SECURITY NOW!

Transcript of Episode #7

SPYaWAREness

Description: Any contemporary discussion of threats to Internet security must discuss the history, current situation, and future of spyware. Leo and I spend a little more time than usual covering many aspects of this important topic. DON'T MISS the Episode Notes Page for this episode!

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-007.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-007-lq.mp3

Leo Laporte: This is Security Now! Episode 7 for September 30, 2005: Spyware.

Steve Gibson is on the line, once again using Google Talk, although we've got evil plans afoot to create our own client, which would be kind of cool. Welcome, Steve.

Steve Gibson: Hey, great to be back, Leo.

Leo: Steve started ShieldsUP! many years ago as one of the first security applications on the Internet, and shortly thereafter discovered something he named called "spyware." How did that happen?

Steve: Right, well, ShieldsUP! was only about four or five months old, and I was sort of, you know, then involved in and getting more and more involved in the whole security on the Internet space. And in fact I was beta testing ZoneAlarm before it was made publicly available. The guys at Zone Labs knew of my work with ShieldsUP!, and they liked it, and they said, hey, you know, take a look at this firewall. Well, what was significant about it is it did outbound blocking, that is, unlike all other firewalls at the time - actually I think AtGuard was also there before. But the idea was it would catch programs that were using your computer connection without your knowledge. And something was on my machine called TSAdbot.

So shortly after running ZoneAlarm, I discovered I had something that was connecting to somewhere. I tracked it down, and it was something that was - for a while it was included in the Windows version of PKZIP for Windows that I was trying. And so, you know, it was in the early days. Well, this freaked me out because I'm one of these people who pretty much feels like he knows everything he's got on his computer. I watch my machine very carefully. So that was the first event.

Then a couple weeks later there was news of something really bad that was installing itself in people's machines. People were finding it by DLL name. It was called Aureate. So I created something called OptOut that was the very first anti-spyware tool. And that's where the name got coined, or the term "spyware" came out of that work. And OptOut was super popular because this company, this Aureate company, was bragging that they were installed in 25 million machines worldwide, and all kinds of freeware was including this thing. The idea was that it would be like the next advertising model. Just the same way that you have ads on the web, they were going to put ads in freeware applications, and so the freeware authors would get paid back by this central advertising agency. The problem is that it was profiling what you did, watching your connection, and sending this data back to them, all without the user's permission. So...

Leo: Yeah, in the early days, I mean, I guess it was relatively benign, I mean, if you're going to put ads in software to support the author, and it was because shareware wasn't working very well. You'd have to monitor the clicks on the ads, and you'd have to replace new ads, so it would be reasonable to have a program that did that in the background.

Steve: Oh, and I don't - I really, to this day, I don't think these guys were ever doing anything wrong, except they weren't asking.

Leo: Right.

Steve: In fact, part of that was the reason I trademarked the phrase "It's MY Computer." Because more and more it seems like people are forgetting that, you know, these are our machines, not their machines that we're just borrowing.

Leo: Yes, that's right.

Steve: So, and exactly as you say, more and more now, of course, the scene has changed. Back then, OptOut was able to scan the machine, find these bad files, and remove them. It turns out that we got feedback that it was fixing people's computers because, for example, after running this freeware, which unbeknownst to them installed this Aureate stuff, suddenly their machines started acting strangely. The problem was the spyware was buggy, and it was a BrowserHelperObject, one of these things called a BHO, which IE can have attached to it, which caused Internet Explorer to load this every time you ran IE. Well, it was buggy, and it was crashing people's machines and Internet Explorer. So OptOut, by removing the software, fixed these problems for people. Well, it turns out that, I mean, it was just a matter of removing the DLLs, and there were no other consequences. Today's...

Leo: Although there was one problem with the spyware, which would be that you would uninstall the original program, PKZIP or whatever, and the adware would stick around.

Steve: Well, now, that's exactly right. And that was one of my real complaints was that, not only did people not know this had been installed, but if the problem occurred, and then they uninstalled the original application that brought this into their system, by design this adware stayed behind. The instructions from this Aureate company were, when you uninstall your freeware, leave our components, these adware/spyware components behind because they're shared components, and more than one freeware utility might be using them.

Leo: Well, in their defense, that's not unreasonable. If somebody's relying on your DLL, you can't assume that, if you're being uninstalled, nobody else is going to want you.

