Unbreakable WiFi Security

Description: Leo and I follow up on last week's discussion of the Sony Rootkit debacle with the distressing news of "phoning home" (spyware) behavior from the Sony DRM software, and the rootkit's exploitation by a new malicious backdoor Trojan. We then return to complete our discussion of WiFi security, demystifying the many confusing flavors of WPA encryption and presenting several critical MUST DO tips for WPA users.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-013.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-013-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, lucky Episode 13: Wireless Encryption Part 2.

Steve Gibson is back, the hero of the hour. Did you get a lot of calls about the Sony rootkit?

Steve Gibson: Yeah.

Leo: I mean, whew, this was a big story. We covered it last week. If you missed it, do listen to Episode 12. This is the copy protection scheme Sony is putting on some of its - Sony and BMG Music are putting on some of their audio CDs that is a hacker toolkit.

Steve: Well, and in fact, Kaspersky Lab reports today in their virus news that there is now a new backdoor Trojan program using, that is, leveraging the Sony DRM rootkit to hide itself in users' systems. If it gets into the system - they're calling it Breplibot.b, I don't know why, but it's about a 10KB size file that renames itself sysdrv.exe.

Leo: And as we know from last week's episode, if you have the Sony copy protection on your system, any file named sys will be rooted, rootkitted. It'll be invisible to every tool.

Steve: Right, any file beginning with the sys string just disappears. So we already see - I mean, and we predicted last week that this was going to happen, never having seen one, that this was a serious potential danger for what Sony had done because, rather than only protecting specifically its own files, the authors of this - that were not Sony, they used a subcontractor - the authors arranged to cause anything beginning with the string sys to disappear, including registry keys and any kind of files that are stuck on the file system...

Leo: That's just so sloppy. I can't believe they'd leave that hole on there. Now, how does this Trojan spread?

Steve: It looks like it spreads by spam email messages.

Leo: Oh, so opening an attachment.

Steve: Tricking people into loading it.

Leo: Okay. So don't download files or...

Steve: And it apparently opens a back door on the user system.

Leo: Don't download files from unknown sites, open attachments. Be very careful. Now, here's a question for you, and a number of people have asked me this. There are some anti-spyware programs that claim to detect the Sony rootkit. Kaspersky must be able to. If it's a rootkit, how can they do that?

Steve: Well, they're able to - well, for example, the Sony rootkit is easily detected. You could simply rename a file to sys.

Leo: Oh, yeah.

Steve: If it disappears, you know you've got the rootkit on your system. You don't even need to use RootkitRevealer, as we were talking about now several times, in order to do a scan of your whole system.

Leo: Yeah, somebody, shortly after we put out the podcast, mentioned that and said he's created a file on his desktop called syscanary, like the canary the old miners used to take down. If that...

Steve: And if it ever disappears...

Leo: If it disappears, you've got trouble. So, okay, so it's easy to detect. Is it easy to remove?

Steve: That's the problem. Now, Sony - there's been, you know, we were part of the initial uproar at this time last week. In fact, you know, we did our podcast a day early because we wanted to make sure this message got out as quickly as possible. Sony has responded to the pressure. They're doing some butt-covering PR spin, saying that there's really nothing wrong with it, but we'll put something on our site that people can use to remove the hiding behavior. The DRM technology stays there, but the hiding behavior at least will be - it'll be shut down.

Now, the other revelation since last week is that Mark at Sysinternals has confirmed a report that he heard. And I have not yet myself - I've ordered one of these CDs that I'm going to be infecting myself with here in a couple days because I want some firsthand experience of this myself. But the Sony technology is also phoning home. It uses the user's Internet connection on the fly, when they're listening to any of the disks that they've purchased using this built-in player. It sends a message back to Sony saying that this particular song or album is being played. Apparently this is for some sort of, like, banner rotation technology that it has to present something to the user. But the problem is this is classic spyware phoning home behavior. It is not disclosed by Sony. And in fact, Sony specifically says that's not being done, yet it's been found in packet capture traces. And Sony's saying, well, but if we're doing it, then we're not keeping any of the information.

Leo: We're not doing it, but if we were to do it, we wouldn't keep it. How can you trust a company that does that? That's terrible.

Steve: Oh, it's so bad.

Leo: All right. So this isn't the primary topic of our show today, but we did want to kind of update you all on that. And so what should we do? I still am kind of baffled about all that.

Steve: Well, I think it's a function of how concerned individual users are. You know, our goal here with these

podcasts is not to tell people what they have to do ever, but to say, look, here's the truth about what's going on. You decide for yourself how concerned you are. As long as somebody knows that this content-enhanced Sony CD technology is installing technology on their system which does allow known Trojans to hide themselves, well, okay, if that's what they want, I have no problem with that, as long as they know.

Leo: Right, right.

Steve: So, you know, we do know that you can go to Sony, you can submit your email address to them to get a link for a remover which will remove this from your system. So you've got to go through some...

Leo: You can't get it any other way? You can't...

Steve: ...in order to get this removed.

Leo: You can't just go to XPC Aurora and download it? You have to...

