[in]security

by Gary McGraw

Is Sony BMG Run By Malicious Hackers? : : :

Sony BMG is interested in stopping you from ripping digital copies of its music—so interested that it'll go so far as to root your box to make sure you can't. There are many reasons why this is an awful development. These include the morally questionable use of a rootkit as a security feature, the fact that malicious hackers can use this rootkit to further compromise machines, and the invasion of privacy that this poorly conceived security mechanism promulgates. But the worst possible effect of the Sony rootkit may be imposed on your IT staff. Put simply, this mess is going to be hard to clean up.

SONY GOES TO THE DARK SIDE

Mark Russinovich of Sysinternals discovered that XCP2, a CD protection scheme peddled by U.K.-based First 4 Internet and licensed by Sony BMG for use on numerous music CDs, monitors computer use and prevents users from ripping CDs. When an XCP2-protected CD is inserted into a Windows PC, Windows Autorun copies a small piece of software onto the computer. From then on, if the user attempts to rip a protected CD, the software replaces the music with static.

Copy protection software is nothing new, so what makes this a rootkit? One of the basic ideas that rootkits employ is stealth. They attempt to hide their very existence from system administrators and others responsible for security. This makes rootkits a very dangerous weapon (rootkits well deserve their place at the apex of the attacker's toolkit). The software in question deliberately cloaks itself from normal diagnostic tools and some security products by hiding certain processes, rewriting the interrupt address table, and interposing on various kernel-level system calls. This makes XCP2 hard to find and thus hard to remove.

MANAGING HACKED MACHINES SUCKS

When supposedly legitimate processes adopt bad behavior, they make administering a machine almost impossible. Finding processes hidden away by XCP2 is difficult and time-consuming on individual PCs. Multiply this by X number of machines in your enterprise, and you can begin to appreciate the problem.

But it gets worse. The Sony rootkit technology not only hides the anti-ripping process, but it will hide any specially tagged process just as well. According to Russinovich, XCP2's stealth mechanism will hide any file, directory, registry key, or process whose name begins with "sys." This means malicious software can take advantage of the existence of the Sony rootkit to avoid detection. In fact, the first malware attempting to take advantage of the Sony rootkit emerged several days after the story broke.

In addition, the Web-based uninstaller that Sony trumpeted to the press (and made very difficult to find and use by actual Sony CD owners) is linked specifically to one and only one machine. That is, it will uninstall only one infected PC. Corporate IT won't appreciate that at all. Plus, according to Ed Felten (www.freedom-to-tinker.com), the Web version of the uninstaller opens a serious security hole on any computer it's run on. Toxic waste anyone? So first corporate IT needs to determine whether this invisible software exists on its machines, and then it needs to safely remove it. Thanks Sony!

> When good processes adopt bad behavior, they make administering a machine almost impossible.

XCP2 may also affect a PC's normal operations. The program scans all running processes on the system every two seconds, querying basic information about the files and consuming up to 1 to 2 percent of system resources (due to sloppy coding). Users have reported serious effects on PCs infected with the XCP2 rootkit, most of which were extremely mysterious until Sony was outed. Lawsuits have already been filed in California and Texas. Shame on Sony. Let's hope the right side prevails.

Gary McGraw is CTO of Cigital, a software quality management consultancy. He is co-author of Exploiting Software (Addison-Wesley, 2004), Building Secure Software (Addison-Wesley, 2001), and Java Security (Wiley, 1996). Reach him at gem@cigital.com.