Steve: That's true, although of course it had the side effect that people would undo what it is they had done, that is, they would uninstall a program that seemed to have hurt their computer, that wouldn't make it better because a piece of the program, this spyware, stayed behind.

Leo: A good point.

Steve: And it was using their machine behind their back.

Leo: And that's the real bottom line, is it should be asking. It is your computer.

Steve: Well, exactly. And, you know, when confronted with this, they said, oh, we tell our developers that they must present the user with a dialogue box that says this is what's going to happen, you know? And if you look at some of the software that was bringing this Aureate stuff around, you know, yeah, nine scroll pages down in the fine print there's something about and, you know, we're bringing some, you know, in order to offer this free software to you we're enhancing it with ads, which are provided from the Aureate

Company. And then in order to provide the ads it must contact the Internet in order to get new advertising material to present to you, blah blah blah. Well, you know, I've tried to read those license agreements. It's not possible.

Leo: Forget it.

Steve: You just say, okay, fine, whatever you're going to do to me, just fine, click next, and you go on.

Leo: Well, you know, those seem like innocent days now, if you fast-forward to 2005. Those things were nothing compared to what we're getting now.

Steve: Oh, Leo, today what's happening is there's like - in the same way that we've seen an escalation in the war between viruses and anti-viruses where, like, viruses were getting more fancy, they're becoming polymorphic, where they're deliberately trying - they're, like, the viruses themselves are working not to be catchable by the anti-virus software. Similarly, this spyware, there's a spyware and anti-spyware back and forth. And so, for example, spyware is adopting technology known as rootkit technology, which is, you know, from the original days of hackers that were trying to surreptitiously install stuff in people's machines that could not be found.

The idea is that an operating system is sort of like the foundation of the way the system operates, and applications run on top of the operating system. And so there's this inherent division between the user space and what's called the kernel space, with the kernel space being down below doing all the work on behalf of requests from the applications. What rootkits do is they actually get their code down into this kernel space, becoming part of the operating system and altering its behavior. So, for example, when an anti-spyware scanner runs to scan someone's machine, looking for a long list of files that are known filenames of spyware that it's searching for, if spyware has beaten it into the system, gotten there beforehand and installed this newer rootkit technology, the spyware itself can lie on behalf of the operating system to anyone who asks what's on the system. So, for example, even a user doing a directory listing or looking at the contents of their system won't see the files. They're literally being hidden by this operating system extension. And...

Leo: You know, I can understand why a virus would do that. They want to hide. But what is the percentage in an advertising company doing that? Don't they know that that's going to, I mean, that people are going to consider them viruses, not ads?

Steve: Yeah, I mean, certainly once upon a time, you know, we were worrying maybe about cookies or beacons, or people were annoyed just by ads on web pages. I mean, you know, the problems that people focused on have evolved over time. And, arguably, spyware has become the number one problem for people using the Internet, most typical people using the Internet. I've got friends who are computer consultants. They now specialize in spyware removal.

Leo: Yeah. I'm sure most people listening to this podcast know exactly what you're talking about. When your friends and family call, that's what they want you to do, basically.

Steve: Right.

Leo: If they're using Windows, they almost undoubtedly have spyware.

Steve: Well, and I think that one of the reasons is that, if we were to create like a distinction between what's a virus or what makes a virus and what makes spyware, the division would be that viruses have typically been created just by, you know, young hackers with time on their hands who wanted to see if they could do it. There was no economic motivation for them, for the virus authors. It was just a matter of, you know, I'm going to see if I can create something that will live, have a life of its own among machines on the Internet, if it can get in the machines and propagate. And, I mean, it's an interesting fact that, you know, very few viruses have been deliberately malicious. You know, people are finding viruses on their machines all the time...

Leo: Lately, anyway. Lately.

Steve: ...which means that those viruses are not destroying their computers.

Leo: Right.

Steve: The viruses are not being nearly as deadly as they could be. So the flipside of that is spyware, where there's always been an economic motive...

Leo: Right.

