SECURITY NOW!

Transcript of Episode #12

Sony's "Rootkit Technology" DRM (copy protection gone bad)

Description: Leo and I discuss details and consequences of Sony Corporation's alarming "Rootkit" DRM (digital rights management) copy protection scheme. This poorly written software unnecessarily employs classic rootkit technology (see episode #9) to hide from its users after installation. It can not be uninstalled easily, it can be easily misused for malicious purposes, and it has been implicated in many repeated BSOD "blue screen of death" PC crashes.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-012.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-012-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 12 for November 2, 2005, a special edition on Sony's Rootkit DRM. Steve Gibson, welcome back from GRC.com.

Steve Gibson: Hey, Leo.

Leo: The man behind SpinRite and ShieldsUP! and, of course, Security Now!, our security expert. His expertise is in taking complex security issues and making them intelligible and understandable for everyone.

We did a whole section, a whole segment on rootkits a couple of segments back. And they've returned to bite us in the butt. What's the latest on rootkits?

Steve: Yeah.

Leo: First maybe we should define "rootkits" for those who missed our podcast on rootkits.

Steve: Rootkit technology is technology which exploits the hookability, the variability of the operating system itself. It changes the way the OS works for the express purpose of hiding malicious software right, like, in plain view, right in front of the user.

Leo: Used by hackers to hide their hacks, originally on UNIX systems but now on Windows systems. And then as we - and if you want more details, you should listen to Episode 9 of Security Now!. But as we mentioned, it's always being used by spyware. But the big story this week is a big company that's using rootkit technology.

Steve: Well, exactly. What happened was that Mark Russinovich of Sysinternals, who wrote the RootkitRevealer that we talked about in Episode 9 and recommended to people that they get in the habit of using, he discovered something on one of his own machines, using his own tool. Actually, he was updating the RootkitRevealer to add some more features to it and, you know, ran it on his system, and there was a bunch of stuff which, you know, he was as surprised as any of us who really know or feel like we know what's in our systems would be. Well, he tracked it down to a commercial Sony CD that he had purchased not long before. And when he stuck it in his computer, it popped up an end-user license agreement, the so-called EULA. And, you know, he clicked on, oh, you know, okay, whatever, because apparently it needs its own player in order to play the music that it comes with.

Leo: This is a kind of copy protection that a number of audio CDs use now. And by the way, I don't know about this particular one, but in the past we've just told people, if you hold the Shift key down when you insert the CD, it will prevent the running of any software on the CD. And that in the past has disabled the copy protection and allowed you to play the CD as you would any normal audio CD.

Steve: Well, and apparently, I mean, I don't know whether this has to be installed, or whether it's only for, like, the extended digital rights management stuff.

Leo: Right, right.

Steve: But what Mark found was that a whole bunch of files and registry keys and, you know, modifications, you know, deep, I mean, true rootkit modifications were made to his system as a consequence of installing this thing.

Leo: Wow.

Steve: So, I mean, you know, the RootkitRevealer did what it was doing. He had no bugs in his code. It was really showing that something had installed itself malicious - well, okay, not maliciously, but really without...

Leo: Sneakily.

Steve: ...giving him any sense for what it was doing.

Leo: Right. So it's being used by Sony to enforce their digital rights management, their copy restrictions on the CD. And is there a credible reason for them to hide this?

Steve: Well, I don't really think so. And what's really interesting is that, I mean, this feels like déjà vu for me because, as we talked about before with our original SPYaWAREness podcast, talking about the Aureate DLL that was bringing advertising software along and going, you know, it wasn't using rootkit technology, but it was installing itself without people really understanding what was going on, a side effect of that was that it was making systems less stable. And it turns out, in researching this, I have found that this has been going on apparently for at least six months, back to, like, March of 2005. People have been getting blue screens when they boot their system, associated with something called the aries.sys driver that Windows complains is a critical system component. Well, this aries.sys is part of the DRM system called XCP which Sony is now installing when you buy one of their disks and stick it in your system.

Leo: Now, Sony doesn't make this copy protection scheme. They're licensing it from another company.

Steve: Correct. It comes from a company in the U.K., and we'll have links to this company in our show notes. What's interesting is that this thing has caused so many problems that even it, this rootkit technology, has a service pack.

Leo: And how do you get the service pack?

Steve: So you download Service Pack 1 of this crap you don't want to have on your system anyway, in order to cause...

Leo: But how do you get the service - how do you even know it's there to get the service pack?

