UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

In re: SONY BMG CD TECHNOLOGIES LITIGATION	Case No. 1:05-cv-09575-NRB

AFFIDAVIT OF MARK RUSSINOVICH IN SUPPORT OF PLAINTIFFS' MOTION FOR FINAL APPROVAL OF CLASS ACTION SETTLEMENT

GIRARD GIBBS & De BARTOLOMEO LLP
Jonathan K. Levine (JL-8390)
Daniel C. Girard (Pro Hac Vice)
Elizabeth C. Pritzker (Pro Hac Vice)
Aaron M. Sheanin (Pro Hac Vice)
601 California Street, Suite 1400
San Francisco, California 94108
Telephone: (415) 981-4800

KAMBER & ASSOCIATES, LLC
Scott A. Kamber (SK-5794)
19 Fulton Street, Suite 400
New York, NY 10038
Telephone: (877) 773-5469

Class Counsel

I, Mark Russinovich, hereby declare as follows:

1. I am an adult over the age of 18 years and am legally competent to execute this affidavit. I make this affidavit in support of Plaintiffs' Motion For Final Approval Of Class Action Settlement based on my personal knowledge unless noted otherwise. If called to testify, I could and would testify to the following.

Background And Expertise

2. I have been a software engineer and technical writer professionally for the past 12 years. I earned my Bachelor of Science from Carnegie Mellon University in computer engineering and my Master of Science from Rennselaer Polytechnic Institute in computer engineering. In 1994, I earned my doctorate from Carnegie Mellon University in computer engineering.

3. Since 1996, I have been the chief software architect and co-founder of Winternals Software, a company that specializes in advanced systems software for Windows. Before founding Winternals Software, I held positions at Compuware NuMega Laboratories and IBM's Thomas J. Watson Research Center. I am a senior contributing editor for *Windows IT Pro* magazine (previously called *Windows NT Magazine*) on the subject of the Architecture of Windows 2000 and am co-author of *Inside Windows 2000* (4th edition). I have given presentations to major computer software industry conferences such as Microsoft Tech Ed, Microsoft IT Forum, Windows IT Pro Magazine's Connections, and MCP Magazine's TechMentor. I co-created a 12-hour self-paced Windows internal video tutorial which Microsoft licenses for worldwide corporate use, and I am a Microsoft Most Valuable Professional (MVP).

4. I am a principal of Sysinternals, a provider of advanced utilities, technical information and source code related to Windows NT/2000/XP/2K3, Windows 9x and Windows Me. I have authored many freeware tools for Sysinternals including Process Explorer, Filemon

and Regmon. I am also the author of many tools used by Windows NT and Windows 2000 kernel-mode programmers, and of the NTFS filesystem driver for DOS. I host a weblog at www.sysinternals.com/Blog. My curriculum vitae is attached hereto as Exhibit A.

Discovery Of The Sony XCP Software Rootkit And Malware

5. Rootkits are cloaking technologies that hide files, Registry keys and other computer system objects from diagnostic and security software. Over the past year, various types of malware, such as viruses, Trojan horses and spyware, have started to use rootkits as a method of "cloaking" or hiding themselves from spyware blockers, antivirus software and system management utilities. In my opinion, there are no legitimate uses for rootkit technologies.

6. At Sysinternals, I co-developed a software tool called RootkitRevealer to find files and Registry keys that are hidden from view. RootkitRevealer pinpoints rootkits by running two scans on a computer system, comparing the results and looking for discrepancies between those results. If one scan reveals an object hidden from the other scan, that object likely is a rootkit.

7. In October 2005, when I was testing the latest version of RootkitRevealer, I discovered evidence of a rootkit on one of my computer systems. Upon further research, I discovered a hidden directory, several hidden device drivers and a hidden application on my system. On October 31, 2005, I published an account of my experiences in discovering this rootkit on my weblog, a true and correct copy of which is attached hereto as Exhibit B.

8. After extensive analysis, I determined that the rootkit had been installed when I first listened to the CD album *Get Right With The Man* by the band Van Zant. See Exhibit B at 4. This album was released by Columbia Records, a division of Sony BMG Music Entertainment. The rootkit and hidden files were installed on my system by anti-copying

software called Extended Copy Protection ("XCP"), which was developed by UK software company First 4 Internet and contained on the Sony BMG music CD. Anti-copying software like XCP is also referred to as "digital rights management" software or "DRM." I understand that Sony BMG has released 27 CD titles containing XCP software.

9. *Get Right With The Man* was the first CD that I had purchased with DRM software. When I placed the CD in my computer, it automatically installed the XCP software and Sony BMG's proprietary media player. The XCP software prevented me from listening to the CD through any program other than Sony BMG's proprietary media player. The XCP software also limited me to burning no more than three (3) backup copies of the CD. In order to listen to or use the CD though my computer, I had to agree to install the XCP software. In addition to installing the DRM software, however, the CD also automatically installed a rootkit.

10. After running further tests on my system, I confirmed that the rootkit and its associated files were related to the XCP software. The rootkit in the XCP software causes a computer's operating system to conceal files, directories, Registry keys and other objects that begin with "sys." Because the XCP software does not prevent other software programs from using the "sys" prefix as a cloaking mechanism, any computer program can hide itself in a computer system by renaming its files to begin with "sys." As a result, the XCP rootkit renders computers susceptible to security vulnerabilities from third parties by disabling firewalls, anti-spyware and other security protection programs. See Exhibit B at 2-3.

11. I searched for a way to uninstall the XCP software from my computer. However, I did not find any reference to the XCP software in my computer's Control Panel's Add or Remove Programs list. I did not find an uninstall utility or directions on the CD or on First 4 Internet's internet website. My efforts to remove the XCP software from my computer manually proved difficult. After I deleted the files manually and rebooted my system, I discovered that the

icon for my CD-Rom drive had been deleted and my CD-Rom drive had been disabled. Because of my expertise with Microsoft Windows, I was able to restore functionality to my CD-Rom drive. I would not expect the average consumer to be able to resolve that problem. See Exhibit B at 7.

12. I checked the End User License Agreement ("EULA") that accompanied the XCP CD and saw no mention of the fact that, by inserting the CD into my computer, I was agreeing to have software placed on my system that I could not uninstall. The EULA also failed to mention the fact that the XCP software would install a rootkit and associated hidden files on my system. See Exhibit B at 7.

13. As the XCP EULA failed to disclose the software's use of cloaking and the fact that the software does not have an uninstall mechanism, it is my opinion that the XCP software used by Sony BMG on these 27 music CDs creates a significant security danger for end users. End users not only install the software when they agree to the EULA; they also effectively lose control of part of their computer. This consequence has reliability and security implications. Specifically, end users have no way to ensure that they have up-to-date security patches for software that they do not know is on their computers. End users also lack the means to remove, update or even identify the hidden software that may be causing their computers to crash.

14. As I described in my weblog published on November 4, 2005, a true and correct copy of which is attached hereto as Exhibit C, the XCP EULA also failed to inform consumers that the XCP software engages in "phone home" behavior, by contacting Sony BMG through the internet and communicating information that could track consumers' behavior. Based on my research and discussions with other interested persons, I understand that the XCP software establishes a connection with Sony BMG's internet website and provides Sony BMG with an

identification code associated with the CD being listened to by the consumer. See Exhibit C at 5-6.

Sony BMG's Initial Response To Consumers' Concerns About XCP

15. Sony BMG's initial public response to the findings that I published in my weblog was simply to refuse to admit that the company had done anything improper. In various news interviews on or about November 1, 2005, representatives of Sony BMG and First 4 Internet said that the disclosures in the XCP EULA were adequate, despite the fact that the XCP EULA did not inform end users that the software automatically installs on a user's system, installs hidden software, and does not have an uninstaller. It is my understanding that Sony BMG and First 4 Internet also publicly stated that the use of a cloaking mechanism in connection with the XCP software was an acceptable practice, and is of no concern to consumers and computer users. Indeed, in a National Public Radio interview on November 4, 2005, Thomas Hesse, President of Sony BMG's Global Digital Business, said: "Most people I think don't even know what a rootkit is. So, why should they care about it?" The full interview and report is available and can be heard on the internet at www.npr.org/templates/story/story.php?storyId=4989260. On November 6, 2005, I published a discussion and analysis of the reactions of First 4 Internet and Sony BMG on my weblog, a true and correct copy of which is attached hereto as Exhibit D.

Sony Releases Cumbersome XCP Software Patch

16. After continued media exposure, Sony BMG released a patch designed to remove the XCP software's decloaking mechanism, on or about November 3, 2005. The Sony BMG patch was a large file, approximately 3.5 MB, which included updated drivers and executables for the XCP software, and which automatically updated all other DRM on the end user's system without first disclosing that it would do so. The Sony BMG patch also was unsafe and had the potential to cause end users' systems to crash and lose data. Because of these concerns, on

November 4, 2005, I discovered and posted a command on my weblog that allowed end users to decloak the XCP software safely, while keeping it on their systems. See Exhibit C at 2-5.

17. On or about November 3, 2005, Sony BMG released a computer program to uninstall the XCP software from their computers (such a program is commonly referred to as an uninstaller). Sony BMG refused to make the uninstaller readily available to consumers, however. Instead, the reference to this uninstaller on Frequently Asked Questions (FAQ) page of Sony BMG's internet website directed consumers to another page. That second, landing page required consumers to fill out a form request that Sony BMG email uninstall directions to the requester. In order to obtain these directions, the requester was required to identify, among other things: the name of the music artist on whose CD the XCP software was placed, the album title, the name of the store from which the consumer bought the CD, and the consumer's email address. There was no way to access the uninstaller without first providing all of this requested information to Sony BMG. Worse, according to Sony BMG's then-posted privacy policy, by filling out a form request for the uninstaller, consumers authorized Sony BMG to use their email addresses for direct marketing campaigns by Sony BMG, its affiliates and other third parties. After submitting the form, requesters received an email from Sony BMG assigning a case ID and directing them to another page on Sony BMG's website, where the consumers were required to submit a second request to uninstall the XCP software. That webpage informed consumers that they should receive an email with a link to an uninstaller within one (1) business day. I never received the promised email. See Exhibit C at 1-2.

18. As I described in my weblog published on November 9, 2005, a true and correct copy of which is attached hereto as Exhibit E, Sony BMG failed to explain why it did not publicize the uninstaller on its website, why it did not make the uninstaller available as a freely accessible download as it did the patch, nor why users had to submit two requests for the

uninstaller and then wait for further instructions to be emailed. While consumers tried to navigate the difficult process of obtaining an uninstaller from Sony BMG, the XCP rootkit remained on their systems and continued to expose them to malware.

19. Since my discovery of the XCP rootkit, Sony BMG's practices have come under fire not only from consumer advocates and computer privacy experts, but also from the federal government. As I described in my weblog published on November 14, 2005, a true and correct copy of which is attached hereto as Exhibit F, I understand from media reports that on or about November 11, 2005, Stewart Baker, the assistant secretary for policy in the Department of Homeland Security criticized Sony BMG at a conference sponsored by the U.S. Chamber of Commerce, saying: "It is very important to remember that it's your intellectual property – it's not your computer. And in the pursuit of protection of intellectual property, it's important not to defeat or undermine the security measures that people need to adopt in these days."

20. Sony BMG announced on or about November 16, 2005 that it would recall XCP CDs. See Russinovich weblog published November 16, 2005 (a true and correct copy of which is attached hereto as Exhibit G). It is my understanding that Sony BMG failed to take action to notify consumers and retailers that the recall was taking place, however. See Russinovich weblog published November 30, 2005 (a true and correct copy of which is attached hereto as Exhibit H). Based upon reports in the media, I understand that, as of the end of November 2005, XCP CDs continued to line the shelves of major retailers in cities around the country including Austin, Philadelphia, Chicago and New York. In addition, although Sony BMG could have taken advantage of XCP's "phone home" capabilities to send a banner advertisement to notify all affected consumers that a recall of the XCP CDs was in place, Sony BMG failed to do so. See Exhibit H at 1.

Sony BMG's MediaMax Software

21. Certain Sony BMG music CDs contain another type of DRM software called MediaMax, which was developed by software company SunnComm International. Like XCP, MediaMax has no uninstaller mechanism and engages in "phone home" behavior without informing end users.

22. On or about November 29, 2005, iSEC Partners, a security research and consulting firm, reported that it discovered a security vulnerability associated with MediaMax, namely that the software creates a risk of a "privilege escalation attack." In a privilege escalation attack, a user with low-rights access to a computer system is able to exploit a security weakness to make changes to the system that only an administrator would be able to make under normal circumstances.

23. In my opinion, MediaMax, while harmful, does not pose the same level of danger to end users and their computer systems as XCP, because MediaMax does not contain a rootkit that installs hidden files on an end user's system and evades detection from firewalls, anti-spyware and anti-virus software.

The Benefits Afforded By This Settlement Address Consumers' Concerns

24. I was retained by Kamber & Associates, LLC to serve as a technical consultant for this litigation shortly after the initial class action complaints were filed with this Court. See Exhibit H at 2. Prior to my formal retention, I had been in communication with Scott A. Kamber regarding Sony BMG's use of the XCP and MediaMax software.

