SECURITY NOW!

Transcript of Episode #52

A Busy Week for Security Troubles

Description: Steve and Leo discuss the week's security woes, covering D-Link and Centrino wireless buffer overflows which allow remote wireless compromise of user's networks and machines. They explore the recent revelation that JavaScript can be used to scan an unwitting user's internal network to take over their equipment. They talk about the purchase of Hamachi by LogMeIn and how Botnets are being used to create fraudulent eBay users with perfect "feedback" in order to defraud even careful eBay users. And more!

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-052.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-052-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 52 for August 10, 2006: Security Bulletins.

Security Now! is brought to you by Astaro, makers of the Astaro Security Gateway, on the web at www.astaro.com.

Time for Security Now! and, well, maybe an anniversary, maybe not, depending on how sticky you want to get about your definitions. It's Episode 52, Steve Gibson.

Steve Gibson: Yeah, I actually got some mail from people who were saying, you know, it's not this episode that's going to be the anniversary, it's the next one. And they were saying, had you numbered your episodes like a programmer, from number 0, then 52 really would be your first anniversary. Instead, you're one off. Like, okay, yeah, that's true.

Leo: Some of my podcasts do have an Episode 0. The pilot is usually numbered 0. But we never did a pilot on this one, so...

Steve: So it would be sort of like celebrating your birthday the day before your birthday.

Leo: Yeah. This is the last podcast of the first year, and the next podcast will be the first podcast of the second year. So when is the anniversary? Now or next week? I don't know.

Steve: I don't know.

Leo: Happy birthday. Happy anniversary. Let's not be too sticky. You know, it reminds me of, in the year 2000...

Steve: Let's have it be on both.

Leo: We'll celebrate both.

Steve: Both, yeah.

Leo: In the year 2000 remember there was that whole debate, is this really the end of the millennium, or, you know, well, it is the end, but is it the beginning of the new millennium? No, 2001 is the beginning of the new millennium, blah blah blah.

Steve: Right. Because there was no year 0.

Leo: Right. It just seems to me to be a semantic quibble. And I'm not going to get in the debate. But happy birthday, happy anniversary, 52 episodes – almost 52 episodes done. Now, that's true, I have to say, we can't celebrate till the end of this episode.

Steve: Well, that's a good point. That's a good point.

Leo: We don't know what's going to happen. Well, I do know one thing. This would normally be our mod 4 question-and-answer episode.

Steve: It would if we hadn't had such a frantic week of security events. We had the Black Hat and the DEFCON conferences in Vegas. And so much was revealed that I want to talk about that I just, you know, we'll just push these questions to our next mod 4 and cover the phenomenal number of things, and many of them very, very worrisome. I wanted to let people know that I'll be talking about a lot of things that they're probably going to want to follow up on. I'll have links galore on our show notes this week. Basically, I'll be making up for all the many weeks where I just say, well, I had no links to share, or, you know, additional notes. So, you know, check back next time.

Well, this page – and you know, Leo, you can copy them onto the TWiT site or refer people to the show notes page on GRC, whatever you want to do. But I want to let people know that there's going to be some things they're going to want to follow up on. Don't drive their car off the road trying to write these down if they're listening to the podcast Friday morning and not wanting to lose this information. It'll all be on our show notes page.

Many people sent me offers or links to what they thought were script-free, CSS-only menus. For one reason or another, none of them worked for me. So I wanted to – in our show notes is a link to the R&D menu that I developed over the course of those two months with the help of the great group of people in our newsgroups. And the menuing system that'll shortly be appearing on GRC is robust to a level that nothing else we have found on the web is. It runs cross-platform on all Mac browsers, all Windows browsers, old browsers, new browsers, I mean, virtually, I mean, almost shoe leather browsers. I mean...

Leo: Let me ask you, because that's difficult without doing logic checks using JavaScript for the browser. How do you do that without saying, okay, if you're Internet Explorer, do this?

Steve: Yeah, I mean, it really is difficult. For a while we had a number of what are called "CSS hacks," which take advantage of parsing errors that specific browsers have. And in fact...

Leo: Of course, if they fix the browser, then they fix that error, you're not going to have...

Steve: Well, I mean, exactly. It's not a, I mean, there were several places where we had them. I ended up working all of them out. So we ended up even virtually hack free. And there might still be one. Now I can't quite remember. There was a Safari behavior where I had to keep Safari from reading one CSS rule. But I've explicitly put the result of this work in the public domain. There's a banner at the top of the page, the mainmenu.css page, saying where I'm placing this in the public domain. I also, not only for myself, but for anyone else, I commented it extensively. I mean, almost a line-by-line commentary of, you know, what the heck this wacky thing is for. I mean, it is a phenomenally complex piece of work. But it's the most robust menuing system I've seen, and it is script-free.

Now, we're going to be talking about scripting here in the rest of our errata because scripting comes up several times this week. And it turns out that, I mean, you know, I surf, as I've said often, with JavaScript, all scripting, disabled because that's the right way to do it. And we'll be seeing a little bit more why here in a minute. But many menus are, as you said, require JavaScript in order to function. And, you know, so I'll go to sites where, you know, they don't work. It turns out that about 10 percent of Internet users are now surfing without scripting enabled. So 10 percent of sites, well, all sites that depend upon scripting for their site navigation are not going to be functioning without someone having to lower their security, enabling scripting, in order to get the menus to work. And it's a constant annoyance for me. So I just couldn't have GRC, you know, need scripting enabled.