Steve: Well, I mean, that's the problem with a software that installs itself surreptitiously in a machine. Or, you know, many people had had these problems and didn't know and didn't, like, logically associate it with the fact that they had played an audio CD in their system. The box comes up, and they click on OK, and off it goes. Well, this just installed a rootkit.

Leo: The license agreement implies that you can uninstall this.

Steve: Correct. And there is absolutely no provision for uninstalling. Now...

Leo: You may think you've uninstalled it, but it's still there.

Steve: Well, actually, it's even worse. I mean, again, it's exactly the kind of things you and I have talked about before. People have used the RootkitRevealer, also the F-Secure product that we mentioned in our Rootkits podcast, the BlackLight product. It showed, back in October, last month, some users use the BlackLight product from F-Secure to also discover this. Well, in trying to remove it, they damaged Windows and lost their CD-ROM drive completely, just disappeared.

Leo: Well, you know, I get a lot of calls on Call for Help and on my KFI radio show from people who have disappearing CD-ROMs.

Steve: I wonder if this could be related to that.

Leo: This has become a very common problem in Windows of late.

Steve: Well, I mean, again, we're reliving history because this is exactly what was happening back with the Ad-Aware stuff, which is why I wrote OptOut in order to scan for and safely remove the Ad-Aware stuff. They had no remover at all. And when people would improperly delete these things - in fact, you and I have talked about how even one of our computers at the office lost its Internet connectivity when an anti-spyware tool just scraped the programs off.

In the case of this Sony DRM rootkit, it installs a filter driver sort of in - it's called a "filter" because it's in line between the operating system and the CD-ROM. And Mark of Sysinternals had exactly this happen. He deleted this file, this sys file, and his CD-ROM disappeared. Now, he knew, because he's a heavy-duty techie, how to go around and how to go about getting it reconnected. But many people have had to install Windows from scratch after removing this thing incorrectly. And in fact, in some postings over on the F-Secure site, they say, yes, BlackLight, our rootkit tool, will discover it. Do not use its deletion or you will lose your CD-ROM drive.

Leo: So let's talk about - there's a number of angles to this story that I think are interesting. But first let's just kind of cover the basics. What do we know, what does Mark Russinovich say this tool does? It looks like it does quite a bit to your system.

Steve: Yes. It's got a collection of files and registry links. So, I mean, it is a true rootkit technology. Now, one of the problems with this is that it was also not very well written.

Leo: Oh, great.

Steve: For example - yes, exactly. It has technology to allow itself to be removed, but it has a driver-unload capability. Mark saw, in looking at this, that it attempts to do so safely.

Leo: But it can't.

Steve: He knows it's not possible to safely remove something that is hooking the kernel the way this thing does, really down deep. There is no safe way to do it. If you do you'll just get blue screens.

Leo: It's rewritten the system service table; and if you remove the entry there, the system crashes.

Steve: Exactly.

Leo: So you can't unload the driver. It leaves the system unstable.

Steve: Exactly. Now, even worse, he discovered in his version that it was also - the drivers were marked as "safe boot" drivers, meaning that, if you reboot Windows into Safe Mode, which is supposed to get rid of anything that could be causing a problem, allowing you to do system recovery sorts of work, then you'd be safe. Well, this thing now marks itself as "safe boot." Apparently it didn't used to because some earlier posts I found had people, they'd figured out how to work around this DRM, that is, you booted into Safe Mode, then you deleted a file called caj.dll, which was this CD-ROM filter driver, then you boot back normally, your CD-ROM is gone, so you delete it from the Windows hardware list and then tell Windows to rescan for any new hardware. Windows would refind the CD-ROM, link it back in, and you'd be set to go again with this DRM bypassed permanently.

Leo: So apparently people were circumventing the copy protection, and Sony, or the makers of this copy protection, decided to make that impossible by making them Safe Mode drivers.

Steve: Precisely.

Leo: Wow.

Steve: Also...

Leo: Yeah, tell us more.

Steve: It also named itself the "Plug and Play Device Manager," you know, which it's not, in order to confuse users who were trying to look at the list of running services and figure out, you know, why their system has started to misbehave.

Leo: This is precisely what hackers do.

Steve: Oh, yeah. And one last thing. What it does is it hides anything that begins with $sys$ dot dot dot, I mean, you know, anything that begins with $sys$ gets hidden by this tool, even things that are not its. So, for example, to test this, Mark renamed notepad.exe to $sys$notepad.exe. It promptly disappeared.

Leo: It's used...

Steve: Even though it was still in the system.

Leo: It hooks into the rootkit and is now a hidden file that cannot be seen.