25. On November 21, 2005, I participated in the initial meeting between Class Counsel and counsel for Sony BMG. I assisted Class Counsel in preparing for that meeting and participated in the meeting telephonically. At that meeting, Class Counsel proposed that Sony BMG take immediate steps to: (1) permanently stop the sale of Sony BMG music CDs equipped

with XCP; (2) eliminate the risk of harm from the XCP CDs presently in circulation; (3) remedy the harm that had been caused to consumers who bought XCP CDs; and (4) address the possibility that a security vulnerability would be discovered (as one subsequently was) on Sony BMG music CDs containing MediaMax. Class Counsel offered my expertise in order to ensure that a pre-settlement remediation program contemplated by Sony BMG would be technically feasible and effective for consumers.

26. At that meeting, Class Counsel and I proposed that Sony BMG use XCP's "phone home" capabilities to send a banner advertisement to notify consumers about the dangers of the software and any eventual class action settlement. Based on my interaction with counsel for Sony BMG during and after the meeting, I concluded that Sony BMG had not contemplated using banner advertisements for these purposes.

27. I am proud that the proposals we advanced at the November 21, 2005 meeting formed the basis for settlement negotiations by Class Counsel, and that the Settlement before the Court satisfied the basic requirements we presented at that meeting. Each of the areas of benefit of the settlement that I describe below was first presented to Sony BMG at the November 21, 2005 meeting.

28. My role as technical consultant continued through the negotiation process. I provided technical advice where needed and reviewed the terms of the settlement with Class Counsel prior to execution.

29. As part of my role as a technical consultant, I am familiar with the Consolidated Amended Class Action Complaint filed in this action. I am also familiar with and provided input on the terms of the Settlement Agreement filed in this action. See Russinovich weblog published December 30, 2005 (a true and correct copy of which is attached hereto as Exhibit I). In my

opinion, the Settlement achieves all of the goals of the litigation, and greatly benefits consumers, for each of several reasons.

a. Sony BMG Has Recalled XCP CDs From The Marketplace, Distributed Patches And Uninstallers, And Provided Incentives For Consumers To Exchange Their XCP CDs

30. Under the Settlement, Sony BMG has agreed to stop manufacturing and distributing XCP CDs and to stop manufacturing MediaMax CDs.

31. In addition, under the Settlement, Sony BMG is recalling all music CDs that contain the XCP software. Under the Settlement, consumers can exchange their XCP CDs with Sony BMG and retail stores, and receive an identical CD without the XCP software. Sony BMG is also providing a variety of incentives – cash and/or free album downloads – to consumers who exchange their XCP CDs, thereby facilitating the XCP CD recall program achieved through the Settlement. The free album downloads provided by the Settlement are available from several online sources, including *iTunes*, which I understand to be the most popular music download format available.

32. As well, under the Settlement, Sony BMG has released and continues to make widely available software programs that will update XCP software and MediaMax software to eliminate all known security vulnerabilities including XCP's cloaking mechanism. Sony BMG has also released and made publicly available uninstaller utilities to enable consumers to remove XCP and MediaMax from their computers.

33. The XCP exchange program and the updates and uninstallers are designed to eliminate the security dangers associated with Sony BMG's DRM software programs.

b. Sony BMG Has Informed Consumers About The Information Exchanged Through Its DRM Software

34. As part of the Settlement, Sony BMG has informed consumers of the information that it collects as part of the "phone home" feature of the XCP and MediaMax software. Sony

BMG has limited this information to that necessary to provide the CDs with enhanced functionality and agreed to destroy that information within a short time of it collection. As a result, consumers now will be aware of the fact that this software transmits information from their computers back to Sony BMG. Consumers who do not want information sent electronically to Sony BMG of course will be able to uninstall the software from their computers.

c. Sony BMG Has Waived Most Of The Terms Of The XCP And MediaMax EULAs

35. Sony BMG has also agreed to waive the most onerous provisions of the EULAs for XCP and MediaMax software. For example, Sony BMG will no longer limit consumers to listening to their CDs only through specific software programs or on certain MP3 players. Consumers will be able to remove the XCP and MediaMax software from their computers, and they will be able to resell their CDs without affecting the license to the digital content.

d. Sony BMG Has Agreed To Institute "Best Practices" For Disclosures, Uninstallers And Security Vulnerabilities Associated With Future DRM Software

36. As a result of the Settlement, Sony BMG has agreed to implement new "best practices" for any future DRM software that it develops or includes on its music CDs. Many of these best practices come in the form of additional, understandable disclosures. For example, the jewel cases for Sony BMG CDs will include a disclosure in plain English that the CD contains DRM software and a description of that software. Similarly, the EULAs for Sony BMG's future DRM software will accurately describe the nature and function of the software in plain English. These best practices should provide consumers with sufficient information in plain English before and during the software installation process to allow them to make an informed decision when they consider accepting Sony BMG's terms and the impact of the DRM software on their computer systems.

37. In addition to these enhanced disclosures, Sony BMG's future DRM software will not be installed on an end-user's computer until he or she affirmatively accepts the EULA. Sony BMG has also agreed to make sure that an uninstaller is available to consumers. Sony BMG has agreed to allow future DRM software to be independently tested for effectiveness and security concerns. Finally, Sony BMG will fix security vulnerabilities discovered in future DRM software or updates to that software. These concessions by Sony BMG are crucial to ensure the security and reliability of consumers' computers from aggressive DRM tactics.

Conclusion

38. In my opinion, the terms of the Settlement address all of the concerns raised by Sony BMG's DRM software and the litigation. Although I understand that approval of the Settlement is a matter for the Court to decide, I have no reservations about giving my support to the Settlement. I believe that the Settlement is the best-case outcome for affected consumers.

39. I believe that this Settlement also will deter other companies from placing rootkits on any legitimate software that they release.

I declare under penalty of perjury and the laws of the United States of America that the foregoing is true and correct.

Mark Russinovich

STATE OF TEXAS)
:ss:
COUNTY OF TRAVIS)

Subscribed and sworn to me this 5 day of April 2006.

Notary Public

L. MICHELLE MILLER
MY COMMISSION EXPIRES
January 11, 2010

EXHIBIT A

Mark E. Russinovich
8622 Navidad DR
Austin, TX 78735
512-695-4076
mark@sysinternals.com

EDUCATION

Ph.D. Computer Engineering, August 1994
Carnegie Mellon University, Pittsburgh, Pennsylvania

M.S. Computer and Systems Engineering, August 1990
Rennselaer Polytechnic Institute, Troy, New York

B.S. Computer Engineering, May 1989
Carnegie Mellon University, Pittsburgh, Pennsylvania

EXPERTISE

Windows internals (all Windows platforms), Linux internals, Windows device driver programming, Windows application programming.

EXPERIENCE

1996	**Co-Founder, Winternals Software (http://www.winternals.com)** Founded software company that specializes in developing advanced systems tools for Windows. Company currently has 75 employees.
1996	**Co-Founder, Sysinternals.com** Founded Sysinternals.com, a web site where I publish system troubleshooting, security, and diagnostic software. The site receives approximately 50,000 unique visitors per day.
Sept. 1997- March 2000	**Research Staff Member, IBM T. J. Watson Research Center** Participated in operating systems extensibility projects and co-developed kernel web server caching technology used in several IBM products.
Sept. 1996- Sept. 1997	**Consulting Associate, OSR Open Systems Resources, Inc.** Developed highly-specialized Windows device drivers and file system filter drivers and taught seminars on Windows device and file system driver development.
Feb. 1996- Sept. 1996	**Developer, NuMega Technologies** Worked on performance monitoring software for Windows NT. Evaluated error detection capabilities of Bounds Checker versus other error detection products. Wrote portions of the SoftICE 2.0 and 3.0 documentation sets, and developed loader utility shipped with SoftICE 3.0 Windows debugger.
Sept. 1994- Feb. 1996	**Research Associate, Department of Computer Science, University of Oregon** Responsibilities included working on government-sponsored research into fault-tolerance for off-the-shelf-applications, hardware and software, as well as development of programming environments with integrated performance visualization.

PUBLICATIONS

Windows Internals, 4th Edition, Mark Russinovich and David Solomon, Microsoft Press, 2004
Inside Windows 2000, 3rd Edition, David Solmon and Mark Russinovich, Microsoft Press, 2000
Senior Contributing Editor, Windows IT Pro Magazine
Have spoken dozens of Windows IT and developer conferences
Regular speaker at Microsoft IT Forum, Microsoft TechEd and Windows Connections.

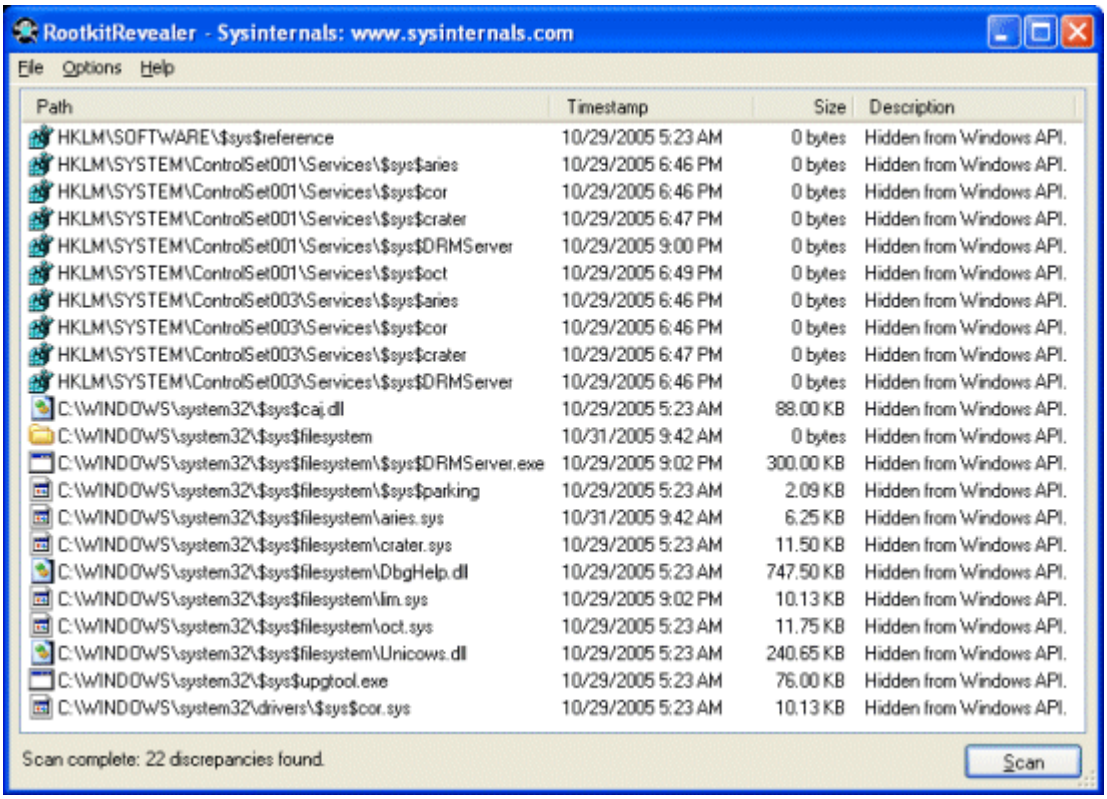
EXHIBIT B

MARK'S SYSINTERNALS BLOG

Monday, October 31, 2005

Sony, Rootkits and Digital Rights Management Gone Too Far

Last week when I was testing the latest version of RootkitRevealer (RKR) I ran a scan on one of my systems and was shocked to see evidence of a rootkit. Rootkits are cloaking technologies that hide files, Registry keys, and other system objects from diagnostic and security software, and they are usually employed by malware attempting to keep their implementation hidden (see my "Unearthing Rootkits" article from thre June issue of Windows IT Pro Magazine for more information on rootkits). The RKR results window reported a hidden directory, several hidden device drivers, and a hidden application:

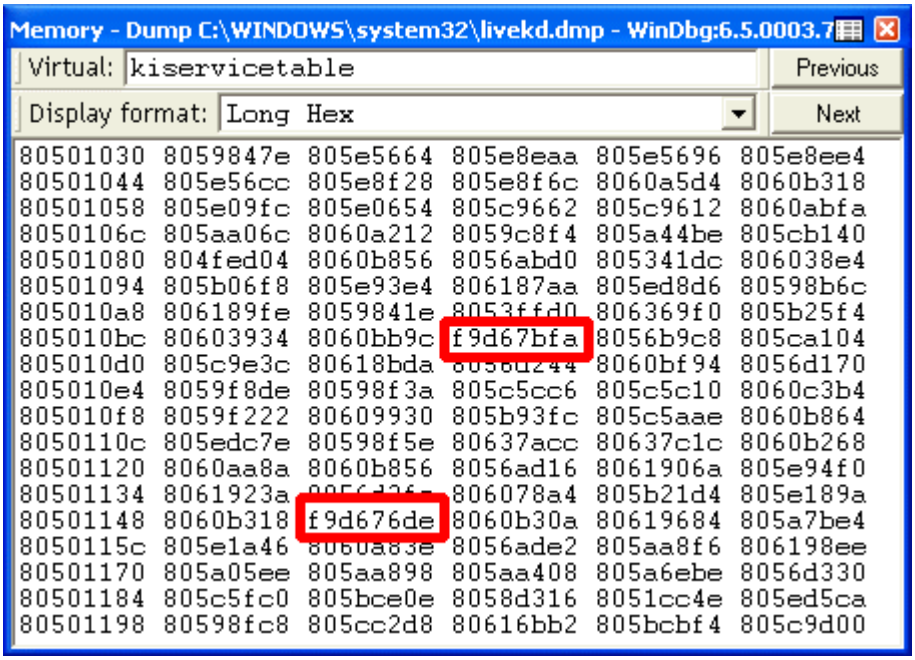


Given the fact that I'm careful in my surfing habits and only install software from reputable sources I had no idea how I'd picked up a real rootkit, and if it were not for the suspicious names of the listed files I would have suspected RKR to have a bug. I immediately ran Process Explorer and Autoruns to look for evidence of code that would activate the rootkit each boot, but I came up empty with both tools. I next turned to LiveKd, a tool I wrote for Inside Windows 2000 and that lets you explore the internals of a live system using the Microsoft kernel debugger, to determine what component was responsible for the cloaking.