And so anyway, so the point is there's a link, it's GRC.com/menu2/invitro.htm, which is just sort of the development menu that we ended up putting together. I say "we," me and all the people in the newsgroup who were, like, pounding on it and testing it and changing the window size and just, you know, I mean, it ended up being a tremendously robust solution, which I just want to bring to people's attention because there was a lot of interest in this notion of a script-free menu. And, you know, I've got one, and I'm giving it away to everybody.

Leo: That's great. That's great. Well, I'm sure the community will be very interested in what you've done and will be borrowing heavily, liberally, from your solution.

Steve: I hope so. It would be great. And I wouldn't have to be lowering my security all the time in order to use other people's menus.

Leo: Right, right.

Steve: Something else happened, well, a number of things. You know how – I don't know how much of an eBay user you are, Leo. But, you know, I...

Leo: I buy stuff all the time. I just bought two things this week.

Steve: Yup, I do, too. I realized I could get the old HP□11C calculators there, which I have now an inventory of, just because I never want to be without them. It's the best calculator ever created. And, you know, one of the things that anyone using eBay depends upon is that feedback because, you know, you want to know that the person you're buying something from is real.

Leo: Right.

Steve: And so you use the community's history with those sellers, and presumably the sellers look at the buyers' feedback to see, you know, okay, everybody is a good guy.

Leo: Right.

Steve: Well, get a load of this. The latest application of Botnets, you know, that we've talked about often, about trojan programs which get installed in people's computers and then use their Internet connections. Originally it was just to attack other people. Then we had spam problems where bots or these trojans were sending spam to people. The latest application of Botnets is creating fake high-confidence eBay users.

Leo: Oh, no.

Steve: They're using – Botnets are being now used to create new fake eBay users. Then they all do one penny, one cent buy-it-now transactions with each other in order to qualify them for leaving feedback. They leave raving positive feedback to create high-quality fake users that are then used by the Botnet runners, the Botnet owners, to create large dollar volume fake sales for something that looks very good. Then that of course allows users to get fooled into trusting someone who's going to take their money and never ship their product.

Leo: Oh, my goodness. Is there any way to spot that?

Steve: You can imagine that eBay knows about this, and they'll be doing, you know, whatever they can, you know, maybe putting little CAPTCHAs on, like, all the pages...

Leo: There you go.

Steve: You know, CAPTCHAs...

Leo: That'll do it.

Steve: CAPTCHAs being those little funky things where you have to type in something that it says in order to prove that you're human.

Leo: It's getting frustrating. There are CAPTCHAs everywhere now. You can't put a comment on Digg without a CAPTCHA. But that's because of these automated solutions that are spamming and doing other things.

Steve: Exactly.

Leo: Yeah. Oh, that's ter- I'm devastated because I do rely on those seller ratings. And...

Steve: Well, yeah. I mean, I've got a 100 percent perfect rating. And I'm, you know, I'm proud of it.

Leo: Well, I guess if you look at – if you read the comments, it should become clear when they're automated and when they're not. There'll be a certain uniformity to them, I would imagine.

Steve: I wanted to let everyone know, both from the standpoint of, you know, Security Now!, and also just, you know, eBay users, you need to be careful. Maybe, you know, maybe for something that's enough high value, have an interchange with the seller in order to get some confidence. I don't know, I mean, but anyway, buyer beware.

Leo: Yeah, no kidding.

Steve: Speaking of buyers, Hamachi was bought.

Leo: This stuns me. I never thought this would happen.

Steve: Yeah, I'm not happy about it because I trusted and got such a good feeling from Alex Pankratov, the developer and guy behind Hamachi. And, you know, I hope they keep it free. Anyway, it was bought by LogMeIn, which has, you know, some related services. Get this, Leo. When we first talked about Hamachi, they had about a quarter million users. Then they had, last December, after we talked about them and, you know, things really began to get going, they were at about three quarters of a million.

Leo: Wow.

Steve: In April, just, what, five months ago, they were at two million.

Leo: Oh, my goodness.

Steve: And now they have three million users.

Leo: Ho ho ho. So you're responsible for a total – two orders of magnitude growth in that company.

Steve: I think Security Now! really did serve...

Leo: Holy cow.

Steve: ...to put them on the map. And of course we also talked about it on Call for Help up in Toronto, so...

Leo: And I do think that word of mouth, it takes over once you get a certain critical mass.

Steve: Of course.

Leo: And so we helped them get to critical mass. And then from then on it was explosive. And I'm glad Alex, good, I'm glad he's going to make some money. I hope he's going to make some good money out of it.

Steve: Well, I mean, it was a beautiful system, well conceived. I always appreciated, I mean, like, right from the get-go, while it was still in beta, the UI was just beautiful, I mean, like really had someone paying attention to it, so...

Leo: Well, and if you wanted to, I guess you could download Hamachi Server right now and not worry about LogMeIn's involvement, just run it yourself.

