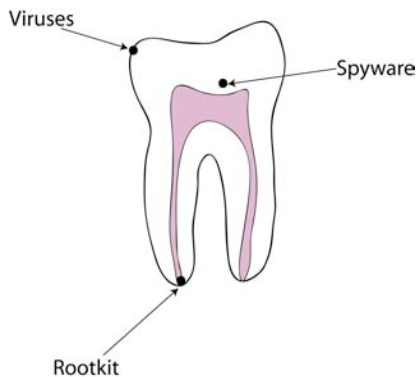


The Right to Infect?

Protecting your systems from music CD based rootkits

Charles Bennett - MBA, Principal Consultant, Triella

Rootkits are the newest form of malware affecting computer systems. They have the capacity to render a system completely useless and can remain undetected by antivirus and antispyware programs. Imagine for a minute that a tooth is representative of the Windows operating system. Following that analogy, malware represents different types of decay that can happen to a tooth.



Viruses, like bacteria, attack the surface of the tooth - or the outer layers of Windows. They are easy to spot and relatively easy to remove and prevent. Spyware attacks at a deeper level within the tooth, often leaving the surface untouched even though there is decay in the lower levels. Your Windows computer may perform just fine, but its security is compromised by a hidden program which is transferring confidential information to an external source.

Rootkits are the worst. For a tooth, fixing this kind of decay would require a root canal. The rootkit also has access to the very life of the tooth and could cause irreparable damage. For Windows, a rootkit operates at the lowest level in the operating system and is able to perform any function without restriction. Rootkits are very difficult to detect as they can shield themselves from programs that operate at a higher level - such as antivirus and antispyware software.

Sony has developed a rootkit and placed in on their music CD's to protect their CD's from being copied. The rootkit hides any file or function which includes the character \$sys\$ at the beginning of its name. It also sends information about where the music CD being played back to Sony. The problem is, the rootkit is poorly written and opens the door allowing virus writers to cloak their viruses from antivirus and antispyware software.

See the sidebar "Chronology of a Viral Exploit Based on XCP" for more information on the impact of this rootkit.

How are you Infected?

An infection happens whenever a Sony music CD with XCP technology is loaded. You will be asked to accept a license agreement (which makes no mention of the rootkit). Upon acceptance, the rootkit is installed and your system is

compromised. This can happen on a home PC as easily as it happens on a corporate PC.

Which Music CD's are Affected?

The following CD's are known to contain the rootkit XCP.

- Trey Anastasio, Shine (Columbia)
- Celine Dion, On ne Change Pas (Epic)
- Neil Diamond, 12 Songs (Columbia)
- Our Lady Peace, Healthy in Paranoid Times (Columbia)
- Chris Botti, To Love Again (Columbia)
- Van Zant, Get Right with the Man (Columbia)
- Switchfoot, Nothing is Sound (Columbia)
- The Coral, The Invisible Invasion (Columbia)
- Acceptance, Phantoms (Columbia)
- Susie Suh, Susie Suh (Epic)
- Amerie, Touch (Columbia)
- Life of Agony, Broken Valley (Epic)
- Horace Silver Quintet, Silver's Blue (Epic Legacy)
- Gerry Mulligan, Jeru (Columbia Legacy)
- Dexter Gordon, Manhattan Symphonie (Columbia Legacy)
- The Bad Plus, Suspicious Activity (Columbia)
- The Dead 60s, The Dead 60s (Epic)
- Dion, The Essential Dion (Columbia Legacy)
- Natasha Bedingfield, Unwritten (Epic)

However, other CD's from Sony/BMG may also contain the rootkit so look for the web site cp.sonybmg.com/xcp on the back of the CD.

How do you Remove the Rootkit

If you go to the following site,

<http://cp.sonybmg.com/xcp/english/updates.html>, you can find a patch to remove the cloaking technology from your computer. This does not remove the rootkit, it only exposes the rootkit to other software. To completely uninstall the rootkit, you must make a request at the following site:

<http://cp.sonybmg.com/xcp/english/form14.html>. Sony will then send you detailed instructions for removing the rootkit. Once removed, you will not be able to play Sony music CD's on your computer.