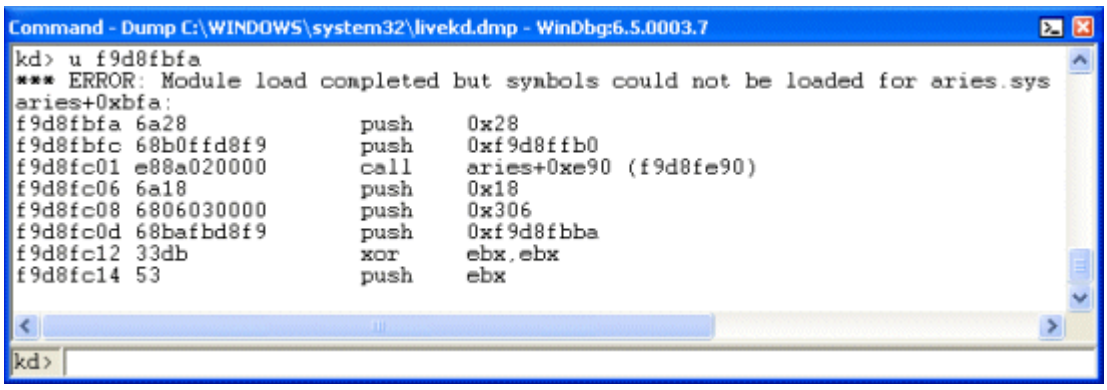
Rootkits that hide files, directories and Registry keys can either execute in user mode by patching Windows APIs in each process that applications use to access those objects, or in kernel mode by intercepting the associated kernel-mode APIs. A common way to intercept kernel-mode application APIs is to patch the kernel's system service table, a technique that I pioneered with Bryce for Windows back in 1996 when we wrote the first version of Regmon. Every kernel service that's exported for use by Windows applications has a pointer in a table that's indexed with the internal service number Windows assigns to the API. If a driver replaces an entry in the table with a pointer to its own function then the kernel invokes the driver function any time an application executes the API and the driver can

control the behavior of the API.

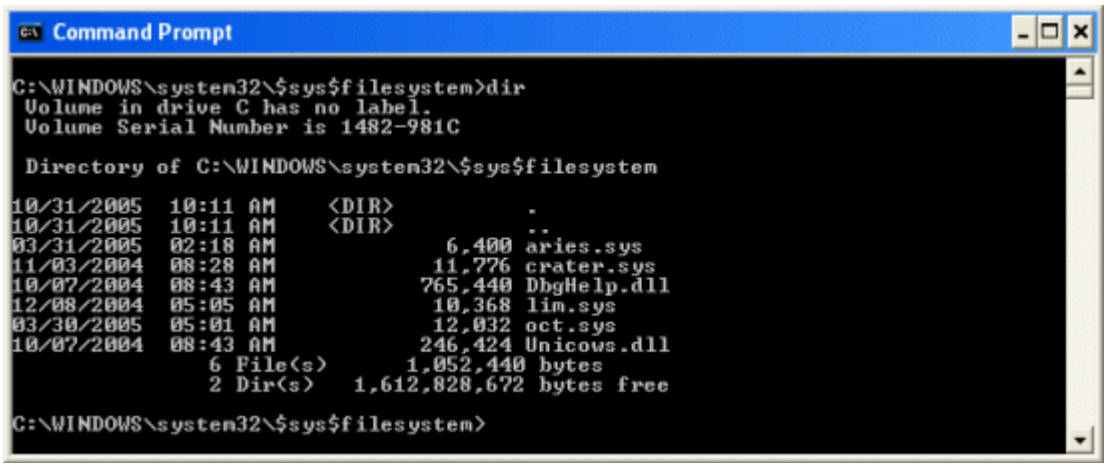
It's relatively easy to spot system call hooking simply by dumping the contents of the service table: all entries should point at addresses that lie within the Windows kernel; any that don't are patched functions. Dumping the table in Livekd revealed several patched functions:



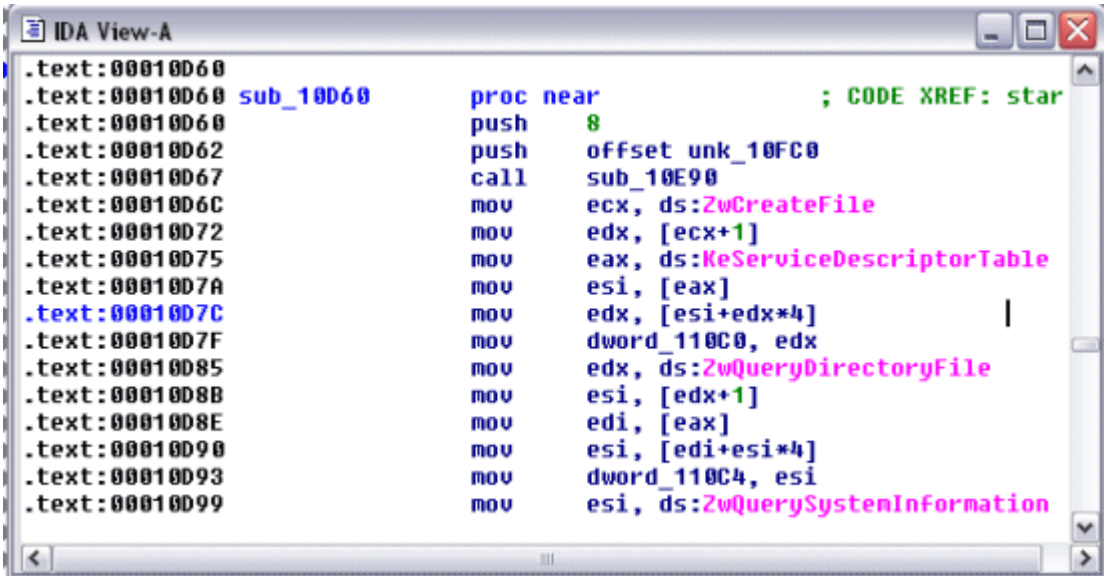
I listed one of the intercepting functions and saw that it was part of the Aries.sys device driver, which was one of the images I had seen cloaked in the sysfilesystem directory:



Armed with the knowledge of what driver implemented the cloaking I set off to see if I could disable the cloak and expose the hidden processes, files, directories, and Registry data. Although RKR indicated that the \Windows\System32\$sys$filesystem directory was hidden from the Windows API, it's common for rootkits to hide directories from a directory listing, but not to prevent a hidden directory from being opened directly. I therefore checked to see if I could examine the files within the hidden directory by opening a command prompt and changing into the hidden directory. Sure enough, I was able to enter and access most of the hidden files:



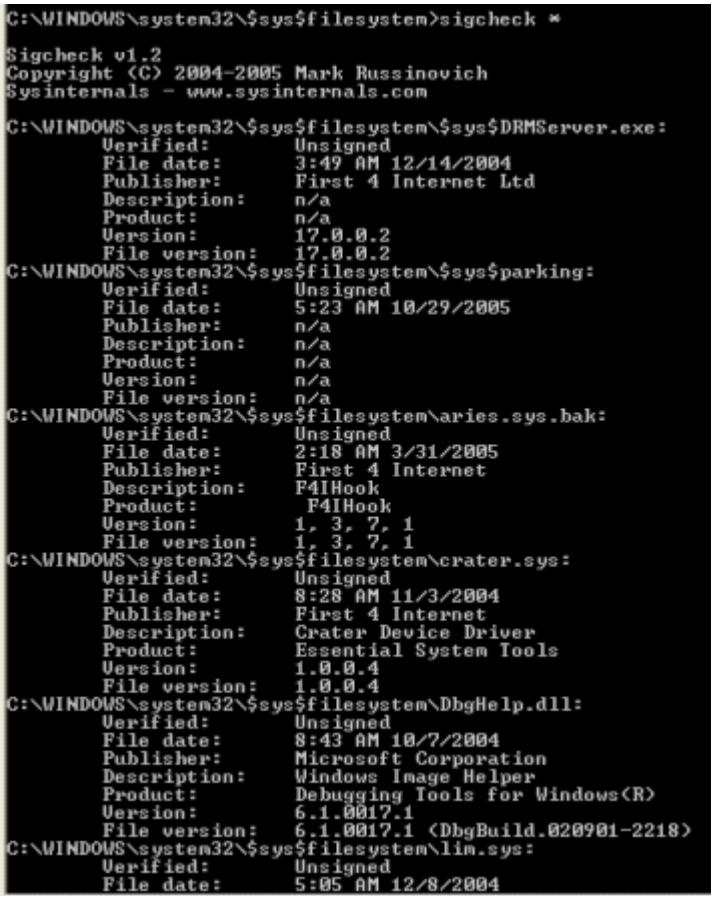
Perhaps renaming the driver and rebooting would remove the cloak, but I also wanted to see if Aries.sys was doing more than cloaking so I copied it to an uncloaked directory and loaded it into IDA Pro, a powerful disassembler I use in my exploration of Windows internals. Here's a screenshot of IDA Pro's disassembly of the code that calculates the entries in the system service table that correspond to the functions it wants to manipulate:



I studied the driver's initialization function, confirmed that it patches several functions via the system call table and saw that its cloaking code hides any file, directory, Registry key or process whose name begins with "sys". To verify that I made a copy of Notepad.exe named sysnotepad.exe and it disappeared from view. Besides being indiscriminate about the objects it cloaks, other parts of the Aries code show a lack of sophistication on the part of the programmer. It's never safe to unload a driver that patches the system call table since some thread might be just about to execute the first instruction of a hooked function when the driver unloads; if that happens the thread will jump into invalid memory. There's no way for a driver to protect against this occurrence, but the Aries driver supports unloading and tries to keep track of whether any threads are executing its code. The programmer failed to consider the race condition I've described. They'll have to come up with a new approach to their rootkit sooner or later anyway, since system call hooking does not work at all on x64 64-bit versions of Windows.

After I finished studying the driver's code I rebooted the system. The cloak was gone as I expected and I could see all the previously hidden files in Explorer and Registry keys in Regedit. I doubted that

the files had any version information, but ran my Sigcheck utility on them anyway. To my surprise, the majority did have identifying product, file and company strings. I had already recognized Dbghelp.dll and Unicows.dll as Microsoft Windows DLLs by their names. The other files claimed to be part of the "Essential System Tools" product from a company called "First 4 Internet":



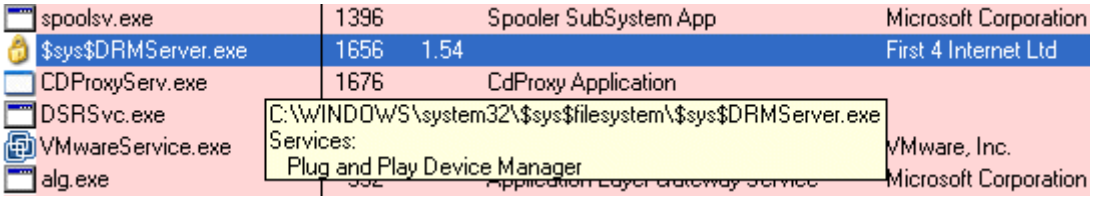
I entered the company name into my Internet browser's address bar and went to http://www.first4internet.com/. I searched for both the product name and Aries.sys, but came up empty. However, the fact that the company sells a technology called XCP made me think that maybe the files I'd found were part of some content protection scheme. I Googled the company name and came across this article, confirming the fact that they have deals with several record companies, including Sony, to implement Digital Rights Management (DRM) software for CDs.

