Router Logs

Description: Steve and Leo clarify the confusion surrounding consumer NAT router logging. They explain why routers tend to overreact to Internet "noise" by "crying wolf" too often, why the logs produced by consumer routers are unfortunately not very useful, and when paying attention to logs does and does not make sense.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-046.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-046-lq.mp3

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

This is Security Now! with Steve Gibson, Episode 46 for June 29, 2006: Router Logs. Security Now! is brought to you by Astaro, makers of the Astaro Security Gateway, on the web at www.astaro.com.

It's time for another Security Now!. That means another foray into the fascinating world of computer Internet security, protecting your system, how encryption works, how ports work, how VPNs work, all of that, thanks to our great teacher and master, the guru of high-tech security, Mr. Steve Gibson. Hey, Steve.

Steve Gibson: Hey, Leo. Great to be back with you this week.

Leo: I think more and more people think of you now as a teacher. You've been so great on these past 45 episodes, 46 now, teaching us about all the basics of this subject. I think it's great.

Steve: Well, I just love the technology. And I've never understood why people seem to think that this stuff is so difficult. I mean...

Leo: Well, now, wait, now, some of it is. And when you've done your darnedest to explain public key cryptography, and even a dunce like me gets it, it's really more a testament to you than the simplicity of the subject. This stuff can be pretty complicated.

Steve: Yeah. Well, I guess it's that there is an easy way to see the concepts. One of the things I've noticed, you're reading an academic paper, and the language is so obtuse and so

confusing.

Leo: Yeah.

Steve: And you look at it over and over and over, or read it all the way through. And then it's like, wait a minute, all they're really saying is this?

Leo: That's all?

Steve: It's like they're trying to justify their third Ph.D. or something. It's like, wait a minute, I could have said that in one paragraph and made it so that my mother could understand it instead of, like, four pages of bizarre arcania which really seems intended to confuse rather than explain. And so I think even, no matter how complex something is, if the goal is to explain it, it's possible to make it clear.

Leo: You're good – I think that's really your skill is reading all this arcane and confusing stuff and boiling it down. So what are you going to boil in your pot today?

Steve: You know, one of the things that I get questions about, I mean, I have for years, and the form at the bottom of the Security Now! page at GRC is constantly getting questions about router logs. People are worried about what their logs are telling them.

Leo: Now, do all routers keep logs? Not all of them.

Steve: I think all contemporary routers now offer the option, at least. You know, you might have some off-market junior routers that don't. But logging is just something that's, you know, it's now on the bullet feature list of any router that's going to be competing with all the others.

Leo: Right.

Steve: And, you know, they want to give you the option of logging.

Leo: So what's in that log?

Steve: Well, mostly nothing. I mean, and...

Leo: A lot of nothing.

Steve: And that really is the problem. Now, you know, we've talked before about the junk on the Internet. And I've talked about how I coined the acronym "IBR," Internet Background Radiation. I mean, it's really what this is, this packet noise, is just Internet Background Radiation. The router log is exactly equivalent to the personal firewalls which pop up an announcement anytime anything unsolicited hits your computer. Well, it's always seemed to me

that personal firewalls were doing this because they wanted to prove themselves useful.

Leo: I'm important. I'm doing something.

Steve: You know?

Leo: I'm busy, busy, busy.

Steve: And of course, exactly, and of course the problem is that in crying wolf as much as personal firewalls do, until you finally uncheck that box that says, you know, notify me when anything wrong happens, you finally – it's like, okay, I trust that the firewall is on. I don't want to know about it every five seconds.

Leo: Right.

Steve: But, I mean, it really is the case that there is just this junk on the Internet. Now, the routers have gone a little bit further, I think, because they're trying to alert users, you know, they're saying that they're firewall-enabled, they're stateful packet inspection, they're doing all this fancy stuff to protect their users. I mean, some routers even say they will protect you from a denial of service attack. Well, I've never...

Leo: How?

Steve: Exactly, I've never understood that claim because the problem, of course, is a denial of service attack is flooding your bandwidth with garbage, and the router could attempt some sort of filtering except that the problem is there's too much data, malicious data, coming to you for the good data to get to you. So the router can't filter what it doesn't receive. And the problem is...

Leo: The denial of service is blocking access, basically. And how's the router going to stop that?

