SECURITY NOW!

Transcript of Episode #58

Two New Critical Windows Problems

Description: Leo and I discuss the breaking news of two new critical Windows problems: A new vulnerability that is being actively exploited on the web to install malware into innocent users' machines – and a workaround that all Windows users can employ to protect themselves. And a serious file-corruption bug Microsoft introduced into last month's security update that affects all Windows 2000 users.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-058.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-058-lq.mp3

INTRO: Podcasts 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 58 for September 21, 2006: Security Alert!

Security Now! is brought to you by Astaro, makers of the Astaro Security Gateway, on the web at www.astaro.com. And by Dell. For this week's specials, visit TWiT.tv/dell. And by Visa. Safer, better money. Life takes Visa.

Welcome to Security Now!. Leo Laporte here, and actually this is a kind of change of pace. We'd already done, recorded a Security Now! when we learned of two serious security flaws. So because we are, you know, a podcast, and willing and anxious to get this information to you as quickly as possible, we'll put off our discussion of Parallels for next week and talk about the security flaws right now. Steve Gibson, what's going on?

Steve Gibson: Well, hey, Leo. The timing of our Thursday podcast coincides perfectly with two pieces of news that I think are both really important. One is there's a new, just recently discovered, zero-day exploit for Windows and IE which can affect people browsing the web. And it turns out Microsoft made a mistake – and this is the second issue – Microsoft made a mistake in last month's security updates. One of their updates can cause, for Windows 2000 users, file corruption. There's a fix available on Microsoft's site, but they don't have the original patch fixed. And so we're going to talk about both of these things.

Leo: Well, let's start with the first one first because we have Eric Sites on the line. He is Chief Technology Officer and VP of Research and Development at Sunbelt Software. We've talked about Sunbelt Software before. They're the great guys...

Steve: Well, yeah. In fact, you know, their Alex Eckelberry purchased our favorite firewall, our favorite personal firewall, Kerio, and sort of rescued it from oblivion. And so we've talked about that on several occasions.

Leo: Welcome, Eric. It's good to have you.

ERIC SITES: Ah, thank you, thank you.

Leo: Eric was telling me that he flew to Czechoslovakia when they acquired Kerio Personal. And they bought it because they were fans of it. You like that firewall.

ERIC: It's a great firewall. Lots of interesting features. One of the only firewalls that has IPS/IDS built into it. And then also the web filtering so you can, you know, get rid of advertisements, get rid of scripting, just by easy little checkbox.

Leo: And I like the price.

ERIC: The price is always good, yeah.

Leo: So first let's talk about this first exploit that Steve's referring to. In fact, I first learned of it when I got an email from a listener in Blackpool, England, who said Steve was right, turn off JavaScript.

ERIC: Yeah. That was initially the first way to deal with the known exploit that's in the wild. But we've since learned that you need to unregister the VGX DLL because you can still be – other exploits can be created that do not use scripting.

Leo: Okay. We'll talk about how to do that so that you can protect yourself. But tell us, first of all, how did you uncover this? Sunbelt was the first to find this flaw.

ERIC: Yes. You know, we have a lot of researchers who basically spend all of their days, you know, searching the web, revisiting old websites that we know of that are used to – that use scripts and things to push malware down on people, push all the bad stuff down to users' desktops when they're just browsing the web. And so we have some automated processes plus these manual processes. And unfortunately the manual processes are still necessary. So while one of the researchers was checking a list of these known websites, he came across these strange pop-ups that normally don't exist when he goes to that website. So he started investigating it more. And it was actually several websites away from the original one he was on because they were using iframes, which is used a lot to direct you to another website that pulls down new data, and then to another website that pulls down other data.

Leo: These iframes are little HTML frames within a page that actually are another page embedded within the page.

ERIC: Exactly. Exactly.

Steve: And 'i' stands for 'inline' frame.

ERIC: Yes. Yeah. So, yeah, we tracked it down to the source. And we've reported on this kit called the "Web Attacker Kit." There's a Russian website you can go up to, you can buy this thing, and they offer, you know, tech support services, just like a real company, everything that a normal software company offers.

Leo: It's 20 bucks.

ERIC: Yeah, 20 bucks. And you give them your server credentials, and they install it for you and configure it for you.

Leo: Oh, hey, that's a deal.

ERIC: Yeah. And the basic idea is that they create a kit that allows you to exploit the users that come to your website.

Leo: So it's purchased by people who just want to distribute spyware mostly?

