Listener Feedback Q&A #56

Description: Steve and Leo discuss the week's major security events and discuss questions and comments from listeners of previous episodes. They tie up loose ends, explore a wide range of topics that are too small to fill their own episode, clarify any confusion from previous installments, and present real world 'application notes' for any of the security technologies and issues we have previously discussed.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-175.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-175-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 175 for December 18, 2008: Your questions, Steve's answers, #56. This show is brought to you by listeners like you and your contributions. We couldn't do it without you. Thanks so much.

It's time for Security Now! Episode 175 in a never-ending saga of security with Mr. Steve Gibson. He's the man in the beret today. Hey, Steve.

Steve Gibson: You're right, Leo. It is never ending and never skipping a beat. Never missing a week.

Leo: He's very proud of that.

Steve: You're somewhere in France as this is being aired.

Leo: Yeah. No, I don't think I'm in France yet.

Steve: Oh. On the 18th? Oh, no. Yeah, the 18th.

Leo: I will be in France. You're right. Oh, my goodness. Yeah, I'll be in Paris.

Steve: Hello from France.

Leo: I'll be sending back pictures. Hello from France. And then next week, Christmas Day...

Steve: Our Christmas Day episode, believe it or not, yes.

Leo: You're going to do an episode. And he's just not going to stop. New Year's Day. He's not going to stop.

Steve: Yup.

Leo: Unbelievable, Steve. You're just trying to beat TWiT. But you know what, this year - we learned our lesson last year. Actually, I learned my lesson in Australia. I went to Australia in the spring. And we skipped, I think, two or three episodes, and the subscriptions just fell off miserably. So this year we're going to do - actually it's going to be kind of fun. Our holiday at TWiT, which is December 22nd, I think, is going to be a special episode with Jonathan Coulton, the geek singer, the guy who did "Code Monkey," and John...

Steve: Oh, neat.

Leo: Yeah, and John Hodgman, his neighbor in Brooklyn, who's of course PC in the I'm a Mac/I'm a PC ads, and a very funny fellow. So it'll be a very special Christmas episode.

Steve: And he also appears with Jon Stewart on "The Daily Show."

Leo: He does, he's on "The Daily Show." He was in the movie "Baby Mama."

Steve: Okay, I'll take your word for that.

Leo: Me, too. I didn't see it.

Steve: Missed that one.

Leo: Really a wonderful guy. Two great old friends who actually were Screensavers fans going way back, and I'm sure Steve Gibson fans.

Steve: Oh, no kidding. So you've known Hodgman from before he appeared on the Apple commercials.

Leo: Not at all. I didn't know he was a fan until he sent me an email. And that was a great thrill for me. So that's been fun. And they're both Yalies. So it'll be kind of an Old Blue Christmas. I'm going to rename myself Jon for the event. So we'll have Jon, Jonathan, and John. And then on New Year's Eve we're going to do a special edition of This Week in Tech which will be a "best of" - the biggest stories, the hottest moments from 2008.

Steve: So you're going to edit the audio out of all the previous...

Leo: Yeah. Tony's working on that right now. In fact, if you have a suggestion for Tony for a great moment in TWiT from the last year, email tony@twit.tv. He's working on that right now. So we're not going to miss an episode. So you think you're gaining on us.

Steve: Yeah, but you're cheating kinda.

Leo: Yeah, you're right. Steve has fresh content every single episode. We have some Q&A. But before we do that, do you have anything you'd like to catch up on, security news?

Steve: Oh, we've got a bunch of stuff. We've got an errata piece and some security news. So absolutely. A listener of ours, Bruce Olin, wrote to say, "Whoops, Steve, 'Coma' was not written by Michael Crichton.

Leo: Oh. That was Robin - that's Robin Cook.

Steve: Exactly. Very good. You pass the trivia quiz test, Leo.

Leo: But no, when you said it, I said, oh, yeah, Michael Crichton. Now I'm seeing the cover, Robin Cook, yeah.

Steve: Exactly. So I wanted to correct the record for that. Also there's just, well, just as we're recording this, which will now be, what is this, two weeks from today on the 18th, I guess it is...

Leo: We're recording this on the 10th.

Steve: Yes, we are.

Leo: This is going to air on the 18th, a week from - a week hence.

Steve: And so new for us on the 10th is just a shocking bit of news regarding Linksys routers...

Leo: Oh, no.

Steve: ...that just surfaced. Get a load of this, okay. And this was reported on Secunia's website. They say a security issue and a vulnerability have been reported in Linksys. Okay, now...

Leo: Everybody uses - everybody uses this router.

Steve: Yes. The Linksys, the WVC...

Leo: No, I don't know that one.

Steve: ...54GC. So again, WVC54GC.

Leo: This is not one of their most popular routers, thank goodness.

Steve: Yes. If you have the router, you want to absolutely immediately update your firmware.

Leo: I think it's a camera.

Steve: Well, it involves an OCX exploit. And what's bizarre is this is not the first time this has happened to Linksys. But receiving a UDP packet on port 916 causes this router to send all of your private information. It sends the login...

Leo: That's terrible.

Steve: It's unbelievable. It sends your login credentials, your username and password, all of your wireless network connection information including your WEP and WPA keys, in plaintext, after it receives this packet on port 916 over UDP. And in their report it says this could be exploited to gain access to sensitive information - yeah, no kidding sensitive - by sending a specially crafted packet to a vulnerable device. So in doing some...

Leo: Now, I'm looking at the model number. This is a - the WVC54GC is a camera. It's a wireless, WiFi G camera.

Steve: Okay.

Leo: So that would even be more serious in that...

Steve: Okay, now, that also makes sense because there is an exploit in an ActiveX, in an OCX control. And what threw me a little bit was that back in March of '07 SecuriTeam had a posting talking about a Linksys WAG200G ADSL modem router. And their report says "...has been found to return sensitive information to anyone sending it a packet to its UDP port 916." So, and again, it sends back the PPoA username and password credentials. And so this was an ADSL modem router where you could send it one presumably from the WAN side, although I haven't confirmed that, and it would send back the product model, the password for the web interface, and the PPoA username and password, the SSID, and the WPA passphrase. So basically it dumps all your private information out in receipt of this packet. I mean, it just - lord knows why that's set up that...

Leo: Well, and if you're using this camera to monitor your situation, they have suddenly access to your camera, as well, which isn't good.

Steve: Right. So their solution is to update to firmware v1.25. So my mistake in thinking that that was a router, the other issue was a router. This one, as you say, is a webcam with firmware. So you need to update to 1.25.

Leo: Okay. Fortunately, that's usually pretty easy. It's just you go into the firmware of the router, go to the interface and say I want new firmware.

Steve: Right.

Leo: Usually it's in the advanced section, yeah.

Steve: Right. Also this was - we have had, a week ago now, Microsoft's Patch Tuesday. So this is an event that we have, as we know, the second Tuesday of every month. This one was a particularly massive one, 19 different vulnerabilities in - well, 19 critical vulnerabilities. There were two privately reported vulnerabilities in GDI where any user opening or displaying a specially crafted Windows metafile could be subject to a remote code execution vulnerability.

Leo: That's an old - that's like we [sputtering]...