Steve: That's a very good point. You could set up your own private...

Leo: Do it quickly.

Steve: Your own private Hamachi network.

Leo: It was never open source, which always bothered me. And this is one of the reasons I'm not fond of closed source. Had it been open source, even had he sold it, you could fork it, and there would always be a free and open version of it, regardless of what he did with it.

Steve: Yup.

Leo: So from his point of view it probably was smart to keep it closed source. He made, I'm sure, some money. But from the point of view of the user community, this is why I rarely will recommend a closed source solution.

Steve: Yup.

Leo: Moving on.

Steve: Okay. Well, got some bad news.

Leo: Uh-oh.

Steve: The bright guys down at EI in Aliso Viejo...

Leo: The great security company.

Steve: The big – and, I mean, they're a bunch of really neat young, you know, like White Hat hackers. They found a bad problem in D-Link routers.

Leo: Uh-oh, I just bought one.

Steve: Early – I know. Early this year they informed D‑link, toward the end of February, and gave them half a year to deal with it.

Leo: Uh-oh.

Steve: D-Link has done nothing. Okay? Now, and it's funny, too, because, I mean, the fundamental principles of security just keep applying. How many times have you heard me talk about not running services or servers, servers you don't need? And how many times have we said disable Universal Plug and Play?

Leo: Mm-hmm.

Steve: Turns out there's a stack overflow, a traditional buffer overrun, in a handful of D-Link routers – the DI-524, the 604, the 624, the 784, the EBR-2310, the WBR-1310, and the WBR-2310. Again, we'll have links on our show notes to EI's page, which talks about this. But reading from what EI said, they said a remote stack overflow exists in a range of wired and wireless D-Link routers. This vulnerability allows an attacker to execute privileged code on an affected device. When a specific request is sent to an affected device, a traditional stack overflow is triggered, allowing an attacker complete control of the router. With the ability to execute code on the device, it is then possible to apply modified firmware and ultimately compromise the entire network.

Leo: So you would use this attack to change the router's firmware and presumably put some code in there that would give you kind of easy access to the network. Now, if the machines on the other end are secure, would that matter?

Steve: Well, there's no way you would want the equivalent of somebody plugging their own connection into your inside, your internal network.

Leo: Right. I mean, you may not – they may have to find another attack to get into your machines. But at least they have unfettered access. It effectively turns off your firewall.

Steve: Well, it does anything it wants to. Now, we should say that this is a Universal Plug and Play server, and that's only facing the LAN side. So first somebody would have to get access one way or another to the LAN interface, that is, you know, so it would have to be code running in your machine that was talking to the router, or if you were using unsecured Wi-Fi, then of course that gives them LAN-side access. So unsecured wireless would then probably be the most typical entry point. But if anyone were, like, out, or driving, and you did not have WEP or WPA security on one of these D-Link routers – which after half a year, I mean, that's annoying. After half a year, this has not been fixed.

Leo: They should fix that, you bet.

Steve: Clearly, there just isn't enough pressure on D-Link to do this, or they would have. So, you know, maybe by us talking about it we'll help to bring some pressure to D-Link and get this firmware updated because that's all it takes.

Leo: Well, this is how EI works. EI's really good. I mean, they do, you know, it's a balance between full exposure and keeping it quiet. So they give you six months. But if you don't do anything in six months, then the only way to put pressure on a company is to announce it publicly.

Steve: Yup, yup.

Leo: You know, the idea – and the companies, of course, all get upset, well, you're telling hackers how to use it. Well, we told you first. And if you didn't patch it in six months, by now many hackers may in fact know.

Steve: Right.

Leo: So the only thing we can do is to tell the world. Boy, that's a shame. Now, it's fortunately not the router I bought, and...

Steve: Good.

Leo: So to lock my router down – first of all, it's not wireless, so that's a good step. Is it sufficient to turn off Universal Plug and Play?

Steve: Yes, because it is an overflow in that server. And, you know, we...

Leo: So we’ve always told people to do that.

Steve: Yes. We’ve always been telling people, unless you know you need Universal Plug and Play, turn it off. It’s a good thing not to have it on because it does allow anything that gets loose in your system to reconfigure your router behind your back. And now we know, because of – on these D-Link routers, because of a buffer overrun in the Universal Plug and Play server running in the router, it allows even a much greater degree of compromise.

Leo: So this is, once again, another reason to do these lockdown things that we tell you to do with your router, including turning off UPnP.

Steve: Speaking of which...

Leo: Uh-oh. Another one?

Steve: Oh, yeah. We all know what a fan I am of client-side scripting. And I’ve got my tongue in my cheek. I’m biting it.

Leo: Firmly.

Steve: Yes. You know, client-side scripting, in email, in web browsers, anything, is bad. You know, and people say, oh, but it’s so nice. It’s like, yes, and it’s bad.

Leo: Now, I’ve always agreed with you when it comes to Active Script because Active Script, which is the Windows technology, really has no sandboxing at all. But surely we’re safe with JavaScript.

Steve: No.

Leo: He said, setting you up.