Steve: ...behind the software. I mean, from the very first moment that TSAdbot that I found from a company called Conducent, this Aureate spyware, there's CoolWebSearch, there's Gator, there's Cydoor, there's, you know, a long list of economically driven installations. And I think that's one of the things that has kept the anti-virus companies from responding for so long. I mean, we've had anti-virus stuff for years. And it really took Microsoft to step into this anti-spyware market to bring the other companies around, I think because you could argue, well, maybe somebody wanted CoolWebSearch. Maybe somebody wanted Gator or Cydoor or one of the things. I mean, the point is there were...

Leo: That's certainly what those companies argue. They say, look, people are asking for - this is - we're not spyware. We're doing what people want.

Steve: We're enhancing their web experience.

Leo: Right. And I can see why companies would have been reluctant because they'd be afraid of getting sued. Gator, very famously, has gone after people.

Steve: Well, exactly. And, in fact, one of the things that I did was, when I started to roll up my sleeves about the problem, was I created a list of known and suspected spyware, and immediately began getting angry letters from these companies...

Leo: Yeah.

Steve: ...saying, hey, you've got us listed on your page of bad stuff. We're not bad. We're good.

Leo: Did anybody ever sue you?

Steve: No. Because, you know, that's just not a battle that I'm in a position to fight. So I said, okay, fine, I will remove you pending further research.

Leo: Right.

Steve: And what happened was a great company, Lavasoft, created essentially the next in line, if you want to make OptOut first, my own little freeware tool, they came along with Ad-Aware. And they were out of the United States, so they were, you know, much harder for anyone to actually sue. And they created a great little scanning tool. I had a dialogue with them, and I said hey, you know, my real focus isn't on this malicious software stuff. I want to stay over on the Internet security side. If you guys will promise me you'll always have a free version, I'm going to formally endorse you guys and, you know, turn this chunk of stuff over to you. And of course they've just been doing a fantastic job.

Leo: So we have you to thank for the fact that this is free. And that explains why both Spybot and Ad-Aware were originally from Germany.

Steve: Exactly.

Leo: They didn't have to worry about the lawsuits.

Steve: Exactly.

Leo: But now everybody acknowledges that spyware is evil.

Steve: Well, as Microsoft has now gotten into the game with their anti-spyware tool, that sort of legitimized the notion that this is bad stuff. And people, again, you know, following my trademarked phrase, "It's MY Computer," people are saying, I don't, you know, I want a choice of whether to have this stuff installed on my computer or not.

Leo: Reasonably so.

Steve: And of course, you know, you made the point about removal, which has become such a problem. One of my employees got, I think it was this CoolWebSearch or Jiffy Search or some random thing, attached to her Internet Explorer browser. My tech support guy ran the various scanners and removers. It apparently removed the file, but in the process it destroyed her Internet connectivity for that machine.

Leo: That's frequently the case. These things are - they've got their grip so tight on your system that removing them can often break your system.

Steve: Yes. Well, you can sort of think of it like links in a chain, where from the Internet to your eyes there's a whole series of different phases that the data goes through. The spyware installs itself as a new link in the chain in order to monitor data coming in, add its own data, and monitor what the user's doing on the way out. So it's very much involved in everything going on with the Internet. So when an anti-spyware tool comes along and simply deletes the files that were part of that link, well, the chain is broken because, in order to install itself, it had to make modifications to the system deliberately to get itself in there. So when you simply delete the files that the system has now become dependent upon by virtue of the installation, you break that chain. And suddenly, you know, this user's off the Internet.

So removing this stuff has become a real problem. You simply can't delete the files. Some of the spyware companies have their own, you know, if you really want to take Gator or Cydoor or CoolWebSearch or whatever off your machine, you know, here's our uninstaller tool, which will do it. And generally that will function because they know how to put the chain back together without, you know, after removing that link.

But one of the real problems of course now is - and this is why it takes days sometimes to get spyware off a machine is that there's often multiple types of spyware. Spyware is now really fighting users who are trying to get it off the machine. I mean, it's become an escalating battle. And often you just, you know, users are stuck with reformatting their machine and starting over.

Leo: Unbelievable. Unbelievable. So you can't really say there's any one way that spyware works. It works in all the different ways that viruses can work. And but can you say - is there a way to kind of prevent it? Is there a behavior that users should have to not get it in the first place?