Steve: Keeps coming back. It's an oldie but a goodie, Leo. It just, you know, we never seem to get rid of those.

Leo: That's frustrating.

Steve: There were also the new Windows Search Service that Windows Update has been

offering me now for several months. And I put it on one machine, curious about what it was. And it was like, eh, no thank you. So now I just mark it as, okay, don't tell me about this any more. I do not want Windows Search. Well, that turns out to have been a good thing because there are two privately reported vulnerabilities, remote code execution vulnerabilities in Windows Search, where if you save a search file, or you click on a specially formed search URL, that can execute code in your machine; four privately reported vulnerabilities in IE, remote code execution which will be triggered by you visiting a specially crafted web page; eight privately reported vulnerabilities in Word and Outlook involving the display of a specially formatted, crafted RTF document, Rich Text Format document; and three privately reported vulnerabilities in Excel, where if a user opens a specially crafted Excel file, remote code execution. So a total of 19 different remote code execution vulnerabilities that were all addressed in this December update. So even though it's been a week ago, I'm sure that our security-conscious users have - those who can have brought themselves up to speed. I just wanted to make sure that users knew. This will require a reboot, which is annoying. But in this case, I mean, this is a mega pack of serious vulnerabilities you want to take care of.

Leo: Mega pack. And by now you should have. In fact, I really have to say that - well, let me ask you. Here we are, it came out eight days ago by the time you hear this. Unless you're listening live, as many of our audience does. Do you recommend automatic updates on Windows? Should it be happening, like, the Tuesday that they put them out, should you be updated?

Steve: I've got mine set for download and notify, but don't install. And I always choose the "custom" mode. I like to browse through them because, for example, I got bit by XP Service Pack 3 that caused some weird things to happen, as did a handful of people. I think you did, too.

Leo: Yeah.

Steve: And things like this Windows Search. I don't want new things added to my system without giving me a chance to audit them and decide if I want that or not. And also I see that Windows has in optional updates, they're constantly modifying the root certificate collection. And that's not installed by default, but I do want to update my root certificates all the time. So, well, and I certainly don't want to have my systems rebooting themselves. I mean, I've got my system running so well that I am literally, except for this annoying, now, constant Windows updating, I don't ever have to restart Windows. I mean, it just goes and goes and goes and goes. And there are times where I'll have pending updates, but it's just not convenient for me to restart because I'll be running browsers with lots of open tabs, and I'm using those sort of as placeholders for things I want to get back to. I'm sort of - I'm using my environment as my to-do list, essentially. So it's not easy for me to shut down, and I need to plan ahead when I'm going to go do a reboot cycle. So anyway...

Leo: Do you recommend that? I mean, is that what you would tell people? I mean, I guess if somebody - if it's your mom, you're going to say apply them automatically.

Steve: Correct. And, for example, I still don't run AV. So I don't recommend that nobody else run antivirus. But, you know, you don't, either.

Leo: Right. That's just you. Yeah. That's us, yeah.

Steve: So I'm doing - I'm working in my own fashion for what works for me. I do want to know in general that these things are available. But I'm still - I still don't have Service Pack 3 installed on this machine. It's like, uh, just something about it seems to be unhappy. So...

Leo: Yeah. Well, I have to say, though, the way it happened for me with Service Pack 3 was I applied it, and Microsoft - on one machine. And Microsoft said nah, and rolled it back. It said I can't do it, rolled it back. And then eventually I guess whatever...

Steve: Really.

Leo: Yeah.

Steve: Interesting.

Leo: So I think they're getting better, to their credit, about avoiding installation. For instance, Service Pack 1 on Vista wouldn't install on machines that had incompatible drivers. But Windows Update was smart enough to get the latest driver when it came out and then apply Service Pack 1 at an appropriate time. So I think for most users it's probably a good idea, unless you're a listener of Security Now! and you know better, to say do it automatically.

Steve: Yeah, and of course in the corporate mode there is...

Leo: That's different, yeah.

Steve: There have been instances where Microsoft's changes have really collided with mission-critical corporate apps. And so there the IT guys are saying, I mean, this is why we've got the Second Tuesday rule is they wanted to lump them all together and do them at once.

Leo: Yeah, yeah.

Steve: One last bad zero-day remote code execution problem...

Leo: Oh, boy.

Steve: ...in the very popular Trillian...

Leo: Oh, I use that.

Steve: ...instant messaging system. You absolutely want to update to what is now 3.1.12.0. Anything prior to that has a zero-day, meaning that it was discovered by it being done to people, remote code execution where Trillian's receipt of an IM can cause code to be executed in your machine. So this is another biggie. Anyone using Trillian wants to make sure they're at 3.1.12.0 or later because this fixes a handful, actually, there were a bunch of different approaches which are being exploited in the wild, and this was found when it was happening to people. Thus the "zero-day" designation.

Leo: Right. Now, the good thing about Trillian is it auto updates. So if you've...

Steve: Good, good.

Leo: It should say, hey, we've got an update. Whoa.

Steve: And I have a very fun Security Now! little blurb.

Leo: SpinRite.

Steve: Yes.

Leo: You're confusing your products, sir.

Steve: I was reading Security Now! on the screen because it's addressed to Security Now! Feedback, which is the way the form submissions come in.

Leo: I see.

Steve: Anyway, this is from Dan Baldwin, who - and his subject kind of, again, caught my eye: "SpinRite Almost Saved a Computer." I thought, huh? So he starts off by saying, "Yabba dabba do." He said, "I am the 'IT department'" - in quotes - "for a local radio station and take care of several computers that are used by the news, programming, production, and sales departments. Recently one of the computers which holds a lot of data for sales, in fact the sales manager's computer, would not boot. I had a friend's copy of SpinRite." Okay, I'm not quite sure how he has that, but he just happened to have a friend's copy of SpinRite, and he "...decided to run it and recover the hard drive, assuming there was no other problem. I put the SpinRite CD into the drive and booted into SpinRite, and it quickly found at least three unrecoverable sectors. We let SpinRite run to the end, then pulled its boot CD and tried to reboot. Oh, no. The screen brought up a message that part of the Windows XP OS was damaged or missing. But at least that was better than before." Because before they got nothing. "Fortunately, the computer had originally been loaded with Vista, but we had replaced it with XP. So we had the disk for the installation, unlike most computers that come with a restore disk, and we put that in the CD drive. When that

came up, I used the "R" command to restore the operating system, XP, to normal function, and all was well again. Thanks to SpinRite for prepping the drive for restoration. Now, having balanced my accounts" - and he says, "I was having financial problems long before the mortgage problem/stock market drop bailout, et cetera - I have sufficient funds to purchase a copy of SpinRite for myself, which I have considered for quite a while as I have been familiar with the Leo/Steve duets going back to ZDTV/TechTV, the Click of Death, and listen to Security Now! podcasts as I drive to work at 4:30 in the morning on Sundays. So that 'yabba dabba do' you just heard a few minutes ago was mine, as my credit card is no longer overdrawn..."

Leo: People know about your yabba dabba do.