Steve: Thank you, Leo. What has been figured out by some guys at a security company, SPI Dynamics, is how standard JavaScript with no bugs, no exploits, no buffer overruns, no mistakes at all, can be used to port scan your internal network, identify devices, take them over, reprogram them...

Leo: Whoa.

Steve: ...and send any information home.

Leo: So by going to a website, running JavaScript, they could do that to my internal network?

Steve: Yes. And there's a proof of...

Leo: Wow.

Steve: There's a proof-of-concept online right now that demonstrates – basically you go to their page. Their JavaScript will scan your internal network and any site you went to that was using scripting, and you can bet that it's not going to take long before this, I mean, this is now out in the wild. This was talked about at the Black Hat conference last week. And so all the bad guys know about this now.

Leo: So should I turn off JavaScript?

Steve: Well, yes. I mean, Leo...

Leo: Oh. But, Steve...

Steve: I've been saying it's bad.

Leo: But Steve...

Steve: This is what I'm talking about.

Leo: None of my sites work without, I mean, nothing works without Java.

Steve: Well, mine does. Why? Because it's possible. I mean, okay, but...

Leo: Yeah, but with all due respect, your site does not do all that much.

Steve: It doesn't jump up and down and dance around. I know. But...

Leo: It doesn't do a lot of things.

Steve: Okay. Let me just...

Leo: You don't set session cookies or anything, right? You can't.

Steve: No, I have – I'm just beginning to use cookies because that's another thing I want to begin...

Leo: But to set session cookies, don't you need JavaScript to do that? Or some scripting.

Steve: No.

Leo: You could do server-side.

Steve: Well, yeah. I mean, cookies have traditionally been server-side.

Leo: That's true.

Steve: Okay, so, okay. SBI Dynamics says, and I've got...

Leo: All right, I'm turning off JavaScript right here.

Steve: ...I've got links to this stuff – says imagine visiting a blog on a social site like MySpace.com, or checking your email on a portal like Yahoo's Web Mail. While you're reading the web page, JavaScript code is downloaded and executed by your web browser. I mean, we all know that's the way these things work. In this case, it scans your entire home network, detects and determines your Linksys router model number, and then sends commands to the router to turn on wireless networking and turn off all encryption. Now imagine that this happens to a million people across the United States in less than 24 hours. This scenario is no longer one of fiction.

Leo: Well, it doesn't break TWiT.tv too much. The only thing it breaks by turning off JavaScript is our Flash Player.

Steve: So they say...

Leo: We can recode that.

Steve: Yes. They say getting inside the Intranet, the scanner is written in JavaScript, which can be embedded into any HTML page. Simply viewing the page downloads the JavaScript along with the HTML to the user's browser, automatically executing the code once loaded. It does not matter if the user is sitting in a coffee shop using a wireless hotspot or inside an office building using a corporate network. If a user can browse the web, he or she can visit a page that includes the scanner and have his or her network, whether internal or external, be scanned and attacked.

Leo: Well, and using MySpace as an example is a very good example because, as we know, the WMF flaw was propagated to a million computers on MySpace just a few weeks ago.

Steve: Exactly. Exactly.

Leo: A lot of unsophisticated users on MySpace.

Steve: Anyway, these guys go on to explain how the equivalent of a ping can be created with JavaScript to ping all the IPs within a range. We know that JavaScript is able to determine the user's IP because we've talked in the past about how some of those sites scare people by saying we know, you know, the private IP of your computer. And we've said before, yeah, okay, big deal, that doesn't do anything. What in this case it tells the scanner what kind of network you're on and what range of IPs to scan for other machines. And they go on to show how this thing can find web servers and then send requests to web servers which may be less secure on the Intranet than they are from the outside on the Internet, where they're worried about, you know, bad guys getting in. And, I mean, basically do anything this thing wants to inside your network.

So, I mean, Leo, the problem is you are going to untrusted sites and running script that they provide. It's just a bad idea. I mean, it's unfortunate that it's bad. But like so many things that we want to do, they're not secure. And here is a perfect example now, finally, of what, you know, valid, non-buggy JavaScript can do on your machine whenever you visit a website that chooses to do this for whatever purpose.

Leo: Well, all I can say is we're going to turn off JavaScript on TWiT and figure out a way to make it work without JavaScript. There are a lot of things that use JavaScript, unfortunately, including ad banners and, I mean, a lot of the 'Net relies on JavaScript.

Steve: Well, you know, Leo, we trust you. I have put you in my trusted list on IE. And so when I go to TWiT, everything jumps around and dances the way you want it to.

Leo: There's not that much jumping and dancing.

Steve: So what I would say is, you don't have to turn it off and not use it.

Leo: Choose safe sites.

Steve: You don't have to turn it off and not use it.

Leo: Right.

Steve: Well, no. Like from your standpoint as a webmaster...

Leo: Right.

Steve: ...what you want to do is you want to focus more on the hopefully growing percentage of security-savvy users who will visit your site with JavaScript at least initially disabled. So, you know, I mean, and certainly I see sites more and more that say, you know, that stop me as I'm trying to enter, saying this site requires JavaScript...

Leo: Yes.

Steve: ...to be enabled. It's like, okay, well, and then I make a decision. How much do I want to go any further?

