SECURITY NOW!

Transcript of Episode #97

Operation: Bot Roast

Description: Steve and Leo discuss the recent news of the FBI's announced crackdown and pursuit of "bot-herders" who individually control networks of remote control DoS and Spam zombies numbering in the many tens of thousands.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-097.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-097-lq.mp3

INTRO: Netcasts you love, from people you trust. This is TWiT.

Leo Laporte: Bandwidth for Security Now! is provided by AOL Radio at AOL.com/podcasting.

This is Security Now! with Steve Gibson, Episode 97 for June 21, 2007: Operation Bot Roast.

Time for Security Now!, everybody's favorite security podcast - are there any others? - featuring the great security guru, my personal friend and hero, the man, the myth, the legend, Steve Gibson. How are you today?

Steve Gibson: The myth. Yes, I'm just a...

Leo: The mythical Gibson.

Steve: ...figment of everyone's imagination. Actually, you know, from the email that we receive, I know that there are other security podcasts. In fact, there's one that was...

Leo: There's quite a few.

Steve: Yes, exactly. But I do hear people saying that the one stands alone from the others. And actually I've been driven to be a little bit curious about what they have meant by that. And so I've listened to some of the other ones. And, you know, they're different than ours in...

Leo: They're different, that's it, exactly.

Steve: Yeah, they're different. And so, you know, to each his own.

Leo: And it doesn't hurt, you can listen to as many as you want. CNET does a security podcast. I have a friend actually in town who does a security podcast. So there's, you know, everybody needs to get as much information about this as they can.

Steve: How many gigs do you have free? We'll fill it up.

Leo: Plenty. So today we're going to talk about - in just a bit we're going to talk about an FBI operation that just recently came to light, and some amazing statistics.

Steve: Yes, Wednesday before last the FBI broke the news of what they called "Operation Bot Roast," which is...

Leo: In an uncharacteristically humorous thing.

Steve: Yeah, it's good.

Leo: I'm impressed. You don't think of the FBI as being jokesters. Operation Bot Roast. Do we have any addendum, errata that we want to cover before we go to the subject at hand?

Steve: We do indeed. There was an errata that I picked up from Justin Alcorn. And he's in Cleveland Heights. He writes, "During Episode 96 Q&A you answered a question about SPF." And of course I remember that. He said, "Everything you said about SPF records was correct, except you didn't answer his question. He had the opposite problem. His problem was that his ISP was dropping email to him because his ISP had implemented an SPF check on incoming mail." You may remember that this was a guy whose brother had, like, created a family domain. And his brother's server was simply redirecting the email from it to the ISP.
I'm surprised...

Leo: Yes, I think I twisted it around because my problem is the opposite.

Steve: Yeah, and I was going to say, I'm surprised I got that wrong, you know, because I'm pretty clear on what the problem was. But anyway, Justin goes on and says, "So the ISP implemented a check on incoming mail. Anyone who has sent an email to his forwarder that had an SPF record was dropped because the DNS record told the ISP that it was spoofed, which of course exactly is what SPF is for." So Justin says...

Leo: But he wasn't losing all his mail, just some mail.

Steve: Right.

Leo: Okay. Wouldn't this be something we would all have happen to us? Because for instance I have my mail sent to leo@leoville.com, but it's not arriving at leo@leoville.com, it arrives at FastMail, you know, through a forwarder.

Steve: Yes, forwarders are the sort of the Achilles heel of - well, that's not really the right expression. But forwarders represent a serious problem for SPF because what SPF sort of relies on is this old notion of mail forwarding, where you could just send your mail towards your destination. For example, if the actual server that was supposed to receive it was busy or offline, you could go to a backup MX server, as it's called, and put the mail there; and then that backup MX server would forward it on to the destination and, like, do retries and so forth. So the whole idea with SPF is it's a way of authenticating the originating email server to the destination which implies no middlemen. But middlemen have always been part of the way SMTP, the Simple Mail Transfer Protocol, worked. So forwarding, which is what is going on here, is a problem.

So anyway, to get to Justin's point, he says, "Either have the ISP whitelist the email forwarding service," and he says, parens, "(not likely), or have his brother implement a Sender Rewriting Scheme, SRS, which will change the envelope 'from' address to a domain that is allowed to send from that server." And so essentially this is the way SPF can be altered to be forwarding friendly, although it may be actually doing more than his brother is able to do. The idea being that his brother's server would receive email and then, rather than just sort of blindly bouncing it onward to the ISP, where you have a problem, that essentially the brother's server would rewrite the envelope to set it as the apparent source, which would then have a matching domain. And presumably his brother's server would also have an SPF record that said we are the authorized originator of the following mail. So there are ways around this. I just wanted to clarify that for the record.