ERIC: Spyware and adware, mostly adware because they want to get paid for the installation of that piece of software on these machines. They'll get a couple of cents for every person that comes by. You know, and we've seen...

Leo: Unbelievable.

ERIC: Yeah, we've seen these guys very successful at it. And what this kit does is it figures out what browser you're using. If it's Firefox, there's exploits in Firefox it knows about. If it's Internet Explorer, there's exploits there. And it figures out what version of the browser you have and then targets a specific exploit to that version. Well, this new exploit works on XP SP2 with Internet Explorer and all the latest patches. So...

Leo: It works, as you point out, on - or actually it was your colleague, Alex, pointed out on the Sunbelt blog, it works no matter how patched your machine is. I mean, if you have...

ERIC: Exactly.

Leo: ...a completely up-to-date machine, it still works.

ERIC: Yeah. And this exploit actually also works all the way back to IE 5.0.

Leo: Do we know if it works in IE 7? We were talking about that earlier.

ERIC: We are still testing that. But there are some instances that it – if it's running on Vista, it doesn't. If you're running on regular XP SP2, we're still looking into to track that down.

Steve: You know, Eric, I think I know the answer to this question. But we've just been talking about this topic, so I'm just going to lead you into this. When you guys are surfing the web and going to probably malicious sites and doing so, how do you guys protect yourselves from actually damaging the machines that are visiting?

ERIC: Well, we use a product called VMware, which is...

Leo: Boy, was that a softball question, Steve. I'm ashamed of you.

Steve: Yup. We've just been talking about virtual machine technology and how they can be used to really provide robust protection. So you guys literally use VMware virtual machines, knowing that nothing that you do inside the machine can get out of there to infect your actual R&D and real research machines.

ERIC: Yeah. We have separate connections from our regular networks to these machines. And then on top of those machines we use VMware plus firewalls. One of the reason we use the firewall is for logging information to see what's coming through the network at a connection level. And then we use packet sniffers on top of that, and lots and lots of little tools.

Leo: Would running a firewall have protected me against this VML exploit?

ERIC: No. Because it looks just like a normal Internet request. And since that request is coming from Internet Explorer, the firewall, all it knows is that, oh, this looks like Internet Explorer downloading something new.

Leo: It's legitimate. It's a...

ERIC: Yeah.

Leo: Yeah. Is it a graphic in the – VML's a vector markup language. It's a vector graphic file; am I right?

ERIC: Correct.

Steve: And have you gone in and looked at the code that is implementing this buffer overflow?

ERIC: Yes, yes. Well, there's the exploit code, and then there's the actual VGX DLL that has the bug in it. So we’ve actually looked at both. And the exploit code uses a technique which can read – once you’ve overwritten a buffer, and since this buffer is on the stack, you overwrite a lot of very important information that allows that new data to gain control of the executing program. So it overwrites this really important information. And then when the function call returns, then it can return to whatever code you’ve given it.

Now, there’s XP, sorry, IE6 SP2 has some things in it that are supposed to stop this. But since this bug is on the stack, and the amount of information you give it kind of blows, what they call “blows the stack,” they overwrite this protection. So there’s a couple of actual exploits out there that are on hacker websites, but currently they don’t have a reliable one that targets IE6 SP2. So right now we’ve still only seen this exploit in the wild is the only one we’ve seen that actually has a true XP SP2, IE SP2 exploit.

Steve: Wow. So it’s sort of advanced that technology, as well.

ERIC: Yeah. The guys who make this Web Attacker Kit, I mean, that’s pretty much their lifeblood is to find new exploits or build new exploits so that they can, you know, sell their services to...

Leo: Steve and I have talked about this before. That’s what’s really changed, I think, in the hacker climate. It’s no longer just for fun or to show off or for bragging rights. There’s money to be made.

ERIC: Exactly. It’s very rare that we see that type of thing anymore. I mean...

Steve: Now, you guys happened to discover this by going around to these sites. We don’t know at this point how long this exploit has been in use.

ERIC: Well, we’ve got, you know, as soon as we found this we started talking to the rest of the security community, the other security companies, antivirus companies, and guys who monitor these exploits, companies like iDefense, mostly that do just pure research. And they’ve gone back through their logs and say that it’s probably been out there for about a week. So it’s actually pretty new. It’s not on that many websites. But the number of websites that are using this exploit is pretty much growing very quickly. A lot of security companies, like Sunbelt, have what are called “web spiders” that can go across the Internet and actually look for certain things. So our spiders are going, looking for the websites that have this exploit on it. Another company that are good friends of ours called Websense is doing the same thing. They’re also, you know, sharing that information with the rest of the security community. We know a few others...