The DRM reference made me recall having purchased a CD recently that can only be played using the media player that ships on the CD itself and that limits you to at most 3 copies. I scrounged through my CD's and found it, Sony BMG's *Get Right with the Man* (the name is ironic under the circumstances) CD by the Van Zant brothers. I hadn't noticed when I purchased the CD from Amazon.com that it's protected with DRM software, but if I had looked more closely at the text on the Amazon.com web page I would have known:

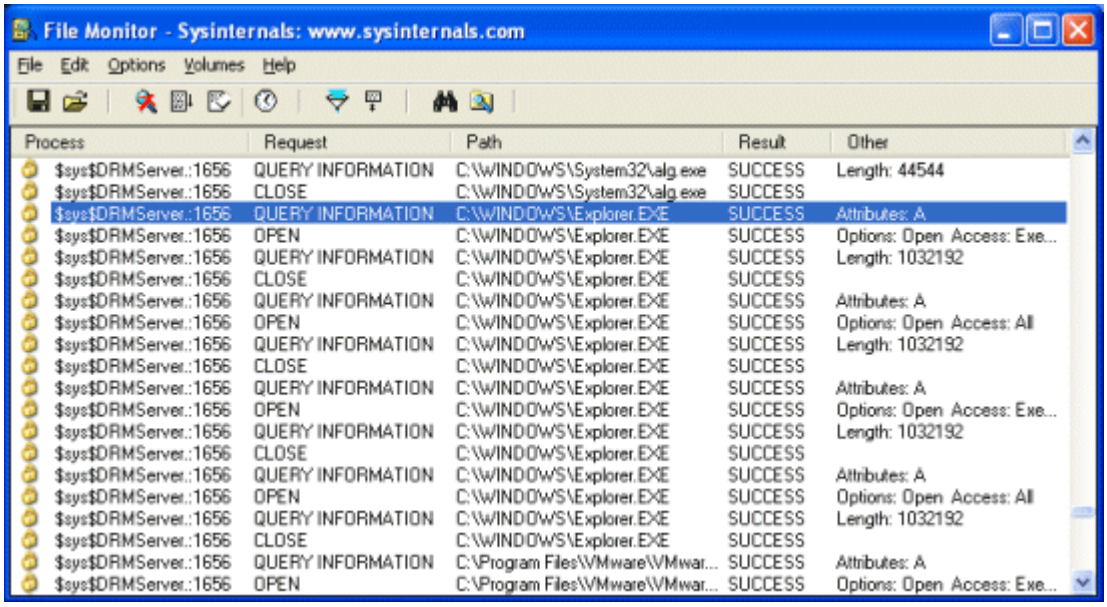
The next phase of my investigation would be to verify that the rootkit and its hidden files were related to that CD's copy protection, so I inserted the CD into the drive and double-clicked on the icon to launch the player software, which has icons for making up to three copy-protected backup CDs:

Process Explorer showed the player as being from Macromedia, but I noticed an increase in CPU usage by sysDRMServer.exe, one of the previously cloaked images, when I pressed the play

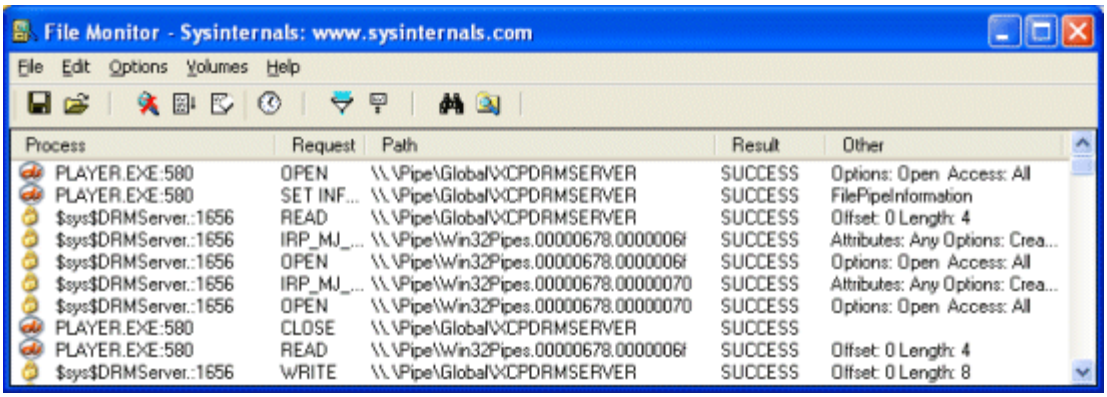
button. A look at the Services tab of its process properties dialog showed it contains a service named “Plug and Play Device Manager”, which is obviously an attempt to mislead the casual user that stumbles across it in the Services MMC snapin (services.msc) into thinking that it’s a core part of Windows:



I closed the player and expected sysDRMServer’s CPU usage to drop to zero, but was dismayed to see that it was still consuming between one and two percent. It appears I was paying an unknown CPU penalty for just having the process active on my system. I launched Filemon and Regmon to see what it might be doing and the Filemon trace showed that it scans the executables corresponding to the running processes on the system every two seconds, querying basic information about the files, including their size, *eight* times each scan. I was quickly losing respect for the developers of the software:



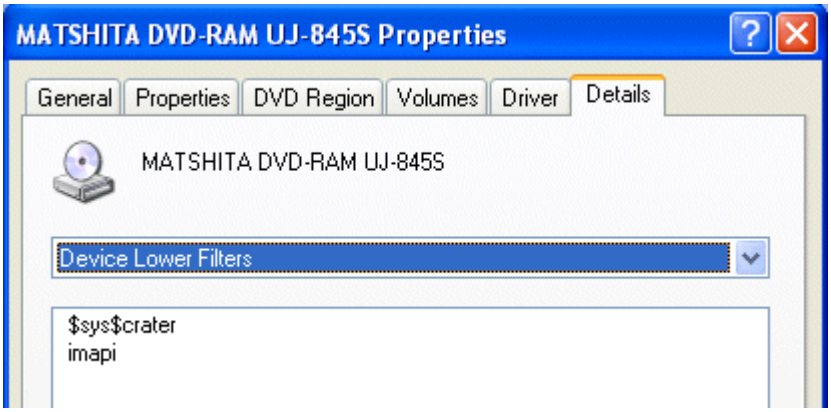
I still had to confirm the connection between the process and the CD’s player so I took a closer look at each process. Based on the named pipe handles I saw they each had opened when I looked in Process Explorer’s handle view I suspected that the player and sysDRMServer communicated via named pipes and so I launched Filemon, checked Named Pipes in the Volumes menu, and confirmed my theory:



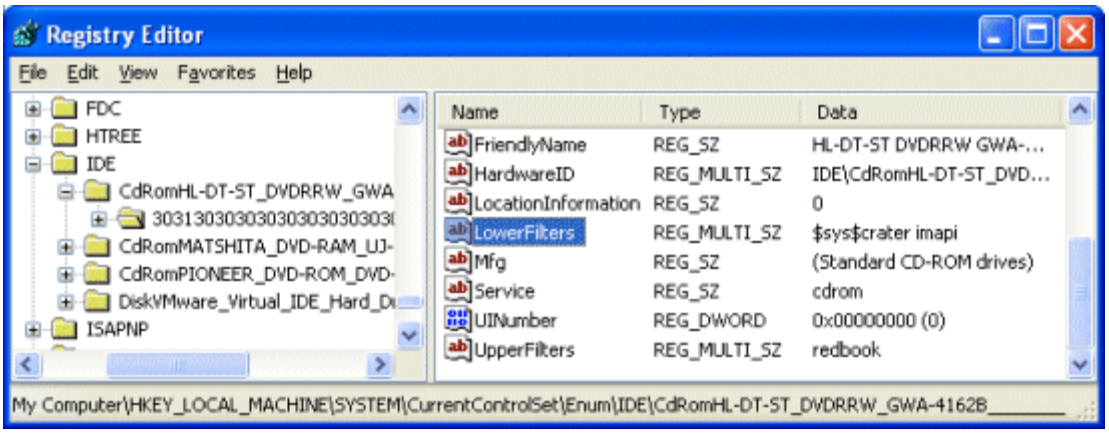
At that point I knew conclusively that the rootkit and its associated files were related to the First 4 Internet DRM software Sony ships on its CDs. Not happy having underhanded and sloppily written software on my system I looked for a way to uninstall it. However, I didn't find any reference to it in the Control Panel's Add or Remove Programs list, nor did I find any uninstall utility or directions on the CD or on First 4 Internet's site. I checked the EULA and saw no mention of the fact that I was agreeing to have software put on my system that I couldn't uninstall. Now I was mad.

I deleted the driver files and their Registry keys, stopped the sysDRMServer service and deleted its image, and rebooted. As I was deleting the driver Registry keys under HKLM\System\CurrentControlSet\Services I noted that they were either configured as boot-start drivers or members of groups listed by name in the HKLM\System\CurrentControlSet\Control\SafeBoot subkeys, which means that they load even in Safe Mode, making system recovery extremely difficult if any of them have a bug that prevents the system from booting.

When I logged in again I discovered that the CD drive was missing from Explorer. Deleting the drivers had disabled the CD. Now I was really mad. Windows supports device "filtering", which allows a driver to insert itself below or above another one so that it can see and modify the I/O requests targeted at the one it wants to filter. I know from my past work with device driver filter drivers that if you delete a filter driver's image, Windows fails to start the target driver. I opened Device Manager, displayed the properties for my CD-ROM device, and saw one of the cloaked drivers, Crater.sys (another ironic name, since it had 'cratered' my CD), registered as a lower filter:



Unfortunately, although you can view the names of registered filter drivers in the "Upper filters" and "Lower filters" entries of a device's Details tab in Device Manager, there's no administrative interface for deleting filters. Filter registrations are stored in the Registry under HKLM\System\CurrentControlSet\Enum so I opened Regedit and searched for sys in that key. I found the entry configuring the CD's lower filter:



I deleted the entry, but got an access-denied error. Those keys have security permissions that only allow the Local System account to modify them, so I relaunched Regedit in the Local System account using PsExec: psexec –s –i –d regedit.exe. I retried the delete, succeeded, and searched for sys again. Next I found an entry configuring another one of the drivers, Cor.sys (internally named Corvus), as an upper filter for the IDE channel device and also deleted it. I rebooted and my CD was back.

The entire experience was frustrating and irritating. Not only had Sony put software on my system that uses techniques commonly used by malware to mask its presence, the software is poorly written and provides no means for uninstall. Worse, most users that stumble across the cloaked files with a RKR scan will cripple their computer if they attempt the obvious step of deleting the cloaked files.

While I believe in the media industry's right to use copy protection mechanisms to prevent illegal copying, I don't think that we've found the right balance of fair use and copy protection, yet. This is a clear case of Sony taking DRM too far.

For an update on the story, read More on Sony: Dangerous Decloaking Patch, EULAs and Phoning Home.

posted by Mark Russinovich @ 11:04 AM (705) comments

EXHIBIT C

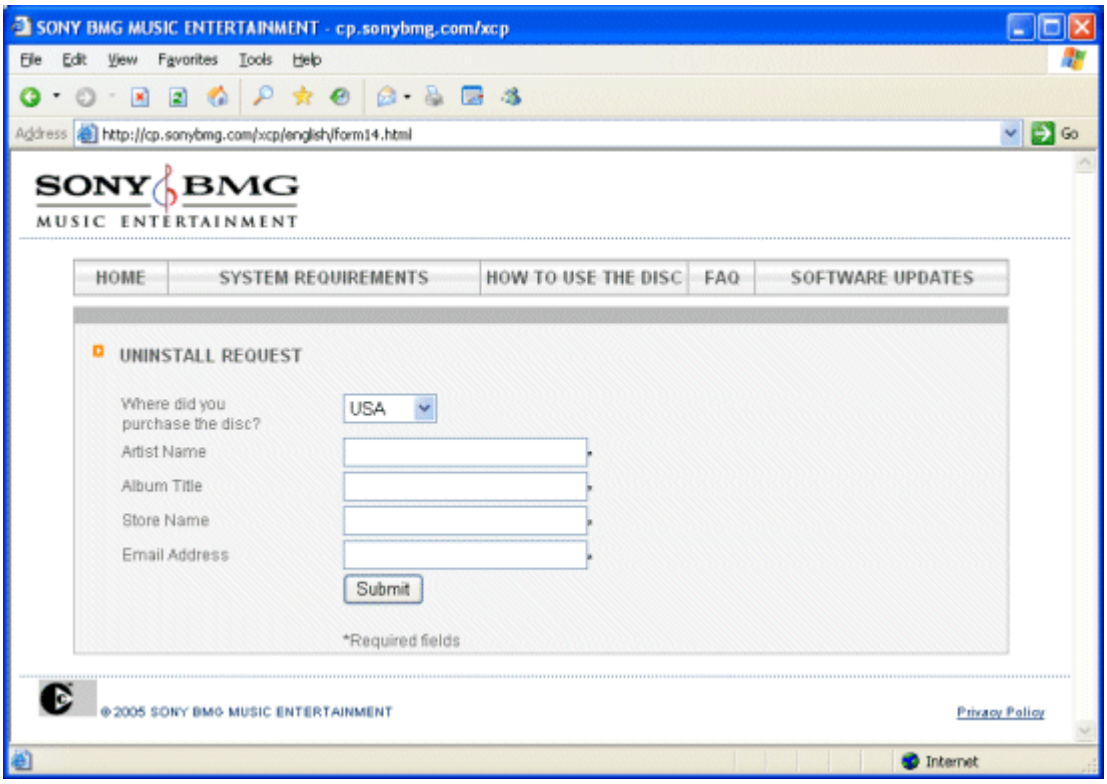
Friday, November 04, 2005

More on Sony: Dangerous Decloaking Patch, EULAs and Phoning Home

My posting Monday on Sony's use of a rootkit as part of their Digital Rights Management (DRM) generated an outcry that's reached the mainstream media. As of this morning the story is being covered in newspapers and media sites around the world including USA Today and the BBC. This is the case of the blogosphere having an impact, at least for the moment. But, there's more to the story, like how Sony's patch can lead to a crashed system and data loss and how Sony is still making users jump through hoops to get an uninstaller. At the core of this story, however, is the issue of what disclosure should be required of software End User License Agreements (EULAs) and how the requirements can be made Federal law.