It's Time to Take Action!

Perhaps it is time to prohibit the use of original music CD's in the workplace. Software that can make a system so vulnerable is a threat to the integrity and privacy of data within any organization. XCP was available for 8 months before any antivirus company detected it - likely because it was music CD based and specific to one vendor. What if a virus writer had detected it first? The potential damage could have been greater.

The response time for antivirus vendors was just one day short of the response time of those creating a virus to exploit the XCP rootkit. In practical terms, considering the time that it takes to distribute an update, the antivirus solution may not have been soon enough for some users.

We can all agree that Sony has the right to protect its intellectual property but I don't think they have the right to steal computer resources with underlying programs or compromise the security of a computer in their quest to protect their assets, particularly in such a covert manner.

Chronology of a Viral Exploit Based on XCP

March 2005 – XCP Created

The company *First 4 Internet* creates a program to protect Sony's music CD's from copying and then cloaks the program using a rootkit. This is a part of Sony's digital rights program - the right to protect their products from piracy. The rootkit is called XCP. New music CD's are released with XCP as a part of the CD. The rootkit prevents the music from being copied to a hard disk or MP3 player and sends information back to Sony about where the CD is being played. There is no disclosure concerning XCP in the End User License Agreement.

November 2, 2005 – Rootkit Discovered

XCP installs, without your permission, whenever you play specific Sony music CD's on your computer. But, XCP is poorly written. When a user attempts to manually remove XCP from a computer, it renders the CD ROM drive inoperable. The software also caused instabilities in Windows sometimes causing systems to freeze altogether. The only way to recover is to reinstall Windows from scratch. There is no uninstallation tool for XCP.

November 6, 2005 – Rootkit Exploited by Gamers

Blizzard, a company that makes the computer game *World of Warcraft* introduced a piece of spyware called *The Warden*, designed to sniff out cheaters using their online gaming service. Because the Sony rootkit was so poorly written, gamers discovered that by just renaming a single file, they could employ Sony's rootkit to mask their cheating efforts.

November 7, 2005 – Law Suit

Italy files a law suit against Sony as certain music CD's install a rootkit on a computer - an act which in and of itself is not illegal but which has significant ramifications for the security of a system.

November 8, 2005 – No Concern

Sony's president, Thomas Hesse, downplays the rootkit as being of no concern. "Most people, I think, don't even know what a rootkit is, so why should they care about it?" he said. At the same time Sony releases a service pack that uncloaks the rootkit.

November 10, 2005 – Antivirus Vendors Respond

Two of the many anti virus vendors officially declare Sony's rootkit as a threat to systems and design removal tools to deal with it.

November 11, 2005 – Sony Rootkit Exploited

Two Trojan virus programs take advantage of the Sony rootkit to hide and distribute themselves from computer to computer over the Internet.

Sony announces that it is suspending the use of XCP technology on its music CD's.

November 12, 2005 – US Class Action Lawsuit Launched

New York and California join Italy in launching a class action law suit against Sony.

November 13, 2005 – More Antivirus Companies Come on Board

Microsoft announces that it will incorporate technology to remove the rootkit into their AntiSpyware software.

November 14, 2005 - Microsoft Steps Up the Campaign

Microsoft announces that in addition to removing the rootkit with AntiSpyware, it will also include the removal technology in the Malicious Software Removal Tool and in Windows Defender, the antispyware software to be included in Longhorn, the next commercially available version of Windows.

Charles Bennett is the President of Triella, a technology consulting company specializing in providing technology audits, planning advice, project management and other CIO related services to small and medium sized firms. He can be reached at cbennett@triella.com or 416.269.4368. For additional articles, go to www.triella.com.

© 2005, by Triella. All rights reserved. Reproduction without permission is prohibited.