Steve: He says, "...though I could get back to overdrawn very easily." And he signed it John Paradox, his cybernym, Dan from Tucson. So thank you, Dan. I have, of course, no problem with your using your friend's copy of SpinRite, and I thank you for buying your own because that's what keeps the yabba dabba dos happening at this end.

Leo: We should explain that every time a credit card clears, not an angel gets its wings, but Fred Flintstone says "yabba dabba do" in Steve's office. It's a complicated story. You just have to take our word for it. That's nice. I think that's what happens. You know, when you don't do copy protection - although you do, I think, a smart kind of copy protection. You kind of watermark each copy; right?

Steve: Oh, yeah. The licensed user's name is in the product. It's built in when they download it. And all I'm saying is take responsibility for the fact that your name is in it and try not to let it get loose.

Leo: Well, and I think as a result you seem to get a lot of email people saying I used it, but it worked, so I'm paying you. If you do a great product, it works, and you're not a jerk about it, people pay you.

Steve: Yeah. And I have no problem with that. I mean, I recognized a long time ago that - and I draw the notion or the line between what is lost revenue and what is not. Certainly there are people who download SpinRite from some piracy site. Actually we've had email saying that they ran an infected copy of SpinRite. So that, like, hurt them more than if they'd bought a real one. So it's not safe, I should mention. I mean, I have talked about this before. And I actually have had email from people scolding me for saying, Steve, you need to tell people that there are trojanized versions of SpinRite. And I've never mentioned that before, but that is the case. We've received feedback from people where they've downloaded something calling itself SpinRite that was actually malicious code. So that's a problem, but it's not my fault.

So but anyway, my point is that, yeah, I recognize there are people who, no matter what I did, they would not purchase SpinRite for whatever reason. So if they run it and take the risks of running a pirated copy, okay, it doesn't represent lost revenue for me. So it's like, well, okay. I recognize that.

Leo: I think that's enlightened, Steve, frankly. I think more people should have that attitude. We start from John Meyer - not that John Mayer - of Orlando, Florida. He says, "Your body is a

wonderland." No, no. He says he stumbled on an interesting revelation. He says: Steve, I found the following blog post by a Microsoft employee. He gives the link. We'll put the link in the show notes. It's a long one. But basically the title of it is "Update on the GDR That Is Coming for NET Framework 3.5 SP1. It contained a note about Patch Tuesday that I was completely unaware of. I thought this was very interesting.

[http://www.hanselman.com/blog/UpdateOnTheGDRThatIsComingForNETFramework35SP1.aspx]

Steve: Yeah.

Leo: Security-related patches are the second Tuesday of every month. We were just talking about that.

Steve: As we well know.

Leo: But then they do more non-security patches on the fourth Tuesday of every month except December. They take the week off. I don't know what's going on there. So these out-of-band patches that you and I talk about all the time?

Steve: Yes.

Leo: They're non-security related.

Steve: Yup. I was unaware of the policy. I went poking around after I received this note from John, seeing if I could find some official policy statement of Microsoft somewhere, but I couldn't. And looking at the blog posting, this guy is speaking very matter-of-factly about it. It's like oh, yeah, you know, we're doing the non-security patches on the fourth Tuesday. It's like, since when? You are? But, I mean, it is the case that stuff seems to trickle in, not on the second Tuesday. And it just didn't even occur to be that those were non-security-related things. So I don't know what that means from, like, an IT management standpoint. But at least our users know that if they get something two weeks after their security patches, it's like, okay, this is a non-security update. So that's cool.

Leo: Right, right. Excellent. Thank you, John. Creighton in Arizona, he's happy to be in a sandbox. We talked about Sandboxie, of course. Thank you, Steve and Leo, for your recent coverage of Sandboxie. I've been a big fan of both of you for years, Leo since The Screensavers, Steve since the worm attack that shifted your focus to security issues. Was that when your system was being attacked?

Steve: He might be referring to the denial of service stuff. Although actually I was focused on security ever since I realized people had their C: drives mapped out onto the Internet and said, okay, this is a problem.

Leo: That's what did it. That's right. You were looking at logs or whatever, and you

were seeing all these people's C: drives.

Steve: Yeah. Well, in fact it was - our office was being set up with an ISDN line, the very first persistent connection to the 'Net. And given that it was persistent, I thought, okay, what's the security implications of this? And this, of course, is years ago. And we received an IP for - or maybe a little block of IPs. And I remember just sort of poking around with a scanner around the neighborhood surrounding that IP address, and there was a bunch of people's C: drives, just hanging out in the breeze. And I thought, okay, there's no way they could know this was going on. I mean, literally anybody could just log onto their C: drive and browse around. It was unbelievable. So that of course was what launched ShieldsUP!.

Leo: That's what we call a "wakeup call."

Steve: Yes.

Leo: Yikes. Anyway, he goes on to say: Thanks to you guys, all of my Internet activity is now sandboxed. That's great. That's really great. Additionally, the sandbox - oh, this is interesting - is actually a TrueCrypt container. So he's using another program we recommend all the time, TrueCrypt, mapped to a drive letter. It's nice knowing that not only am I protected from malware trying to do permanent disk writes, but also the privacy of my browser usage is utterly assured, as nothing I do while online is written to the disk in the clear, but rather to the encrypted container, and then thrown out. This is a paranoid fella. But, you know, there's no overhead. I don't think there's any overhead to doing this. So...

Steve: No.

Leo: ...this is great. He says: I'm very careful how I spend my money. I expect you're similarly careful when you recommend something. Certainly buying SpinRite, which has saved my bacon once already, is something I'd put in my, quote, "Gee, I'm glad I bought that" column. And now Sandboxie, firmly in that column. My thanks goes out to the invisible staff that make GRC, the podcast, and TWiT run so smoothly. They deliver week after week and deserve mention as well. Thank you, thank you. Well, thank you, Creighton. That's a nice letter.

Steve: Yup, I know you've got a good staff, and I certainly do, too, Leo.

Leo: Well, you know, what's interesting, and I think you were talking with Dane about this when he visited you for lunch, neither of us have vast operations. You used to have - he said you used to have 20 employees?

Steve: 23. We got up to 23 people. And my lack of hair is a consequence of that.

Leo: Yeah. We have two full-time employees, Dane and Tony. And they both work on Security - Tony works like the dickens on Security Now! and all the shows. And Tony of

course - Dane is, of course, doing all the payments and the money stuff. Frederique, our office manager, is doing all the bookkeeping. I know you have a very good office manager. And then Colleen does the infrastructure, yeah. And that's it. And you have, what? You have an office manager...

Steve: And a tech support guy.

Leo: And that's it.

Steve: We're 100 percent virtualized now. They both work out of their homes.

Leo: That's great.

Steve: It's just - it's perfect.

Leo: Yeah. I really think that's great. That's all you need. But if you have good people.

Steve: Yeah.

Leo: We're very lucky, you and I.

Steve: Well, and the key is they're people I trust to do the job with absolutely no oversight and management. They don't need me to tell them what the job is. They know.

Leo: Autonomy. Yeah.

Steve: Yeah.

Leo: I think that my guys would say that, too, that I hardly ever breathe down their neck. Only once or twice a day. And I do it in a loving way. They are in the other room, I have to say. They're not offsite.