Steve: I guess - I think you can do that, too. And get this removed from your system. Then, if you ever make the mistake of installing one of these Sony audio CDs into your computer, as you said last week, Leo, hold down the Shift key.

Leo: Right.

Steve: Or, if you're a more security-concerned user, you might have already disabled the CD autorun feature in your system, which otherwise causes this thing to present you with a EULA. If you ever see the End User License Agreement because you forgot to hold down the CD, decline the installation and, you know, play the CD normally, or hold down Shift when you put it in to prevent this thing from being reinstalled.

Leo: Right. Okay. It's too bad. And I hope, you know, there are lawsuits, class-action lawsuits. I suppose some aggressive district attorney in some state or country might actually go after them for...

Steve: I think there is some governmental action I heard in Ireland somewhere. And there's an ambulance-chasing class-action-happy law firm in San Francisco that's filed against Hewlett-Packard and Toshiba and everybody you can imagine. And they're, you know, rolling up their sleeves to go after Sony now.

Leo: Okay. So, you know, and I have to say I'm actually pretty disappointed with Sony's response to this. They have minimized consistently. They've lied, obviously. Well, it sounds like they've lied anyway about the phoning home issue. And they're really not taking responsibility in a way that I would hope they would.

Steve: Well, it's certainly been a good object lesson for other people...

Leo: Yes.

Steve: ...who will hopefully not follow in Sony's footsteps.

Leo: Yes.

Steve: And, you know, I don't think we've seen the end of this. I'm going to take a look at the CD myself. I may have one suggestion next week, in next week's podcast, which you and I will be doing from Toronto

again.

Leo: That's right, yeah.

Steve: Otherwise, I think this issue is behind us.

Leo: All right.

Steve: Anybody who's interested, by the way, can just put "Sony rootkit" into Google and stand back.

Leo: You'll find plenty about it.

Steve: Yep.

Leo: Well, yeah. And it was kind of timely because we had just talked about rootkits. So I'm glad we had talked about them because then, lo and behold, it became an issue, so. But we had also started a conversation about protecting yourself on a wireless network, and that's a very important conversation day in, day out, as well. So let's get back to that. When last we spoke, we pretty much debunked the notion that MAC address filtering had any impact on security. SSID hiding, useless. WEP encryption broken and next to useless. It sounds like the best way to do this is WPA.

Steve: Yes.

Leo: In fact, the only real way to secure a wireless network is with WPA.

Steve: Yes. Just to clarify the issue of SSID and MAC filtering, because I got a lot of mail from people after I said, you know, it was not useful for security, complaining about my position on that. So...

Leo: Wait a minute. Wait. How could they complain about your position on it? What you were talking about is factual.

Steve: Well, yeah, but...

Leo: Do they dispute that at all?

Steve: Well, I guess maybe the problem is what I mean by security. MAC address filtering and SSID hiding, and also changing the SSID from the default, which typically is Linksys or D-Link or Netgear or whatever, those are useful for preventing inadvertent use of your access point by a neighbor who just has, you know, not implemented any security themselves. Many people were of the feeling like, hey, you know, encrypting my home network is a pain because I have...

Leo: More of a pain than MAC address filtering? No, that doesn't make any sense. In MAC address filtering you've got the MAC address of each device you have to enter in. You enter in the password once in WPA encryption, and that's it.

Steve: Well, but, for example, if, you know, what I'm citing from people is they've got friends who come over with a wireless laptop who want to use their access point.

Leo: Yeah?

Steve: So I guess, you know, somebody who's into this is able to add their MAC address of their wireless NIC on their laptop to their permissions list on their access point. They know how to do that flexibly and so forth. They don't have to modify their friend's laptop at all.

Leo: Just give your friend the password, and he can log in.

Steve: I know. I know.

Leo: It doesn't - it's not logical. These people are not being logical. You either...

Steve: No. What I want to clarify is that...

Leo: All right.

Steve: ...the use of MAC address filtering is not secure, nor is SSID hiding or changing your SSID from the default, because both of those are easily obtainable just by sniffing the air.

Leo: Right.

Steve: However, they are useful to prevent inadvertent use by a neighbor of your access point. So...

Leo: I have an analogy for this, Steve.

Steve: Okay.

Leo: Let's say you don't want to lock your door because you want your kids to come in and out of your house freely. So you don't lock your door. You have no security. But just to kind of discourage burglars, you put a big sign out front that says you have an alarm system. Now, in fact, you don't have an alarm system, and the door isn't locked. But you've put a sign up that says you do. That's that kind of security. I think it's not particularly logical. If you ask me, give your kids a key and lock the door.

Steve: Well, again, it's not secure. It prevents...

Leo: It's pretending to be secure.

Steve: Well, maybe we need another word. I mean, it's very weak authentication is what it is. And authentication is different from security.

Leo: Okay.

Steve: It's not authentication of your wireless devices that cannot be broken, which is to say even that can be breached. But it's weak authentication, which is better than none if you want to prevent your neighbors from inadvertently using your system. But it should never be confused with security, and that's what we're going to talk about with WPA.