Steve: Exactly. And in fact, all any router can do that says it's going to do denial of service protection is to block traffic from getting through. The problem is, no good traffic is able to get through anyway. And just blacklisting an IP in your network doesn't help because even the machines that are not under attack all share the same IP, that is, your router's public IP. Which, you know, which is being swamped by traffic to the extent that no valid packets are able to reach it. So, you know, I mean, these claims that the router manufacturers, I mean, lord knows you and I preach the security and value of NAT routers almost constantly because it's such a tremendous security tool. But, you know, them saying that, oh, we're going to protect you from a denial of service attack is just nonsense, unfortunately.

Leo: On the other hand, they certainly could log it, and you'd see it happening, I guess.

Steve: Well, and that's the problem is – and that brings us back to logs – is that what the routers are doing is trying to make sense of noise. You know, it's literally like tuning your AM

radio in between stations and hearing the shhhh and trying to find something of value in the static.

Leo: So there's so much going on that it's not obvious what's really going on?

Steve: Well, actually there's so much going on that there's nothing going on. I mean, that's exactly what's happening is that, you know, we've talked before about how the Internet will never be cleansed of worms, of our old past-generation worms, Code Red and Nimda and so on, and MSBlast, that copies of these worms are on machines randomly out scanning the Internet, sending – basically creating Internet Background Radiation on an ongoing basis. So every IP on the 'Net is going to get some of these packets sooner or later from these machines. And there's even misconfiguration of systems where packets that have no business being on the 'Net, strange protocols and broken things, just sort of wander into a machine from time to time. I mean, it's really instructive to put a packet sniffer on, just like on a cable – on a raw, unfiltered cable modem line and just look at the junk that is coming in. Now, the problem is the routers don't understand, or they don't want to understand, that nobody needs to be advised about this. I mean, the point, I guess, is, if somebody is under denial of service attack, they know it.

Leo: Yeah.

Steve: And in fact, what I've seen...

Leo: If you can't get online.

Steve: Exactly.

Leo: You may not know why. I mean, it would be nice if a log said, oh, look, you're getting all of these packets pointed at you from this bad guy, because then you would know, well, that's why I can't get online.

Steve: What I have seen, however, is that, based on the logs that people send me saying what do you think of this, there'll be a router that says they're in a denial of service attack. And I look at the log, and it shows that they're getting one packet about every five seconds from somewhere. Well...

Leo: That's not a denial of service attack.

Steve: No. I mean, that wouldn't deny anybody service. But the router, again, in trying to justify itself and prove its value, is aggregating this information and seeing, oh, look at all these SYN packets that are coming in. Well, yeah, if you wait an hour, and you've got, you know, 26 of them, well, that's not a denial of service attack.

Leo: Right.

Steve: And so what's happening is people are really being needlessly alarmed. I mean, some

people, I guess, who want to watch their router logs, after a while it must be the case that they become inured to these kinds of reports and just go, well, okay, I think my router's a little log-happy here. Because I don't feel like I'm under denial of service attack, and everything's just fine, even though the router assures me that I'm being attacked by somebody in China somewhere, or who knows where. So it just...

Leo: It's advertising. It's advertising for what a good job it's doing.

Steve: Yeah. And I wanted to – I just wanted to take some time, give it a podcast, and talk about, you know, these NAT router logs because...

Leo: Is there anything you can glean from them at all? No. It sounds like that's a no.

Steve: I really don't think so. Sometimes you will get, if your IP changes, you will start getting, like – in fact, I remember seeing this myself. Your IP will change, and suddenly you'll start getting a lot more logging, for example, because the IP you just inherited belonged to somebody on the Kazaa filesharing network, or on Morpheus or something.

Leo: So there's all these people trying to log in to get files.

Steve: Exactly. And so suddenly all these peers that were hooked up to this IP that belonged to somebody else are now trying, you know, still, I mean, as I remember, because I saw this often back when I was looking at this stuff closely, suddenly you'd have all this traffic, and it takes a long time for that traffic to subside, for the peer-to-peer network to decide that, okay, you really are gone, and you're not coming back anytime soon.

Leo: Right.

Steve: So, you know, I was never...

Leo: It's funny because we had a BitTorrent server once on my website, and now I continue to get hundreds of hits a minute from other BitTorrent clients looking for the tracker.

Steve: Exactly.

Leo: So I can vouch for that, absolutely.