Garrett Lucas in West Virginia wonders why Microsoft is "sort of" updating his machines: Steve and Leo, thanks for the great job with Security Now!. I've been with you all since the beginning. I have my requisite copy of SpinRite as part of the toolbox. However, my question is about how Windows Update works with multiple computers on a network. I have three computers on my home network. I use them for various tasks. I'm very strict about keeping my computers updated and patched. And I made sure last week that all three of my computers were up to date and no high-priority updates were available. I heard that there were going to be several patches on the 9th. That's Patch Tuesday.

Steve: That's that mega - the mega patch one.

Leo: Right, right. So I fired up all three PCs just now to update them. The first computer I updated said there were five high-priority updates, including some kind of core pack. However, when I tried to update the other two computers, I was told no high-priority updates were available. I'm a little confused. If all my computers were up to date last week, why wouldn't they all need updating today with the new patches? I have XP Pro on all three of them, and I can't figure it out. The only thing I wondered was if Microsoft looked at anything having to do with IP addresses when sending out the patches, maybe saying, well, we sent out this patch to that IP address, we don't need to send it again? He said, but wouldn't all three machines need the same updates and patches? What's the story here?

Steve: You know, I have wondered the same thing.

Leo: You see the same effect?

Steve: I've seen the same phenomenon where, if I go to a machine and update it, I'll go to another one, and it'll say, well, now, there's a difference between using the web interface explicitly and the little yellow shield that comes up down in your tray. I've noticed that the presence of the yellow shield tends to be lazy. And my guess is that Microsoft is just sort of distributing the updates out. That is, if you explicitly say does this machine need an update, it may be that Microsoft is busy right now, that is, they're doing some load balancing, and they're saying, okay, we're going to temporarily say no until we have some more bandwidth available because we're already busy pumping out updates to a gazillion people at the moment. So we'll let that one float back a little bit, and we'll get it a couple hours from now. But I've definitely seen sort of this strange phenomenon of not all security updates available in all of my machines at the same time.

Leo: Yeah. I'll have to look. I haven't seen that, and yet that wouldn't surprise me. We also know that Microsoft rolls these out, though. Right? They don't - to keep their servers from getting bogged, they don't do it all at once. Some people are...

Steve: Well, and that's exactly what I mean. By this sort of distributed, I don't know if you'd call it a "rollout," but essentially not telling every - they couldn't tell every single Windows machine on the planet that they've got multi-megabytes of new stuff to download.

Leo: Right. That's 200, what is it, 200, 300 million machines. No, maybe more.

Steve: Some of these updates are, like, replacing most of the OS. So when Microsoft, you know...

Leo: Well, I mean, even Microsoft...

Steve: ...does an SP3, for example, that's a 500-meg blob.

Leo: Well, we know those, in fact, they take several weeks sometimes to push those out.

Steve: And so clearly they're doing some sort of staggering release of this. Which is what I think accounts for what I and what Garrett have seen. And I'm sure a number of our users with multiple machines have seen the same thing.

Leo: But if you check later, does it happen in the same - in a 24-hour period, or...

Steve: I've seen it appear, like, even a day or two later.

Leo: Yeah, okay. That makes sense. I mean, how many Windows machines - there might be a billion Windows machines out there. I think it probably...

Steve: However, whenever I have explicitly gone to Windows Update or Microsoft Update to launch the browser task, I've never been lied to. That is, as far as I can remember it's always told me, oh, yeah, we've got some stuff, here you go. And then I browse through it. I choose, again, the custom mode and select what I want it to do.

Leo: That's because nobody does that.

Steve: Probably.

Leo: I mean, yeah, so few people do that, they can afford, you know, they can serve all of them, I'm sure.

Steve: Exactly.

Leo: Yeah. Robert Berry in North Carolina wonders if it's safe not to scan. He says: I'm setting up a new laptop for my daughter to use. I want it to be secure without the security getting in her way. Most AV programs perform regular scans of the entire system, usually scheduled for the middle of the night, maybe once a week. The problem is the laptop's typically powered off or suspended when it's not in use. That means a scheduled scan ends up running the minute somebody turns on the computer, trying to use it. And of course everything bogs down. So I'm thinking of turning off the scheduled scans and relying instead on the real-time protection, which presumably works through hooks in a file system. Assuming the virus info is updated frequently, isn't that enough? I don't really see what a scheduled scan would add, if every change to the file system is scanned as it happens. That's a good question.

Steve: It's a great question. And it has also a perfect answer.

Leo: Okay.

Steve: The problem is that we know that AV is inherently a reactive process. That is, that's the problem, is that AV signatures are being updated periodically in response to the appearance of new problems that are discovered in the wild. That is, it's not - the AV can't update ahead of seeing something. So imagine the scenario that you've got current patterns. Then you go somewhere and acquire a virus which is brand new and not yet in those AV patterns. Well, that means that the scan as it comes into your system will not see it, and it'll get in because it's newer than your most recent update. Okay?

Leo: Okay.

Steve: Then if, say, the patterns got updated, well, the patterns got updated to now catch and see that virus which was in your system, it was already in. So if you tried to acquire another copy of it, then the newer patterns would catch it. But it would only be by doing a scan using the updated patterns of the entire system that a virus that had slipped in through that window of opportunity, between successive updates, that's the only way that one would get seen. So you absolutely need to periodically scan because you want to catch anything that might have slipped in between the time of - in that interval between virus updates. And so I would say scanning is not entirely optional. It's something you could maybe take some control over so that it's not becoming a real problem. But it's definitely something you do need to do periodically.

Leo: Weekly?

Steve: Well, you know...

Leo: That's what they usually recommend.

Steve: Yeah. I mean, the question would be what damage is going to be done by the virus. I mean, there's no hard and fast rule. It's all sort of a heuristic stew. So it's like, well, nightly, if you leave your machine on. Or maybe come up with some sort of behavior where the laptop does get left on overnight on a certain time. Or a scan is manually started when you go to dinner or something. I mean, the idea being it is important to do it. If you're going to rely on AV to protect you, you can't only rely on what it knows about what's coming in over the wire as it does. You need to be able to have it take a look at things that are on your machine. And there are various installations of AV where it's cryptographically transmitted, but then it doesn't unbundle itself until it gets into the system. So again, it might be missed until it's actually present. So scanning is definitely something you don't want to put off, if you're a person who relies on AV.

Leo: And, you know, you can just control the schedule or say - I do most of that kind of automatic stuff, like backup scanning and stuff, right after the end of the workday, like 5:00 or 6:00 p.m. So I know the system will still be on.

Steve: And it's like defragging. No one wants to defrag their disk while they're trying to use the computer actively.

Leo: You can't.

Steve: Exactly. So many of us will deliberately start a defrag process when we're going out to dinner. And we come back, and it's done. So I would say putting scanning in the same class as that, where you give it some deliberate focus of your schedule.

Leo: I've never asked you this. Do you have an AV product you recommend?

Steve: No.

Leo: Okay.

Steve: I don't know much about them, actually.