Leo: Right.

Steve: So from a webmaster standpoint, I would just say think, you know, disable JavaScript on your browser, use your own site, see if it's okay. And if not, ask your web designers to do a better job for non-scripted browsers who visit. Because if I had my way, everyone would have their scripting disabled by default until they chose to deliberately trust someone.

Leo: Well, and that's certainly how I'm going to set up my browsers from now on. But a great many sites, you know, all the AJAX functionality that we've come to expect, that's all JavaScript.

Steve: As a matter of fact, the SPI guys specifically address AJAX and talk about how JavaScript, because it's a component of AJAX, it is becoming, you know, more pervasive. And now we've seen it's not safe.

Leo: Oh. This is devastating. Fortunately, most of my sites – my sites make very little use of JavaScript, except for the admin interface, which is an AJAX interface. So all you'll lose is the ability to play a Flash Player. But for instance, there's some things that, well, I'll have to look at them. They're things like it won't launch iTunes when you click the iTunes button. So even a simple site like mine, JavaScript is fairly important for.

Steve: I know. Believe it or not, we got one more bad one.

Leo: All right.

Steve: It turns out that Intel Centrino Wi-Fi chip drivers have a bad bug in the frame processing, which – and this is one thing that also has come out just in the last week. Intel Centrino, you know, the widely deployed wireless chipset family that lots of laptops are using, has – the Windows drivers have a very bad bug that allows you to bypass Wi-Fi security. Any...

Leo: Now, is this the demo they did at Black Hat where they took over a MacBook? Is it the same flaw?

Steve: No, that's a different flaw.

Leo: Another flaw. Wonderful.

Steve: Yes, another flaw. This affects only Windows drivers. Again...

Leo: Now, Intel did ship new drivers for its Wi-Fi shortly after the Black Hat demo. I wonder if that fixed this flaw.

Steve: Oh, yes. This flaw has been fixed. I'm wanting to tell people about it. I mean, unlike the JavaScript problem, which, you know, we're stuck with...

Leo: We can't fix that.

Steve: ...this is a bug, it has been patched. Again, links on our page take you to a downloadable tester that will tell you what version of Centrino you have and which ones are vulnerable. And then Intel has a patch. Unfortunately, the patch is just huge. It's 130MB to download this. Although you don't have to install all that, but you do have to download that blob. And then, and in fact, on one of my tablets I was – I had a buggy driver in one of my tablets. On my little Libretto, it doesn't use Centrino, so I was fine there. But anybody who's got, like, that Centrino label on the back of their – or maybe the underside of their laptop ought to take a look at this because it is – the thing that's scary about it is that no encryption and protection saves you. This is an error in the packet processing, the frame processing before we get to encryption and security and decryption. So potentially somebody sending this specially malformed packet could execute code. Oh, and the code executed is at the privileged level of the driver, which of course is the kernel. So...

Leo: Is always Ring 0. That's how a driver has to work, yeah.

Steve: Exactly. So full kernel privileges.

Leo: Oh, wow.

Steve: So anybody using Centrino wants to get this stuff from our show notes and get themselves patched immediately.

Leo: Now there is, of course, this larger issue, which was demonstrated at Black Hat, with almost all, they said, Wi-Fi drivers. Similar buffer overflow, I expect, although they did not tell the world how the exploit worked.

Steve: Right.

Leo: But they attacked a MacBook. Of course they had to use a third-party Wi-Fi card to do it, which nobody would do since you already have one. But...

Steve: Right.

Leo: ...they said, and we used a MacBook because Mac users are so smug, we just wanted to show them they have problems, too. But it is a problem on Windows machines just as much. So this...

Steve: Yup.

Leo: There are holes in these drivers. But it's a really scary thing when you have security flaws in a driver.

Steve: Well, yes, and especially one on Wi-Fi because of the wireless problem, I mean, the opportunity to do wardriving, and one which affects you independent of WEP or WPA encryption. I mean, there is no protection for this other than patching the driver immediately. And because it's wireless, inherently, I mean, people have talked about the possibility of a wireless worm. Because a worm could jump from one wireless notebook to another, like in an airport or in a coffee shop, or even in a corporation where a lot of people are using, like, internal Wi-Fi hotspots.

Leo: I have to say it sure sounds like the hackers are winning today.

Steve: It's been a busy week.

Leo: This is bad. Do you have any good news at all?

Steve: I have a piece of really neat good news.

Leo: Thank you. Can you end with that?

Steve: Yes. And as a matter of fact, it is the last one of my lengthy list of errata for the week.

Leo: Because I don't want to end on such a scary note here.

Steve: There's a group called the Stop Badware Coalition that is developing a list, a comprehensive list of sites that are known to have malware content. Google has just started working with them.

Leo: Oh, wonderful.

Steve: And it's really cool. Google will alert anyone who clicks on a link which is going to a site which is known or believed to have some sort of spyware, malware, or just sort of generic badware. It'll instead take the user to this Stop Badware Coalition page...

Leo: Oh, fantastic.

Steve: ...just to give them a warning that, you know, you should know that there's, you know, there's been some concerns raised about the site you are about to visit. Do you want to keep going?

