SECURITY NOW!

Transcript of Episode #145

Secunia's PSI

Description: Steve and Leo focus upon a comprehensive and highly recommended free software security vulnerability scanner called "PSI," Personal Software Inspector. Where anti-viral scanners search a PC for known malware, PSI searches for known security vulnerabilities appearing in tens of thousands of known programs. Everyone should run this small program! You'll be surprised by what it finds.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-145.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-145-lq.mp3

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

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

This is Security Now! with Steve Gibson, Episode 145 for May 22, 2008: Secunia PSI. This show and the entire TWiT broadcast network is brought to you by donations from listeners like you. Thanks.

It's time for Security Now! with Steve Gibson. We are going to talk about protecting your butts. That's what Steve's expert at.

Steve Gibson: PYB.

Leo: PYB, Protect Your Butt. He is the guy who created or coined the term "spyware" when he first discovered it on his system way back when, wrote the first antispyware program, and has handed it off since to many other folks. But that was just the beginning of many, many free security programs he's created, including the very famous ShieldsUP!. Of course his bread-and-butter is the world's best disk recovery and maintenance utility SpinRite. Steve Gibson, hi.

Steve: Hey, Leo, great to be back with you for Episode 145.

Leo: You're beating TWiT now.

Steve: 145.

Leo: We'll do 145 this Sunday on TWiT, so you're two days ahead. Congratulations.

Steve: Having started much far behind, we're making good progress.

Leo: It's those lazy TWiT guys. So we're going to - today we're going to talk about a way to protect your system, your PC; right?

Steve: Well, yes. It's - I don't know if I'd describe it that way. I would say it's, from my experience, an absolute must-try utility. It's free, which it's being published and authored by a well-known security group who I've known of for years, that is a - it's a scan of all the software that you've got installed for known security vulnerability. So it's, I mean, I think of it as the next thing we need for our Windows machines after we've got Microsoft Update and/or Windows Update, Microsoft Update being sort of the more comprehensive of those tools. You know, that keeps Windows current. This thing does its job for everything else. And, I mean, on every single machine I have, even well-maintained machines, there isn't one where it didn't show me I had a couple of applications with known vulnerabilities.

Leo: Really.

Steve: Yup.

Leo: Well, I wish they made this for web servers because I had a little problem yesterday with hacking, and...

Steve: Oh, no.

Leo: Yeah. I think I had a disgruntled user on our private TWiT forums, who I had to ban. He was just horribly offensive, and I banned him. And about an hour later a SQL injection attack, and all the data had been overwritten by a hacking, you know, a hacker tag. And then he did the same thing to another website on the same SQL server. So I have to figure out where that vulnerability lies. I don't think it's in the forums software because it also happened to WordPress. I think there's some vulnerability into my SQL server.

Steve: Ouch.

Leo: Ouch. So I'm embarrassed to admit that that happened. In fact, I don't - I haven't really admitted it anywhere else because I don't want to give him any publicity, of course. But since this is a security podcast he probably doesn't listen to it. Most script kiddies don't.

Steve: I would imagine that, yeah, exactly.

Leo: And, you know, I think it really is a - it's a scripting, you know, I could tell it was a kit attack, you know, something he'd downloaded from the Internet. But now I have to go figure out what's wrong with my SQL.

Steve: Yeah, there are now botnets which are specializing in SQL injection attacks of websites because this is just - it's a huge problem that they're, I mean, basically web servers are now the prime target for these kinds of attacks, like for where we are in the first half of '08. And this is going to be the SQL server injection attack problem. I mean, the number of hits on servers that are attempted to be compromised has gone way up in the last months.

Leo: Yeah, yeah. It's too bad, but and so we need - I guess probably there are programs like that program you're going to talk about in just a little bit that will do that for web servers. If anybody finds one, let me know. I'd love to run an automated program that says, oh, here's hole number one, hole number two, hole number three and so forth. Are any big security stories out there you want to cover before we get to...

Steve: Oh, I've got a bunch of stuff, as always. I did want to mention that we talked last week about the what was for us new discovery of PayPal's one-time-use credit card.

Leo: Which I've now used, like, eight times.

Steve: Oh, I love it. Well, I mean, okay. I love it with reservations. First of all, the good news is there is a Firefox plug-in in addition to an IE plug-in.

Leo: Oh, cool.

Steve: And they both behave themselves very well. I have been impressed when I've gone to an eCommerce site and gotten to the page that wants the information. The plug-in is watching my pages. It recognizes, ah, here's the shipping address, here's the billing address, here's the credit card information. And it populates all the fields for me, including populating the field for the one-time use credit card.