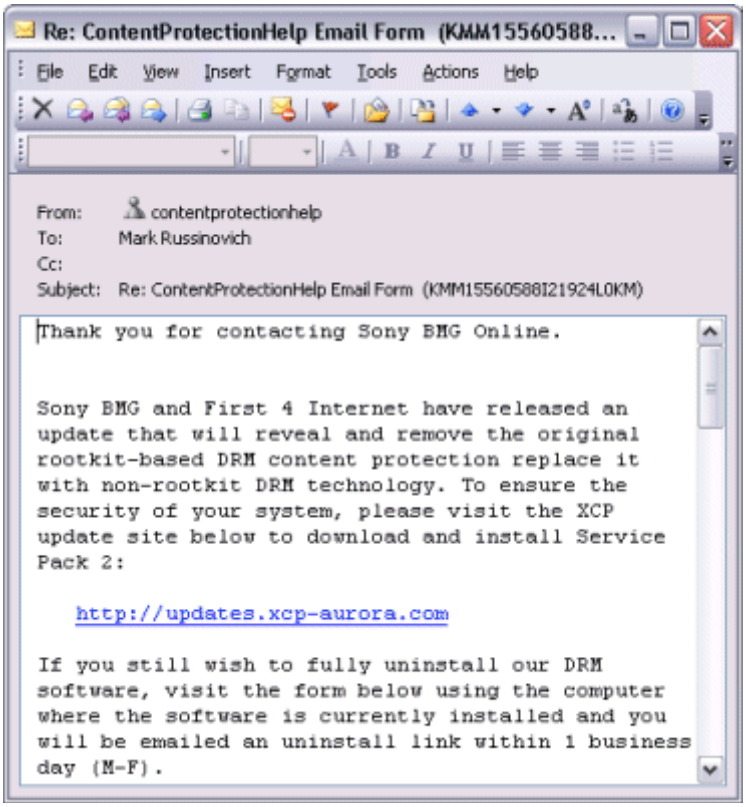
The Uninstaller

Despite a chorus of criticism over Sony not delivering an uninstaller with their DRM software, Sony refuses to admit blame and to make an uninstaller readily available. The uninstall question on Sony's FAQ page directs you to another page that asks you to fill out a form requesting for uninstall directions to be emailed to you:



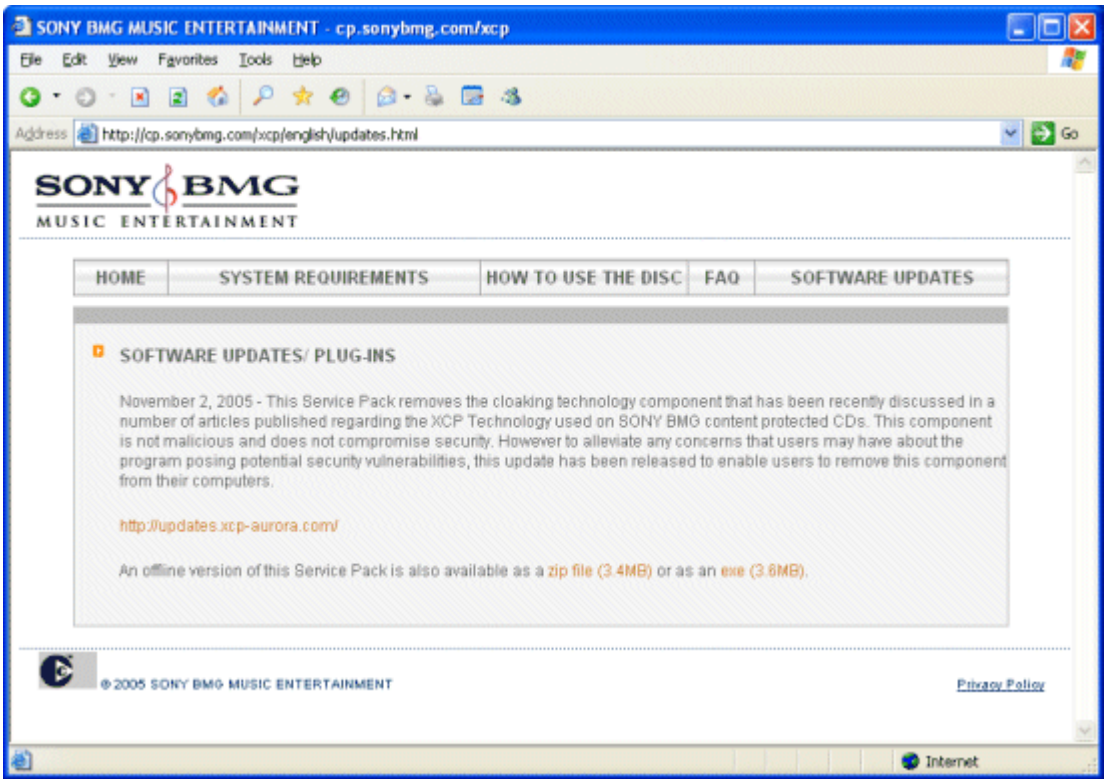
There's no way to access the uninstaller without providing this information, and clicking on the Sony privacy policy link at the bottom of the page takes you to a notice that your email address can be added to various Sony marketing lists.

A few minutes after submitting the form I received an email assigning me a case ID and directing me to another page on Sony's site where I would have to submit an uninstall request a second time:



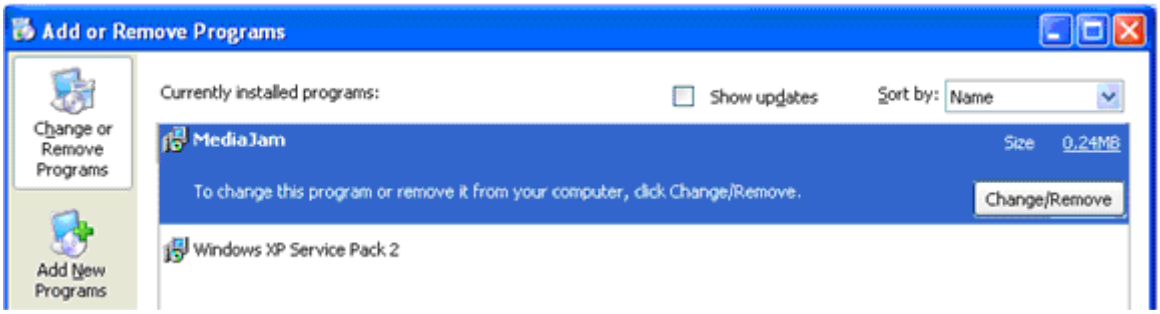
I've filled out the second form and am waiting for the follow-up email.

The Patch
You can the get to the patch supplied in the above email from the same Sony support site under Software Updates:



The download text claims that the rootkit does not pose any “potential security vulnerabilities,” however it’s obvious that any software that cloaks files, directories and Registry keys beginning with a certain string of characters is a clear security risk. An innovating exploit of the rootkit utilizes it to compromise the World of Warcraft anti-cheat system.

The download of what should be a small patch is around 3.5 MB because it includes updated drivers and executables for the DRM software that the patch also installs (again, no mention of this is made in the download description). Interestingly, after installing the patch a new entry showed up in the Windows Add and Remove Programs utility, but it’s only because I checked immediately after I ran the patch that I knew it was related to Sony:



Nowhere up to now have I seen the Sony Player or DRM software referred to as “MediaJam”. I looked in the Program Files directory and the only file in the new MediaJam subdirectory was Unicows.dll, a Microsoft DLL:

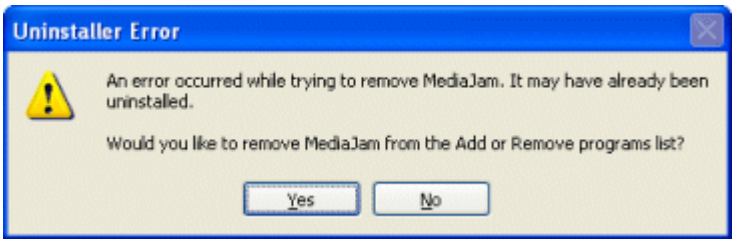
```
C:\Program Files\MediaJam>dir
 Volume in drive C has no label.
 Volume Serial Number is 1482-981C

 Directory of C:\Program Files\MediaJam

11/04/2005  10:22 AM    <DIR>          .
11/04/2005  10:22 AM    <DIR>          ..
10/07/2004  08:43 AM           246,424 Unicows.dll
               1 File(s)        246,424 bytes
               2 Dir(s)   1,357,377,536 bytes free

C:\Program Files\MediaJam>_
```

Assuming that uninstalling MediaJam would uninstall the DRM software, I attempted to do so but was greeted with this dialog:

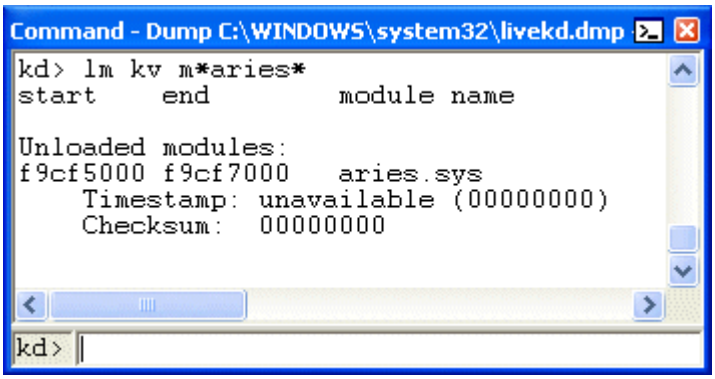


It looks like their rush to get the patch out precluded any kind of testing.

The actual decloaking, which is the only value the patch advertises, simply performs the equivalent of the following Windows command:

net stop “network control manager”

“Network Control Manager” is the misleading name the developers assigned to the Aries driver so the command directs the Windows I/O system to unload the driver from memory. After the patch had completed I dumped the system call table in LiveKd and noted that the redirected entries had returned to their standard values and that the driver had unloaded from memory:



However, Sony’s uncloaking patch puts users systems at risk of a blue-screen crash and the associated chance of data loss. The risk is small, but I made the point in my last post that the type of cloaking performed by the Aries driver prohibits safely unloading the driver while Windows is running:

It’s never safe to unload a driver that patches the system call table since some thread might be just about to execute the first instruction of a hooked function when the driver unloads; if that happens the thread will jump into invalid memory. There’s no way for a driver to protect against this occurrence, but the Aries driver supports unloading and tries to keep track of whether any threads are executing its code. The programmer failed to consider the race condition I’ve described.

If the developers had heeded this warning the decloaker would have required the system to reboot so that the Aries driver could remain active through the shutdown, but then not load on the next reboot.

I urge Sony to make a real uninstaller readily available for download and to make both the de-cloaking and uninstaller unload the driver safely. In the meantime users can perform a safe decloaking by opening the Run dialog from the Start menu, entering “sc delete sysaries”, and then rebooting. This sequence deletes the driver from the Windows Registry so that even though its image is still present on disk, the I/O system will not load it during subsequent boots.

EULAs and Disclosure: Sony’s Player Phones Home

There’s more to the story than rootkits, however, and that’s where I think Sony is missing the point. As I’ve pointed out in press interviews related to the post, the EULA does not disclose the software’s use of cloaking or the fact that it comes with no uninstall facility. An end user is not only installing software when they agree to the EULA, they are losing control of part of the computer, which has both reliability and security implications. There's no way to ensure that you have up-to-date security patches for software you don't know you have and there's no way to remove, update or even identify hidden software that's crashing your computer.

The EULA also makes no reference to any “phone home” behavior, and Sony executives are claiming that the software never contacts Sony and that no information is communicated that could track user behavior. However, a user asserted in a comment on the previous post that they monitored the Sony CD Player network interactions and that it establishes a connection with Sony’s site and sends the site an ID associated with the CD.