Leo: Okay. And I don't know why I'm not having the problem because I do the same thing. So I guess just not everybody pays attention to this stuff.

Steve: Well, that's exactly what's still happening is, for example, if a recipient of email who has SPF technology has it active, for example, they'll query the originating server's DNS records to attempt to get a list of IPs or machines that are valid originators of mail from that domain. If that sender has no SPF record, which is still very much the case, then most ISPs will say, oh, well, we didn't get any information one way or the other, so we'll allow it. But if there is a DNS record, it either matches the incoming mail or doesn't. If it matches, then you have a high degree of confidence that this mail is not spam and valid. If it doesn't match, you have a high degree of confidence that it is invalid and should probably be just dumped into the spam folder. So but there is that middle ground which is no DNS record, no SPF support at the originating end, in which case most ISPs will say, well, okay. We don't know either way, so we'd better let it through rather than just drop it summarily.

Leo: Right, makes sense. So any other mail?

Steve: Well, I did have...

Leo: ...mailbag thing we do now.

Steve: Yeah, I want to try to get more of our listeners' comments and things. And I've got actually a couple for next week cued up. But I didn't want to do any more because I had sort of a longish but really sort of interesting SpinRite story to share with our listeners. This is from a guy named Harry Liddenfeld. And he says, "Steve, let me start by saying I've been a big fan of

Security Now! with you and Leo since Episode 1. Up until this past week I've never had a need for SpinRite since I've listened to you and Leo about backing up." So Harry's into making backups, which we always say; and it the case that, you know, that's really your first and best line of defense. And he says, "I work at a courthouse here and inherited the security card access server and system for the courthouse from the county. Their solution to backup was CDs on a CD writer. The database has over 500 people in it." And so this is like secure access control stuff for the courthouse. "Their database has over 500 people in it, and the number of CDs required were getting out of hand..."

Leo: Like thousands, I would imagine.

Steve: Yeah, "...and didn't make any sense. We had a computer crash about two years ago, and I gave the county the backup CDs. They were unable to restore the database, saying that some of the CDs were corrupt. So we had to manually reenter the complete database, which took days of painstaking work."

Leo: Hey, at least they had it, they could do it.

Steve: Well, yes. And he said, "I promise...." They must have a hard copy if they're having to hand enter it. He said, "I promised that would never happy again, so I purchased Norton Ghost and another hard drive and ran Ghost. Then I would do just weekly backups of data files. Lo and behold, the main hard drive failed, and I rebooted the system off the ghosted hard drive and was up and running in minutes." Okay. "Two days later, that hard drive started to have issues, and I had not yet purchased another hard drive as the county still wants to use their CDs. I was in fear of losing everything, so I purchased SpinRite..." he says, parens, "...(for myself because the county wouldn't buy it)..." close parens, "...and immediately started it in Level 2 mode. That was at 10:00 a.m., and it ran for just over four hours. And by 3:00 p.m. that same day I booted the system back up, and everything was back to normal. But here's the best part. The original hard drive that had failed and wouldn't boot up any longer, after running SpinRite it booted up normally and faster than ever before."

Leo: He fixed that one, too.

Steve: And he says, "SpinRite to the rescue once again." He says, "I once again ghosted the main hard drive and also have a second ghosted hard drive offsite in a secure storage just in case. Thanks again, Steve, for all your hard work. You've saved me days, possibly weeks of data recovery."

Leo: We might mention, by the way, that we don't recommend SpinRite as a backup solution. You should still back up. But it's sure nice to have in your toolkit.

Steve: Exactly. Well, I mean, here's a perfect example of some guy who was doing everything right. He was backing up to a second hard disk. He was making a full image of the drive and doing it every couple weeks, being as conscientious as he could. But the drive he was relying upon essentially as his offline mirror, it began to fail. And what was cool was that he ran SpinRite on that before it had died, and then...

Leo: But it did fix the old one, which is...

Steve: Yeah, mostly out of curiosity he then ran, since he had SpinRite now, he ran it on the one that had completely gone belly-up, and SpinRite brought it back to life.

