detected, why they are dangerous and why their use is increasing.

Rootkit as a term originally referred to a special set of Unix tools that would hide the trace of any unauthorized user thus allowing the intruders to maintain so called *root* on the system without the system administrator even seeing them. The term however is not restricted to Unix based operating systems any longer, as similar tools now exist for other operating systems such as Microsoft Windows.

The Kaspersky Lab report also indicates rootkits' popularity is partly due to the fact that internet offers the source codes of many rootkits[5]. It's relatively easy for virus writers to make small modifications to such code. Another factor which influences the increased use of rootkits is the fact that most Windows users use the administrator's account, rather than creating a separate

user account. This makes the rootkit installation on the target machine much easier.

Authors of spyware primarily use rootkits to thwart anti spyware scanners. Rootkits also are used to protect programs known as Trojan horses, which allow remote spammers to take over your PC and use it to launch avalanches of e-mail. And, of course, the virus writers can use rootkits to disable malware scanners and block access to Web sites that contain security tools

Some of the well-known anti-virus software suppliers are seriously concerned with controversy over the use of rootkits in their products. The rootkit tools are known to exist in different versions of Microsoft Windows, Linux and Solaris. The files in a hidden directory or location will not be scanned during the scheduled or manual virus scans[6], providing a perfect hiding ground for Trojans, viruses and other malware. These factors are contributing to the rapid growth of rootkit reports and a steep increase in their presence. (Fig. 1) Kapersky Labs reported on their website, www.viruslist,com that rootkit usage grew 413% from 2004 to 2005,(Fig. 2) representing by far the fastest expanding type of malware.

The rootkit controversy started to come to light in the media and business with the findings of Mark Russinovich, a software developer and designer for Winternals Software of Austin, TX. Russinovich is considered an expert on rootkits and is credited for developing RootkitRevealer, software to combat this technology.[7] Russinovich discovered the presence of a rootkit like program on a copy of Sony BMG's *Get Right With The Man*, a CD release of southern rock group Van Zant. Sony had placed the code on the CDs in an effort to reduce piracy but in the process created a sand-storm of public outcry. Russinovich's findings were followed by those of Dan Kaminsky, and independent computer security analyst and advisor[8]. Kamisnky estimates that over 500,000 machines are infected world wide by the Sony borne rootkit.[9] Today, the global music giant faces mass criticism and class action lawsuits on this dangerous security loophole. They are in a process of replacing the affected CDs across the globe, estimated to be over 2 million in number[10]. The findings that some anti-virus companies were using similar rootkits in their security solutions gave a different dimension to the issue.

The discovery of the presence of rootkits in Sony BMG CDs and the following public and government outcry have led to a class action lawsuit against the record label. This pending case and its impacts will be discussed in further detail later.

Now that we have looked at the basics of rootkits and their emerging threat, The next thought is looking into how to combat this issue. There are two main ways to detect the presence of a rootkit: scanning and event monitoring. The scanning technique involves comparing a view of the system using user-space tools and a view from inside the kernel. If anything is hidden, it should be visible in the kernel, but not in the user space[11]. There are several weaknesses with this approach. For one, if the kernel has been infected by a rootkit then there is a high chance the results of the scan of the kernel will also be incorrect. One way around this issue is by shutting down the computer and booting from an alternative source that you know is clean [12]. The other weakness is the fact that rootkits are able to escape detection by hiding from the scan. Most rootkits are able to hide from all processes except those designed to detect the specific rootkit. The other option to detect the presence of rootkits is the event monitoring method. This method uses intrusion-prevention systems that monitor system behavior from the inside the kernel. IPS programs are able to block kernel modules such as rootkits from loading. Properties and other characteristics of the modules are inspected to see if the module appears malicious. This process must be completed because other safe kernel modules are often used such as antivirus programs and only the possibly harmful ones would need to be detected. The event monitoring also has drawbacks by as mentioned before by often classifying safe programs that use kernel modules as harmful[13].