I decided to investigate so I downloaded a free network tracing tool, Ethereal, to a computer on which the player was installed and captured network traffic during the Player’s startup. A quick look through the trace log confirmed the users comment: the Player does send an ID to a Sony web site. This screenshot shows the command that the Player sends, which is a request to an address registered to Sony for information related to ID 668, which is presumably the CD's ID:

```
⊟ Hypertext Transfer Protocol
  ⊞ GET /toc/Connect?type=redirect&uId=668 HTTP/1.1\r\n
    Accept: application/*, audio/*, image/*, message/*,
    User-Agent: SecureNet Xtra\r\n
    Host: connected.sonymusic.com\r\n
    Connection: Keep-Alive\r\n
    Cache-Control: no-cache\r\n
    \r\n
```

In response the Sony web site reports the last time a particular file was updated:

```
⊟ Hypertext Transfer Protocol
  ⊞ HTTP/1.1 200 OK\r\n
    Date: Fri, 04 Nov 2005 15:50:38 GMT\r\n
    Server: Apache/1.3.27 (Unix)\r\n
    Last-Modified: Wed, 23 Feb 2005 17:17:04 GMT\r\n
    ETag: "6d58a-10-421cba90"\r\n
    Accept-Ranges: bytes\r\n
    Content-Length: 16\r\n
    Keep-Alive: timeout=1, max=100\r\n
    Connection: Keep-Alive\r\n
    Content-Type: text/xml\r\n
    \r\n
```

I dug a little deeper and it appears the Player is automatically checking to see if there are updates for the album art and lyrics for the album it’s displaying. This behavior would be welcome under most circumstances, but is not mentioned in the EULA, is refuted by Sony, and is not configurable in any

way. I doubt Sony is doing anything with the data, but with this type of connection their servers could record each time a copy-protected CD is played and the IP address of the computer playing it.

The media has done a great job of publicizing this story, which has implications that extend beyond DRM to software EULAs and disclosure, and I hope that the awareness they're creating will result in Congressional action. Both the software industry and consumers need laws that will clearly draw lines around acceptable behaviors.

The story continues with Sony's Rootkit: First 4 Internet Responds.

posted by Mark Russinovich @ 12:04 PM (204) comments

EXHIBIT D

Sunday, November 06, 2005

Sony's Rootkit: First 4 Internet Responds

First 4 Internet, the company that implements Sony's Digital Rights Management (DRM) software that includes a rootkit, has responded to my last post, More on Sony: Dangerous Decloaking Patch, EULAs and Phoning Home. They rebut four of the points I raise in the post. Their first statement relates to my assertion that Sony's player contacts Sony's web site each time it runs and sends the site an ID associated with the CD the user is playing:

The player has a standard rotating banner that connects the user to additional content (e.g. provides a link to the artist web site). The player simply looks online to see if another banner is available for rotation. The communication is one-way in that a banner is simply retrieved from the server if available. No information is ever fed back or collected about the consumer or their activities.

I speculated that the player sends Sony's web site a CD identifier as part of a check to see if new song lyrics or artwork was available, which they essentially confirm. Their claim that the communication is "one way" from Sony's web site is false, however, since Sony can make a record of each time their player is used to play a CD, which CD is played, and what computer is playing the CD. If they've configured standard Web server logging then they are doing that. As I stated earlier, I doubt Sony is using this information to track user behavior, but the information allows them to do so. In any case, First 4 Internet cannot claim what Sony is or is not doing with the information since they do not control those servers, and the First 4 Internet response fails to address the fact that the End User License Agreement (EULA) and Sony executives either make no mention of the "phone home" behavior or explicitly deny it.

Another point that I made in the post is that the decloaking patch that Sony has made available weighs in at a relatively large 3.5 MB because it not only removes the rootkit, it also replaces most of the DRM files with updated versions. First 4 Internet responded with this:

In addition to removing the cloaking, Service Pack 2 includes all fixes from the earlier Service Pack 1 update. In order to ensure a secure installation, Service Pack 2 includes the newest version of all DRM components, hence the large file size for the patch. We have updated the language on our web site to be clearer on this point.

It's not clear to me what they mean by "a secure installation", but like most of the disclosure in this story, they've acknowledged the updating nature of the patch only after someone else has disclosed it first. What's also lost in their response is that Sony DRM users not following this story as it develops have no way of knowing that there's a patch available or that they even have software installed that requires a patch.

Further, Sony's patch is dangerous because the way that it removes the cloak could crash Windows. I discussed the flaw in the patch's decloaking method in the first post and again in the last one (I also provide a simple way for users to remove the cloak safely), yet First 4 Internet refuses to recognize it. They contest my claim in their comment:

This is pure conjecture. F4I is using standard Windows commands (net stop) to stop their driver. Nothing more.

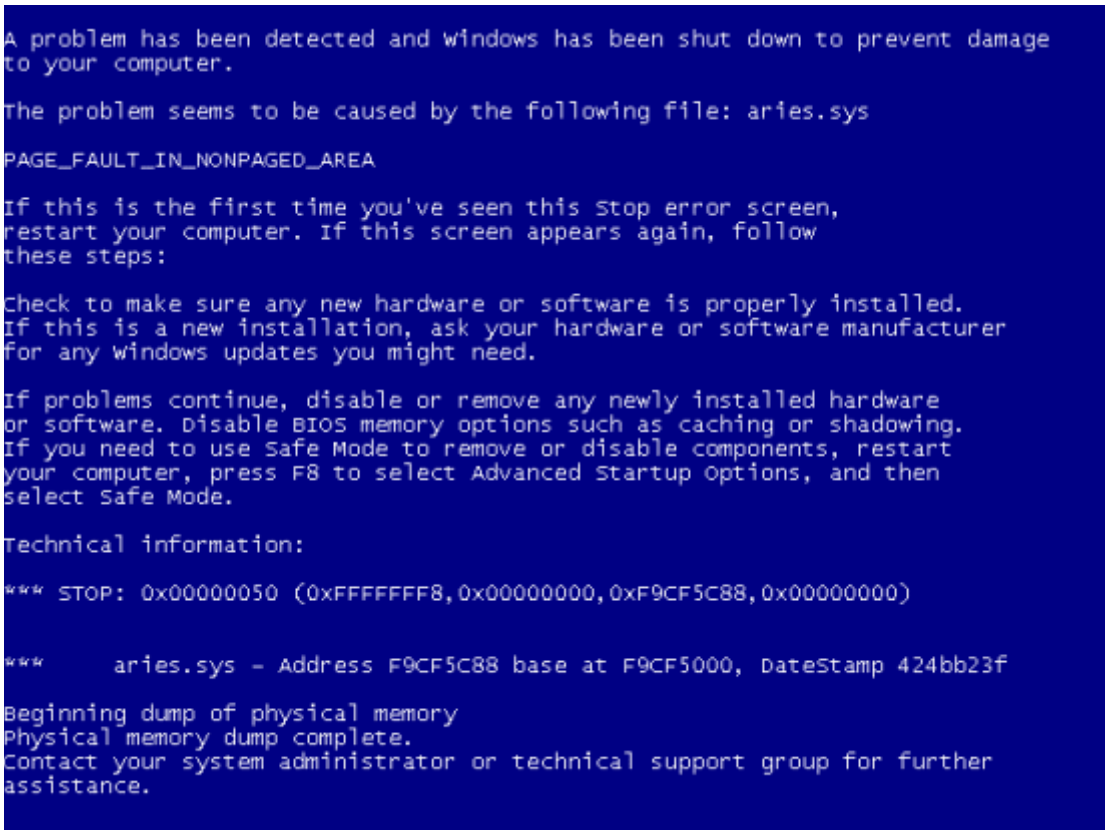
While the probability of a crash is relatively small, its not "pure conjecture", but fundamental to multithreaded programming concepts. Anyone that writes Windows device driver code must have a firm grasp of these concepts or they can easily introduce bugs and security holes into Windows. Here's one of many scenarios that will lead to a crash when the patch decloaks Sony's rootkit:

1. Thread A invokes one of the functions that Aries.sys, the Sony rootkit driver developed by First 4 Internet, has redirected
2. Thread A reads the address of the redirected function from the system service table, which points at the rootkit function in Aries.sys

3. Thread A executes the first few instructions of the Aries.sys function, which is enough to enter the driver, but not enough to execute the Aries.sys code that attempts to track threads running within it
4. Thread A is context swapped off the CPU by the Windows scheduler
5. The scheduler gives thread B the CPU, which executes the patch's "unload driver" command, unloading the Aries.sys driver from memory
6. The scheduler runs thread A again, which executes memory that previously held the contents of Aries.sys, but is now invalid or holds other code or data
7. Windows detects thread A's illegal execution and crashes the system with a blue screen

First 4 Internet's failure to imagine this control flow is consistent with their general failure to understand Windows device driver programming.

As further evidence of this, I've performed further testing of the Aries.sys driver using a program I wrote, NTCrash2, and found that Aries.sys fails to perform basic checks on the data passed to it by applications. NTCrash2 passes randomly-generated invalid data to Windows APIs and on a stock Windows system simply receives error codes from the APIs. However, when NTCrash2 runs on a system that has the Sony rootkit installed Windows crashes. Here's an example Windows blue screen that identifies Aries.sys as the cause of a crash that occurred while NTCrash2 ran:



Besides demonstrating the ineptitude of the First 4 Internet programmers, this flaw highlights my message that rootkits create reliability risks in addition to security risks. Because the software package that installed the rootkit is hidden when Windows is running (in this case Sony's DRM software), and even if exposed not clearly identified, if an application triggers one of Aries.sys's bugs a user would have no way of associating the driver responsible for the resulting crash with any software package they have installed on their system. The user would therefore be unable to conclusively diagnose the cause of the crash, check to see if they have the most recent version of the driver or of uninstalling the driver.

First 4 Internet and Sony also continue to argue that the rootkit poses no security vulnerability, repeating it in the description of the patch download. Any software that hides files, processes, and registry keys based on a prefix of letters can clearly be used by malicious software.

First 4 Internet's final rebuttal relates to my complaint that as part of a request to uninstall their DRM software Sony requires you to submit your email address to their marketing lists. First 4 Internet says:

An email address is required in order to send the consumer the uninstall utility. The wording on the web site is the standard Sony BMG corporate privacy policy that is put on all Sony web sites. Sony BMG does nothing with the customer service data (email addresses) other than use them to respond to the consumer.

The Sony privacy policy the comment refers to clearly states that Sony may add a user's email address to their marketing lists:

Except on sites devoted to particular recording artists, we may share the information we collect from you with our affiliates or send you e-mail promotions and special offers from reputable third parties in whose products and services we think you may have an interest. We may also share your information with reputable third-parties who may contact you directly.

Again, the fact is that most users of Sony's DRM won't realize that they even have software that can be uninstalled. Also, the comment does not explain why Sony won't simply make the uninstaller available as a freely accessible download like they do the patch, nor why users have to submit two requests for the uninstaller and then wait for further instructions to be emailed (I still have not received the uninstaller). The only motivation I can see for this is that Sony hopes you'll give up somewhere in the process and leave their DRM software on your system. I've seen similar strategies used by adware programs that make it difficult, but not impossible, for you to remove them.

Instead of admitting fault for installing a rootkit and installing it without proper disclosure, both Sony and First 4 Internet claim innocence. By not coming clean they are making clear to any potential customers that they are a not only technically incompetent, but also dishonest.

More on the story in Sony: You don't reeeeaaaally want to uninstall, do you?

posted by Mark Russinovich @ 7:29 PM (145) comments

EXHIBIT E

Wednesday, November 09, 2005

Sony: You don't reeeeaaaally want to uninstall, do you?

A few days after I posted my first blog entry on Sony's rootkit, Sony and Rootkits: Digital Rights Management Gone Too Far, Sony announced to the press that it was making available a decloaking patch and uninstall capability through its support site. Note that I said *press* and not *customer*. The uninstall process Sony has put in place is on par with mainstream spyware and adware and is the topic of this blog post.

As I've stated several times already, Sony's rootkit hides the Digital Rights Management (DRM) files from users that have it installed, so users not monitoring the developments in this story are unaware of the scope and intrusiveness of the DRM. The End User License Agreement (EULA) does not provide any details on the software or its cloaking. Further, the software installation does not include support information and lacks a registration option, making it impossible for users to contact Sony and Sony to contact its users.

What if a user somehow discovers the hidden files, makes the connection between files and the Sony CD that installed them, and visits Sony BMG's site in search of uninstall or support information? Or what about the unsuspecting Sony DRM user that happens to visit the Sony BMG site to look at their other offerings? Will these customers learn about the patch and uninstaller?