Leo: All that data entry for nothing.

Steve: Yeah.

Leo: Maybe that's why they didn't want to pay for it, they didn't want to know. They didn't want to find out. Well, that's a nice success story.

Steve: I thought it was a really neat, interesting story.

Leo: So, are you ready to talk about bots?

Steve: Well, what we learned last week - it was Wednesday before last, so eight days ago - the FBI made some real news with their announcement of several things. They had arrested three, what they're calling "bot-herders." I mean, I have to say these press releases from the FBI are unlike their typical press releases. They first formally called this, like an ongoing project that they have that they really have not talked about before, Operation Bot Roast. And they are, in their press releases they talk about these bot-herders. They have arrested a guy named James Brewer from Arlington, Texas; Jason Michael Downey in Covington, Kentucky; and Robert Alan Soloway from Seattle, Washington. It turns out that they're now saying, that is, the FBI is saying that they have confirmed at least a million consumer PCs are infected with bots of one sort or another.

Leo: Yeah, although even this is a low number compared with other estimates, like Vint Cerf's estimate that it's 160 million.

Steve: My goodness.

Leo: But a million's a lot.

Steve: Well, yes. There are three major gangs of some sort that are now actually having turf wars over the bots.

Leo: Oh, interesting.

Steve: Because they get paid by spammers based on how many bots they're controlling. And of course those who have the most bots get more money. So essentially it's like here's these hundreds of millions of innocent PCs, Windows PCs - as far as I know all the bots, certainly all that I've come in contact with and have heard about, are Windows-based bots. And so they're like raw material for these gangs to now have turf wars over. And what they're in fact doing now is deliberately targeting each other's bots and stealing already infected computers from each other, literally fighting over these things. So...

Leo: Wow, isn't that amazing.

Steve: So what's interesting, of course, I don't know whether our listeners know that I got directly involved in this myself when on Friday, May 4, 2001, so a little over six years ago, I was sitting here working on a Friday evening, and GRC dropped off the 'Net. We just disappeared off the Internet. And I had known theoretically about bot attacks and denial of service attacks and all that, but had never experienced one myself. Of course those days are fond memories, when I still had my DoS innocence. GRC lost that in spades.

Leo: Maybe you should explain what all of this is, what a DoS is, what a botnet is. I mean, we've talked about it before, but just for those who are just tuning in...

Steve: Well, certainly I think all of our listeners will understand that a DoS - DoS is an acronym standing for Denial of Service. What it typically means in this day and age - which actually is somewhat different than what it meant 15 years ago or 10 years ago. Today it's essentially a flood of Internet traffic aimed at one or more, but only a few, targets. And there are so many computers on the Internet now which are - many of them are on 24/7, you know, they're always available, or they come and go, but at any given time many machines are obviously on the 'Net at one time. What happens is that those are used to send a high volume of traffic, each one sending pretty much as much as it's able to, which coming from all directions around the globe focus their traffic to some site, an Internet web server, or in some cases an individual, or in some cases we've even had attacks against the main DNS servers that hold the Internet together, essentially, attacks on the Internet itself. The FBI in their statement, in their advisory they said, because of their widely distributed capabilities, it says the government considers botnets now to be a growing threat to national security, the national information infrastructure, and the U.S. economy.

Leo: Well, that makes sense because of how botnets are used.

Steve: Well, and so to finish on this sort of explanation, what happens is, one way or another, people get themselves infected. Now, obviously infections are not news for anyone on - really anyone today with a PC on the Internet. There is spyware, there's malware, there's viruses, there's all kinds of different malware of various sorts that you can get injected or loaded or invited one way or another on your machine. One class of this bad stuff are called "bots." What makes a bot special is that it is a piece of code which arranges to run, very much like a trojan, it arranges to run in your machine, to survive attempts at removal - I've got a friend, in fact you met him, Bob, who's up in Vancouver, who does sort of IT work for various companies. He got really fascinated by one particular trojan of some sort which got into one of the companies that he does consulting for. Someone, some employee, you know, brought it in on his laptop from outside, and this thing immediately spread throughout the company. And, you know, Bob's been doing this stuff for about 20 years now. He's close to as good as you can come. And he just, I mean, this thing's been driving him nuts because he cannot get rid of it. He's gone through the directories. He's the kind of guy who knows what every file in Windows is for, I mean, he knows at that level of detail much more than I've ever bothered to. And this thing, on one machine, it just keeps coming back. And that's really the evolution we've seen over the last five years. And you've talked about this, Leo, about how it used to be that it was possible to remove spyware. And now spyware has gotten so pernicious and so crafty at hanging on in a system that you often just have to roll back to a restore point that you hope was not infected or restore from an image at a time that you had no infection.