The actual removal of the rootkit presents other problems. Where a virus attempts to spread, a rootkit tries to remain in a single system. The payload of the rootkit attempts to make sure the system remains compromised by the rootkit[14]. Removal of the rootkit from a system requires removing the rootkit itself, and the payload. Due to rootkits primarily being kernel modules that affect the operating system this task is

daunting. To remove the rootkit and payload without causing damage or instability to the operating system is very difficult. Russ Cooper, founder of the NTBugtraq mailing list, notes that "only a person with very little knowledge would try to remove a rootkit"[15]. It appears that once a system has been affected by a rootkit the only 100% safe stance to combat the infection is total reformatting of the hard drive and reinstallation of the operating system[16]. The sentiment that rootkit removal is difficult and possibly damaging is echoed by multiple experts who have spoken in regard to the current Sony BMG case as well.

"The road to hell is paved with good intentions", historians are unsure of exactly who said this, although it often credited to Samuel Johnson, in any case it seems relevant to Sony BMG Music's current situation. Sony BMG, like other record companies is looking for ways to copy protect its music to help prevent piracy and illegal copying. In this quest they along with First 4 Internet Ltd developed a type of DRM (digital rights management) software that they dubbed "sterile burning"[17] this embedded program was included on 52 CD releases from the music mogul. The good intentions of the program were to allow users to play the CD in their computers as well as convert the music a format supported by MP3 players. However it also imposed a limit of how many times the CD could be digitally copied, or ripped, to 3.[18] The negative effect of this protection software soon surfaced when internet security experts noticed the presence of rootkits on otherwise clean computers that had been used to play Sony BMG music CDs.

The issue for Sony BMG lies not in the use of DRM software and rootkits to implement it but rather in the manor it was done, and the potential security hazards that accompany it. Critics of the software, including Texas Attorney General Greg Abbot and the Electronic Frontier Foundation feel that Sony did not do enough to inform and educate consumers about the type of program they were using and the possible effects it could have on system operations.[19] In order to play a copy protected disc such as those distributed by Sony BMG the user must agree to a consent form which in turn allows the rootkit files to embed in the computer and allow the

DRM software to operate. However, security experts have labeled the Sony BMG software, titled XCP, as a type of spyware after having determined that it secretly sends information about music that the PC is playing[20] and that because the software is very difficult to uninstall and is vulnerable to viruses it is potentially malicious.[21] Attempts to remove the software have proven difficult and in some cases costly, as current editions of spyware and adware removal programs have no effect on the programs. Manual removal of the files is also limited to only the most sophisticated and experienced computer users, as Russinovich was quoted as saying "The Average user would not be able to remove [the Sony BMG DRM] without losing…the CD [drive]. Even a sophisticated user would have trouble."[22] The problem lies in the fact that removal of certain portions of the code will disable the computer's optical drives, CD, CD-RW, etc.

So far security and virus experts have identified one virus that operates on the Sony BMG XCP rootkit and attacks computers that the program operates in.[23] and security firm Sophos has identified a trojan horse program that uses XCP to open a gateway to other malicious programs.[24] Sophos senior analyst Gregg Mastoras stated that "Sony thought they would help stop music piracy. But it's opened a vulnerability that hackers have exploited."[25]Another company has began to see issues evolving from the Sony BMG software as well, Blizzard Entertainment, a video gaming company has reported that its users are finding ways to manipulate the Sony BMG program to allow them to cheat while playing an online game, *World of Warcraft,* these gamers are using the cloaking abilities of XCP's rootkit to hide from game monitors that prevent cheating.[26]

Russinovich pointed out that Sony BMG does offer an online resource for uninstalling the software; however his attempts to navigate Sony BMG's formal procedures were not successful. Billboard magazine researchers also had the same results, and were unable to get assistance from Sony BMG in resolving the issue.[27]

For Sony BMG this issue goes beyond disgruntled customers, concerned security experts, and aggressive State Attorneys (Texas has strict anti-spyware

laws) the company faces a large cost involved in the recovery and replacement of affected CDs as well as potential liabilities for affected computers. Another costly figure for the company is lost sales revenue; estimates are that the Van Zant release where the program was first disclosed could see sales losses of 50,000 plus units[28]. Sony BMG reports that 52 titles (Fig. 3) were copy protected with this software and that 5 million CDs were shipped with 2.1 million of those being sold into circulation[29] while Kaminsky pegged 500,000 as the number of computers likely running the software[30] worldwide.