Steve: Exactly. That's a perfect example. So if people wonder why their traffic as being logged by their NAT router sometimes is in huge dose and sometimes much lesser dose, if in fact they had their router unplugged or turned off and then turned it back on, there's a chance they got a new IP that might have belonged to somebody who was much more active doing things in a peer-to-peer network. And so, again, you'll get a ton of traffic, and then it'll subside over time. So the log might be useful for that.

Leo: You look at your router logs. Is there something quantitatively different you get from your router than the standard Linksys router will give you?

Steve: Actually the only times I look at my logs are if there's something happening that I do need to know about. If something seems off or wrong...

Leo: So there's something you're looking for, then, in the log.

Steve: Exactly. I'm trying to figure out specifically what's going on, but down at the traffic level. Now, the other real problem with the logs is that they're incomplete. It's sort of like a junior log that you get with most of these NAT routers. And so often, for example, people will send me a chunk of log saying, hey, Steve, you know, what do you think this is? And the problem is, I can't tell. Nobody can tell because the router is sort of saying just enough to raise the question of what's going on, but for example it isn't telling you what the TCP flags are of the packet coming in. It's just claiming that it's an attack of some kind. And so, for example, many times it's got nothing to do with being an attack, and only if we had a complete log entry could we then say for sure, ah, this is what this is.

So one of the differences between sort of a junior consumer log and, you know, real professional network gear logging is professional network gear logging often tells you much more than you want to know, but at least you have what you need to know. Whereas NAT routers are often not providing you sufficient information to actually perform any useful diagnosis. And that's my complaint is they're just sort of bubblegum logs. I mean, they're just, you know, they're just there to sort of add a feature to the router.

Leo: Right. This one logs.

Steve: It could be interesting. But actually it's one of the reasons, it's one of the benefits to going to, like, a real UNIX or Linux system, you know, an inexpensive PC running NAT routing software. And we've talked about many of the standard, off-the-shelf, easy-to-configure, like SmoothWall and Monowall systems, where those systems have real logging facilities. And there you're – first of all, one of the things they don't do typically is bother you with trying to interpret their logs. The logs are there, if something arises where you need to go look at them, and they're complete. So that's the kind of logging that makes sense. You know, log traffic if you want to. But if you're going to log it, log it completely so that something is useful and can be really determined from the log. But, you know, sort of this half measure of NAT router logging in a standard consumer NAT router, it just makes no sense to me at all. It, I mean, it is falsely positive alarming people, and the information it contains is insufficient to provide any useful diagnosis if you wanted to.

Leo: Is it essentially the same kind of thing you get when you run a software firewall and it's popping up alerts every five seconds?

Steve: Yeah, it's exactly that. And in fact, in some cases it's weird. I've seen situations where a NAT router will alert somebody hours after they've been doing something on the 'Net that causes the alarm. What must be happening is that the router is aggregating traffic, trying not to produce multiple alarms. So it's like it's seeing some things going on, then it's deliberately waiting some length of time to see whether any more junk comes in that's associated with that same remote IP so that it can associate all of that into a single event report. The problem is, that event report is then popping up at a time, or presenting itself at a time which is

disconnected from the user's actions which may have caused that event.

Leo: So it makes it even more baffling.

Steve: And that's another thing that confuses people.

Leo: What is this?

Steve: And so someone will say, hey, look at this log, and here's what happened. And it's like, okay, well, there's nothing in the log you've shown me that's about what happened. So they'll go back several more hours, and there's the traffic, hours before, that caused this report. So I can understand the logic in the router manufacturer's mind. I mean, some router programmer thought it would be really cool, you know, to wait a while so that multiple events for the same activity were not being reported. The problem is, that induces confusion in the consumer's mind, who doesn't understand why something happened now, you know, an hour after they haven't been using their computer. And the fact is, that leads them to believe now they're under attack, when in fact it's something they were doing hours before, where if the report occurred then, they'd go, oh, yeah, I know, I'm doing that.

Leo: Right, I've got BitTorrent running or whatever.

Steve: Yeah, exactly, you know, or a peer-to-peer system or something which is causing these sorts of reports.

Leo: Well, can we talk a little bit about this Internet Background Radiation and what it is? You mentioned, and we've talked about before, things like worms like Sasser and MSBlast that just continue to float around as long as there are unpatched Windows 98 machines on the 'Net, they'll just continue to float around.