Leo: It’s pretty hopeless.

Steve: Yeah. So anyway, what happens is, what makes a bot a bot is it lodges itself in your system, virtually irremovably, and arranges somehow to enlist itself to receive commands. The most popular, still to this day, means for doing so is that the bot will join into an IRC chat channel, a hidden, private, password-protected chatroom where all the bots of a given bot-herder, to use the term which is now becoming common...

Leo: I like that. It’s very descriptive.

Steve: It’s perfectly descriptive. They’ll all convene. Now, I want to point people to this document that I created after I rolled up my sleeves six years ago because what I ended up doing was essentially reverse-engineering a bot that someone provided and figuring out what it was doing. Then I created my own pseudobot to emulate the protocol this bot was using. I got the IRC RFCs, the specs for the way IRC works, which I’d never looked at before, and I quickly wrote a bunch of my own sort of benign bots to join in the party as if mine was a legitimate one that had infected a computer. That allowed me then to watch what was going on and learn about what was happening.

And essentially I ended up being able to infiltrate this network and ended up having some conversations with some of these bot-herders about what they were doing. And I’ve got all the transcripts. I show a screen of all these bots checking in. This particular one was called "evilbot." And they literally, they logged into the chatroom and saluted and said, "Evilbot 3296 reporting for duty." And so you could literally, I mean, I was actually watching the screen scroll as these bots were coming and going, as the users of the computers that had unwittingly been infected, as they turned their machines on and off, these bots came and went. And at any time - in this case there were only a few hundred. The frightening thing is that these networks have now grown to tens of thousands and in some cases hundreds of thousands of machines.

So you have all these machines all logging into a chatroom. Well, then the bot-herder himself or herself logs in to the chatroom and issues commands which will be seen as chat operates by everybody logged in. And so literally this person issues commands saying, okay, everybody, go attack a certain domain name, or go attack a certain IP, or here’s where you go to pick up a list of spam addresses, and I want you to all start sending spam. So essentially it’s centralized control of a worldwide, massively distributed network of slave computers which could be used for many purposes. It used to be they were only used for attacking because this thing all grew out of script kiddies, you know, sort of junior hackers home from school in the afternoon, blasting each other off the network, trying to obtain control of IRC chatrooms. And so they were using their own IRC chat mechanisms which they had developed bots for to attack each other because, if you - I can’t remember the term now for the person who’s running an IRC server for...

Leo: The mod, or the moderator, or the...

Steve: It’s the equivalent of a moderator.

Leo: The channel op, channel op.

Steve: Channel op, that’s exactly it, yes. And so if the channel op goes offline, then somebody else has the opportunity to come in and take over. So they were literally blasting each other offline in order to sort of play capture the flag of these chatrooms. And as a channel op then you have the ability to kick other users offline. And so, I mean, it sort of started off being...

Leo: Benign.

Steve: ...you know, horseplay among teenagers. Unfortunately, even then this was all illegal because they were using other people's machines, remote-controlling them in order to do their dirty work for them. So what's happened is it's evolved now into huge spambot networks. They are able, because they're command driven, they're able to launch denial of service attacks. And now they're renting out their DoS services to third parties who want - for example, gambling sites, someone who's a competitor of a gambling site will hire a botnet service to blast the competitor off the 'Net at a critical time during a horse race or a boxing match or something. And, I mean, this is what's going on all the time.

So what I'm really glad for is that the FBI has, first of all, it's taken them, frankly, years to get themselves up to speed and organized. But they clearly are now organized and are pursuing these guys. So, for example, this James Brewer in Arlington, what got the FBI's attention was that his bots infected a number of Chicago area hospitals. And so critical PCs running intensive care software were being brought down and their bandwidth saturated, which they needed, by this guy's bots. And as soon as you start messing up hospital systems, that raises red flags at the FBI. And so the FBI doubtless did something very much like what I did, was once they had their forensics guys up to speed and understanding how to deal with this, they sequestered one of these bots, grabbed it, probably deliberately infected a honeypot machine of their own, and then watched this thing connect into bot-herder central, wherever that was, and then began the process of backtracking the individual who was communicating with the bots.

