Security firms react to rootkit

November 17 2005

Following a week of extensive public criticism, Sony BMG's problems continued as class-action lawsuits and public letters were released in response to an anti-piracy program found on a number of its music CDs.

XCP (Extended Copy Protection), developed as a means of copy protection for Sony by British software company First4Internet, drew attention from the software industry when Mark Russinovich, chief software architect of Winternals Software, released his findings that the software functioned as a rootkit, or hidden program, that could not be safely removed from a computer's operating system without disabling additional features.

The program, which installs itself without the user's knowledge when certain Sony BMG music CDs are inserted, has been considered dangerous by many security experts. The application runs invisibly within the system and allows other programs to do the same provided the filename begins with a "sys" character string.

"Apparently they're trying to hide the rest of the copy protection software from users who were trying to get rid of it," said Edward Felten, professor of computer science and public affairs at Princeton University. "The problem is that it hid more than that software and hid any files, programs and registry entries that started with the prefix. Malicious software could give itself that name and be invisible at that point."

According to Russinovich's weblog of the rootkit discovery, deletion of the XCP program disabled access to the CD-ROM drive.

"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," wrote Russinovich. "Worse, most users that stumble across the cloaked files with a root kit removal program scan will cripple their computer if they attempt the obvious step of deleting the cloaked files."

"The protection software simply acts to prevent unlimited copying and ripping from discs featuring this protection solution," Sony BMG said in a statement posted on its Web site last week. "It is otherwise inactive. The software does not collect any personal information nor is it designed to be intrusive to your computer system."

Mikko Hypponen, chief research officer of F-Secure, a computer security firm, acknowledged the network functions. The software, which

runs a background network function, contacts a pair of Sony servers and reports which audio track is being listened to as well as the computer's hardware identification information.

Hypponen went on to explain how the program has been adapted into a viable means of creating viruses that would be impossible to locate using anti-viral programs. To date, four known instances of the B-Replicant virus family have emerged using the rootkit's technology as a means of hiding themselves within the system. These viruses, which operate over a network, can be used to remotely control an infected computer for malicious purposes such as attacking a Web site with large amounts of network traffic.

Sony BMG has made a removal utility available for download but has come under fire for creating further vulnerability through its use. The utility installs software that may enable the Internet Explorer Web browser to be controlled by a remote host if the user visits malicious Web sites.

"At the personal level, I think Sony is doing stunts like this because they're worried about the market share within mobile devices," said Hypponen. "They used to own the market with the Walkman, which was circumvented in just a few years. One of the functions of the program is that it prevents the music from being moved to an iPod. These files move just fine to a Walkman."

"There's a lot of rhetoric against illegal copying and a lot of pressure on executives to do this, but in that fight, companies go too far. There is zero evidence that this program stops illegal copying," said Jason Schultz, a staff attorney for the Electronic Frontier Foundation, a digital-rights advocacy group. "There's so much pressure just to do something that they roll out these technologies without thinking of the customer."

Security firms such as Symantec and F-Secure have updated their clients to detect and safely eliminate the XCP program. Microsoft has also updated its anti-spyware program to remove the underlying code.

To date, Sony BMG has recalled the more than 4 million XCP-enabled music CDs from store shelves and is planning a campaign to replace the 2.1 million that have been sold.

Sony BMG and First4Internet were not available for comment.