Leo: Well, see, I haven't - I didn't know that. I've been going to the PayPal page and getting that information, cutting and pasting and everything.

Steve: And that's why I wanted to make sure you and our listeners who use Firefox knew that this is available for Firefox, as well. It's not currently compatible with the Firefox v3 beta. I would imagine they'll be fixing that or they'll, you know, one way or another that'll get resolved for us. But it runs on Firefox 2. And it's very convenient. I mean, it's way more convenient to use the plug-in than it is to have to go over to PayPal all the time and do that, go through that manually. You do have to authenticate yourself. So I've got my little football, my PayPal football, not far from me. And log in, give them a football number, and then they sort of run a fun little animated, you know, like breaking the code sort of thing as they invent a credit card number. I also liked the fact that the expiration that it chooses is always next month. And there was something I signed up for...

Leo: Well, it's always next month unless you pick the...

Steve: The recurring.

Leo: The multi-use one, right. And then it's 2010, I think.

Steve: Yes. There was something that I wanted to subscribe to that sort of had this annoying, well, you know, unless you remember to cancel your subscription, we'll just automatically bill this card every period. And I'm thinking, ah, no you won't, baby, because this card is good once. But anyway, so...

Leo: I did find one little issue on Amazon.com. If you purchase something from a third party, you can't use the card for Amazon because the third party is the one using it.

Steve: Oh, yes.

Leo: I think that that was what happened. I'm not sure. But I got - every time I've used a third party it's been rejected. So...

Steve: And I've never had a rejection. So, yeah.

Leo: Hmm. Have you always bought on Amazon direct from Amazon, or are you buying from third parties?

Steve: Yeah, oh, yeah, Amazon loves me. The first couple of years of Amazon I was getting Christmas presents from them.

Leo: Oh, me, too. But sometimes now when I buy on Amazon it's through Amazon, but it's not Amazon, it's another company.

Steve: Yes.

Leo: And, now, maybe there was something else going on. For instance, my PayPal has a fairly low limit, so it may be that they just prevented it because it went over the limit. I'm not sure.

Steve: Now, my standard annoyance with PayPal does apply. This is something we've talked about before. I don't want them pulling from my checking account. I don't like that. I want them pulling from my registered credit card. And we've talked about how when I'm purchasing from PayPal, every single time, because there's no way to change that preference, you've got to go in and manually override PayPal's default of pulling from your registered checking account. Well, using this one-time use credit card there is no way to do that. You have no option. And so I'm going to have to say to Sue, who keeps track of my checking account and stuff, I'm going to say, okay, Sue, now there's going to be some little weird things happening here. I hope that doesn't throw off her balancing my books at the end of the month.

Leo: That's too bad, yeah.

Steve: It really is annoying. So...

Leo: Yeah, because there's really no interface to say anything about it. It just gives you the card number.

Steve: Correct. Correct. And, oh, you can create an outstanding balance with them. So I guess I could move a block of money in, keep a balance with PayPal, and then they would pull from that. Which may be what I do. I mean, I really do like the idea of using one-use credit cards. And that's why the idea is, of course, spreading around the industry slowly.

Leo: Yeah. And as I mentioned last week, there are credit - I think most credit card issuers will do it. It's just not as easy. It's more difficult to find. It's almost as if they don't want to.

Steve: None of mine do. So I don't...

Leo: Oh, really.

Steve: ...have a choice at this point. I wanted to also mention we talked about last week how the extended validation display, the green window, the URL window, which is supported in IE7, we talked about how it is disabled when you disable the phishing filter, and how annoying I found that, and superfluous, and without any reason. The IE8 beta does not have that behavior. So the good news is, even if you do disable phishing in IE8, which they call the "safety filter," sort of more generic, I guess, you do keep the extended validation display enabled. So at the point that we begin to move over to IE8, we'll get the extended validation display regardless. I also screwed up last week telling everyone that last weekend was the weekend of "The Andromeda Strain" miniseries.

Leo: Wasn't it?

Steve: No. That's the good news for those of you who...

Leo: You didn't miss it.

Steve: ...forgot. You did not miss it. It's actually on Memorial Day itself, meaning it's next Monday, May 26. I've got my date straight this time. I checked three times. TiVos all know about it. A&E's website agrees with me. I said, okay, I'm going to get this right. So it's two hours on Monday the 26th, and the concluding two hours the following night on Tuesday the 27th. So it's going to be a four-hour event by the Scott brothers, Ridley and Tony, who have produced this. And again, the trailers and previews really look good. And there was one - I mentioned also that the DVD would be released next month. Some person who had never seen it was already badmouthing it as a review on Amazon, saying that it completely destroyed, you know, the wonderful classic from 1970, the original one. It's like, okay, yes. I mean, that was a great movie. I've seen it many times.