Leo: It's, you know, the more I learn about this, the more I realize it's impossible - there are a number of companies that will have a kind of a set of viruses that they throw the AVs at, and then they give you a score. Virus Bulletin does that. And AV companies hate this. I've talked with AV companies. They say, you know, you just tune the - you tune the antivirus to work with the set. It's a synthetic. It's not a good measure. And yet measuring the effectiveness of an antivirus in the wild is next to impossible. So I don't know how you do it. The only thing we've ever done is measure how much impact the antivirus has on your system. And then you just have to say, well, I hope it catches everything. I mean, I don't know what you do. I don't know what you say. I mean, it's something that, you know, you need a PC Magazine and a lab. And unfortunately all these guys are shutting down their labs now. It's not a good - it's not a moneymaker.

Steve: I'm very careful with what I do. I run with scripting turned off. I just - the nature of my computer use is very proscribed, I think, compared to most people. So I'm not just wandering around clicking on things. And maybe because I'm a mature adult I'm not intrigued by some of the more dangerous areas of the Internet, where were I a young teen I might be much more likely to get myself in trouble. So I think my own demographic habits don't put me at risk to much degree. I'm a boring user of the Internet.

Leo: Well, and you also don't - I think now the number one vector, I would guess, is clicking - and in fact I think I just read a study that said this - is not attachments in email anymore. And I think we've trained people pretty well not to open email attachments. But clicking links that either take you to a site loaded with malware that just tries every exploit, or explicitly says, oh, you need new Flash. Download Flash and install. And you know enough, I know enough, anybody that listens to this show knows enough not to do that. It's nave users who go, oh, yeah, I often need a new Flash. They go download it, something didn't happen right, oh well, oh well, and they go on. And they're the ones who are infected.

Steve: Yeah.

Leo: So I think it's navet in many cases.

Steve: No, you're right. And in fact one of the other - one of the recently very effective approaches, unfortunately, is something gets in your machine, or you're browsing and you run a script, and then the script generates a pop-up that says, oh - and it looks very much like Windows. And it says that it's scanning your system for malware. And then, oh, surprise, it finds something.

Leo: Quite a bit, yes.

Steve: Yes. And then it says, oh, you need to update your AV. Click here to purchase an update. And, I mean, even the most...

Leo: Suspicious? Paranoid? Careful? Cynical?

Steve: Yeah, I was going to say, it really - that approach catches out even relatively experienced users because they're used to Windows popping things up, and they just assume this is Windows. I mean, they don't get that - and in fact it can even be disconnected from your going to a page. Someone might be skeptical if the moment they go to a page it pops up a pop-up because lots of people had that happen back in the advertising pop-up days. But it's possible for scripts now to use various means to delay notification so there isn't the association between the web page you went to that initiated this and the presence of the pop-up. So it seems more like it's Windows doing it for you. And, I mean, again, it's a social engineering sort of hybrid attack. But I read somewhere that one third of the viruses now, or malware, in people's machines are coming in that way, from something popping up and saying, oh, we're going to check your system for malware. And in fact, if you purchase from them, of course, they collect your credit card information, as well. And what you download is a trojan that is remote controlled, that lets them take over control of your machine.

Leo: This is...

Steve: It's getting a lot of people.

Leo: It says Antivirus 2009 at the top of the window, looks very realistic. And, yeah, we get a lot of calls on the radio show from people. A lot of them don't even know that they've been bit.

Steve: Right.

Leo: Richard Warriner, Bedford, U.K., has been playing with his new PayPal footballs. Stop playing with your footballs. Steve, he says - although I play with mine all the time. There's something about it. You just want to, you know, kind of press the button and - ooh, it's so fun. After the heads-up on the show a couple of weeks ago that PayPal dongles were now available in the U.K., I got myself a couple. I now get

prompted to enter my security key number when logging in, either via the dongle or sent direct to my mobile. However - you know, his cell phone - there is still the option to click that I don't have my dongle, and then I can log in via security questions. It seems crazy that this backdoor exists. I kind of am with him on this.

Steve: Yeah.

Leo: And there's no way to disable it. The only solution seems to be changing the answers to the security questions to the wrong reply so that nobody can guess them. The issue here is that one of the options is my bank account number, but I can't enter bad info here as PayPal uses it for funds, and it needs to know that number accurately. Am I missing something? Is this a hole? Is this a bad thing?

Steve: Why don't we go ahead and read the next one, from Theo.

Leo: Okay.

Steve: It's about the same issue, and we'll talk about them both at once.

Leo: Yeah. This is - I'm glad that they wrote in because this has kind of bugged me for a while.

Steve: Yup.

Leo: Theo is Theo Jones in London. He says: Love the podcast. Just checked out the PayPal security key, new to us in the U.K. So we're getting a lot of new users on this one. But they're smart, and a red light goes off for them. He says: It gave me the option to use my phone as a security key instead of getting the football. This is the thing that I like that my bank is doing lately. So when I log in, it sends me a text message with the number. Hey, great. However, I decided to look at the option for "I don't have a security key with me." It gave me two options to identify myself, bank account number or security question. I was very surprised. My bank account number is an eight-digit number. They gave me the last two digits so I'd know which one it is.

Steve: So, you know, blank out the first six; right.

Leo: It's only six. My bank account number is not exactly public knowledge, but it's not super secret. I've given it to several friends and family members. And I think it's on the check. It's on your check.

Steve: Yeah.

Leo: It is in the states. Everybody you write a check to has your bank account number. It's on various bank statements, too, which could fall into the wrong hands. I understand this is still two-factor authentication. But it seems like the fact that the random element of the security key being lost reduces security to quite a large degree, in fact to where we were before. Because the hacker just says, well, I don't have the key. It's actually quicker for me to bypass my own security key and type in my account number. Am I right? Am I missing something? What do you say to these people?

Steve: Yeah. I mean, I'm impressed with both questions, and I am really disappointed with PayPal. I followed up and looked at this. And in addition...

Leo: But everybody does it, Steve. They have to because people lose the dongle.

Steve: Yes. It is a perfect example of compromising security for the sake of convenience. And, I mean, I could understand doing it if they allowed you to disable it. When I told them that I don't have my dongle with me, I get one additional thing. I get the security questions, I get my bank account number, and the credit card that I have registered with PayPal. So three different options. And, I mean, and no ability - I clicked on them. I explored around. There's no ability to say I do not want fallbacks for my dongle. I mean, it is truly not secure. And it just, I mean, the only benefit you get, if you don't choose those, is the one-time password aspect, where - which is of course why the football exists in the first place, is so that if something were monitoring your log-in, if there was a sniffer, then it wouldn't be able to use the same code to pretend to be you again. Whereas if you did use one of your fallbacks, then a sniffer watching you log in would be able to do so. So there is still a benefit to using the one-time password aspect.

But both of these guys are right. PayPal has substantially reduced the overall security of their log-in. And as we know, just, I mean, all of our listeners know it's a fundamental aspect of security that the more ways you offer of getting in, the lower the overall security of the result is. It's just like how many times I've griped about all of the root certificates that are now in our browsers. That list just goes on and on and on. And it's like, you know, all it takes is one of them to make a mistake in issuing a certificate, and we're in trouble. And so the more you have fundamentally, the less your security is, the less secure you are. And similarly, the more different ways to log in, fundamentally the less secure that is. And so, I mean, I'd absolutely take responsibility for having my football with me and disable the alternatives. But there's no way to do that with PayPal right now.