Leo: Do you have any idea of how many people use this Web Attacker Kit?

ERIC: I know personally of over a thousand websites that are using this kit.

Leo: What kinds of websites?

ERIC: Oh, just all kinds of this – pretty much anything. Most of it’s porn sites. Some of it...

Leo: They’ve got to put something up to get people to come to the site.

Steve: Well, and like how about fake freeware and shareware download sites?

ERIC: Yeah, well, that and – mostly, though, it's cracks or serial number sites.

Leo: Oh.

ERIC: Or what they call "warez sites."

Leo: Yeah.

ERIC: And the problem is, it's not the thousand websites we know of. It's all the other sites that use one of these iframes that communicate back to one of these sites. So there's, you know, that web is weaved very deep. So there's any number of websites you may go to, and it doesn't actually have the exploit on it, but it points back to another website that does.

Steve: Right.

ERIC: Now, there are many – well, the best way to protect yourself from this exploit right now – and the only way, since Microsoft hasn't released a patch for it – is to unregister the vgx.dll, the DLL that has the bug in it that these guys are using to exploit your system.

Steve: Right. We have complete instructions on our page, on the Security Now! page. Along with each podcast we have a page of additional links and information. And so I've got instructions there on that page for all of our listeners. You can follow...

Leo: It's just – it's a command line, is that it, just a simple command line?

ERIC: Yeah, a very simple command line.

Steve: Yeah, it's very simple. You just cut it right off the page, drop it into the Run dialogue off of the Start button, and you get a little pop-up that confirms that the DLL has been unregistered. You should then reboot your system to flush it out if it's already been loaded by an instance of IE, which is probably unlikely, but it's better to be safe than sorry. And from that point on, your system is protected.

Leo: Is there any side effect to doing this? What am I going to lose?

ERIC: There are a few websites that use VML. There are some advertising websites that have little banners and things. So if you go to, like, a news website, and it has a little banner, sometimes those banners will use VML to animate things.

Leo: So I'm not going to see a bunch of ads, big deal. I can live with that.

Steve: And Leo, the whole, you know, the whole vector graphics movement is – it's relatively new technology for the web, so it's very sparsely used. I doubt that anybody who did this and unregistered this, essentially turning off the ability for their systems to render these vector images on the web, I don't think anyone would notice any difference. And certainly it makes sense to do this until Microsoft is able to catch up with their next, you know, their early October patch cycle.

Leo: What kind of consequences could I expect if I don't do this? Let's say I go to one of these bad sites that's running Web Attacker. What's going to happen to me?

ERIC: Well, here's another interesting tidbit that's not widely known, that since VML is kind of embedded into Internet Explorer, and email systems use Internet Explorer to display HTML pages, you can actually craft an HTML page with this VML exploit in it that does not use scripting, that bypasses your Outlook protections and will actually exploit Outlook also. But right now it's only certain versions of Outlook.

Leo: And what happens after the exploit explodes?

ERIC: Well, as soon as you look at that email, and you view it in the preview pane or open up that email, that exploit can download whatever it wants to your machine.

Leo: So spyware, malware, trojans...

ERIC: Spyware, keyloggers. The first site we came across with this, in the morning it was only downloading one program, an adware called Virtumondo, which displays advertisements. By the late afternoon it was downloading 50 other pieces of malware, which included keyloggers, tons of adware, all kinds of stuff.

Leo: So what happens? The community, the bad website community goes out and says, hey, we found a – we've got a great way to get your software. Anybody want to buy some computers? They do an auction or something and say – and that's how they get all this new malware? People say, oh, yeah, please put mine on there?

ERIC: No, no. There's – all of the adware companies, they have services. You go up, you sign up for the service and say, hey, I want to install your software on the people who come to my website. And they give you some information that allows them to track how many people from your website install this stuff.

Leo: So you'll have a referrer code that they can then...

ERIC: You have this code, or some other information. And they basically – money automatically shows up in your account every month as...

Leo: It's tempting.

ERIC: ...you install this stuff.

Steve: Leo?

Leo: No, no, I'm not going to do it. But it's tempting. Look. This is an interesting debate, of course, is when do you reveal this publicly? Microsoft would far prefer people don't tell anybody about this. And the security community, you know, is constantly debating whether to reveal these exploits or not.

ERIC: Yeah.