And of course essentially that's the weakness of the system. The IRC chat system is used obviously to create a layer of insulation between the bot-herder and his bots to hopefully keep him from being easily findable. But the people who run these bots, they don't know whose computers they're commandeering. Certainly this James Brewer guy didn't know that a number of his bots were causing serious problems for Chicago area hospitals. We could hope that he has enough morality to not have done that deliberately. And in fact the way these machines get infected is just by visiting websites, by people opening malicious email, you know, all the standard means for infecting computers can be employed for distributing bots.

And so the point is that the bot-herders have no idea whose computers they've commandeered. And what's happening, now that the FBI considers this a serious threat to national security, is the FBI doubtless has lots of honeypots that they are deliberately infecting with these bots or allowing to become infected, and then they're starting the process of backtracking the communications back to the bot-herder. And, you know, this is not fun and games anymore. This is serious business now. And the problem, of course, is that there's substantial economic benefit now to the bot-herders. It used to be that it was, you know, teenagers blasting each other off the 'Net to play capture the flag; now it's I will sell you my network to use for launching - in fact, one of these guys, I think it was this Robert Alan Soloway in Seattle, tens of millions of pieces of spam sent from his network.

Leo: It's amazing. It's really amazing. I've seen these bot networks at work, too. And what's interesting is how quickly they fill up, as you mention. It's instant, boom boom boom, every second another computer is co-opted and joins the net.

Steve: Well, and in fact I remember when I was really involved in this - I am really no more now, I mean, it's evolved to a whole different plateau. But I got involved, as I said, six years ago, early in the game. And I participated passively, just listening to dialogues among these bot-herders because I ended up tracking them down, following them around. You would see someone refer to, oh, let's go over here. And they didn't know that I was already there listening, so I'd follow them over there. And I remember listening to them talk about putting out a new bot, like in the evening, and coming back the next day after school, and they had...

Leo: School.

Steve: Exactly, I mean, they were in high school or junior high, you know, they'd get home from school in the afternoon, and that new bot would already have 3,000 hosts.

Leo: Yeah, yeah. That's why a million is - so is the FBI, are they using any specialized tools to track these botnets down? How are they going about this? Have they talked about that at all?

Steve: No. They're being close-mouthed about it because of course they don't want anything that they're doing to be defeated by talking too much about it. And as is always the case, there isn't a single universal solution because, for example, in the case of these gangs who are fighting each other, they're creating different bots and essentially anti-bot bots, and they're spitting out, like, 20 new ones a day. So the actual bots themselves are evolving at a very fast pace. Ultimately, though, the Achilles heel, to answer your question generically, the Achilles heel is that there's nothing to prevent good guys from deliberately infecting their machines with bots and then backtracking.

Now, you have to imagine - because Microsoft has been involved in this initiative, too, since 2004, so for the last three years. And now of course we've got the Malicious Software Removal Tool as part of the Windows Update suite of software. And I notice every second Tuesday I'm getting an updated version of that. So at some point, once the bots that are malicious are known, I would imagine that information finds its way to Microsoft, and then Microsoft adds the signatures for removing these things to the degree that they're able. So there is a means for proactively dealing with the neutering and removal of the bots.

The problem is, and this is something that we researched extensively back in the, I think it was Code Red worm, there was no way for the FBI to directly remove this malware even though the FBI probably has the IP addresses of all these infected machines. The reason the FBI says a million is they've been collecting IPs. And so they know the IPs of the infected machines. But as we know, that is, Security Now! listeners will know, just having the IP of the machine tells you little other than who the ISP is that the machine belongs to. In order to push it further you'd have to get subpoenas, the FBI would have to give subpoenas to the ISP compelling the ISP to release the names and addresses of the owners of the IP at that given time. The ISP may want to comply, but the terms of service gives their customers certain rights of privacy. So the ISP needs the FBI to subpoena this information from them in order to cover them legally against actions by their customers.

So the point is, all of this is a moving target. It's happening quickly. The bots are changing and literally evolving. Users are hanging up, changing their IPs. And essentially there's no direct way for the FBI to access those end-users' computers because that's illegal, even if it's the FBI doing it.

Leo: Interesting. So that makes it difficult for them to pursue this, I would guess.