Steve: Right.

Leo: Is some of it from hackers also? I mean, I get the impression that they're kind of going around looking for vulnerabilities all the time. Is that true?

Steve: You know, I think that is still the case. It seems it's getting less attention now, I think because there's so much noise on the 'Net. I mean, it used to be, for example, that...

Leo: This is so-called "port sniffing," right?

Steve: Exactly, or port scanning.

Leo: Right.

Steve: It used to be that people who were watching their router logs and who were, like, took it upon themselves to police the Internet, I mean, I'm not kidding, they would be – when random packets from somewhere hit their machine, they would look up the ISP that owned that block of IP addresses and send abuse report email saying, somebody in your network just scanned my computer. How dare they?

Leo: I remember getting callers like that, yeah, yeah.

Steve: Oh, yeah. And, I mean, thank God at least that has tended to subside. And the reason is, no one could keep up with that anymore. I mean, there's just so much stuff on the 'Net. But it is the case that there are malicious people, now and still, scanning the Internet, looking for specific vulnerable ports. You know, we've talked about, for example, my network, I just couldn't have telnet, the standard telnet port 23 open and exposed on my own network because the appliances that I could telnet to didn't have sufficient and adequate security. So the idea would be that there are scanners running right now somewhere, many of them in the world, that are just slowly, methodically sweeping the IP space of the 'Net, looking for anyone who will accept a TCP connection on port 23. That means...

Leo: You know – oh, go ahead, I'm sorry.

Steve: No, no.

Leo: I'm just saying, I've seen these hacker tools. Whenever there's an exploit that comes out, the hacker tool comes out. And they're very simple. I mean, any script kiddie – and that's the problem is that most of these aren't really proficient hackers – can run a little program that says, okay, what IP addresses do you want to scan? Let's see, one to one million. And what ports do you want to attack?

Steve: Yup.

Leo: You know, here's a few. And they press a button, and they walk away, and all of a sudden they've created a huge amount of chatter going on.

Steve: Now...

Leo: Even if they got in, they probably wouldn't know what to do. I mean, I don't know what they're going to do with that result, but...

Steve: Well, and of course the very same tools, the famous one is Nmap.

Leo: Right, which is actually a very powerful tool.

Steve: A very powerful scanner. I mean, if you put "port scanner" into Google, you know, stand back because, you know, it's a type of tool that many people have written. And Fyodor's Nmap is a very powerful scanner which I'm sure is being employed for malicious purposes. And in fact the exact scenario you mentioned, where you put in an IP range and a port range, I was

talking a couple weeks ago about how it was Windows's open filesharing dilemma that years ago induced me to create ShieldsUP!. Well, I used a scanner just like that, and I said find port 139, TCP port 139, and I put in the range of IP addresses surrounding the IP I had received from our ISP for our ISDN line. And up popped all these computers that were accepting connections on port 139.

Leo: Right.

Steve: I mean, they had Windows filesharing open and exposed, and many of them had drives C and D and E and F and G, all freely available on the Internet. So the good news is, these sorts of problems have diminished. But, for example, filesharing, my ISP for my cable modem provider, Cox, they're blocking now 137 through 139, and 445, and a few other commonly attacked Microsoft ports, which is really a service for their users, so they're automatically preventing anyone from the outside being able to get in. However, you're still able to, from within the Cox network, you're able to provide or to create scans because they're only protecting at their border.

Leo: Yeah. So these...

Steve: But at the same – I'm sorry. But at the same time, to really get back to answer your question, some of the traffic that's Internet Background Radiation is coming from, essentially, automated non-sentient worms that are just out there scanning around, that we're never going to get rid of. But it is the case that other traffic, well, some other is Windows Messenger pop-ups. I still see a lot of that happening. That's junk on port 135.

Leo: Right.

Steve: You know, trying to spam people who have a naked machine with no firewall who have Windows Messenger running. And that must mean that they're not up to Service Pack 2 of XP because that finally, you know, XP's firewall blocks that. And the Messenger service is finally not running by default...

Leo: It would be really interesting to...

Steve: ...[indiscernible] running before.

Leo: ...to run Ethereal or some sort of network packet analyzer to just watch kind of this background noise and kind of break it down. I wonder – I'm sure some security group has done this – you know, what percentage is, you know, Sasser, what percentage is this, what percentage is that.