Steve: Spyware gets into machines because it's bundled with software. And in fact that's become - that was always the original entry vector for spyware. You know, just exactly as I said, where I with a very early version of PKZIP for Windows brought along that Conducent adware, this advertising-enhanced spyware has been the original way stuff got onto your machines. And in fact you'll now see download sites, reputable download sites, or even freeware will explicitly say this is really, really free. We don't include - there's, you know, no other stuff, no spyware, no adware, nothing bundled in with our tools, because so many companies for a while were trying to do that.

Leo: Is there one kind of software that's, I mean, I know music-sharing software, Kazaa, for example, tends to install a lot of other stuff on your system. Is there a particular area that you should watch out for?

Steve: Well, there is downloading freeware and running freeware...

Leo: A lot of freeware.

Steve: You want to make sure that this stuff is really spyware clean. So I still think that that's generally the way people get stuff on their machine is by running software which has this malware attached to it.

Leo: Right.

Steve: So use reputable sites, you know, Download.com, CNET...

Leo: SnapFiles.

Steve: That's the one I was trying to - I was drawing a blank on that. SnapFiles, you know, sites that really take responsibility for the quality of the software. I would say that's number one. In general, when systems have been really massively infected, there is music-sharing software present.

Leo: That's very common, yeah.

Steve: There's Kazaa, there's iMesh or whatever. I think...

Leo: Whether it comes from Kazaa itself or comes from downloads that you're doing with Kazaa.

Steve: Well, exactly. I think that it's - very often it's the behavior of the people who are, you know, they have a behavior of sharing music, and along with that goes, oh, let's just go get software from wherever, it doesn't matter.

Leo: Right.

Steve: Now, I mean, if you treat your computer like a toy, like a little entertainment toy, then that's what it's going to become. It's going to get infested with this stuff. If your computer is a tool that you really want to keep running in good shape, you have to treat it with respect and recognize that there's just a lot of bad stuff out there. And on the Internet...

Leo: I'm going to recommend a wonderful website. There's actually two very useful websites in this area besides your own, which is SpywareInfo.com and SpywareGuide.com. And I use SpywareGuide to look up software before I install it because they have a very complete list of programs that contain spyware.

Steve: Yeah.

Leo: And so it's a good idea to check before you install something. And SpywareGuide.com - we'll put these links in the Show Notes.

Steve: Yeah, I think that's great advice, Leo. And again...

Leo: How about infection from the web? Does that happen by just going to a website? Is that happening now, as well?

Steve: Well, yes. We have the problem from day one that - well, I guess it wasn't one because browsers used to be safe. What happened is that. in this goal towards making the web more seamless and providing enhanced services, web pages have, of course, not been static for a long time. They're just not, you know, dead pages that you read. Instead, more and more they're doing more stuff. Netscape gave us JavaScript, introduced the notion of scripting to web pages. Well, that was the first problem. Microsoft, unfortunately, when they were early on competing really ferociously with Netscape, they took the technology they had, which was ActiveX technology, and essentially brought it to their browser, so that when you visit a website, this ActiveX technology uses either the Java scripting or Microsoft's Active scripting to download code, without asking you, from that website and running it on your machine.

Now, in a perfect world, that's very cool because it means that, essentially, they've granularized software, and websites become application servers, so users can do all kinds of advanced things. The problem is, as we well know, it's not a perfect world. So you can have malicious code, which is also downloaded into your machine, just, I mean, in all the same ways that we've been talking about malware getting into your machine by piggybacking on freeware, now with Microsoft's formal blessing, just going to a website that has malicious intent can install stuff on your machine. And in fact that's the way people get these browser add-on things. You know, I mean, they're constantly getting them. They're getting reinfected. They go, what do I do? How do I keep from getting this stuff on my computer? I'm not installing anything. I'm just going to websites. And that's all it takes.

Leo: So how do you prevent that?

Steve: Well, certainly not using Internet Explorer immediately solves this problem with ActiveX because Internet Explorer is the only browser that is - now, I should also say Internet Explorer or any of the IE variants. There are a number of other browsers, sort of non-mainstream browsers, that are really still IE, they just put some different window dressing around it. For example, they'll add tabbing features or various other things to the IE core, but it's still really IE. So, for example, Opera, which is a completely non-Microsoft browser, or any of the Mozilla browsers, you know...

Leo: Firefox or...

Steve: ...the Firefox of course being the most popular.

