# Sony Root Kit Warning

By Holly Lisle

This is passed on from Jerry Pournelle, who is as unimpeachable as sources get. Does not affect me – I work on a Mac. Could very well affect you.

> *This is a Chaos Manor Warning. I would be shouting if I were not concerned that it would trigger your spam filters.*
>
> *You may or may not be familiar with the Sony Music CD Root Kit problem.*
>
> *Let me begin with the warning: do not buy or install any Sony Music CD on your PC. The records play just fine on other systems. There's no problem with Mac or Linux or with self contained music players.*
>
> *But if you try to play that record on your CD, it will tell you that you must install the Sony CD player codec (you can't play the record through Microsoft Media Player or any other stuff you have installed on your system).*
>
> *DO NOT INSTALL THAT SOFTWARE. If you do you may never be able to get it off there short of scrubbing your system down to bare iron, reformatting, and reinstalling everything. I wish I were spoofing you, but I am not. This is a serious warning.*
>
> *Moreover, if you have given a Sony Music CD to anyone as a gift, and they have tried to play that music on their PC (not Mac, not a standalone player, not Linux, but Windows PC) then their systems are infected, and it is exceedingly difficult – exceedingly difficult – to remove that infection in a way that doesn't blue screen of death the PC.*
>
> *MY ADVICE IS NOT TO BUY ANY SONY MUSIC CD.*
>
> *I have heard nothing about Sony movie DVD's having any such*

*infection, but it's possible. So far all my Sony DVD's have played with Power DVD and I have not been asked or required to install any special Sony software to play a Sony movie DVD; if I am asked to do so I will refuse, and so -hould you.*

*Understand that the Root Kit on the Sony Music CD is a deliberate installation by Sony as part of a Digital Rights Management scheme. They will now, if you jump through enough hoops, send you a patch that will make their scheme visible – like all root kits, their original installation so infects your operating system as to hide in a directory your operating system literally cannot see or access – but it still does not remove it.*

*I'll have more on removal in the column and at another time this being column time. I will also have a warning in my Christmas Shopping List in the column.*

*DO NOT BUY SONY MUSIC CD*

*This is a serious infection: the scheme has actually been used by third parties to hide other malware on systems that have the Sony root kit installed, and others have used the Sony root kit to hide cheat software for World of Warcraft. Even if you think you know what you are doing, you should not fool around with this stuff. It's dangerous, it's very difficult to remove, and there is a very real risk that you will have to reformat your disk and reinstall your OS and everything else.*

*For more information see:*

*www.theregister.co.uk …*

*www.theregister.co.uk (second article)…*

*www.sysinternals.com…*

*The last reference is to the Sysinternals page where an incredulous Mark Russinovich relates how he found the root*

*kit on his system: the root kit has been out for months, and this is the first indication of it's existence.*
*Sony did a splendid job of stealthing this.*

*I will have more in the column and on the web page. If you have bought and installed a Sony Music CD on your PC, *you need more help than I can give you*. Start with the Sysinternals page, and *proceed with extreme caution*.*

*And the best of British Luck to you.*

*Best regards,*

*Jerry Pournelle*
*Chaos Manor*