Steve: Oh, it really is interesting, Leo. I mean, it is absolutely interesting. I remember from the last time I was doing it, when I was, you know, focusing on my cable modem traffic. And I think it's when I was dealing with Wicked after – the 13-year-old kid who'd attacked GRC years ago. I spent a lot of time looking at the traffic and having just a constant log running, showing me what was coming in. And it's a mixture. Now we have worms. We do have advertisers trying to send you, you know, Windows pop-up Messenger. And then you've got the occasional clear port scan. In fact, I've got several different IP ranges. And I remember when I was watching

those ranges, you could see packets arriving, for example, SYN packets on port 23, that would just sequentially arrive at successive IP addresses. So it's literally a linear scan through a range of IPs, something looking for an open server on a given port. And it's going on all the time.

Leo: It's really kind of amazing. I suppose, you know, five years from now you'll still see a Sasser on the 'Net and this stuff. You know, it'd be kind of senescent since there won't be anything for it to attack anymore. But as long as there's one infected Windows 98 machine out there, it'll continue to bang on the door.

Steve: Well, it's funny, too, because in the old days, you know, meaning six years ago, you could look at your cable modem light, and you could use that light to determine when you had traffic with your computer. Now that light is never...

Leo: It's always on.

Steve: Yes, exactly, it is never not flashing because there's just all this junk out there on the cable modem, and even on a DSL line, which is just, you know, it's just, again, it's IBR. It's Internet Background Radiation. So I guess my message would be, for people who are concerned about their NAT router logging, telling me – if it's too noisy, if you're worried that there's some valuable information there, I would suggest that it probably is more the router trying to justify its existence than it is useful.

The logging can be useful if you are forensically trying to figure out why something doesn't seem to be working in your network. For example, if you were looking for incoming traffic because you had believed that you'd opened a port that was going to allow traffic from, like, a friend of yours who was trying to connect into your system, well, the log there might tell you that it was blocking and dropping packets from a certain IP. And in fact, we briefly mentioned this idea, which I think is actually kind of clever, of allowing two routers to connect to each other by sending traffic to each other and having each router look at its own log to determine what port and IP that traffic is coming from, and then have the computer that's reading the log send traffic outbound to that IP and port, which would allow you to do a NAT traversal without needing a third party. I've never seen that written or heard of it before, but it would be kind of a cool way, using the router's logs, to perform a non-third-party NAT traversal.

Leo: Hmm. Well, that's an interesting idea.

Steve: So it can have applications. But again, I think it's mostly useful for forensic or diagnostic purposes, not useful for alerting you to attacks. The fact is, technically we are all under attack all the time. I mean, truly.

Leo: So stop sending us your logs.

Steve: And that's why, you know, any Windows machine, recently created Windows machine that isn't patched fully, stuck on the Internet with no firewall protecting it, will be – I mean, tests have been done. It is taken over within minutes, literally, of being stuck on the 'Net. Every IP is constantly under, quote, "attack," unquote. So that's why stick a NAT router on your network and just ignore it. It is protecting you. Or just make sure you've got your firewall running on your PC, if you're not behind a NAT router. And again, ignore all that nonsense. It's one of the reasons that Microsoft's Service Pack 2 XP firewall is so quiet, and it has no option for pop-ups. I mean, they don't offer that as an option, as far as I know. I guess there's a log

that you can turn on in XP's firewall. I think I remember seeing some logging that, again, for diagnostic purposes is useful; for warning you of attacks is not. Because, again, we're all under attack.

Leo: Steve, you've done it again. And mainly I think, because both of us handle questions from people, you know, what does that mean, what does this mean, it's really mainly just to calm people down. It's okay. It's normal. It's just noise.

Steve: It's Internet Background Radiation.

Leo: More information always on the website at GRC.com/securitynow. That's where you'll find transcripts of this show and every show. We've done all 45, 46 episodes now. And also, of course, 16KB versions for the bandwidth impaired, still on modems, or people who just don't have the time to download a higher quality version.

We also remind you that that's the home for SpinRite, which is everybody's favorite, my favorite disk maintenance and recovery utility. The stories keep coming in. If you want to read some amazing testimonials, visit SpinRite.info. Steve puts new ones up all the time, and it just – they're heartwarming stories. It must make you feel very good that...