Leo: Holy cow.

Steve: It's very cool. And get this, Leo. It turns out that in a study they did a few months ago, prior to launching this, 10 percent of search results are of sites that have this collision of known badware.

Leo: Wow.

Steve: So one out of 10 links that Google returns, or any other search engine is returning – of course this is a great advantage for Google. And the Stop Badware Coalition guys are first working with Google. It's not an exclusive relationship, so you can imagine that all the other search engines are going to want to jump on this. Because, I mean, basically it's a cool service for protecting users from going to sites that have known problems.

Leo: It's a huge burden and a lot of power in the hands of Stop Badware. I should point out that Stop Badware is a coalition. Google, Lenovo, and Sun Microsystems are partners. It's kind of – it was – I think it's kind of a – I'm not sure, but I think it's kind of a newer group that was started kind of with this in mind.

Steve: Yes, and only recently.

Leo: Yeah. In conjunction with Harvard's Berkman Center. So, and Oxford University's Oxford Internet Institute. So these are good people. Consumer Reports is involved, as well. So I think that this is good. I mean, there is a lot of power now that this group has because...

Steve: Oh, imagine being incorrectly listed.

Leo: It would be, you know, devastating.

Steve: Oh, my goodness.

Leo: So it's important that they really be, you know, above suspicion in any way and that they be absolutely objective. And apparently they're so. I mean, I'm impressed with what they've done.

Steve: Yup.

Leo: So, and thank you, Google, for doing this. It's a risky thing for Google to do. I mean, it puts – it exposes them, as you know.

Steve: I think it's a next step. I mean, ultimately it's like – it's the kind of thing where it's like, yeah, I wish I'd thought of it. I mean, it's...

Leo: But it’s a risky thing to do because you’re going to get sued.

Steve: Yup.

Leo: I mean, let’s face it.

Steve: Google is being sued all the time anyway because people are pissed off that they’re not ranked where they think they should be in Google’s engine, so...

Leo: So thank you, Google, for taking the hit for all of us on this one. It’s an important thing to do. I bet you – you said other search engines should do this. They may be forced to just because Google’s doing it, and it’ll be one more reason for everybody to use Google. But I bet you there’s a lot of resistance among the management of these search engine companies saying, geez, we don’t want to go out on a limb like that.

Steve: Yeah. I mean, it’s just – who would not – I mean, if you were – you didn’t have any other reason to use Google, like liking it, if you were using other search engines, you could...

Leo: Now use Google.

Steve: I was going to say, who wouldn’t prefer that, just to have that extra layer of protection? So everyone – before long it’ll just be the way it’s done.

Leo: And as it should be.

Steve: Another step forward.

Leo: Exactly. Well, I’m glad you ended on a happy note. Actually I have one more story to add that really isn’t security, it’s more about privacy. But it just raises the issue of search engines and how much they know. I don’t know if you saw the New York Times article, I think it was today, about America Online. You may remember last week America Online admitted, and later apologized...

Steve: The screw-up, yup.

Leo: Yeah, that they gave a lot of information about searching – they published it. What did they do? They gave it out, or they – I can’t remember...

Steve: I didn’t follow it closely, either. I just knew that they were embarrassed, and they were apologizing for some sort of information disclosure.

Leo: They collected, well, they made a list of 20 million web search queries on AOL. And, now, you might say, as AOL did, well, they're anonymous. We're not giving out personal information. This database is just what people search for. We numbered the users so no one knows who it is. Well, an intrepid reporter for The New York Times looked at the information. And, you know, it's not as anonymous as you might think. He actually tracked down No. 4417749, mainly because her searches, as most of our searches would, I think, gave a lot of information about who she is. She was searching for landscapers in her hometown and searching for people with a last name that was similar to hers. And, I mean, it was enough information that this reporter was actually able to talk to her.

Steve: Wow.

Leo: So that's a terrifying thought. Would you like all the things you've searched for in the last year to be published on the Internet?

Steve: No. And, I mean, you could argue that it would be easy for people to also, to, like, misinterpret what we're searching for. I mean, after all the revelations this year about the NSA, you know, watching us, I'm – and there was something just the other day. I was – it was something to do with a suspicious, you know, anti-terrorism sort of website thing. And I just thought, boy, I mean, it's kind of creepy to think that what we do on the 'Net may be watched, and somebody may be interpreting our intentions, which of course, you know, that's the leap that they have to make is understanding why it is that a person is going there.

Leo: AOL did pull the search data off of its site over the weekend, apologized for the release. They're saying it was an unauthorized move by a team who actually just wanted to benefit the academic community, you know, here's a lot of raw information that maybe you can get some value out of.

Steve: Yeah.

Leo: So they did – I think they did it in the best intentions. But it just points up that, you know, there is a – you don't need somebody's name to know a lot about them.

Steve: Well, and, you know, that's really – it's funny you say that because one of my arguments against the whole third-party cookie thing is the aggregators are saying, oh, no, this is anonymous. It's like, eh, it starts out being anonymous. But when you acquire enough information – and that's the whole point of aggregating data. You aggregate all this, and you end up with something that can sometimes not be so anonymous.

Leo: I'll put a link along with your links to this New York Times article. It's quite...