Leo: What process do you go through about revealing this?

ERIC: Well, we have a pretty defined set of procedures that we look at when we come across things like this. And usually those procedures come down to, you know, if it's in the wild. If it's in the wild...

Leo: Once it's out there, you've got to tell the world.

Steve: I was just going to say, in this case, as a zero-day exploit, it's, you know, there's no reason not to immediately get the word out so you can start protecting users.

ERIC: Yeah. I mean, you have to. You have to contact the security companies. You have to contact the AV companies so they can write signatures for these web pages.

Leo: Do you call Microsoft, too?

ERIC: Yes. Yeah. That's about the first thing you do. You always call the vendor, whoever makes that software that's got the exploit on it, you talk to them and say, hey, you know, we've found this. If it's something that you haven't seen in the wild, you go through a period of letting them fix this bug, however long it takes.

Leo: Right, right.

ERIC: Sometimes it may take a month, four months, five months, six months. Hopefully...

Leo: Sometimes longer.

ERIC: ...by six months they get it fixed.

Leo: I've talked to some guys at EI who have known about an exploit for a long time. And eventually your patience wears thin, and you just feel like you have to tell the world.

ERIC: Yeah. I mean, sometimes that happens. And their feeling on it – I'm not picking on EI, but other security researchers, a lot of usually the independent guys, they'll release it just to get that vendor to fix that bug.

Leo: Or just to get some notoriety. I mean, if you're a small guy, and you want to get a name for yourself, that's one way to do it.

ERIC: Yeah, yeah. Unfortunately, that does happen. But, you know, our procedures are, if it's not in the wild you tell the vendor, let the vendor fix it, and you just keep checking with them and saying, hey, guys, you got it done yet? Is it fixed? You got it tested?

Leo: When you called Microsoft yesterday, what was their response?

ERIC: They – usually don't get a lot of response from Microsoft. You basically get a lot of canned information that says, okay, we're looking at it.

Leo: Right.

ERIC: And then usually they'll start publishing this information through their normal channels so that everybody gets the information at the same time. So they started doing that. And now you've got a TechNet article out there that basically gives all the information that, you know, an IT company would need, the antivirus guys, other security companies like ourselves.

Leo: Eric Sites is the VP of R&D at Sunbelt Software, sunbelt-software.com. And of course we tell people to go there for the free Kerio Personal Firewall, a great firewall. But we also thank you for giving us an update on this VML exploit, too, Eric.

ERIC: You're welcome.

Steve: Yeah, thanks so much, Eric.

ERIC: You're welcome.

Leo: Take care.

ERIC: Thank you.

Leo: Thanks. Now, that's just Exploit No. 1, Steve Gibson.

Steve: Yes, it's been a busy day.

Leo: We ain't done yet. What...

Steve: Okay. I want to – before we leave this, I want to make sure that people get basically the main headline takeaway issue, which is all versions of Windows using IE, you know, modern versions of IE 5 and 6, have in them a newly discovered buffer overrun which is being actively exploited, as we heard Eric explain, on the ‘Net to install, you know, all kinds of bad stuff. Microsoft has said that, unless they change their mind and release a patch for this sooner, it’ll be part of the early October update cycle. So, you know, three weeks from now, or almost four. So in the meantime it is possible to just remove this VML-rendering capability by unregistering it from the system. The system will then just sort of not know about this bad DLL where the exploit exists. Your browser will lose the ability to render vector graphics. But almost no one uses that now. I mean, it’s not like you wouldn’t be able to show GIFs or JPGs. They all still work just fine. It’s only this special type of scalable line drawing, which is what is lost.

So on the Security Now! page we’ve got the specific information, a link to Microsoft’s Security Advisory, and a very clear explanation of how just to cut and copy this one line, drop it into your Run menu, executive it, you’ll get a little pop-up saying the DLL has been unregistered. Then after you reboot your system you are completely protected from this. And I really recommend everyone do this. A month from now, and we’ll remind people, you’re going to want to reregister this after Microsoft has fixed it. So you will restore the ability to render these vector graphics because ultimately in the future it may end up being used more. But it’s almost not used at all today.

Leo: But don’t run out and do it right away. Wait till we tell you it’s safe to do so.

Steve: Exactly.

Leo: So this second exploit is not nearly as much of a concern, in fact it’s no concern for XP users, but it is something to worry about for Windows 2000.