Leo: That was Dustin Hoffman in that; right? Or was that "Outbreak"?

Steve: That was "Outbreak," which I really liked, too. I've seen that a number of times, too, really like "Outbreak."

Leo: Who was in it, though? I remember "Andromeda Strain" very well, but I confuse the book and the movie because the book's so visual, you almost think you're seeing it.

Steve: Yeah. I have no problem with there being another one. It doesn't, in my mind, destroy the old one. I mean, I can still watch that if I want to. But here's this, this really looks like it's going to be, you know, good fun remake. And on the topic of sci-fi, [sigh], Peter Hamilton has started another trilogy.

Leo: I am still stuck in the middle of "Night's Dawn." It is the longest book I've ever read. It's on my Kindle, thank goodness, or I'd be carrying 80 pounds of books around. I love it, but I keep looking down, you know, the Kindle shows little dots as you're progressing through the book, and they're not moving very...

Steve: Oh, no, they're not going to move much. I was - I had some time to kill Friday afternoon, actually before seeing "Iron Man" for the second time, which I really liked, again.

Leo: You saw it again, wow.

Steve: It was wonderful for me. And so I was just browsing through Barnes & Noble and the sci-fi section of paperback land. You know, it's very familiar territory for me. It's becoming less more so now that I've moved over to eBooks. But sticking out on the bookshelf of paperbacks was this huge, I mean, it looked like a dictionary. And it was titled - it had Peter F. Hamilton's name on it. And it was titled "The Dreaming Void." And I'm thinking, oh, well, this is new. And so it was $29.99 at Barnes & Noble. It was $9.99 on Kindle. And then I - it's set way in the future. 3589 is the year where this thing is set. So it's 1500 years beyond where we were with the whole Prime drama, "Pandora's Star" and "Judas Unchained."

Leo: Oh, so this might really be the third of that.

Steve: No, no, no.

Leo: It's not.

Steve: This is its own standalone trilogy. What's weird is, there are some characters that have been brought over from "Pandora" and "Judas." So you probably need to read those first in order to get into this. But frankly, I mean, Leo, I feel a little bit the way you do. I mean, from what I've read online, various reviews, it sounds like this is another monster, huge, deep character development, lots of threads running in parallel, I mean, it's another one of these big Hamilton projects. And I don't have the strength for it right now.

Leo: Yeah, I know what you mean. But it's nice to have it in abeyance, isn't it.

Steve: It is nice to know that it's there. I'm actually finishing up the third of [Michael] McCollum's Antares trilogy, which I'm rereading just because it's just such a fun, simple, light space opera.

Leo: Yeah, yeah, I loved that. That was a wonderful book.

Steve: And in a bizarre thing that we've never done before, I have a wedding anniversary wish, wanting to wish a married couple who listen to our show a happy wedding anniversary. They'll be - their anniversary occurs before our next week's podcast will air. That is, their anniversary is May 22. And Sven Thomas asked me if I would just wish them, he and his wife, a happy wedding anniversary. They've been listening to Security Now! since the beginning. They love the show. And so Happy Anniversary to Sven and his wife.

Leo: You say "they." So you think she's into this, too, huh?

Steve: He says, "Steve, my wife and I have been listening to Security Now! since Episode 1 and have greatly enjoyed listening to you and Leo talk about everything from turning worms to your run-in with DoS and the many discussions on network security," blah blah blah. And...

Leo: That's great.

Steve: ...they're using an Astaro Gateway.

Leo: Well, they must be a geek couple. That's good.

Steve: Yeah.

Leo: I like that.

Steve: And he didn't say which anniversary it is, but I wish them many more.

Leo: Very happy - many returns of the day and happy congratulations. So do you have any errata or addenda you want to do from last week?

Steve: Well, two little things. I wanted to mention over on the security news side, nothing really has happened in the last week, security-wise, although what's funny is every one of my XP machines has insisted on having Service Pack 3 installed, even when they are fully patched. So what was happening for me was there was the second Tuesday of the month where we talked about a substantial set of updates, remember there was Office and something in the Jet database both needed to get fixed.

Leo: Yeah, I remember that.

