The Brains Behind the Operation
infectionvectors.com
November 2005

Overview

At this point, the world has heard about and reacted to the Sony/BMG anti-piracy software that is installed on unsuspecting users' machines when the attempt to listen to an audio disc on their PCs. The term "unsuspecting" is used because even one gives Sony the heaviest benefit of a doubt on the issue, there is no evidence that they were ever going to tell their customers that the "player" they were installing also came with a program that hid files from file managers, the same way a rootkit does. This article takes a look at the Sony/BMG case and how it fits into the history of malware.

Mine is Yours

Napster pushed music sharing, and the legal matters surrounding it, into living rooms around the world. Record companies complained of lost revenue due to the explosion of pirated music sharing made possible by the Internet. "Sharing" should be called out as a matter of semantic debate for the record industry as they have clearly defined all "sharing" as stealing. Even after winning lawsuits against Napster and numerous individuals, most companies recognized the futility of trying to eliminate music sharing. It may well be from this frustration that Sony decided to take more extreme measures in fighting song theft.

In October of 2005, Marc Russinovich described the rootkit found on his system and how he tracked it back to a Sony/BMG CD he had played. The software (which is installed with the player that is required to listen to the CD on a PC) hides itself and associated files by making significant changes to the local machine (for the technical rundown, see Russinovich's excellent article).

Since that time, public outrage has been tremendous, as one would expect. Not only has Sony/BMG seen countless articles chastising them for such a blatant disregard for PC and PC user safety in the name of their own profitability, but they've also had to witness the malware-writing community using the Sony rootkit for its own ends (a Trojan known as Breplibot was the first to utilize the file hiding functionality of the Sony software). In addition, the state of Texas has sued the company in the US for violating the privacy of users.

Good Idea in Theory

Although Sony/BMG committed a major blunder in adding such software to their CDs, it was not the first time such a mistake was made. Throughout the history of computer malware are examples of "unintended consequences" from applications that were considered beneficial by their authors.

The first of such examples that is considered here is Pakistani Brain, which was created by two brothers to protect their intellectual property from being stolen (just as in the case of Sony's music CDs). Brain, as it is often referred to in the media, was added to prevent unauthorized software copying, and although there are no data destroying components to the virus (it was rather difficult to remove at the time and does change volume labels, etc.), it created quite a panic as it spread. The two brothers responsible for the malware cite the lack of criminal charges against them as evidence that the US wanted to cover the evidence that copyrights were not respected/protected domestically.

The Welchia worm (aka Nachi) appeared as an answer to the Blaster outbreak in 2003. The malware attempted to install the patch required to deflect Blaster and related worms after it infected a host. Whether or not this worm was really intended to be a "good" piece of malware is debatable. However, the awful consequences of Welchia are not, the network traffic and system instability created by the code wrecked networks in late 2003 and spawned numerous variants in 2004. No one has been charged with writing or releasing the original Welchia worm.

Liability

The Texas case (if it is the first to go to trial) will be especially interesting for malware researchers as it will point out how much responsibility a malware creator has with regard to "unintended consequences." It is an excellent test of such limits as it has garnered a good deal of public attention, involves a very well-known company, and comes after the software was exploited by other nefarious individuals.

If Sony/BMG is liable for the damage caused by their malware, even if that is just privacy violations (as opposed to being responsible for downstream infections of Trojans like Breplibot), then the malware authors of the world will have a significant precedent against them the next time one of them finds their way to court.

Infectionvectors.com has additional reports covering topics of virus writer liability and the professionalism of malware coding. For details, see http://www.infectionvectors.com.

References

Mark Russinovich's Artcile on the Sysinternals site:
http://www.sysinternals.com/blog/2005/10/sony-rootkits-and-digital-rights.html
"Sony, Rootkits and Digital Rights Management Gone Too Far." 31 October 2005.

Copyright © 2005 infectionvectors.com. All rights reserved.