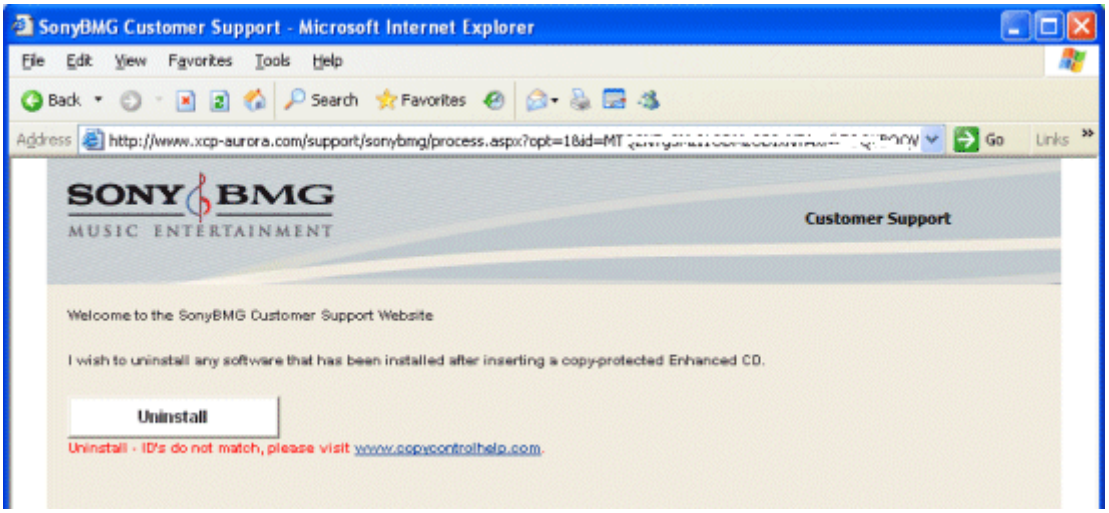
See for yourself. Visit www.sonybmg.com and search for the support site Sony has made available to the press. There's no information on this story anywhere on the front page, no support link, and the FAQ only contains information about Sony's merger with BMG. The fact that Sony's announcement was directed at the press and that they've made no effort to make contact with their customers makes the patch and uninstall look solely like a public relations gesture for the media.

Sony even gives those users like me that are aware of the "uninstaller" several hurdles to jump over. First you have to go to Sony's support site, guess that the uninstall information is in the FAQ, click on the uninstall link and then fill out a form with your email address and purchasing information, possibly adding yourself to Sony's marketing lists in the process.

Then, after you submit the information the site takes you to a page that notifies you that you'll be receiving an email with a "Case ID". A few minutes later you receive that email, which directs you to install the patch and then visit another page if you still *really* want to uninstall. That page requires you to install an ActiveX control, CodeSupport.Ocx, that's signed by First 4 Internet, enter your case ID and fill in the reason for your request. Then you receive an email within a few minutes that informs you that a customer service representative will email you uninstall instructions within one business day.

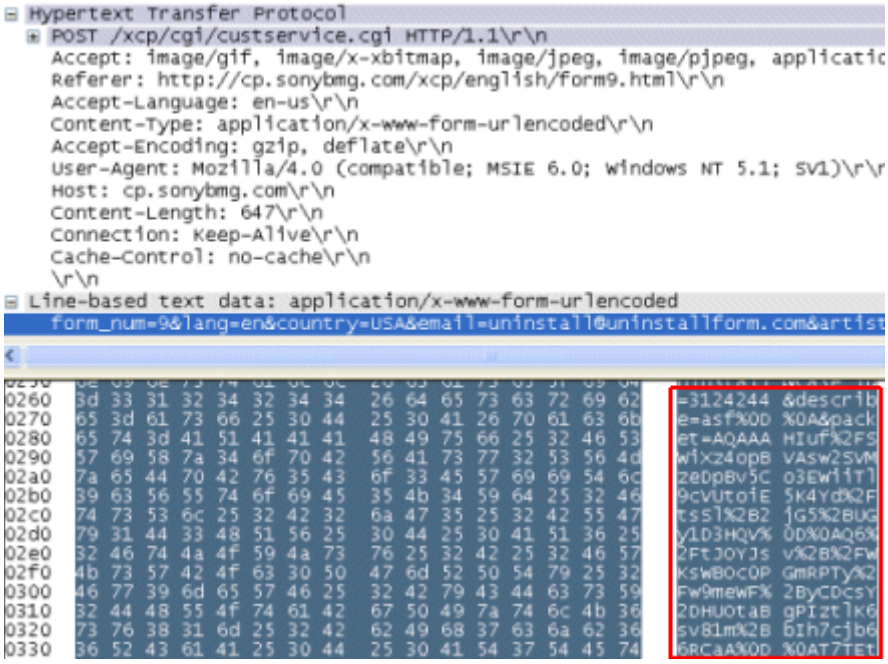
When you eventually receive the uninstall email from Sony BMG support it comes with a cryptic link in the form http://www.xcp-aurora.com/support/sonybmg/process.aspx?opt=1&id=XYAUfasSFoSdasfDoFPPEWFFEoibnaZPQlSfFgKGSGGIAAAAAAAAAAA (I've modified the link so it doesn't work) to your personalized uninstall page. Interestingly, the email address has a confidentially notice, which implies to me that Sony has something to hide, and it informs you that the uninstaller will expire in one week.

If you visit the uninstall page from the computer where you filled out the first uninstall form then the DRM software is deleted from your system. However, if you visit it from another computer the page requires you install the same CodeSupport ActiveX control as the uninstall-request page, but then even if the computer has the DRM software installed you get this error:

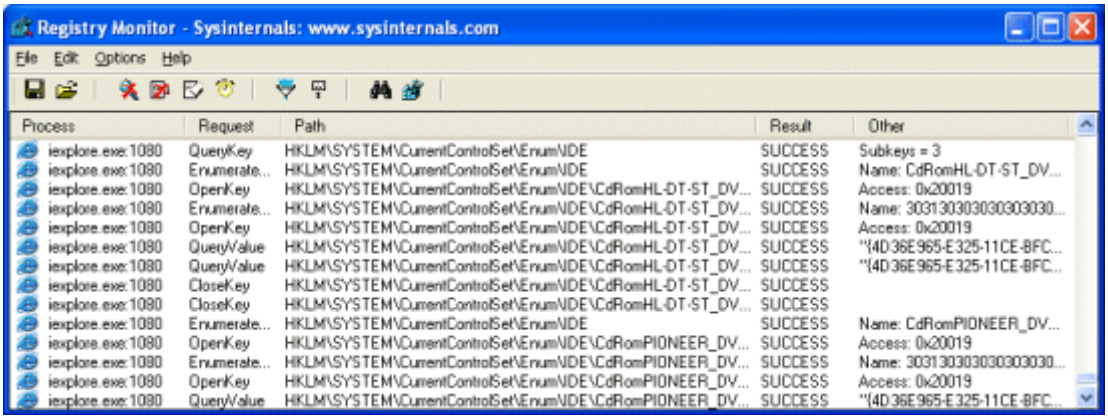


Besides the obvious question of why there's not a universal uninstall link, the error also begs the question of how the Sony site knows that the uninstall link is for a different computer? For that matter, why do you have to install an ActiveX control just to fill out a web form and why does that form have to be filled out "using the computer where the software is currently installed"? The email, web page and ActiveX control offer no hints.

I of course decided to investigate. A network trace of the ActiveX control's communication with the Sony site using Ethereal reveals that the control sends Sony an encrypted block of data:



A Regmon trace of the ActiveX control's activity when you press the submit button on the Web page reveals that the encrypted data is actually a signature that the control derives from the hardware configuration of your computer:



The uninstall link Sony sends you has your case ID encrypted in the address and when you visit the uninstall page the ActiveX control sends the hardware signature to Sony's site. If the signature doesn't match the one it stored earlier with your Case ID when you made the second uninstall request the site informs you that there's a case ID mismatch.

While I've answered the question of how the uninstaller knows if the uninstall link is for your computer, I can't definitively answer questions like:

1. Why isn't Sony publicizing the uninstall link on their site in any way?
2. Why do you have to tell Sony twice that you want to uninstall?
3. Why is the email with the uninstall link labeled confidential?
4. Why does Sony generate a unique uninstall link for each computer?

Sony has left us to speculate, but under the circumstances the answer to all these questions seems obvious: Sony doesn't want customers to know that there's DRM software installed on their computers and doesn't want them to uninstall it if they somehow discover it. *Without exaggeration I can say that I've analyzed virulent forms of spyware/adware that provide more straightforward means of uninstall*.

For those readers that are coming up to speed with the story, here's a summary of important developments so far:

The DRM software Sony has been shipping on many CDs since April is cloaked with rootkit technology:

- Sony denies that the rootkit poses a security or reliability threat despite the obvious risks of both
- Sony claims that users don't care about rootkits because they don't know what a rootkit is
- The installation provides no way to safely uninstall the software
- Without obtaining consent from the user Sony's player informs Sony every time it plays a "protected" CD

Sony has told the press that they've made a decloaking patch and uninstaller available to customers, however this still leaves the following problems:

- There is no way for customers to find the patch from Sony BMG's main web page
- The patch decloaks in an unsafe manner that can crash Windows, despite my warning to the First 4 Internet developers
- Access to the uninstaller is gated by two forms and an ActiveX control
- The uninstaller is locked to a single computer, preventing deployment in a corporation

Consumers and antivirus companies are responding:

- F-Secure independently identified the rootkit and provides information on its site
- Computer Associates has labeled the Sony software "spyware"
- A lawfirm has filed a class action lawsuit on behalf of California consumers against Sony
- ALCEI-EFI, an Italian digital-rights advocacy group, has formally asked the Italian government to investigate Sony for possible Italian law violations

More on the story here.

posted by Mark Russinovich @ 11:31 AM (229) comments

EXHIBIT F

Monday, November 14, 2005

Sony: No More Rootkit - For Now

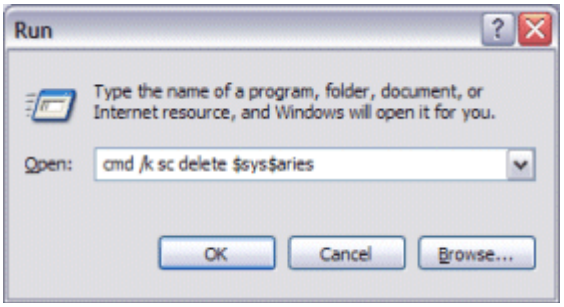
There have been several significant developments in the Sony DRM story since my last post. The first is that, despite Sony's and First 4 Internet's claims that their rootkit poses no security risk, several viruses have been identified in the wild that exploit the cloaking functionality provided by the rootkit. Besides F-Secure and Computer Associates, most antivirus companies were slow to label the Sony rootkit as a risk. But the discovery of viruses that use the rootkit to hide files has caused many to identify and disable the rootkit in their latest scanning signatures. My guess is that they were waiting for an actual security threat to shield them from a potential problem with Sony. For example, Microsoft initially responded cautiously when questioned about its position on Sony's use of rootkits, but Jason Garms, a member of the Microsoft Windows Defender team (formerly Microsoft Antispyware), announced in the Windows Defender blog this weekend that Microsoft is also releasing signatures and a cleaner for the rootkit.

While I'm glad that the viruses have resulted in continuing media coverage of the story, the viruses being discussed in the media are not really the primary security issue. The viruses simply take advantage of the Sony rootkit if it's present, but could just as easily install their own rootkit to hide their presence on the system. If a user activating the virus, which is transmitted as an email attachment, is running with administrator privileges, the virus can install a kernel-mode rootkit just as powerful as Sony's. But even if the virus is activated from a non-administrator account it can install a less powerful, though still effective, user-mode rootkit. The bottom line is that it's not rootkits themselves that are the problem; it's the inability to manage the objects that they hide that creates security, reliability and manageability problems.

I'm not the only one that realizes the dangers of rootkits, especially those bundled with commercial software. On Friday, the US Chamber of Commerce co-sponsored a conference in Washington, D.C. on combating intellectual property theft. The conference concluded with a panel that included major representatives of the entertainment and technology industries such as the chairman and chief executive officer of the Recording Industry Association of America (RIAA) and Stewart Baker, the assistant secretary for policy in the Department of Homeland Security. Baker concluded with a comment aimed squarely at Sony: "It's very important to remember that it's your intellectual property -- it's not your computer. And in the pursuit of protection of intellectual property, it's important not to defeat or undermine the security measures that people need to adopt in these days."