Steve: So it was a big important cycle for updates. So even when you're completely current, you still have to do the whole Service Pack 3. Now, they're saying online that there's like a - the way it happens is you update your Windows Genuine Advantage tool, and then it comes up and bugs you again about your settings for automatic updates, which mine are set to download them but notify me and not install them so I can choose when I want to do that because almost always you've got to reboot your system, and I don't always want to, you know, I've got so many things going at once it's like, okay, I don't want a forced reboot right now. So I like to have that control.

Leo: Well, the first thing I asked you when you told me about the security program is do I have to reboot? I hate rebooting.

Steve: Yeah, it is, it's inconvenient. So once the update for Genuine Advantage happens, then you get sort of a special screen that's promoting the use of Service Pack 3. Now, they say it's a 66MB download. Yet Service Pack 3 is huge. It's 300 and some-odd - 324MB. And so for me it's like, well, I've got it on a bunch of thumb drives around here. So I just go and say, okay, fine, I'll take care of that myself. But I don't know what happens if you push past that and effectively refuse to download Service Pack 3. But it's probably a good thing to do. Again, my theory is that Microsoft is now testing everything against fully patched, current machines. People who run into trouble sometimes do because they're not keeping themselves current. And so I think it's just like, okay, I've given up this idea of selectively installing these things. It's like, eh, no, just come on, go ahead and do it.

Leo: Well, you know, you're downloading the network or the IT install, which is the full install. You could all, I mean, I think if you do Windows Update it's smarter about that, wouldn't necessarily do that, all of that stuff.

Steve: Ah, that is very - a very good point.

Leo: Yes. So you're getting - when you do the IT install, the full install that you can put on a CD, it's going to give you everything because it's not making any assumptions about what you've done already or not. I imagine, I mean, I remember Service Pack 2 was 273MB, I think. So Service Pack 3 would probably include everything in Service Packs 1 and 2, as well; right?

Steve: Well, it does need to be - it needs to be installed after Service Pack 1 or Service Pack 2.

Leo: Oh, okay.

Steve: So it has that as a requirement. So there's some stuff that it makes - that it assumes you're going to have, you know, probably the few things it didn't change between then and now.

Leo: Oh, that's interesting, okay. Because, yeah, in the past service packs included - were basically a rollup of everything.

Steve: Right.

Leo: So now they want you to have SP2 installed first.

Steve: Yes. And, you know, of course many XP systems are XP with Service Pack 2. That is, as you get them they've already got the Service Pack 2 rollup, essentially, preinstalled in them, sort of merged in. So, and in my case it makes sense for me to download the full network install and stick it on some thumb drives because I've got so many machines around here that otherwise I'd just be redundantly downloading the smaller one multiple times. So it does make more sense to do it once. And then you end up with a much faster, a much faster setup each time because you're not sitting around while it redownloads it again, so. And I did have this time as a little bit of a twist, a different twist, an interesting SpinRite story because this one's subject was "My First SpinRite Failure."

Leo: My what? You're going to tell people how SpinRite didn't work?

Steve: Indeed.

Leo: Steve?

Steve: This is Matt Clipper, who wrote from Phoenix, Arizona, a Security Now! listener. And he said, "Hi, Steve. I've been a SpinRite customer since March '06 and a fan of yours since first seeing you on The Screensavers many years ago."

Leo: All right.

Steve: That, of course, was your show, Leo, many years ago.

Leo: Yeah. That was the Click of Death I think you were talking about for ZIP drives.

Steve: Yup. He said, "I've also been a listener of Security Now! since Episode 1. I'm not an IT professional, but all my family and friends apparently think I am. I actually have a mechanical engineering background, but I've always been into computers and technology, ever since my grandfather bought an 8088 IBM clone when I was about 10 years old. Even at that time I was the only one who could figure out how to do anything with the computer." Especially that machine, you know, an 8088 with a couple floppies in it. Anyway, so he says, "Anyway, I've used SpinRite dozens of times to recover hard drives of my own and my friends and family. However, I've come across my first hard drive that I haven't been able to recover with SpinRite, and I was hoping you might be able to offer some advice. My sister has a Barracuda 7200rpm, model blankety-blank, whatever, hard drive that has failed. The only thing that's really on it that she wants to recover are all the digital photos of her son that she's taken over the years. She sent the hard drive to me, and I installed it in one of my PCs. At first it wouldn't even be detected by the BIOS, or spin up, for that matter. I tried a few tricks such as freezing the hard drive and tapping it with a rubber mallet to loosen any stiction that might have built up. I was finally able to..."

Leo: You know, we should mention that that's an approved procedure; right?

Steve: Oh, absolutely. I've done it myself.