Leo: Those don't have ActiveX. You can actually add an ActiveX plug-in to Firefox, which seems like a bad idea. But normally they don't have ActiveX, and they don't have active scripting, which is another problem.

Steve: Right. The problem, of course, is that there are some sites, notably Microsoft's own, you know, Windows Update site and those things, that still do require that you have IE. So you're probably still going to have it on your machine. Certainly it came with. But for most of your browsing, if you stay away from Internet Explorer, and you use a non-Microsoft browser, you're not going to have the problem of this stuff getting into your machine all the time just by visiting websites. Then...

Leo: So update, use - that's very important, too, Windows Update regularly, use Internet Explorer for that, but then don't use Internet Explorer for anything else.

Steve: Right, because the second way things get into your machine - the first is by formal policy. The second way is by defects that are known in browsers. There are historically many faults in Microsoft Windows browsing technology where, again, just going to a website that runs some scripting on your browser, I mean, I'm just fundamentally anti-scripting. There are ways we could have done most of the things we do with scripting without using scripting. The problem is, I mean, scripting is code. It's sort of, you know, semi-tamed, neutered code, but still code. And mistakes in that scripting technology can be exploited and are exploited so that just visiting sites can infect you by taking advantage of known problems with Internet Explorer, most of which have already been fixed. So keeping Windows updated is the way to keep those things from crawling into your system just by visiting a website.

Leo: So update, use Firefox. Should you use anti-spyware software, as well?

Steve: I know that most people are. And so I would never want to recommend against it. I'm, you know, I like to keep myself as simple as I can. The top three anti-spyware tools that, used in conjunction, generally find everything - I'm not going to say they always do because, again, it's an ongoing battle back and forth. But no one tool does as good a job in terms of covering the landscape as using multiple tools: Microsoft's own anti-spyware, which is still in beta, but clearly they're committed now to getting into the removing the stuff market; the very first scanner that followed OptOut, which is the Lavasoft Ad-Aware anti-spyware; and, finally, the Spybot Search & Destroy which you mentioned, those are the top three. Many people run all three of those from time to time, scanning their machine to make sure that nothing has gotten into their system.

Leo: And the good news is all three are free, although the bad news is Microsoft has for some reason decided not to support Windows 98 and ME with their anti-spyware solution. You have to have XP to use it, which is too bad.

Steve: Yeah. The flipside is that most of the newer spyware, since the market has moved so strongly to the Windows 2000, XP, 2003 and so forth platform, we're beginning to see these older machines aren't getting infected because they're just too old.

Leo: Oh, interesting.

Steve: They don't have these problems. They don't have the technologies that are now being leveraged against users who have them. The one last thing I ought to say, because frankly it's what I do, is the idea of running - and we're going to talk about this in future Security Now! podcasts because I think there are ways to make this more feasible, and that is locking down your browser, essentially disabling scripting completely so that sites are unable to run code on your computer. Now, for the majority of sites you visit, that's not a problem. But some e-commerce sites, certainly Microsoft's site that's trying to do active things, there are sites that require scripting. So the reason this is a problem is by locking down your browser you are definitely breaking some sites that have become scripting dependent.

So in Internet Explorer they have this notion of zones, where you have a trusted - you have the so-called Trusted Zone and the Internet Zone. And what you're able to do is you're able to manually put the web domains of sites you trust into your Trusted Zone, so IE is sort of like a chameleon. It will dynamically change its settings depending upon where you go. You could, if you trust Amazon.com and eBay.com and your banking domain and some e-commerce sites, you know, PayPal, for example, you put a list of all the places you go that you trust and that need scripting in the list of trusted sites. And then you lock down the Internet zone so that most sites are unable to do anything to your browser.

Leo: Or you just...

Steve: And that's really the safest way to function.

Leo: Or you just don't use Internet Explorer.

Steve: Or, exactly. Although, you know, in fairness, we are now seeing exploits against Firefox because it's now becoming popular enough...

Leo: Right.

Steve: ...to be a target. So, I mean...

Leo: But it's harder to do with Firefox because you don't have the benefit of ActiveX; right? I mean...

Steve: Yes. Certainly in terms of one thing people could do that would generally make them safer is to use Firefox. And Firefox is a great browser.