Steve: Which means that, if this software became prevalent, that junior hackers who don't have the ability to create a rootkit themselves could simply name their files sys, and they'd all be - they would all disappear, courtesy of Sony's copy protection.

Leo: Let me underscore this. Sony is installing, without your knowledge and with really very weak permission, a program that allows any hacker, whatever his skills, to hide files on your system without your knowledge. They're putting a rootkit on your system that could be used by any moron.

Steve: Exactly.

Leo: This is just appalling. Now, Sony, as we speak, has not responded to these allegations. But what's good news is that this is being picked up everywhere: PC Magazine; PC Pro; Slashdot's written quite a bit about it. There's also a good article in The Washington Post. The Washington Post has a good security column on there, and the author of that has written a little bit about it. So it's getting coverage.

Steve: Yes. Some guy who was blogging on MSNBC, a regular columnist, wrote a story yesterday about how he was going to be listening to and reporting on a new piece of audio CD that he had. He put it in his drive, it popped up this EULA, and he clicked No. He said, wait a minute, I don't want software installed on my system in order to listen to an audio CD. Then he did a little looking around and realized how glad he was he clicked on No.

Leo: Yes. Well, I wonder how many of us have done this and exposed ourselves to this rootkit. Do we know which CDs it's on?

Steve: Apparently, Sony's been using this kind of technology for on the order of a year or more. There was another rootkit-ish technology they were using by a different name before this. But at least six months this goes back. And again, the good news is, RootkitRevealer, that we've talked about before, will let people know if they've got this on their system.

Leo: If you run RootkitRevealer, what string should you see? We've mentioned before there are a number of false positives you can get with RootkitRevealer that are okay - Kaspersky's Antivirus, Norton's Trash Protect.

Steve: Yes.

Leo: But is there a distinctive string that you'd see that would let you know that in fact you have the Sony/BMG protection on it?

Steve: Yes. You want to look for the sys on the files directory off the system 32 folder and a whole bunch of registry keys. All are protecting themselves and hiding themselves with this sys.

Leo: Are these the null-terminated string registry keys that we had talked about before? Or null...

Steve: No, it's just this prefix of sys.

Leo: sys, okay.

Steve: That's really the tip-off. Now, we'll have in our show notes a couple other links because Sony - the good news is, Sony is getting a huge amount of heat from this. You know, they are not saying they're not going to use it, but they do have a page now where they give you a link over to the XCP-Aurora.com site, where there is something that will remove this finally from your system.

Leo: And have we verified that it actually does that without crashing you?

Steve: No, but I've seen a whole bunch of blog postings from people who have said that - and explained that what it does is it'll - the other thing is it has to install one more thing. It works with an Active-X control, so you have to give it permission to install an Active-X control in your system in order to offer you the Service Pack 1 upgrade to this heinous bit of software. And then if you say No, it has an option for deleting it.

Leo: Brian Krebs, who writes the Security Fix column in The Washington Post, says that Sony says that any CD labeled "Content Enhanced and Protected," and it would be on the front and the back of the product, could contain this rootkit. And he said that he did a quick search on Amazon.com site. There are 24,000 of these CDs out there.

Steve: Oh, boy.

Leo: So it's a serious issue.

Steve: Well, and the other thing that's really interesting, too, is that Mark technically violated digital rights management law...

Leo: The DMCA, yeah.

Steve: Exactly, the DMCA, by figuring this out.

Leo: It was illegal to do what he did. And this is the problem. This is a situation that our lawmakers have gotten us into because they're in the pockets of the recording industry. And the recording industry clearly has no scruples when it comes to protecting their intellectual property. Well, I hope that Sony does the right thing and pulls it back. Nevertheless, that means there's still probably a lot of computers infected out there.

Steve: Well, and many people have written to the groups and the bands whose CDs did this to their machine.

Leo: Good.

Steve: Typically, these people have responded that they had no idea...

Leo: No, of course not.

Steve: ...this was going to be done.

Leo: And unfortunately the bands, in their defense, have no control of this at all. I'm sure their contracts, you know, specify that Sony can do anything they want on the CD.

Steve: Right.

Leo: You'd have to be a pretty big band to say no to Sony in this case. Well, I think what it means to me is that I'm going to be much less likely to buy a CD from Sony from now on. Certainly, if you put an audio or - this is, by the way, true of movie CDs in another way. There's a player that movie CDs install, the InterActual Player, that is known to disable CD-cracking software, DVD-cracking software on your system. So I guess the bottom line is, if you're using a computer to watch movies or listen to music, and it asks you may it install some software, to say no. And I would imagine that holding the Shift key down would still work in preventing that software from running.