Leo: Whack it.

Steve: Well, you don't want to freeze the hard drive. You want to - but putting it in a refrigerator to cool it off, just changing the temperature of the drive can sometimes really help in, like, real end-of-life situations. So this guy...

Leo: And stiction is where the head has kind of somehow gotten adhered to the surface of the platter.

Steve: Well, yes, it's caused because the head is incredibly smooth, the platter's incredibly smooth, you get actually a level of molecular bonding where those two surfaces, they become so tightly connected that the platter is unable to get itself started because the head has enough mechanical advantage that it'll just keep the motor from being able to start the drive.

Leo: So you whack it with a mallet, or I use a screwdriver. And just the jolt is enough sometimes to release the head.

Steve: Yup, yup. But that's more of a historical problem. I'm surprised if it's a newer drive. But, you know, it was - if he was in a situation where the drive wasn't spinning up, that's certainly something I would try. So he says, "I was finally able to get it to spin up and get the BIOS to recognize the drive, but couldn't get my system to read anything on it. At that point I tried SpinRite. But it would only get a few squares into the data recovery before the hard drive would stop spinning again." He says, "So I did some research and decided to buy a replacement logic card for the drive off eBay, thinking that it might have been the culprit." I mean, that's the next best thing you could do after all of this. And he says, "I made sure it was for the same hard drive model, same firmware version, even the same manufacturing location and approximately the same date of manufacture. I removed the old logic card, installed the replacement, and voila. No improvement whatsoever." So he says, "I'm not one to give up easily, clearly. But based on your expert opinion, is there any hope left? Thanks in advance for any advice you might provide." So, no. Matt...

Leo: It's a dead drive.

Steve: You have done everything humanly possible. You can cut out a chunk of this MP3 and email it to your sister, who will know that you have gone beyond and above the call of duty, that there is, I mean, short of literally submitting this thing to a professional data recovery facility that unfortunately charges, you know, many thousands of dollars to pull this thing apart, I just can't think of anything that you could do. Within your own shop, you've done everything possible.

Leo: Yeah, I mean, you know, I talk about this on the radio show all the time where you have soft errors, the kind that, well, either an unerase tool or SpinRite can fix, depending on whether it's a file system level or if it's, you know, a sector level. But then there's hard errors. There's physical damage. Software's not going to fix physical damage.

Steve: If the heads fall off the drive, then there's just nothing. Or if it won't spin up, or if it spins down before you can get to the area that you want to recover, I mean, this drive sounds like it's in really bad shape. So, yes.

Leo: Sometimes I worry that - I talk about SpinRite. I love SpinRite so much. I want to make sure that people understand it fixes a category of problems, not all hard drive problems.

Steve: Yes. I mean, I'm frankly surprised that SpinRite is able to do as much as it can. I mean, just as a piece of software, it performs miracles. But if you don't have a drive there, if it really is a doorstop, then there's nothing any software could do to help you out.

Leo: Right, right, yeah.

Steve: It certainly does have limits.

Leo: Well, and that's why there are people like DriveSavers, who have cleanrooms and guys in bunny suits, and they have every hard drive mechanism, all hard drive parts. And if a hard drive, if, you know, the bearings are frozen up and it can't spin, they can take it out, disassemble it in this cleanroom, replace the bearings, replace the platter, replace the motor, replace the head, whatever needs to be replaced, and that's why it costs thousands of dollars for people like that to get your data back. That's a whole 'nother...

Steve: It's the next level. And when your data is that important and, I mean, if it's worth many thousands of dollars, and $89 SpinRite was unable to save the problem - and by the way, I should mention that we absolutely offer SpinRite with money-back guarantee. We don't have a demo, and we've never been able to do a demo because unfortunately demoing it would solve the problem. I mean, it would...

Leo: Well, there are people, and it drives me crazy, you couldn't do this, but it really drives me crazy, some unerase programs do a, quote, "demo," where they say, oh, yes, I can see all your files, give me 500 bucks. And it drives me crazy.

Steve: Yeah, yeah.

Leo: You wouldn't do that. I can't imagine you ever doing that. And there are reasons, technically, you couldn't probably know ahead of time whether you'd be able to fix something.

Steve: And Leo, we give people their money back with no questions asked.

Leo: That's the best way.

Steve: So if somebody did use SpinRite, and it did recover their data, and they want to go to the trouble of asking for their money back, I'm not going to say no. It's like, okay, fine, you know. I don't regard that as a sale that I lost. It wasn't $89 that got away from me. And in the process maybe this person will recommend SpinRite to somebody else.