Leo: Yeah. There are other tools that modify your system and protect you. In fact, I think it's important to turn on the immunization features of Spybot Search & Destroy and the real-time protecting in Microsoft's anti-spyware because both of those kind of are more active in preventing spyware infections. And frankly, as you pointed out, once you get spyware, it can be dang difficult to get rid of it.

Steve: Yes.

Leo: Much better not to get it in the first place.

Steve: In the long term, we're going to have to see some evolution of the operating system itself. The problem is we're still bringing along sort of this historic presumption that all software is good, that all software is something that you want to run. And the fact is now for, you know, a decade, that's not been true.

Leo: Right.

Steve: Viruses are software we don't want to run. Malware, spyware, software we don't want to run. But, you know, that's out there now. So our operating system is still designed to run everything with the presumption that it's good software. That has to change. And over time, you know, ultimately that's what we're going to have to see changing.

Leo: Well, Steve, you know, unfortunately there's no, you know, great answer right now except to change your behavior, you know, maybe change some of your software and run anti-spyware. Do you think victory against spyware is possible in the long run?

Steve: In the long run I really do. It's going to - as always with security we're going to be trading off convenience for safety. You know, adding a personal firewall makes you safer because you'll know if something is in your machine trying to phone home. But it means that things are popping up. It means that you have to give applications permission to use the Internet. Clearly, that's a burden. Actually it's why Microsoft hasn't done that so far, and the third-party firewall technologies do. So there we've had to trade off convenience of just assuming that, you know, all software on the machine is good for being much more careful and safe. So the future I think we can presume we're going to see even more tradeoff of convenience. But, you know, anyone who's had a real spyware infestation on their machine will say, bring it on. I don't want the spyware.

Leo: It's terrible.

Steve: I'm willing to take more responsibility.

Leo: Right. And the other side I should mention because I don't want to leave this out. People who are using Macintoshes don't yet have anywhere near the spyware issue. Not that that will continue that way. But for now there are some anti-spyware programs on the Macintosh site, but they're really not necessary.

Steve: Yeah, and that's a good point. We're beginning to see Apple, you know, in the second Tuesday of the month patch cycle, bringing, you know, finding problems...

Leo: They do it more often than that even, actually.

Steve: Yeah.

Leo: They do it pretty regularly.

Steve: Yeah.

Leo: But most of the time they're exploit patches, not specifically spyware patches. Although, you know, I think it's only a matter of time before people start targeting the Apple platform. I think it's a little bit more difficult to infect, fortunately. Just like Firefox, you don't have the same kinds of ActiveX and active scripting technologies.

Steve: Right. And if we resume that the model will be spyware and viruses, viruses generally are written by people just, you know, because they want to. And they write them for the machines they have.

Leo: Right.

Steve: Most of the young malicious hackers have Windows machines, so they write viruses for Windows machines. And, frankly, there's a huge, now, base of technology for virus writing that...

Leo: Makes it easier.

Steve: ...supports that creation.

Leo: Now, you say "viruses," but you're including spyware when you say "virus."

Steve: Well, no, I was deliberately meaning viruses.

Leo: Oh, okay.

Steve: Because, as opposed to spyware, you might imagine spyware would happen for computers over on the Mac side because of the possibility of a real economic incentive.

Leo: Right.

Steve: Whereas viruses, I don't think so so much.

Leo: Right, right, right. Well, it's always great to talk to you, Steve Gibson. We thank you for all your good work and for sending this information along. I know you've created a page talking about spyware. And that's available online at GRC.com/securitynow.htm, as are all the back issues of Security Now!, both in high-quality 64KB MP3, as well as 16KB MP3, for those people who have slower bandwidth or smaller storage media. Steve likes to play stuff back on his Palm. I think that's why.

Steve: Yes, I'll mention that, for people who've been following along so far, this last week the Security Now! page got a huge facelift. We've added some more features. We've always had text transcripts. Now they're also in a really nice HTML format that is easy to view. And that page is turned into a PDF. And every single episode has Show Notes. In this Episode No. 7's Show Notes is a whole bunch of stuff that's worth taking a look at, too.

Leo: Oh, that's fantastic. We thank Mark Blasco of Podcastthemes.com for our new theme. I hope you enjoy it. And of course America Online's podcast network, American Online Radio at aolmusic.com, for providing the bandwidth for Security Now!. Steve Gibson, thanks. We'll talk again next week.

Steve: Looking forward to it, Leo, thanks.