Sony BMG appears to be looking to reduce the fallout from this snafu by seeking an out of court settlement to the class action lawsuit filed in Texas. The suit, filed under Texas law could have proven extremely costly for Sony. Texas law provides for up to $100,000 in damages to be paid for **each** violation of its anti-spyware law.[31] However Sony has announced a proposed settlement in which they will be replacing all affected CDs with CDs not containing this particular form of copy protection. This settlement provides a combination of a minimal cash payment and 1-3 free online album downloads. However it has not been accepted yet and many people in the legal environment still feel that Sony is not doing enough to resolve the issue or to increase awareness of the problem and the recall of CDs. New York Attorney General Eliot Spitzer and his staff were able to obtain copies of DRM containing CDs from retailers such as Wal-Mart and Best Buy more than a week after Sony called for a recall and exchange program.[32] Spitzer's office is also considering a class action suit on behalf of New York consumers and Cindy Cohn a spokesperson for the Electronic Frontier Foundation is calling for Sony to take a more active role in recalling the CDs through advertising on radio and in retail outlets.[33]

It is too early to tell how costly this will be for Sony BMG as lawsuits and settlements are still pending, and the loss of future sales due to consumer animosity may be difficult to account for; however costs for manufacturing and return fees have been estimated as to be as high as $6.5 million.[34]

Rootkits alone are not going to pose the next huge security threat to business or to consumers.

However their manipulation and usage by hackers and virus writers can be significant. The potential for public and legal outcry, as evidenced by the Sony BMG issue is great and the costs associated with that can be even greater. How this technology will continue to develop and be used will have to be monitored, until that time it is essential to keep an open eye on the rootkit issue.

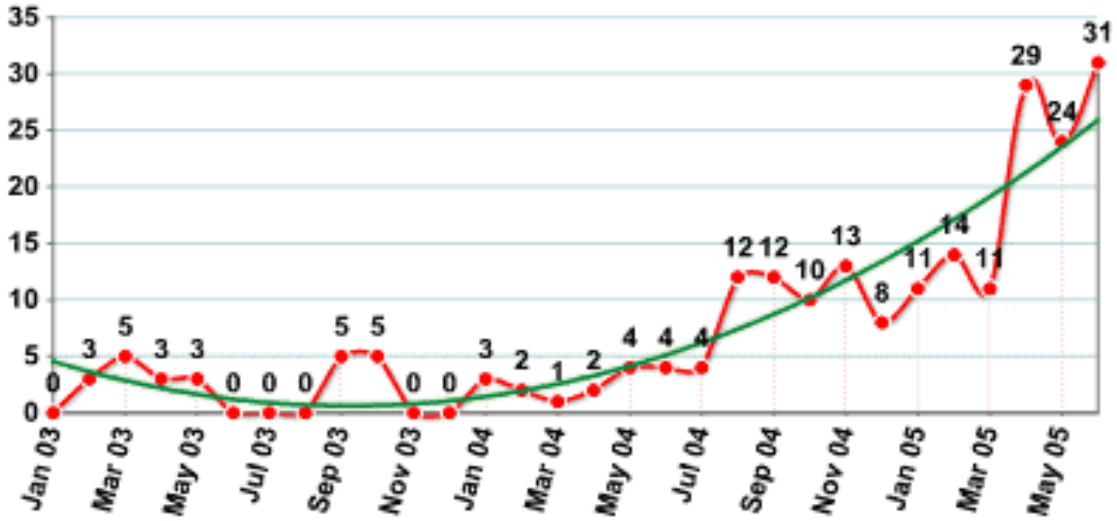

Figure 1: Increase in rootkit usage by malicious programs Source: www.viruslist.com

Behaviour	Change in number of malicious programs (2005 vs 2004)
Backdoor	95%
Trojan	90%
Trojan-AOL	—
Trojan-ArcBomb	—
Trojan-Clicker	86%
Trojan-DDoS	—
Trojan-Downloader	272%
Trojan-Dropper	212%
Trojan-IM	—
Trojan-Notifier	—
Trojan-Proxy	68%
Trojan-PSW	122%
Trojan-Spy	104%
Rootkit	413%
TrojWare	**124%**