Steve: Yeah, actually I need – I keep saying that I'm going to catch up. I've got a whole bunch more. I think the last one is a couple months ago that, you know, somebody's system wouldn't boot anymore. And...

Leo: Well, they're constant, though. You get them every day, so...

Steve: Yeah, exactly.

Leo: Yeah. So SpinRite is available at GRC.com. And if you deal with drives, you need SpinRite. You know, I think a lot of people go to very fancy, expensive – and I mean thousands of dollars – disk recovery places. When in fact, if it's just a soft error, if it's just a formatting error or a software error or an operating system error, it's almost, you know, they can't do anything that SpinRite can't.

Steve: Well, the other thing, too, is with drives being so big, there are many areas of drives that aren't visited very often. And one of the nice things that SpinRite does is, when you turn it loose on your system and let it run overnight or, you know, however long it takes, depending upon the speed of the whole system, it's reading and writing every single sector of your drive several times. It reads it, it inverts the data, writes it back, reads that, inverts it again, writes it back, and reads it again. So it...

Leo: Kind of exercises it.

Steve: So it really exercises it. And that's important because drives are now handling their own defects. But if a sector defect gets too big to be corrected, then you've got a problem. The cool thing is that SpinRite essentially lets the drive inspect itself by asking it to read and rewrite and reread the entire surface. So any trouble which is beginning to occur, SpinRite essentially shows the drive that, hey, you've got a problem with this sector. And...

Leo: Map it out, get rid of it.

Steve: Exactly. Map it out. It removes it from service, and it swaps a spare in. So as a preventive maintenance tool, and as a means just to check to see what condition your drives are in, I mean, there really is nothing like it.

Leo: With these big 500-gigabyte drives now, I run SpinRite on every new drive just because I don't – proactively, I want to make sure that there's nothing wrong with that drive before I start, you know, committing important things to it.

Steve: It's funny, in the old days we got in, well, we didn't get in trouble, but there were some manufacturers that would over-order the – and we're talking, like, well, okay, Compaq. I mean, you know, major computer manufacturers.

Leo: They're gone now. We can talk about them.

Steve: Right. In fact, I just realized that. They would over-order the number of drives they needed, use SpinRite to qualify them at the loading dock, essentially an incoming QA, and then return the excess drives that were the least good as determined by SpinRite. So, I mean, it really has that sort of like, you know, diagnostic and long-term preventive maintenance capability.

Leo: Well, I wish drive manufacturers would just do that before they leave the factory. I would buy – I would pay a premium for a drive if it said "SpinRite tested before shipping." I would buy – I would pay a premium for that.

Steve: Maybe someday.

Leo: Hey, you know, we were talking about all of this router activity and monitoring and so forth. If you are administrator of a big network, you certainly need to do this kind of thing. You need to constantly keep an eye on things. And you need a router that's a little smarter than the average Linksys. You need the Astaro Security Gateway. Astaro is, of course, the sponsor of Security Now!. We're really glad to have them. All open source, they make great stuff.

They've just released a brand new product, the Astaro Command Center Version 1 – ACC, they call it. It's free for all users of the Astaro Security Gateway. So if you're a network administrator with multiple gateways, you can manage them, you can control them, you can monitor them, you can look at threat levels, all from one central command post that's got a beautiful map of the world. It's just really slick. ACC is one of the many reasons to look at the Astaro Security Gateway.

If you're a small or medium business, and you need superior protection from spam, from viruses, from hackers, plus complete VPN capabilities, intrusion protection, content filtering, and an industrial-strength firewall at an easy-to-use, high-performance appliance, contact Astaro, Astaro.com, or call 877-4AS-TARO for a free trial of an Astaro Security Gateway appliance in your business. I use the 120, and it's really neat. You can, by the way, download it for home users. There is a free version. The software is available. So if

you've got an old PC lying around you'd like to turn into a super bulletproof, super extra-powerful gateway, download the software for free. Astaro.com. I thank them for their support of this podcast.

And as always, I thank Steve Gibson for his tireless work protecting us, educating us, and helping us get the most out of our technology: GRC.com. I'll see you next week, Steve.

Steve: Okay, Leo.

Copyright (c) 2006 by Steve Gibson and Leo Laporte. SOME RIGHTS RESERVED

This work is licensed for the good of the Internet Community under the Creative Commons License v2.5. See the following Web page for details: http://creativecommons.org/licenses/by-nc-sa/2.5/