Experts: Sony Plan Widens Security Hole

By BRIAN BERGSTEIN, AP Technology Writer

2 hours, 48 minutes ago

BOSTON - The fallout from a hidden copy-protection program that Sony BMG Music Entertainment put on some CDs is only getting worse. Sony's suggested method for removing the program actually widens the security hole the original software created, researchers say.

Sony apparently has moved to recall the discs in question, but music fans who have listened to them on their computers or tried to remove the dangerous software they deposited could still be vulnerable.

"This is a surprisingly bad design from a security standpoint," said Ed Felten, a Princeton University computer science professor who explored the removal program with a graduate student, J. Alex Halderman.

"It endangers users in several ways."

Sony apparently has moved to recall the discs in question, but music fans who have listened to them on their computers or tried to remove the dangerous software they deposited could still be vulnerable.

"This is a surprisingly bad design from a security standpoint," said Ed Felten, a Princeton University computer science professor who explored the removal program with a graduate student, J. Alex Halderman.

"It endangers users in several ways."

The "XCP" copy-protection program was included on at least 20 CDs, including releases by Van Zant, The Bad Plus, Neil Diamond and Celine Dion.

When the discs were put into a PC — a necessary step for transferring music to iPods and other portable music players — the CD automatically installed a program that restricted how many times the discs' tracks could be copied, and made it extremely inconvenient to transfer songs into the format used by iPods.

That antipiracy software — which works only on Windows PCs — came with a cloaking feature that allowed it to hide files on users' computers. Security researchers classified the program as "spyware," saying it secretly transmits details about what music the PC is playing. Manual attempts to remove the software can disable the PC's CD drive.

The program also gave virus writers an easy tool for hiding their malicious software. Last week, virus-like "Trojan horse" programs emerged that took advantage of the cloaking feature to enter computers undetected, antivirus companies said. Trojans are typically used to steal personal information, launch attacks on other computers and send spam.
Stung by the controversy, Sony BMG and the company that developed the antipiracy software, First 4 Internet Ltd. of Oxfordshire, United Kingdom, released a program that uninstalls XCP.

But the uninstaller has created a new set of problems.

To get the uninstall program, users have to request it by filling out online forms. Once submitted, the forms themselves download and install a program designed to ready the PC for the fix. Essentially, it makes the PC open to downloading and installing code from the Internet.

According to the Princeton analysis, the program fails to make the computer confirm that such code should come only from Sony or First 4 Internet.

"The consequences of the flaw are severe," Felten and Halderman wrote in a blog posting Tuesday. "It allows any Web page you visit to download, install, and run any code it likes on your computer. Any Web page can seize control of your computer; then it can do anything it likes. That's about as serious as a security flaw can get."

Sony BMG spokesman John McKay did not return calls seeking comment. First 4 Internet was not making any comment, according to Lynette Riley, the office manager who answered the company's phone Tuesday evening in England.

Mark Russinovich, the security researcher who first discovered the hidden Sony software, is advising users who played one of the CDs on their computer to wait for the companies to release a stand-alone uninstall program that doesn't require filling out the online form.

"There's absolutely no excuse for Sony not to make one immediately available," he wrote in an e-mail Tuesday.

Other programs that knock out the original software are also likely to emerge. Microsoft Corp. says the next version of its tool for removing malicious software, which is automatically sent to PCs via Windows Update each month, will yank the cloaking feature in XCP.

Sony BMG said Friday it would halt production of CDs with XCP technology and pledged to "re-examine all aspects of our content protection initiative." On Monday night, USA Today's Web site reported that Sony BMG would recall the CDs in question.
Macromedia warns of security risk from Flash bug at Computerworld, Nov 07

Good puts security management on the air at Computerworld, Nov 07

Technology News

Web Site to Blend Journalism With Blogs AP
Feds Urge Us to Pay Our Taxes Online AP
Microsoft Launches Search for Businesses AP
Online Extra: 37 Signals, 1 Clear Message BusinessWeek Online
More Americans get their newspaper at the click of a mouse: report AFP

Most Viewed - Technology

Feds Urge Us to Pay Our Taxes Online AP
Microsoft to remove Sony BMG malware Reuters
iPod helped turned around Apple: Dell CFO Reuters
Opinion: A dim view of Spotlight Macworld.com
BlackBerry Gets a Boost PC World

MagicRAM PC Card Hard Drive
The MagicRAM PC Card Hard Disk provides a cost effective solution and offers one of the lowest costs per MB of any removable storage in a Type II PC Card format. Available in 2GB and 5GB.
magicram.com

Pc Card Hard Drive - Yahoo! Shopping
Search, compare and save. Visit Yahoo! Shopping to compare products and prices from thousands of your favorite stores. Consumer reviews, store ratings and more.
shopping.yahoo.com

PC Card Hard Drives at Shopping.com
Find, compare and buy products in categories ranging from hard drives to PC laptops. Read product reviews and compare prices with tax and shipping from thousands of online stores.
www.shopping.com