Figure 2: Growth Rates for various trojan-type programs Source: www.viruslist.com

ARTIST	ALBUM
A Static Lullaby	Faso Latido
Acceptance	Phantoms
Amerie	Touch
Art Blakey	Drum Suit
The Bad Plus	Suspicious Activity?
Bette Midler	Sings the Peggy Lee Songbook
Billie Holiday	The Great American Songbook
Bob Brookmeyer	Bob Brookmeyer & Friends
Buddy Jewell	Times Like These
Burt Bacharach	At This Time
Celine Dion	On Ne Change Pas
Chayanne	Cautivo
Chris Botti	To Love Again
The Coral	The Invisible Invasion
Cyndi Lauper	The Body Acoustic
The Dead 60's	The Dead 60's
Deniece Williams	This Is Niecy
Dextor Gordon	Manhattan Symphonie
Dion	The Essential Dion
Earl Scruggs	I Saw The Light With Some Help From My Friends
Elkland	Golden
Emma Roberts	Unfabulous And More: Emma Roberts
Flatt & Scruggs	Foggy Mountain Jamboree
Frank Sinatra	The Great American Songbook
G3	Live In Tokyo
George Jones	My Very Special Guests
Gerry Mulligan	Jeru
Horace Silver	Silver's Blue
Jane Monheit	The Season
Jon Randall	Walking Among The Living
Life Of Agony	Broken Valley
Louis Armstrong	The Great American Songbook
Mary Mary	Mary Mary
Montgomery Gentry	Something To Be Proud Of: The Best of 1999-2005
Natasha Bedingfield	Unwritten
Neil Diamond	12 Songs
Nivea	Complicated
Our Lady Peace	Healthy In Paranoid Times
Patty Loveless	Dreamin' My Dreams
Pete Seeger	The Essential Pete Seeger
Ray Charles	Friendship
Rosanne Cash	Interiors
Rosanne Cash	King's Record Shop
Rosanne Cash	Seven Year Ache
Shel Silverstein	The Best Of Shel Silverstein
Shelly Fairchild	Ride
Susie Suh	Susie Suh
Switchfoot	Nothing Is Sound
Teena Marie	Robbery
Trey Anastasio	Shine
Van Zant	Get Right With The Man
Vivian Green	Vivian

Figure 3: Sony BMG CD List

[1] Anonymous (Kaspersky)
[2] Anonymous
[3] Mashevsky, Monastrysky, Sapronov
[4] Mashevsky, Monastrysky, Sapronov
[5] Mashevsky, Monastrysky, Sapronov
[6] Tittel
[7] Roberts (November 7, 2005)
[8] Roberts (November 15, 2005)
[9] Roberts (November 15,2005)
[10] Christman, Garrity
[11] Williamson
[12] Kay
[13] Williamson
[14] Kay
[15] Kay
[16] Kay
[17] Roberts (November 7, 2005)
[18] Austin
[19] Austin
[20] Austin
[21] Christman, Garrity
[22] Roberts (November 7,2005)
[23] Christman, Garrity
[24] Garrity
[25] Garrity
[26] Garrity
[27] Garrity
[28] Hesseldahl
[29] Hesseldahl
[30] Roberts (November 15,2005)
[31] Austin
[32] Hesseldahl
[33] Austin
[34] Christman, Garrity

References

Anonymous. (2006). You Don't Say. *IT Architect,* 21. 1. 18 Retrieved 2/19/2006 from http://proquest.umi.com.ezproxy.piedmont.edu/pqdweb?index=10&did=965809151&SrchMode=1&sid=1&Fmt=3&VInst=PROD&VType=PQD&RQT=309&VName=PQD&TS=1140389351&clientId=30061&cfc=1

Anonymous (2006) Glossary of terms: Rootkit. *Kapersky Lab/* Retrieved 2/19/2006, from http://www.viruslist.com

Austin, Liz. (2006, November 21) SONY BMG Sued Under Anti Spyware Laws. *Associated Press Online.* Retrieved 2/19/2006 , from http://web.lexis-nexis.com.ezproxy.piedmont.edu/universe/document?_m=417eae75e70ecbebe88a473229bd96d6&_docnum=12&wchp=dGLbVtz-zSkVb&_md5=09e2337835358164e6518f60236b77ea

