Subject: Re: Rootkits and Renguard
Posted by light on Fri, 11 Nov 2005 22:18:18 GMT
View Forum Message <> Reply to Message

the term root-kit is going to be mis-used so many times.

A rootkit is a set of software tools frequently used by a third-party (usually an intruder) after gaining access to a computer system. These tools are intended to conceal running processes, files or system data, which helps an intruder maintain access to a system for purposes unbeknownst to the user.
http://en.wikipedia.org/wiki/Rootkit

And here is the section on Copy-Protection:

Rootkits as copy protection

There are reports as of November 1, 2005 that Sony is using a form of copy protection, or digital rights management, on its CDs called "XCP-Aurora" (a version of Extended Copy Protection from First 4 Internet) which constitutes a rootkit, surreptitiously installing itself in a cloaked manner on the user's computer and resisting attempts to detect, disable, or remove it. Much speculation is taking place on blogs and elsewhere about whether Sony might be civilly or criminally liable for such actions under various anti-computer-hacking and anti-malware legislation. Ironically, there is also speculation to the effect that the bloggers who point out what Sony CDs do, with technical details, may also be committing a civil or criminal offense under anti-circumvention provisions of laws such as the Digital Millennium Copyright Act in the United States. [3] [4]

On November 2, 2005, Sony released a patch to remove this rootkit, while continuing to maintain that it is not malicious and does not pose a security risk. But the patch itself has come under fire as well. First, it requires ActiveX controls to install, and therefore is only available to users of Microsoft's Internet Explorer. Second, the update is more than 3.5 megabytes in size, and appears to contain new versions of almost all the files included in the initial installation of the entire DRM system, and some new files as well. It appears that the patch is adding things to the system, and once again, not informing the user of exactly what is being done.[5][6]

Informed opinions differ on the security implication of this Sony 'XCP-Aurora' technology as there is evidence that the software has caused Blue screen (BSoD) errors on Windows systems while in normal use. In addition the software has been criticized as poorly implemented and the file hiding scheme could be used to hide arbitrary files on a PC simply by prefixing the filename with sys.

Further commentary, including security implications, can also be found on the Security Now! #12 podcast with Steve Gibson and Leo Laporte, entitled "Sony's 'Rootkit Technology' DRM (copy protection gone bad)."

A class-action lawsuit has been filed on behalf of California consumers who may have been harmed by anti-piracy software installed by some Sony music CDs. A second, nationwide class-action lawsuit is expected to be filed against Sony in a New York court on Wednesday seeking relief for all U.S. consumers who have purchased any of the 20 music CDs in question.[7]

On November 9, 2005, security companies Sophos and Symantec announced that they had discovered viruses which were exploiting the Sony rootkit in order to gain access to affected systems.[8]. These viruses are appearing primarily on the form of emails with attachments. ZoneAlarm users were protected by the an "os firewall" in their paid products.

As of November 10, 2005, World of Warcraft hackers have confirmed that the hiding capabilities of Sony BMG's content protection software can make tools made for cheating in the online world impossible to detect. The software - deemed a "rootkit" by many security experts - is shipped with tens of thousands of the record company's music titles. Furthermore, experts at SophosLabs™, Sophos's global network of virus and spam analysis centres, have detected a new Trojan horse that exploits the controversial Sony DRM (Digital Rights Management) copy protection included on some of the music giant's CDs.[9][10][11][12]

Again from: http://en.wikipedia.org/wiki/Rootkit

I love WikiPedia