Leo: Yeah, yeah. Or my bank. And, you know, my bank is using the cell phone thing, where they send you a passcode.

Steve: Oh, and get this, Leo. I don't know if you heard. But there's some dialogue. Apparently some of the carriers are going to start doing a surcharge if a non-phone sends you a text message.

Leo: Yeah, I did see that.

Steve: And that is so annoying because texting is probably the largest profit center...

Leo: Oh, yeah.

Steve: ...of telephones. It's, like, zero bandwidth in terms of usage of bytes traveling through the air. And they make more money from texting than from anything else. And so now they're going to start, I mean, who would send a phone a text message except some sort of an authentication loop? And now they're going to hit you with some extra charge for that.

Leo: Yeah, it's like three - actually, who they hit is the bank. It's, like, three cents. But, you know, people use it for Twitter and other things. It's a gateway to SMS via email, and they want to charge you for that. I agree with you. I did the math once. Even if you use all 140 characters every time that you send a text message, at the rate they're charging, 20 cents a message, that's $1,500 a megabyte. That's a good profit.

Steve: And Leo, in terms of data bandwidth, when you compare that to speech, speech, which is a constant flow of bytes between you and another party, compared to a single shot of, you know, a short burst of data, there's no comparison, the bandwidth consumed by audio versus SMS. I mean, SMS ought to be absolutely free.

Leo: Or at least cheap.

Steve: Yeah.

Leo: I'm with you on that one.

Steve: [Indiscernible] take your money, so that's what they're going to do.

Leo: Cell phone companies, these guys, just they're awful. Just they deserve every bit of opprobrium they get.

Steve: It's a racket.

Leo: It's a racket.

Steve: And by the way, I did finally go to Verizon and try typing on the Storm. And, no.

Leo: Yeah, I got a Storm here.

Steve: No.

Leo: Yeah, I got a Storm here. It was a little hard to - you know, if you want a BlackBerry, get the Bold. The Bold has a real keyboard. It's a nice...

Steve: But the Bold forces you over to AT&T, and I will not go there.

Leo: Oh, you're Verizon, that's right.

Steve: Yeah. And so I'm hoping that BlackBerry - there'll be enough backlash from people who actually want to type on a keyboard that they'll move their newer technology to another BlackBerry that Verizon will carry which will still have a keyboard on it.

Leo: I think Verizon will get the Bold pretty soon. You know those exclusives don't last very long.

Steve: Ah, that would be perfect. Because the Bold would be absolutely the right phone, except that it's on the wrong carrier.

Leo: Right, it's AT&T right now. But I think that that...

[Talking simultaneously]

Steve: ...phone carrier.

Leo: Yeah, isn't that kooky.

Steve: Yeah.

Leo: No, I agree with you. I have a Storm here, just for review, and it's that clicking thing, it's just too hard to type on the screen.

Steve: And I was doing a little bit of a search through my Kindle the other day that has that same sort of little thumb keyboard? And I was really surprised how fast I can type on that.

Leo: Oh, yeah.

Steve: I mean, that's the right thing.

Leo: That's all you need. I like real keyboards. I do, too. Kyle Hasegawa of Tokyo, Japan clarifies Zone Labs' DNS usage. Remember we had last time a question saying, hey, I was watching ZoneAlarm with Wireshark and all this. Dear Steve and Leo: After

hearing about ZoneAlarm phoning home from one of the other listeners, I decided to test this out for myself. I set up a virtual machine to install the latest ZoneAlarm v8.0.065.0000 and enabled PCAP on my router. Here's what I found. ZoneAlarm does not send DNS requests to its own servers. But it does request lookups of zonelabs.com and register.zonelabs.com on the DNS servers configured in Windows. In fact, I don't think an application can override the system's DNS server list when making DNS requests through ServiceHost.

Steve: I think that's probably true. I was wondering about that myself.

Leo: ZoneAlarm does phone home just after installation, but it does so using a normal browser window and some ASP thank-you-for-installing pages with non-personal information about your instance of ZoneAlarm appended as query string parameters. Also, strangely, ZoneAlarm does continue to query zonelabs.com every 10 seconds. That's what our other listener was seeing.

Steve: Right.

Leo: But these are normal queries to the configured DNS servers. There's no extra data going on. So what's going on? Why is it doing that?

Steve: Well, I wanted to clarify. We left this sort of pending. What the other user saw with Wireshark was not queries to Zone Labs' servers, but queries of Zone Labs. So he saw this little 10-second heartbeat querying zonelabs.com. The only thing I can think is that maybe it's a way of detecting 'Net connection, whether your system is currently connected to the Internet. Because those queries are not - if they're just going out to your registered DNS servers, the first time you do it it's going to cache in your ISP's resolver, as we all know from understanding how DNS works. Subsequently, for as long as the TTL, the Time To Live, of the records which were received from Zone Labs servers are living in your own ISP's cache, it's going to be responding.

So my feeling is this must be a way, this must be the way that the ZoneAlarm Firewall keeps a constant watch on whether you have an Internet connection or not. Because when you drop off the Internet, then the system's attempt to get an update on zonelabs.com would fail. And so that must be what it's doing. It's using this little heartbeat to sense a connection to the system's configured DNS servers. When that no longer exists, that will fail. And so that's the way Zone Labs knows, or ZoneAlarm, the product, knows that your machine is no longer on the Internet. But it's definitely not a phone-home technology, and there's no information dribbling out of them, from what Kyle has said. And what Kyle has said makes absolute sense to me.

Leo: Well, I'm glad to get that. And as I said last time, we're just listening to what the listeners are saying. We haven't done any verification on our own. So there's two different stories going on, and who knows what's really going on. But that kind of makes sense. It's a ping to say, am I alive?

Steve: Right.

Leo: And that would make sense. And with no extra data going out. And that's not - what Kyle is saying is not inconsistent with what our first guy was saying. He wasn't looking at what they were sending out.

Steve: Right.

Leo: Okay. Actually we have two Sandboxie comments here, one from Mathieu in Montreal, Canada. He was kicked out of his 64-bit sandbox. Hi, Steve. I just wanted to give you and listeners of the fine Security Now! show a heads-up concerning the compatibility of Sandboxie. Yeah, I heard other people say this.

Steve: Oh, yes.

Leo: In fact, when we were talking about Sandboxie I heard this from the chatroom. I was looking forward to trying it out on my new Vista 64 computer until I found out that Windows PatchGuard prevents the use of Sandboxie. PatchGuard is the technology Microsoft has put in to say you can't modify the kernel.

Steve: Yes.

Leo: Sandboxie is such a great concept, but I guess I'll have to stick to virtualization for now unless there are enough voices heard at Microsoft to make the move and allow us to disable or bypass PatchGuard for selected applications. Thanks for the wonderful show. Also Peter J. in Orangevale, California. He's using Sandboxie, but he says only for the time being. Hi, Steve and Leo. I'm a regular Security Now! listener, have been since the early episodes. After listening to the recent Sandboxie episode, I finally decided to buy it after having used it since you guys talked about it a couple of years ago. I love the program, find it extremely useful.