Christman, Ed. Garrity, Brian. (2005, November 26) Sony BMG Recalls CDs. *Billboard,* 117. 48. Retrieved 2/19/2006, from http://web12.epnet.com.ezproxy.piedmont.edu/citation.asp?tb=1&_ug=sid+1ED1AE25%2D238E%2D41D8%2D86E1%2DF53E1E9F1A95%40sessionmgr5+dbs+aph+DBC8&_us=frn+1+hd+False+hs+True+cst+0%3B2+or+Date+fh+False+ss+SO+sm+ES+sl+0+dstb+ES+mh+1+ri+KAAACBUB00021309+ED72&_uso=hd+False+tg%5B2+%2D+tg%5B1+%2D+tg%5B0+%2D+st%5B2+%2D+st%5B1+%2D+st%5B0+%2DSony++BMG++Recalls++CDs+db%5B0+%2Daph+op%5B2+%2DAnd+op%5B1+%2DAnd+op%5B0+%2D+mdb%5B0+%2Dimh+08B4&fn=1&rn=1

Garrity, Brian. (2005, November 19) Sony BMG's Copy Protection Incites Global Controversy. *Billboard*, 117. 47. Retrieved 2/17/2006, from http://web12.epnet.com.ezproxy.piedmont.edu/citation.asp?tb=1&_ug=sid+1ED1AE25%2D238E%2D41D8%2D86E1%2DF53E1E9F1A95%40sessionmgr5+dbs+aph+DBC8&_us=frn+1+hd+False+hs+True+cst+0%3B2+or+Date+fh+False+ss+SO+sm+ES+sl+0+dstb+ES+mh+1+ri+KAAACBUB00021358+0503&_uso=hd+False+tg%5B2+%2D+tg%5B1+%2D+tg%5B0+%2D+st%5B2+%2D+st%5B1+%2D+st%5B0+%2DSony++BMG%27s++Copy++Protection+db%5B0+%2Daph+op%5B2+%2DAnd+op%5B1+%2DAnd+op%5B0+%2D+mdb%5B0+%2Dimh+A81F&fn=1&rn=2

Hesseldahl, Arik. (2005, November 29) Spitzer Gets 0n Sony BMG's Case. *Business Week Online* Retrieved 2/19/2006, from

http://web.lexis-nexis.com.ezproxy.piedmont.edu/universe/document?_m=706d399bca088b451b8218cb3fb7016d&_docnum=13&wchp=dGLbVlb-zSkVb&_md5=9621c95cc1c1b3d298d462e30d41058e

Kay, R. (2006, January 30). Rootkits. *Computer World,* Retrieved 2/16/2006, from http://www.computerworld.com

Mashevsky, Yury. Monastrysky, Alexey. Sapronov, Konstantin. (2005, August 19). Rootkits and how to combat them. Retrieved 2/19/2006, from http://www.viruslist.com/en/analysis?pubid=168740859

Mashevsky, Yury. (2006, February 8). Malware Evolution: 2005. Retrieved 2/19/2006, from http://www.viruslist.com/en/analysis?pubid=17894694

Roberts, Paul. (2005, November 7). DRM Software Uses Rootkit Techniques. *E-week.com* Retrieved 2/19/2006, from http://web.lexis-nexis.com.ezproxy.piedmont.edu/universe/document?_m=de07810df145603bb14d99d43f633649&_docnum=18&wchp=dGLbVlb-zSkVb&_md5=b49bf3346d14c0b89ae953e7efc27a79

Roberts, Paul (2005, November 15). Sony's Rootkit Is on 500,000 Systems, Expert Says. *E-Week.com* Retrieved 2/19/2006, from http://www.eweek.com

Tittel, Ed. (2005, December 14). Rooting Out Rootkits. *VAR Business* Retrieved 2/19/2006, from http://www.varbusiness.com

Williamson, M. (2005, December 7). The secret life of a rootkit. *Compuer World*, Retrieved 2/17/2006, from http://www.computerworld.com