Leo: And I bet it doesn't happen that much because frankly, even if it doesn't solve your particular problem, it's so useful. You know, I got a frantic call Saturday, right before the radio show, from my wife's great-aunt, Auntie Dawn - actually aunt, Auntie Dawn - saying, "Oh, Leo" - she's in her 70s - "Oh, Leo, there's pop-ups on my screen, and bad stuff is popping up, I can't control it. And I called my ISP, and I don't know what to do." And, you know, I really feel there are a lot of people out there I feel for who just don't know - most users, I would guess, don't know what to do. Anyway, Auntie Dawn is coming up, and we're going to get it fixed for her. And of course one of the things I'll do is run SpinRite on it. And it's a case of, you know, maybe SpinRite isn't needed. But it's just a good thing to have. And if it is needed, you're really glad you ran it.

Steve: Yeah, I told the story about taking the manager of CPK's laptop, that was that crazy thing that had 86 processes running in it and...

Leo: Exactly.

Steve: Using up all the RAM it had just to get booted up, and it wouldn't do anything. And after I reinstalled XP from scratch I did give it a SpinRite pass. It took about two hours. I think it was an 80GB drive. Maybe it was 60GB. But, you know, it went through, I mean, it was just in beautiful shape afterwards. And so I was able to say to him, look, this is an old tank. I mean, it was a big old heavy Dell laptop that he'd bought refurbished three years ago. And, I mean, it was a monster. But the hard drive is in beautiful condition, which I now know thanks to giving it a SpinRite pass. So, yeah, it wasn't for data recovery, it was for the confidence of the drive's future.

Leo: Prophylaxis.

Steve: There you go.

Leo: And, you know, that's a very good reason to have and own a copy of SpinRite. I'm very glad that I have one. Let's talk about Secunia.

Steve: Secunia, yes. These are the guys that have produced something that I unequivocally - well, okay, one equivocation - almost unequivocally recommend. Some people are going to be a little put off by the fact that this does phone home in order to check the signatures of their software with Secunia's database. So that's the only caveat I have. I don't care. I use it, and I am really pleased with this thing. What this does is it is a very lightweight scanner. The downloadable executable is 485K. It behaves itself very well. I am very impressed with it. First of all, these guys are an old world - well, old world, they've only been around since 2002. So...

Leo: That's a long time.

Steve: ...they're six years old. Well, in our industry and in Internet years that's 200 years. I'm very familiar with their name because I see their name coming up all the time on vulnerability reports. They've got a staff of people that look at, that find, independently find vulnerabilities in software, much like the guys at EI do, and like McAfee and Symantec and all the other guys. And so anyway, so I'm seeing them talked about often, and I'm often at their website reading details of the vulnerabilities in specific software that I want to track down and understand better, often in order to talk about it here on our podcast.

Well, they've been working for some time now on a scanner, that is, to take advantage of this database they've built up of known vulnerabilities in common programs. They have a database of tens of thousands of program signatures. So, for example, when I ran it on my own main machine - this was this quad core monster that I had just set up - it found seven different problems. It notified me that the version of Opera that I had installed was 9.26, that there was a known vulnerability in 9.26, and that 9.27 was available. It found an old version of UPX, that's the executable compressor that I've been using to squeeze the air out of my Windows EXEs, just to make them smaller, because the portable executable format, PE format that Microsoft developed for Windows is just incredibly inefficient. It's just got huge blocks of unused space in it. So UPX compresses. Well, I had version 1.2. It was working just fine. But the Secunia PSI scanner told me that there was v3.02 available. So it was like, oh, cool, I didn't know that. I mean, I would have never known that unless something had gotten me to get up and go check manually. I also learned, although I had just installed the current version of Wireshark, which is the renamed version of Ethereal, the very nice open source free packet capture and display utility, I had version 0.99.8.0. I didn't even know it had gone to v1. But this PSI scanner knew. And I had just, again, like a week before, I had downloaded a copy of Wget, which is a little command line utility. It's a really nice GNU utility that allows you to grab web resources. It's sort of like right-clicking and doing Save As in your browser. But there are often times where you're not able to do that. And Wget does restartable downloads. It's just packed with features. Anyway, the one I had, had a security vulnerability that was known. And the PSI scanner knew about it.

Leo: Wow. So that's what it's getting - when you said it phones home, it's going out and it's say, okay, I see Steve has Wget. Let me see if there are any vulnerabilities. That has to be updated all the time, so that has to be local to the Secunia servers.