Steve: Cool.

Leo: ...quite amazing. Well, now that we've scared the pants off of everybody, and maybe cheered them up a little bit with the Google information, I think it's time we adjourned this edition of Security Now!. But we'll be back next week. Do you want to pick up the virtualization topic?

Steve: Yes, that's what we're going to do. I'm going to talk about sort of the granddaddy of commercial companies, VMware, which I've actually been using for many years. And so we're going to kind of cover what they offer and their products and give people some introduction to that. And that'll be our next step in discussing virtual machine stuff.

Leo: I can't wait. Of course we want to thank the folks at Astaro for providing the wherewithal to continue this podcast. It's their support really that encourages me so much with Security Now! because, you know, we could go on doing this for a long time out of our own pocket. But the fact that somebody, a company like Astaro has come along and said, you know, it's worthwhile, we want to help support it, it just really – it makes me feel good. They are the makers of the Astaro Security Gateway. If your small or medium business network needs superior protection from spam, from viruses, from hackers, as well as complete VPN capabilities, intrusion protection, content filtering, and an industrial-strength firewall, all in an easy-to-use, high-performance appliance, contact Astaro, www.astaro.com, or call (877) 4AS-TARO, you can schedule a free trial of the Astaro Security Gateway appliance in your business. And of course, as always, non-commercial users, you and me, can download the software version of ASG for home use absolutely free. That's also at Astaro.com. And for a low price, I think it's 79 euros a year, you can add very strong antivirus, antispam, and other protections to it that's automatically updated. It really is a great solution if you've got an old box lying around that you could put Linux and Astaro on. This is a really neat thing to do. Astaro.com.

Of course, Security Now! is provided by Steve as a pro bono benefit to the community. But if you'd like to benefit him back, I just talked to somebody, it's so funny, this week who said, yeah, I bought a copy of SpinRite. I didn't need it, I just wanted to give something back to Steve. You don't have to buy it if you don't need it. But if you need file maintenance and recovery – I shouldn't speak for you, Steve. But I think you would agree with me. Don't buy it if you don't need it. But if you have a hard drive, you might want it. SpinRite is the absolute best in file recovery and disk maintenance. It's available at GRC.com. And if you want to read some testimonials, SpinRite.info is a great place.

Steve: And you're right, Leo, I mean, I would never ask anyone to spend $89...

Leo: You don't need donations.

Steve: Right. My whole goal here is just to plant the seed. I mean, sooner or later pretty much everybody who uses a PC over a long period has some sort of a disk crash, I mean, you know, a physical problem that they turn their machine on and it says, you know, "No operating system found." It's like, I mean, or...

Leo: Let me ask you a question. Because what happens with SpinRite is you make a boot CD or a boot floppy that'll run SpinRite. Because you run it from DOS, basically.

Steve: Correct.

Leo: Now that Macintosh runs on Intel, can I use it on my Mac machine, on an Intel...

Steve: You know, we're getting questions about that. And I don't know yet.

Leo: You have a Mac Intel. Why don't you try it?

Steve: Well, you know, I do. But I'm liking the Mac...

Leo: I don't think it'll boot.

Steve: I'm liking the Mac so much that first I cut the hard drive in half using Apple's Boot Camp.

Leo: Right.

Steve: So it was half Mac and half Windows.

Leo: Right.

Steve: And I got Windows installed and set up, and it all worked really well. It's like, okay, cool. Now I've got, you know, Windows on this really nice Mac hardware. Then I was using the Mac for a while, and I was thinking, I'm kind of liking this Mac side. So I wiped out the Windows side, and I used Boot Camp again to repartition it. And this time I only gave Windows 10GB out of my total of 80. And now it's gone completely.

Leo: Oh, no. Don't tell this...

Steve: Well, because one of the tools we'll be talking about is Parallels...

Leo: Yes, I love it.

Steve: ...which is a virtual – it's a virtual machine technology for the Mac which, on an Intel machine, runs Windows at full speed in a window.

Leo: I love it.

Steve: So, I mean, well, it's a cool solution because, for example, I've got some friends that I would like to have always had on a Mac, except they, like, need one particular application. I've got a really great realtor friend, and she has to have her...

Leo: The multiple listing or something.

Steve: ...this one application for her multiple – it is, it's her multiple listing thing, and it only runs under Windows. So this is like a perfect solution for her.

Leo: So it's not that it won't check the disk, because it's file system independent, right?

Steve: Well, yes. Because it's about the physical sectors. SpinRite actually runs underneath the level of the file system, dealing with the actual recording of data on the disk, and doesn't care what the data is that it's reading. It works to recover it and also to remove bad sectors from use, swapping them out with spares that the drives always have.

Leo: So it would work on Linux, it would on a Mac. The issue really is booting it.

Steve: People run it on their TiVos.

Leo: Oh, yeah, of course, it'd be great for that, yeah.

Steve: I mean, they fix – SpinRite'll fix TiVo drives that are in trouble.

Leo: Right, right.

Steve: So in theory. However, it is down at the bare metal. I wrote it, of course, all in Assembly language. And it's, you know, it was...

Leo: There's no BIOS, there's no traditional BIOS on a Mac.