Steve: Yeah, no, they've talked about working with CERT, the group out of Carnegie-Mellon, to somehow notify end-users directly. But I noticed in one of the reports, one of the main techies at the SANS Institute that also covered the story, who's been very involved in this work, he says, well, you know, how are they going to do that? We’ve been trying to notify users with their DShield service for years. And they’ve learned how ineffective that process is because it’s not the smart users. It’s not, frankly, the people listening to Security Now!, not the people within range of our voices, Leo. It’s people who really aren’t paying attention to security who will glibly click on any link that comes in the email. And those are the machines that are crawling around with this stuff. They’re not going to DShield to see if their IP is listed as probably being a source of attacks.

Leo: Well, imagine their reaction if they get a letter, an email from the FBI saying we think you’ve been compromised. I think we’ve trained most listeners well enough to go, yeah, right, I’m going to click that link.

Steve: Well, and that’s exactly the problem, too, is armed only with the IP, there is no way that you can send email to an IP. You can only send it, of course, to an email address. And...

Leo: Aha, good point. But I think that’s why really the first line of defense should be, once again, the Internet service providers, that they could tell them, look, these IP addresses in your system are compromised.

Steve: Well, that’s a very good point. And that’s something where, I mean, that’s an aspect of controversy. Certainly you could argue that the ISP could see and will see an abnormal amount of outgoing traffic from specific customers. If that customer did that a lot of the time over the course of a week, the ISP could reasonably assume something is wrong on this customer. The problem is, that begins to involve the ISP in issues of quality of service. And the ISPs are super reluctant to begin to say, well, we’re going to take any responsibility because, when they fail to do so, then potentially that makes them liable.

Leo: Right, right. I think that’s who really - once again, I mean, with spam, with this problem, it’s the ISP who really needs to step up and who seem to be so reluctant to do so. But maybe someday. These are the guys who are putting us online. And I think they have some responsibility. They know what’s going on. They can tell there’s traffic like that going on if they wanted to monitor it.

Steve: You absolutely could tell. Now, you might also argue that there really isn’t the monitoring tools available to do this. I mean, they see traffic going out through their router. But they would need to log it over a period of time and then classify it to see that one given source IP or a collection of source IPs is sending a high level of traffic to a collection of destination IPs. So that really requires some proactive steps on the part of the ISP. Your point is exactly right, Leo. Because the ISP is at the border, they are seeing all of the traffic transit their network. So they potentially have the information. But going from that to basically processing all of their logs for this reason really requires a next level of involvement. And no one has compelled them to do so. Now, if the FBI starts rattling sabers and saying, wait a minute, ISPs are enabling this - oh, and I forgot to mention, the FBI is also saying the majority of these bots are in the U.S.

Leo: Yes, yes. By the way, very important.

Steve: So it’s not like they’re all over in China somewhere, where we really can’t get to them. They’re here. And so you could imagine some Congressman gets a bee in his bonnet and floats some legislation to begin to try to increase, exactly as you say, Leo, the level of responsibility that ISPs have as the people who are providing the bandwidth for their customers to the

Internet, what responsibility does the ISP have to take some measures to thwart this kind of activity. Because that would do it. That would end this overnight.

Leo: Fascinating stuff. And as always, you've exposed us to something new and interesting, the seamy underbelly of the Internet. And, yes, go ahead.

Steve: I was going to say that I do want to recommend our listeners go over to GRC and add themselves to the already million people that have downloaded the PDF I have there that tells the story of me learning about what this was in detail and then rolling up my sleeves and backtracking, basically infiltrating several of these networks and going about solving the problem and learning about what was going on. I think people would really find it interesting.

Leo: Yeah, yeah. Steve Gibson is available, you can get that white paper, of course, on his experiences with DDoS attacks; but he's also got, oh, so much other great stuff there, including his free security software like ShieldsUP!, DCOMbobulator, Shoot The Messenger, LeakTest. I saw one the other day that I'd forgotten about, and I never mention, and it's such a cool little program, it's not a security program, but Wizmo. I love the little Wizmo. Really a great free program. Lots of good stuff there, including 16KB versions of this podcast, if you've got a dialup system or you just want really small files; and transcripts, too, so you can read along. Share it with your organization. If you want to improve security in your organization, Security Now! is an advanced course in security. Almost a hundred shows now. And that's GRC.com. Were you about to say something? I heard you take a deep breath, Steve.

Steve: I was just going to say that it's been another great episode, and I'll look forward to talking to you next week, Leo.

Leo: Good.