Steve: Yes. Now, so okay, so what it does is - it is lightweight. It does not sit here and stomp all over your machine. I mean, that's why I'm not installing any Symantec stuff or McAfee stuff because these things are - they're huge, and they just muck up everything. So this thing is very small and well behaved. It does put itself in the Start Menu. And it's happy to run in your tray. Well, again, I'm not somebody who's got 85 processes running all the time. So it's like, okay, I gently took it out of my - under my startup group because I don't want it running all the time. I'll run it when I want to just do a check. But when you run it, even then it's very well behaved. It doesn't saturate your machine. I found out it was using, like, 5 percent of one of my processors. So it's like, okay, I mean, this is an impressive piece of work. So it runs through, it looks at every executable, DLL, and ActiveX control. It generates a fingerprint of it. And for example, on one machine I had 85 executable things. And it then...

Leo: And you were complaining about your friend.

Steve: No no no no no no. Not running.

Leo: Oh, I see, executables available. I get it. I get it.

Steve: Exactly, on the hard drive. Total count installed on the hard drive.

Leo: That's nothing.

Steve: I know. And so it found those that, well, those were things that it knew it knew about. So it does download - it downloads something ahead of time, and it shows you what it's doing, and you can sort of see the progress as it goes along. It's downloading some updated something or others. Then it scans. And after that, apparently it - everything is over HTTPS, so it sets up SSL connections to their servers. And it then checks to see for the information that it then needs to download to show what it knows about these programs. And my point is that what you end up getting, in my opinion, is worth that tradeoff because you don't just get something that says, oops, you've got a problem.

And the reason I'm so stoked about this is what you get is so comprehensive. For every single thing, they've got what they call their "toolbox" - a download solution button, a solution wizard, you can rescan the program, get online references, technical details, open the folder where it resides on your machine. You can tell this you want to ignore that in the future. Or it just has a little quick link to Add/Remove Programs if you just want to go there in order to remove it. So with all this information, when you expand it, it shows you links to the manufacturer's most recent version.

I mean, I guess my point is that this is so much more than just, oh, you've got some problems. It will take anyone through the process of deciding if this is a problem for them and helping you, for example, the solution wizard in one case was a little popup dialogue that just sort of took me through removing, downloading, and reinstalling an updated version. So, I mean, it's very easy to use also. I'm really impressed with these guys.

Leo: Is it essentially just looking for applications with known security flaws? Or does it also look at other parts of your machine and say there's a flaw here, there's a flaw here.

Steve: No. It's just applications with known flaws. It does have access to Microsoft's Windows Update database. That's one of the things it needs is to be able to contact Microsoft because it's checking the Windows components versus Microsoft's Windows Update database. But it's not checking your apps for unknown vulnerabilities. Basically it's a very sophisticated version management system. And it's not checking apps that don't have problems. So it's not just - it's not going to tell you that WinZip, there's a newer version of that. It's not trying to do that. It's saying the version of WinZip you have has a known vulnerability, I mean like known to the world, not just known to these guys, because they've got a team of people that are looking at, you know, they're in the mailing lists and blogs and reading all the security vulnerabilities, and this is free. They have a commercial version that they called NSI, which is their network operable solution. And I think they charge $30 US, 20 euro, per workstation per year.

Leo: That's not bad.

Steve: So in a corporate environment this allows you, either with or without something running on the client side, it allows, like, a central panel to keep track of all of the machines within an environment and make sure that there are no known insecure problems in the apps of any of those machines.

Leo: It doesn't sit and run in the background all the time, though, unlike Norton or McAfee. You just run it whenever you feel like. It's a scanner that you run on demand.

Steve: Well, that's how I run it. It does, as I said, it does put itself in the startup group. So it would like to be sitting there and, like, checking in the background. I don't know how often it checks. Maybe daily or something. There's tons of settings. It also shows you, not only where your insecurities are, it shows you end-of-life products. I had - oh, it was UPX. I just clicked the end-of-life tab and got myself sidetracked here. Yeah, because this UPX v1, they flagged it as end-of-life. And it'll show you a list of all the programs that you have and the versions that it detected and whether they've been patched. So, like, patched things, things that have known problems and were then fixed, it found three instances of Adobe Flash, or Macromedia Flash, that were known. And I said, wait a minute, three? And it said there was a general plug-in, an ActiveX control, and an Opera plug-in, and they were all older, even though my machine was only, like, two weeks old, and there were known problems with them.

Leo: Wow.

Steve: So anyway, I just want to - I recommend this. We've got the links on my show notes. I'm sure you'll have them on yours, Leo.

Leo: You bet. But it's psi.secunia.com.