Steve: Oh, then you're right.

Leo: So I don't think it'd work.

Steve: It's not going to bring all of the stuff around it. Still does – it expects to see a PC. So you're correct, Leo.

Leo: But I have a feeling, gang, with Steve's new love, that maybe somebody for Mac users, too, there'll be a SpinRite.

Steve: Well, and Mac people do use SpinRite by pulling the drive out...

Leo: Right, right.

Steve: ...and sticking it over on a PC. So...

Leo: It would work – that would work fine, then.

Steve: And it does, and...

Leo: Okay.

Steve: ...people have done it a lot.

Leo: Okay, that's good to know. GRC.com. That's also where you'll find the show notes, the 16KB version of this show for the bandwidth-impaired, and Elaine's fantastic transcriptions, for those who'd like to read their Security Now!, or many do, read along with Steve.

Steve: I'm seeing notes from people who are using Google to find the transcripts, which then lead them into the podcast.

Leo: Interesting.

Steve: And so we're acquiring people who are doing Google searches for things, and they run across the transcripts. And so it's really nice because Elaine's transcripts mean that Security Now! is searchable.

Leo: Right. Well, and I will add that it is going to be searchable in another way because we've done a deal with Podzinger, which is a BBN company, and they do amazing work in voice-to-text. And they are scanning now all of the TWiT.tv network programs, creating transcriptions – not as good as Elaine's, they're computer transcriptions – but good enough for searches. And we're soon to implement a new search box that – we already have a text search box on TWiT.tv, but we'll have a text and audio search box that will allow you to search any of the podcasts. And this will be great. So if you want to know more about Netstat, you can go and type "Netstat." Not only will it take you to the podcast where Steve talked about Netstat, it'll take you – it'll queue it up to that portion of the podcast.

Steve: Oh, very nice.

Leo: Isn't that nice? So there's a little player, you press play...

Steve: And you're able to do that without any scripting. That's amazing.

Leo: Yeah. We'll see about that. I don't know. It might not work without – I think as a goal for all websites, and certainly for mine, eliminating all scripting is, you know, all client-side scripting is worth doing.

Steve: Or a reasonable compromise, I think, is to minimize the impact from not scripting. You know, so as a – I think a responsible webmaster should just turn scripting off and, you know, see if the site is still usable. Maybe not all the bells and whistles are still working; but at least, you know, you could get around.

Leo: Well, of course I did do that the minute you told me earlier in the podcast. And as I mentioned, the only thing that seems not to work is the Flash-based player. I guess it uses a little – in fact I know it uses a little JavaScript to pull up the player.

Steve: Right.

Leo: But we can change that. That's just an easy thing to change. But the search still works, by the way.

Steve: Right. For people who are Firefox users, there's a very nice Firefox plug-in called NoScript.

Leo: Oh.

Steve: And NoScript does exactly what I recommend doing, and that is it allows you to run, by default, with scripting disabled, and then whitelist sites that you trust, you know, Google...

Leo: Excellent.

Steve: ...Amazon and so forth. So you get the best of both worlds. You get scripting – and TWiT.tv, of course. You get scripting for any sites you visit, it automatically turns it on on the fly, in the same way that Internet Explorer uses its zones in order to give you different levels of security, depending upon whether it's a default Internet site or one that you have explicitly trusted. So it's called NoScript for Firefox. And...

Leo: I was going to – I almost gave a point to Explorer and said this is a reason to use Explorer, because of that capability. So I'm glad to know about NoScript. That's good.

Steve: Yup.

Leo: Yeah. All right. We will say goodbye to you now. We'll be back next week talking about virtualization, and specifically VMware. Remember, TWiT.tv is a place to find, not only this podcast, but a great many others. We're actually going to be up to a dozen podcasts soon on all topics technology oriented. And if you'd like...

Steve: My God, you must be busy, Leo.

Leo: I, you know, I've decided to really make this my full-time job. I kind of was on the fence for a while. But...

Steve: It's working.

Leo: Now that we're getting advertising, we're getting – the donations have been very strong. And by the way, the fact that we have advertising doesn't mean stop donating. I really appreciate those donations. The reason is we use the donations to support infrastructure, which includes, of course, server expenses, equipment expenses, rent, that kind of thing. And the advertising money goes to the hosts, you know, to pay for them. Because everybody, including Steve, are doing it voluntarily right now. And me. But, you know, it's exciting. I think things are really going well. And I really think there's an interest in this kind of information. I know, if Security Now! didn't exist, I would be missing a lot of really important information. So I'm very grateful to you, Steve, for doing this for a year for – actually you're starting to get a little money now that we have advertising.

Steve: Well, and the audience seems to be holding. I mean, we're holding strong...

Leo: Well, we're growing. Oh, we're growing, baby.

Steve: Is that what the last number showed?

Leo: Yeah, if you look at the last numbers, I think some of the strongest numbers we've had yet.

Steve: Very nice.

Leo: So I'm very encouraged. People do like what we're doing, and we appreciate it. We're glad you listen. And we hope you'll be back next Thursday for another exciting, thrilling, gripping, and let's hope not so depressing, episode of Security Now!.