Steve: Well, and it freaked me out, Leo, because by pure coincidence – I don’t often update my main GRC servers because they’re working fine, they’re in a very secure and protected environment. You know, I’m not there using a browser on the server or surfing around the ‘Net. So the vulnerability window is much smaller, for example, for a typical server than it is for a user’s workstation where they are out there poking around. But as it happened, I was and did completely bring, not the main GRC server, but another ancillary server, up to speed last week. I patched...

Leo: Oh, you timed it so well, Steve.

Steve: Oh, my God. I completely patched it. Everything was fine. Then I got wind of this second issue, which is as follows: It turns out that the last month security update – this is the, I think it was August 8, it’s when Microsoft did, you know, their standard monthly update. One of the patches – and again, we’ve got links and all the specific information on the Security Now! supplementary page for this Episode No. 58 of Security Now!. One of their patches had a bug, as they call it a “regression bug,” where they broke something...

Leo: A regrettable bug.

Steve: Yeah. They broke something that they were trying to fix. And this was a kernel privilege escalation exploit which they were patching. Well, it turns out that what they broke, only for Windows 2000, and only for NTFS, and only for compressed files, is any compressed file on NTFS, which actually is redundant because FAT32 doesn’t do, you know, that level of compression.

Leo: Right, right.

Steve: If it's updated or created or changed, and the file is larger than 4K, it can become corrupted. So, I mean, it's a serious problem. It's a file corruption bug which was intro...

Leo: That's a really bad bug.

Steve: It's really bad. And I got a kick out of, well, I got a sad kick out of Microsoft's, like, what to do if you have this problem. They say, well, restore from a backup prior to doing this. It's like, okay.

Leo: Because you've lost all your data. And so...

Steve: Yeah, because...

Leo: ...might be a good idea to restore it.

Steve: Because it is capable of corrupting files under Windows 2000 which are compressed. Now, for example, I deliberately will compress whole directories like my, you know, on my personal system, my source code directory is compressed because source code gets such a tremendous advantage from compression. So it occupies much less space.

Leo: Right.

Steve: So, okay. So the way things stand at this point, Microsoft has just released a fix for the problem. That is, there is a fix that can be easily installed. I immediately did this over on the server because last week I, by updating myself to the most recent latest and greatest security, I introduced this vulnerability. It does require a reboot. I was trying to think whether it did or not. Because I tried to install it a second time, and it knew that it had already been installed. So there I did not require a reboot. But anyone using Windows 2000, I strongly recommend you go to, again, to Security Now's supplementary information page. I've got all the details and links there. You can install a patch for their patch which broke this problem. And then they have not yet fixed the original patch from last month. So you can fix this in the meantime. And, you know, then this second really bad problem that only affects Windows 2000 users will be resolved.

Leo: Wow. Wow. Well, I'm glad, you know, the beauty of podcasting is we're very flexible. And if there's a need for an update, we will do it. And that's one of the reasons I like doing Security Now!. And of course, if this had happened on a Tuesday, we'd do it on a Tuesday because it is that important. We want to let you know.

Steve: Yup.

Leo: We will defer our discussion of Parallels to next week. We do thank you for listening.

We do remind you, of course, that the show notes are online at GRC.com. And this is one where you do want to go to those show notes to get that command line that will unregister the VLW – or is it VWL? I can never remember.

Steve: It's actually – it's vgx.dll.

Leo: It's the DLL that allows the vector library.

Steve: Yes. You're not able to delete it or rename it because Windows...

Leo: You have to unregister it.

Steve: Yes. Because Windows is watching for that and will automatically replace it from its DLL cache. So unregistering it and then rebooting your system, everybody listening to this who's using Windows wants to do this as soon as they can because, you know, as Eric said, this thing is spreading like wildfire because it is a brand new exploit that allows anyone who's innocently visiting a website or opening email to get themselves infected.

Now, it is worth mentioning something Eric didn't mention and we didn't bring up. The exploit code does run within the privileges of the currently logged-in user. So if you were a limited user, if you were not logged on as administrator, I mean, you still don't want this thing in your system. But it's another demonstration of the benefit of not running as an administrator because, as we know, here we are, you know, bringing this news to our listeners immediately. But "immediately" is a week after this has already been out in the wild. No doubt tens of thousands of users have already been bitten by this who have been going to these websites, you know, just innocently browsing the 'Net. So even though we're getting the information out immediately, had users not been running as administrators, if they'd been running as a limited user – and in fact I'm getting a lot of email from people who are saying, hey, you know, I've been trying that, and it's not as bad as I thought it would be. So it's not really that burdensome. And you would have always been more protected than you would be if you were running as an administrator. So, you know, again, that's always a good idea. And it would have made you more safe. Although still, you certainly don't want to be browsing sites and letting anything crawl into your machine.