Unfortunately, there has been some confusion with regard to the level of cleaning that antivirus (AV) companies are providing for the rootkit. Some articles imply that AV companies remove all of the Sony DRM software in the cleaning process, but they are in fact only disabling and removing the Aries.sys driver that implements the rootkit cloaking functionality. Unfortunately, all of the AV cleaners I've looked at disable it improperly by unloading it from memory - the same way Sony's patch behaves - which as I noted previously, introduces the risk of a system crash. While they post disclaimers on their web sites to that effect, they should use the safe alternative that I described a couple of posts ago, which is to delete the rootkit's registration from Windows so that it won't activate when Windows boots:

1. Open the Run dialog from the Start menu
2. Enter "cmd /k sc delete sysaries"
3. Reboot



Perhaps the biggest news in the story last week is Sony's first public response since one of their executives stated in a National Public Radio interview, "users don't know what a rootkit is, and therefore, don't care." Mid-day Friday Sony announced, with the hope that press coverage wouldn't last through the weekend, that it would temporarily cease production of CD's containing First 4 Internet's XCP technology, the software that utilizes the rootkit. They have also finally added a link on the Sony BMG web site, under the News section, to the decloaking patch and uninstall link:

SONY BMG STATEMENT

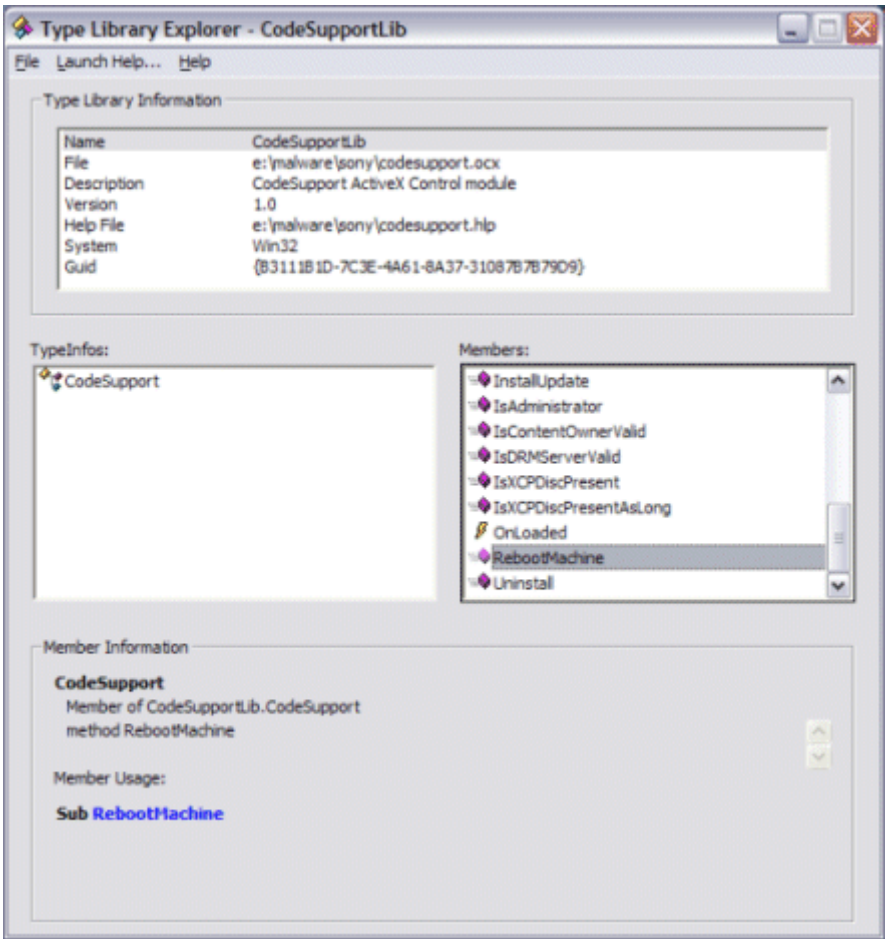
We are aware that a computer virus is circulating that may affect computers with XCP content protection software. The XCP software is included on a limited number of SONY BMG content protected titles. This potential problem has no effect on the use of these discs in conventional, non-computer-based, CD and DVD players.

In response to these events, SONY BMG has swiftly provided a patch to all major anti-virus companies and to the general public that guards against precisely the type of virus now said to exist. The patch fixes the possible software problem, and still allows CDs to be played on personal computers. It can be downloaded at http://cp.sonybmg.com/xcp/. Starting today, we will also be adding this link to the SONY BMG label and corporate sites. We deeply regret any possible inconvenience this may cause.

We stand by content protection technology as an important tool to protect our intellectual property rights and those of our artists. Nonetheless, as a precautionary measure, SONY BMG is temporarily suspending the manufacture of CDs containing XCP technology. We also intend to re-examine all aspects of our content protection initiative to be sure that it continues to meet our goals of security and ease of consumer use. More information about our content protection initiative can also be found at: http://cp.sonybmg.com/xcp.

It's a small first step on Sony's part. Sony still makes no admission of guilt, though by this time I'm sure that legal exposure prevents them from doing so. In addition, the use of the word "temporarily" disturbs me. Are they just waiting for the media attention to fade before starting up again?

More importantly, Sony is making no effort to withdraw existing CDs that are already on the market and the uninstall process is still spyware-like with its use of an ActiveX control during the request for uninstall and actual uninstall. ActiveX controls are a commonly-used attack vector for malicious web sites and one of the blog comments from the last posting by Matti Nikki points out that the First 4 Internet control contains scriptable methods that can be activated without the user's knowledge or consent. His site demonstrates how he can reboot your system using one of the methods. The control exports 22 scriptable interfaces, as seen here in a screenshot of Type Library Explorer from iTripoli, and the shoddy nature of First 4 Internet's other code gives me little confidence that there aren't vulnerabilities that could be used by malicious site to gain control of systems on which the control is installed.



I've said it before, but obviously need to say it again: Sony needs to make the uninstaller freely available as a standalone executable download so that users can choose to safely and easily discontinue use of this nefarious software.

posted by Mark Russinovich @ 4:49 AM (97) comments

EXHIBIT G

Wednesday, November 16, 2005

Victory!

I'm proud to announce a significant victory in the ongoing Sony Digital Rights Management (DRM) saga; Sony has capitulated almost entirely. While not publicly admitting blame for distributing a rootkit, providing no uninstall for the DRM software, implementing a music player that sends information to Sony's site, and supplying a remotely-exploitable ActiveX control for the on-line uninstall they eventually made available – all without any disclosure to users – they have come close.

Sony BMG's site now includes a prominent link on its front page, "INFORMATION ON XCP CONTENT PROTECTION," that takes visitors to a page with a statement from Sony that declares its concern over the security issues raised by its software. The first paragraph points out that Sony licensed the software from First 4 Internet, which while true, does not hold Sony any less responsible for its use of the software or the contents of the End User License Agreement (EULA).

The paragraph continues by saying that Sony will offer consumers that have purchased the spyware-laden CD's with unprotected versions, that they are suspending production of the rootkit-based CD's and that they are recalling existing from store shelves, which they've said elsewhere comes to around 2 million units. Furthermore, Sony has finally withdrawn the spyware-like uninstall-request process, which included the download of an ActiveX control that's proven to be its own security risk, and promises the imminent release of a stand-alone uninstaller. Note that because the control is also used in the update patch, I strongly recommend that you do not apply the patch to disable the cloaking, but instead follow the manual steps I've outlined to disable the rootkit and wait for Sony to address the flaws.

Why did I qualify my statement regarding their response? Two reasons: first, as I've stated, they don't admit wrongdoing, only that the software was a security concern. Second, there's no statement on Sony's site or their press releases regarding future policy. They go as far as saying that they "will continue to identify new ways to meet demands for flexibility in how you and other consumers listen to music", but say nothing about their stance on rootkits or disclosure during software installation.

Speaking of disclosure, I hope this story isn't over. Attention now needs to turn to the broader issues that go beyond DRM to software in general. They include acceptable behavior of commercial software, from both legal and ethical standpoints, and appropriate disclosure of software behavior. We've been living in a world of hazy laws surrounding EULAs and ideally this case will lead to more clearly defined laws and standard judicial principles.

There are several pending class action lawsuits, likely more to come, and its my expectation that a U.S. government agency will eventually announce a formal investigation. The Federal Trade Commission is the one most likely to take up the case and if so, some of its recent actions against spyware vendors may have set promising precedents.

Of course, this first victory would not have happened without your participation in bringing the story to the attention of the media both in this blog and in other publications. I congratulate everyone that voiced their concern over the trend Sony's software portended and I encourage you to continue to fight for a long-lasting resolution on the issue of software installation and disclosure.

posted by Mark Russinovich @ 7:42 AM (167) comments

EXHIBIT H

Wednesday, November 30, 2005

Premature Victory Declaration?

Two weeks ago I declared victory in what the media is now referring to as the “Sony rootkit debacle”, but now I’m wondering if I jumped the gun. It turns out that the CDs containing the XCP rootkit technology are still widely available, there’s still no sign of an uninstaller, and comments made recently by the president of the Recording Industry Association of America (RIAA) make it clear that the music industry is still missing the point.

I declared my victory a few hours after Sony announced that it would withdraw the somewhere between 2 and 5 million (the number varies depending on the source) infected CDs that are on store shelves. However, even close to two weeks later it’s obvious that Sony has done little to advertise to store owners, even larger chains, that a recall is in place. They were present in stores in the Austin, Philadelphia and Chicago areas And as of last week Eliot Spitzer, the Attorney General of New York State, reports that his investigators found them in the New York City area. Many store clerks were unaware that a withdrawal had even been ordered.

At the same time that Sony announced the recall it also withdrew the flawed DRM-software uninstaller it had posted and its statement to the public dated November 18, which is still posted, they promise “We will shortly provide a simplified and secure procedure to uninstall the XCP software if it resides on your computer.” That was two weeks ago and still there’s no uninstaller. I could write an uninstaller in an hour based on my own research of the software without access to the source code. They have source code and an existing uninstaller. I find the delay utterly inexcusable.

As for notifying consumers of the problem, Ben Edelman has researched the phone-home behavior of the Sony Player software that comes on the CDs and found that, if it wanted, Sony could inform every infected customer that a recall is in place. That they haven’t taken advantage of that is particularly telling.

Besides the various comments and actions Sony has made it’s obvious that they didn’t, and still don’t, understand the issues they’ve raised from the perspective of their customers. The president of the RIAA, Cary Sherman, held a question and answer session with college journalists on November 18, just after Sony announced the recall, where he had this to say about Sony’s actions:

The problem with the SonyBMG situation is that the technology they used contained a security vulnerability of which they were unaware. They have apologized for their mistake, ceased manufacture of CDs with that technology,and pulled CDs with that technology from store shelves. Seems very responsible to me. How many times that software applications created the same problem? Lots. I wonder whether they've taken as aggressive steps as SonyBMG has when those vulnerabilities were discovered, or did they just post a patch on the Internet?

First, Sony never admitted to or apologized for making a mistake, they expressed “regret” for “any inconvenience” they caused customers. Second, Sherman overlooks the fact that more than a security vulnerability, the Sony software actively hides from customers, is not uninstallable, and sends information to Sony servers without disclosure or consent, not to mention Sony’s subsequent behavior with respect to the onerous multistep uninstall request procedure. Does he consider that behavior “responsible”? And I wonder if he still agrees that Sony’s withdrawal and uninstaller development efforts are “aggressive”? My guess is that he would, despite the evidence to the contrary.

Perhaps the strongest evidence of Sony’s own confused view of their actions is their response when F-Secure, a Finnish antivirus company, contacted them about the rootkit a month before I initially blogged about it. Business Week has an article on the inside story that documents Sony’s attempt, which it appears my blog post foiled, to sweep the whole thing under the rug.

Sony’s day of reckoning is coming, however. Last week my home state of Texas filed a law suit in civil court that charges Sony with violations of an antispyware law that the Texas legislature passed in September. How many violations? Several thousand since each Texas consumer that’s installed the XCP software counts as a violation. If Texas gets the $100,000 per violation that they are asking for,

the maximum fine under the new law, Sony will feel some real pain. If you haven't seen the news conference where Greg Abbott, the Attorney General of Texas, announces the suit I recommend you do: "Sony, don't mess with Texas computers!"

And that's just one law suit. There are still pending class action suits in several states, including one filed last week by the Electronic Frontier Foundation (EFF), Eliot Spitzer may file suit on behalf of New York consumers, and I'm serving as an expert for New York attorney Scott Kamber in the national class action suit.

Like I've said before, I hope things don't end when the suits end, but that there's some lasting policy change to the way that software installations disclose their effect on our computers. Would this have been the mainstream story it's become if the Sony XCP EULA disclosed somewhere deep within it that hidden software would be installed and that the player would contact Sony's site with a CD identifier so as to obtain banner information? I'm afraid that, while just as unethical, that behavior would be legal in most states, even ones with spyware laws. Are we okay with that?

Finally, here's a funny comic related to the story (my apologies to Celine Dion fans...never mind).

posted by Mark Russinovich @ 3:48 PM (98) comments

EXHIBIT I

Friday, December 30, 2005

Sony Settles

I'm proud to announce that a major step forward in the legal phase of Sony's rootkit: Scott Kamber and Sony have filed a proposed settlement for the national class-action suit brought by Scott. While I didn't participate directly in the negotiations, I'm serving as an expert for Scott and provided input on the terms, which I think are a significant victory for the consumer.

I won't recount the specifics of the agreement, which incidentally isn't final until approved by the Southern US District Court of NY, because other articles have already summarized them. However, the basics include consumer incentives for returning their DRM'd CDs in the the form of money and/or free albums (from a choice of sources, including iTunes!) and independent oversight for the next two years over Sony's DRM development and EULAs. In addition, Sony waives most of the terms of the existing XCP and MediaMax EULAs and allows customers that experienced computer problems as a result of the software to file independent claims outside the settlement.

Reaction to the news has generally been positive, but there are some that believe that Sony has been dealt little more than a slap on the wrist. I had no reservations giving the settlement my approval and think that this specific circumstance has had a best-case outcome for those affected.

I certainly don't think that this should be the end of the general story, though. While Sony is now bound, at least in the short term, to constraints that protect the public from repeats, other companies still have great leeway in their approach to DRM. I've made it a theme of my posts on this topic that the government needs to formalize in law some of the core guidelines of the Sony settlement. Fundamentally, users need to have enough plain-English information presented to them during a software installation, DRM-protected or otherwise, that helps them make an informed decision when they consider accepting a vendor's terms and the software's impact on their system. It should also be law that vendors must include a local uninstall functionality. Until changes are made we're all at risk of losing control of our computers to aggressive DRM tactics.

posted by Mark Russinovich @ 10:39 AM (33) comments