However, after I browsed around in the Sandboxie forums I noticed the author said there will never be a version for the 64-bit version of Windows due to PatchGuard because it prevents modifications to the kernel. That made me very disappointed since Sandboxie is one of those applications I'd like to make a part of my software arsenal for years to come. I suspect there isn't a good way of bypassing PatchGuard. Actually we know there is. You've talked about it, Steve. But is there a way that Sandboxie can live on without having its hooks into the Windows kernel? Is there a way to do that? I just don't want to lose such a great platform once I finally make the switch to the 64-bit platform. Thanks for a great podcast.

Steve: Everybody who is interested in 64-bitness has been concerned about this. In the second case, Peter is using a 32-bit system, but he can foresee the day that he'll be migrating to a 64-bit platform, probably Vista. And so he's unhappy that he'll be unable to use Sandboxie there. And our first questioner says he's already on Vista 64 and can't use it at all. It causes a - first of all, we got a huge amount of our listeners who wrote in, said wait a minute, how can this be? How can it not work in 64 bits? And over in Sandboxie's own forums this is a real sore point.

I've discussed it with Ronen. And he's not at all happy with Windows, or with Microsoft over this. But it is an absolute fact of what PatchGuard does. In order for Sandboxie to do its

sandboxing, which is completely different from the way Windows operates, Windows has no inherent capability to, like, to create sort of this forked caching area, which as I described Sandboxie is the way it works, is when it opens a file or even a registry region where it wants to make some changes, those changes are caught and written instead into the so-called "sandbox," which is just a set of files sort of off to the side. And then any reads are intercepted and fed back from the sandbox. So the application sees that it's written, even though it's only written to a private copy, essentially. It creates like a little private fork off of the operating system where all the changes go.

To do this you absolutely, because there's no facility built into Windows to allow this, you have to intercept Windows, the API, the Application Programming Interface in the kernel and essentially filter, is the term, filter those things like file reading and writing, and registry key opening and reading and writing, and all the various things that applications might do to modify the system. You have to insert yourself down there and intercept those. Well, that is also, unfortunately, exactly what rootkits do, is hook the kernel in order to hide themselves. So exactly what PatchGuard is designed to prevent, and it does very effectively, is what Sandboxie needs to do in order to do its job. So there's a complete collision.

Now, the early versions of the 64-bit XP had weak PatchGuard that Sandboxie was able to live with. And so Ronen went to the trouble of doing a 64-bit driver. He had 64-bit hooks. And there was a 64-bit Sandboxie which actually is still available from his site that runs under 64-bit XP. But then later, along came an update as one of those serialized-looking updates, and he shows you which one it is on his site. And the update strengthened XP's 64-bit PatchGuard technology, brought it up to Vista strength, and Sandboxie would no longer work. It would immediately crash the system when it attempted to come in, and Sandboxie attempted to - when Sandboxie's service started up, which is where it then hooked these API calls, it would immediately crash the system, which is what PatchGuard does. I mean, it's a deliberate shutdown saying the OS has been corrupted. The only thing it can do is just refuse to go any further, and it just shuts down.

So, I mean, this is a huge concern for the people who love Sandboxie because they want Sandboxie in the future, in fully patched Windows 64 or in Vista 64. But there just isn't - there is not a way to do it. I mean, it's just oil and water. You cannot make them cohabitate.

Now, you'll remember that some of the firewall vendors were upset by this, too, because firewalls have traditionally been deep kernel hookers in order to install themselves, since Windows did not provide the hooks that firewalls needed. So Microsoft produced a PatchGuard API to allow those sorts of things to be done. Unfortunately, it's not extensive enough to allow Sandboxie kinds of things to be done. It's not a general purpose patching facility. And the problem is, you can't create a workaround, or the bad guys would use it. The instant there was a way for Sandboxie to do the things it does, there would be a rootkit that whatever it was that Sandboxie was doing, this rootkit would do it. So, I mean, Microsoft has to create an absolute barrier.

And so essentially people want what Sandboxie is doing, but they want it in an environment that is absolutely resistant to having the kernel modified. Now, you could argue that, okay, fine. If Vista 64 doesn't let me do this, do I need Sandboxie? And the answer is yes because what Sandboxie is doing is preventing modification, and sandboxing and caching modification, which is a different sort of behavior than what PatchGuard is preventing. PatchGuard is protecting the OS, but not necessarily the configuration of the OS. It's protecting the function of the OS. So PatchGuard is protecting changes to the configuration, which Vista 64 and the patched XP 64 doesn't do. So having PatchGuard doesn't obviate the need for Sandboxie, but it does unfortunately prevent Sandboxie.

Leo: And we - go ahead.

Steve: And it's just, I mean, it's just like game over. Ronen is really not happy because he feels the pressure. He invested in a 64-bit solution. He had one. It's still available. But if you install - and if you remove that one little update in XP, then Sandboxie will work with the reduced PatchGuard strength. But that's not a good solution for the long term. And he recognizes that fully, and he's just fuming over the fact that he can't go into the future with 64 bits due to PatchGuard.

Leo: Well, I'm sympathetic with Microsoft. I think the key is that, if Microsoft's going to do this - which I think they should do, I don't think anybody should be allowed to modify the kernel - then Microsoft has to provide Sandboxie-style sandboxing. Right?

Steve: And unfortunately this is a good enough idea that you can see, you can foresee Microsoft saying, hey, that's kind of cool. Let's add that.

Leo: Well, hire Ronen or give him some money. I mean, I'm sympathetic with Ronen. But I think you and I both agree that PatchGuard is a necessary step forward with Vista. That's what we've talked about; right?

Steve: Yes. It is. It's a good thing, and so is sandboxing. I think that if - I wouldn't be surprised to see, well, I mean, remember once upon a time Windows had no firewall. We were all jumping up and down, saying gee, let's add a firewall to Windows. Well, Microsoft got a clue finally. Took a long time. They added a firewall to Windows. I wouldn't be surprised if some future version of Windows offers sandboxing natively. But I can absolutely guarantee that there's no way that Microsoft is going to be hiring Ronen or giving him any money because that's just not the way Microsoft works. They'll just do it themselves.

Leo: They'll do it themselves. And didn't we talk, when we talked about PatchGuard - maybe it was on Windows Weekly, but I think it was on Security Now!. There are ways around it, aren't there? Remember it was kind of not the strongest - it was like Microsoft saying, hey, guys, get ready because we're going to really enforce this. But they're not yet a hundred percent enforcing it. Or are they?

Steve: Well, it's been so long since I looked at it closely, and I'm not a Vista user. So I remember something about that, but I don't remember whether it was PatchGuard. It might - there are many different new security features in Vista. And so it might have been something else.

Leo: My dim memory, and I may be wrong, is - and I'm sure we'll be corrected - that in this instance the way they implemented PatchGuard on Vista 64 was as much to say to legitimate companies, hey, don't base your business model on modifying the kernel. Going forward we're not going to allow it. But if you were willing to be illegitimate, there are ways around PatchGuard. If you were willing to break the rules, there are still ways around it. And I guess the message was, hey, Symantec and Ronen and everybody, you're a legitimate business. You don't want to break the rules here. And going forward, you're not going to be allowed to. That's my memory of the discussion,

but I don't remember the details on that. So I think there is a way around PatchGuard, in other words. But I could be wrong. You're the expert.