Steve: Yes, that will prevent the autorun. Now, one other nice feature - again, this goes back to what we've often talked about security-wise, if you do not have administration rights, this cannot install itself.

Leo: Oh, very interesting, another reason not to run as root.

Steve: Exactly. So many administrators have mentioned in various postings that users came to them when they installed some music on their machine, or tried to just play some music on their machine at work, because the work machines were locked down and their employees were running without administrative rights, this junk would not install itself on their machine. And Sony has on their site, actually has pages explaining, here's how you add administrative rights because you're going to have to have those in order to use our little player with our music CDs.

Leo: Oh. Appalling. Appalling. And this is just, I mean, just appalling. Well, we've met the enemy, and he is Sony/BMG. I hope people are listening and write to Sony, write to the bands. And I think the best thing to do is at this point stop buying Sony CDs. In fact, I wouldn't buy a CD that says "Contents Enhanced and Protected" on it of any kind. Do not buy a CD that says it's copy-protected.

Steve: Well, in fact, a number of people, posts in the various blogs said, you know, way to go, Sony, you've really made me want to legitimately purchase music now.

Leo: Yeah. This is, of course, what we've talked about. And we talked about this on TWiT. It's just turning people into criminals. You do this, you go far enough, people are going to stop buying music.

Steve: Right.

Leo: Well, Steve, I thank you for the update on this. It couldn't have been more timely that we covered rootkits. I would encourage people to go back to Episode 9, if they haven't heard it, when we talk about the rootkits and the potential problems. And here it is, three episodes later, and one of the biggest companies in the world is foisting them on us.

Steve: Well, and what's neat is that, you know, we have talked about, and there exist, tools that will find these. And now, thanks to all the furor which this has generated, there is a safe removal tool from the authors of the software, which, you know, always...

Leo: If you trust them.

Steve: ...ultimately comes along afterwards just due to end-user demand.

Leo: Well, but as we know from other software quote "removal tools" that the spyware companies gave us, you can't always trust them to do the right thing and remove their software properly.

Steve: Well, and here's an interesting issue, too, Leo. Will the current anti-spyware and future anti-rootkit scanners label this as a rootkit?

Leo: Right. Because of course in the past they've bowed to commercial pressures and said, oh, well, I guess it's not a rootkit if Sony's doing it.

Steve: Yeah, I mean, so in terms of the standard non-supertechie rootkit scanner stuff, the stuff that the typical end-users run, will it deliberately ignore the Sony DRM rootkit and not tell somebody that it's on their system...

Leo: Just appalling.

Steve: ...or not?

Leo: It's just appalling. And in fact it ought to because it's not - whether you think Sony's benign or not, it's not merely Sony protecting its DRM. It's so badly done that it gives a backdoor to any hacker who wants to hide files on your system.

Steve: And has been known to create unstable booting situations where people are getting blue screens every so often when they boot, for reason of not being able to find this aries.sys driver.

Leo: Once again, I'm going to go out and run RootkitRevealer on all my systems and make sure I didn't accidentally install it. And if I find any Sony/BMG disks, I'm going to put a pile in the backyard. Anybody wants to bring theirs over, we'll be burning them later tonight.

Steve: Well, and if nothing happens between now and next week's Security Now! podcast, we'll do our third installment on how to be really, really secure with wireless networks.

Leo: Good. Unless something else breaks. Yeah. But that's part of the mission of this show is to give you the latest breaking news, as well as, of course, tutorials on all of the fundamentals of security.

More information on this topic and all of our Security Now! podcasts, both in high-quality and 16KB versions, as well as transcripts, are available at Steve's site, GRC.com/securitynow.htm, that's the URL. Steve, I want to ask you to update the podcast URL on your page to - the redirect that I use never changes, it's leo.am/podcasts/sn. It did point to a site which has been changed. So make sure you use, if you subscribe to this podcast, leo.am/podcasts/sn. And...

Steve: I'll do it right now.

Leo: Yeah, because we want to make sure everybody gets a copy of this particular episode of Security Now! And iTunes has it right. All the other places, if you subscribe through My Yahoo!, iTunes, Odeo, PodNova, they'll all get you the file. And of course you can always get the latest file at GRC.com/securitynow.htm.

Our thanks to the good folks at AOL Radio for broadcasting Security Now! on their podcast channel and hosting our files for free so that everybody can get a copy of it: AOLmusic.com. Thank you, AOL. And thank you, Steve Gibson. Your information couldn't be more timely. This is important stuff.