Steve: Yes. Or if you just put into Google "Secunia PSI," it's the first link that comes up. And then as you said, the URL is psi.secunia.com. It takes you to the page. It is completely free for personal use, or they do have the corporate use solution, as well. I think, I mean, I know our listeners, I have a sense for who they are from all the great feedback that we get. I am really impressed with this. I mean, this is something I'm running on, and I have run, on all of my machines. There isn't a single machine where there wasn't something I didn't know. And our listeners are people who want to know. This will tell them.

Leo: You know, the other question somebody had from the chatroom, SelfishMan asked, 64-bit Windows applications, he said it seems to have some trouble with those. Is that the case?

Steve: Ooh, that's out of my experience. I'm not over in 64-bit land. But I can certainly believe it.

Leo: I wouldn't be surprised. I mean, that seems to be a - 64 bits seems to be the sticking point for a lot of software.

Steve: Yeah.

Leo: Free Secunia. We'll have links at Steve's page and at my page. You can go, by the way, to Steve's site, GRC.com, and get 16KB version of this show for the bandwidth-impaired, full transcripts for those who like to read along while Steve speaks, which frankly I wish I had that luxury, but I don't as they transcribe them after we record them. I don't think they've yet found a time machine that allows Elaine to go backwards and do it. But you could find all of that at GRC.com as well as all the different security software Steve's written - ShieldsUP!, Shoot The Messenger, DCOMbobulator. You don't still have that original antispyware program you wrote on there, do you?

Steve: OptOut was the original program.

Leo: OptOut.

Steve: And it was so heavily linked to by the time I decided that I wasn't going to pursue this spyware issue - and the Ad-Aware people said, okay, we'll always make a free one, and I said okay, good, I don't want to have to do that, that's not my thing. But it was so heavily linked to that I replaced it with something that just said OptOut is no longer being maintained, you can go to the Ad-Aware people to get something that'll take care of your machine. So it's sort of there. It's sort of a stub of OptOut is there just to let people know where they should look.

Leo: Yeah, you never get rid of the stuff. The Click of Death program's there, isn't it?

Steve: Yeah, TIP, Trouble in Paradise.

Leo: TIP, that was it.

Steve: TIP, yup.

Leo: I mean, I imagine somewhere there's somebody with a ZIP drive.

Steve: Oh, then if they've still got a ZIP drive, they definitely need some salvation from the trouble of...

Leo: The Click of Death. They may well have it. I'll never forget that. That's when we first met. That must, you know, last week was the 10th anniversary of ZDTV, of our launch in May 11, 1998. And so...

Steve: Wow.

Leo: ...you must have been on in the first couple of years, I would guess.

Steve: I guess. It was, you know, it was...

Leo: Maybe 2000, thereabouts.

Steve: First time we met.

Leo: No, because Kate was still on when you came in.

Steve: Actually, Kate, I'll never forget this, it was so fun because I'd been on several times talking about hard drives and Click of Death and so forth. And, I mean, you had known of me. We had known of each other.

Leo: I read your column for years.

Steve: Right. And it was Kate who found ShieldsUP!. And so during the show they had like a Kate's Picks or a Kate's Discoveries or something. And she said, hey, I found this really cool security testing thing called ShieldsUP! from Steve Gibson. And you were sort of like, what? Our Steve Gibson? You know, I thought he was a hard drive guy.

Leo: Well, thanks to IceStrike in our chatroom, who's watching on the live, you know, we stream these shows live now at TWiTLive.tv, IceStrike said you were first on The Screensavers June 17, 1998. So Steve, our friendship is almost 10 years old now.

Steve: Whoa. That's very cool.

Leo: That's cool, isn't it? I like that. Thank you, IceStrike, for looking that up. So 10 years later, and we're still talking about security. Not about ZIP drives anymore. 100MB drives. You can now, you know, in your cereal box you get 128MB for free. And you can buy 3GB or 4GB flash drives for less than one disk would have cost you in those days.

Steve: Yeah, .1GB is the...

Leo: .1GB.

Steve: .1GB was the ZIP drive.

Leo: Steve Gibson, thanks so much for joining me. GRC.com. Go there, too, to get SpinRite, the finest disk recovery and maintenance utility in the world. I'll be using it when Auntie Dawn comes up on Friday.

Steve: And we should remind people that next week will be a Q&A episode, and to go to GRC.com/feedback in order to send me stuff, which I'll read and we'll talk about.

Leo: Great. Steve, thanks for talking to us, and we'll see you next time on Security Now!.

Steve: Okay, cool.