I did really love it that – in fact, well, I did really love it that these guys are using VMware. Wasn't that perfect, Leo?

Leo: Yeah, yeah.

Steve: They're using VMware in order to go to these places, knowing that the stuff will be contained within a virtual machine and not able to get out and infect their machines.

Leo: Well, you said that. You said that a lot of security companies did that. And it makes sense. Why should you, you know, risk your own hardware to test this stuff? And that's how you do it.

Steve: Right.

Leo: Steve, we of course are sponsored today and every day, every week, by Astaro Corporation, makers of the Astaro Security Gateway line of network security appliances, complete protection from network, web, and email security threats, at Astaro.com. A great opportunity for those of you who listen to Security Now!, Astaro is offering Security Now! listeners a free demo unit to test to protect your networks. Call 877-427-8276. Mention that you heard it on Security Now!. Or you can go to Astaro.com, and you'll get a free demo unit. They'll ship it to your business or office in one business day. So, but do mention Security Now! because we'd like to let them know that we're glad they're listening and sponsoring this show. That's Astaro.com.

Also a tip of the hat to Visa and Visa's double layers, multiple layers of security, protecting your credit card. Make sure you sign your card. Choose a PIN that's unique and secret. Memorize it, don't write it on the card. And check your financial statements regularly. Visa wants you to know that it's safe to use your Visa online. Safer, better money. Life takes Visa.

And as long as I'm talking, let's get one more mention in here for the TWiT Dell ads. We've got a great Dell pick this week, a very affordable and I think a very good system, both laptops and desktops, at TWiT.tv/dell. If you're about to buy a new computer, check it out, TWiT.tv/dell. And in fact, if you use that link to buy any Dell, we get credit. And we appreciate it if you do that. TWiT.tv/dell. Thanks to all three for sponsoring Security Now!.

And thanks to you, Steve, we're going to get this out quickly. Probably take a little while to get the transcripts up because Elaine won't have much time. We're recording this minutes before it actually goes live.

Steve: Right.

Leo: But the transcripts will go out as soon as Elaine – thank you, Elaine, for an emergency job. But the good news is you'll have next week's podcast early. [It's okay, guys, really. I'll be unregistering that DLL along with everyone else! – Elaine]

Steve: Yes, and I will mention for people, this is important enough that I'm going to be putting links to all of this information on the GRC.com homepage.

Leo: Good.

Steve: So anybody who is, like, really in a hurry to get this, don't even worry about navigating through Security Now!, just go to the homepage, GRC.com. At the top of the page there will be a link to the Security Now! Episode 58 page that's got all the information to allow people to protect themselves. And I should also say, you know, certainly everyone listening to this knows people who they care about who are using Windows who are not listening to this.

Leo: Spread the word, yeah.

Steve: Please, yes, spread the word. You can either give them the instructions yourself because it's very easy to unregister this DLL, or you can certainly aim them at Security Now's page, where I've got all the instructions written out.

Leo: And of course that Windows 2000 file corruption bug, if you know friends who are running Windows 2000, you might tell them about that, too, before they corrupt their data. Unfortunately, this is one thing that SpinRite cannot fix. This is a file-level corruption, and SpinRite doesn't deal with the file level. It deals with the hard drive level. But if there is ever a problem with your hard drive or a file recovery issue, there is no better software out there than SpinRite. And get it at GRC.com or go to SpinRite.info for a list of wonderful testimonials of people who Steve has saved.

Steve: I've been getting so much email from people, Leo. It's just – I just love it.

Leo: Isn't it nice? I think sometimes – I'm not saying we don't like to get paid. But the acknowledgement really is, in many ways, the way we get paid. It really is nice to know that you're doing something that's helping people. It's a great feeling.

Steve: Yup.

Leo: Steve Gibson, thank you so much. We thank also our guest, Eric Sites from the Sunbelt Software company, for being on the phone with us. We don't usually have guests on the show; but since you know these guys, and we could get them quickly on, it's really nice to have them on.

Steve: Oh, and Eric was wonderful.

Leo: Yeah. He's very knowledgeable.

Steve: Yeah, really, he was really good.

Leo: Yeah. And these were the guys who found it, so it's always great to get them on. I'm Leo Laporte. We will see you next Thursday on Security Now!.