Steve: I can guarantee you that Ronen is unable to operate with it. So whatever...

Leo: Well, but he may not want to do the things required to break it, in other words.

Steve: No, that's not, I mean, it cannot work. It absolutely will not work because he did all those things originally and was compatible with XP's PatchGuard before they strengthened it up to Vista level.

Leo: Right, right. Okay. Daniel Smith in Sioux Falls, South Dakota added an exclamation point to Wizmo. Wizmo! Bang. He says, "Wizmo Fixed It." Wizmo. I love Wizmo. I'm glad we can give a plug to Wizmo. Dear Steve: To start off, thank you for all you do. Now onto the feedback. I'm a desktop support representative at a company. And recently we've been having problems with a few brand new PCs. I just put them into service. For whatever reason, these systems refuse to log off. They refuse - this is very common. I see this all the time. They won't shut down or reboot for any of the users they were assigned to. Now, I was getting frustrated. I was going to create batch files to have these users run to use Windows' built-in shutdown command, when for whatever reason I remembered your dinky little Windows gizmo - no offense intended. I figured I'd give it a shot on a user's machine. I have nothing to lose. Your application, all of your applications have a great track record of being solid and dependable. I wanted to see what would happen. Also Wizmo would be easier for an end-user to operate than my little batch file. At first we tried Wizmo's "nice" command to log the user out. Windows said unh-unh, not gonna do it. We then got serious, asked Wizmo to make Windows an offer it couldn't refuse. You do have that switch; right? Forced, forced it to shut down.

Steve: And literally, you put an exclamation point on the end of the verb "Shut Down" or "Log Off" or "Reboot." I call it - I don't want to offend our users. I call it the "Dammit Variation." Shut down, dammit.

Leo: Shut down, dammit. Lo and behold, in the battle of wills, Wizmo won. Windows logged the user off. But wait, there's more. After that point I thought we'd have to continually use Wizmo on those systems. Since we're a corporate environment, we're leery about continued use. Going to the bank, oh, let me shut down, I've got to use Wizmo. Despite Wizmo being a free piece of software, it's still another application that has to be installed, tracked, okayed by the powers that be. However, my Windows user decided to try logging out the normal way without Wizmo's help. This time Windows did it. It would restart, shut down, log off, everything. We got the same results on the other machines that were also exhibiting the problem. Before Wizmo, they didn't work. After using Wizmo to teach them a lesson once, they all worked. Needless to say, you gave me a great Christmas gift. I've installed Wizmo on all my personal machines. Now I have it on my work machines. It's free, by the way. I'm still not installing it on every machine at work. However, I'm keeping it ready in case anyone complains about Windows giving them trouble. Thank you for this excellent tool, and have a Merry Christmas. Hey, that's really cool.

Steve: And I have no idea why.

Leo: Well, when Windows won't shut down it's because there's a process that won't exit properly, usually; right?

Steve: Well, yeah. That I know. And there's also - sometimes it'll sit there saying "Saving user preferences" or something.

Leo: I hate that. I have that all the time.

Steve: Oh, goodness.

Leo: So what does the bang do? What does it say? I mean, is it a different call to...

Steve: Yeah. Yes.

Leo: Are you using interrupts? What are you doing?

Steve: Well, down in the API there is a force option. And so I don't know what it does. But I say, okay, I'll give the user the option of forcing it. And so it may just say, look, give apps some time and then force them to shut down. What's bizarre is that apparently doing this once fixes the problem then on. So you no longer need Wizmo at all. You can just use the regular Windows shutdown, logoff, and reboot, whatever.

Leo: Does the force lose data if you have unsaved files, things like that? Will it force close...

Steve: I don't think so. No one has ever, I mean, I don't know. Since I don't know what it does, I really don't know what the implications are.

Leo: Probably, you know, it's probably setting a higher standard for, like, am I going to stick around.

Steve: No one has ever complained of Wizmo costing them, like, any sort of data loss. I would be extremely surprised if that were the case. But, I mean, because it is part of the API. And I would be surprised if anything in the API allowed you to, like, deliberately close a file that had been - that hadn't been saved.

Leo: I bet you there's something Microsoft's doing, like saving settings or something, there's some script that runs once. It must be a run-once. And when you do this force, it figures, hey, I did it, and it never tries again.

Steve: Whatever it is, it works. So I just wanted to share it with our listeners in case anyone has encountered this problem before. There is a free fix for it, and apparently you only need to use Wizmo once, and then it teaches Windows a lesson.

Leo: It's going in my database because I get this call weekly on the radio show.

Steve: Perfect.

Leo: Windows won't shut down? Wizmo.

Steve: With an exclamation point.

Leo: Bang.

Steve: Wizmo Bang.

Leo: I love it. Andrew Green of Tampa, Florida, shares his Knuckle Print of the Week Story. I love these. Hi, Steve and Leo. Last week I took the drive over to Universal Orlando. Being a Florida resident we got annual passes, a slight discount. When we got there, they scanned your pass, and you're required to provide a fingerprint. It's obviously leaking over from the Disney folks next door. Now, being a listener of Security Now! since Episode 1, I knew this wasn't a good idea. I told the attendant I didn't want to do it. She said I have to. So like your previous correspondent, I used my knuckle. She said no, it has to be a fingerprint. After a bit of arguing, we got a manager who reluctantly put a sticker on my pass stating "Check ID." This guy might be a sneak-in type. Battle won.

If that were not bad enough, some rides didn't allow bags, but they provided free lockers. The locker system was automated, and no attendants are around. Your key? Your fingerprint. The system checks your - I'm sure they think, oh, is this cool, we'll do this. The system checks your fingerprint twice, assigns you a locker. When you return you enter your locker number and your fingerprint. If they match, it opens. Luckily we didn't have any bags. But besides the fingerprint issue, there was no way to unlock your locker without a valid fingerprint. So if you forget what finger you used, or they don't align correctly, your locker won't open. There seemed to be no way to override this system since no other information is taken other than your fingerprint. What would prevent someone from getting an attendant and asking them to open your locker? I saw no reason why this could not happen. I don't know if they have more traditional lockers. We didn't have any bags; we didn't bother worrying about it. If you go to Universal, pack light, make sure you have your ID, and stand up for your privacy. Keep up the great work. Boy. That's a story.

Steve: Yeah, this is the sad consequence of fingerprint technology becoming inexpensive.

Leo: All of this bio...

Steve: Well, yeah, I mean, fingerprint readers are now very inexpensive. And it's like, oh, this is wonderful. Let's just put fingerprint readers everywhere. And unfortunately, you know, fingerprints are personal property. We've talked about it. Fingerprints is not something that you want to be sending out in digital form all over the place.

Leo: So modern. We use fingerprints. We're the future.

Steve: Yeah, we ought to come up with, like, some sort of a - remember how on "Hitchhiker's Guide to the Galaxy," Arthur Dent had - I guess it was Arthur - had an electronic thumb that was - it was a way of, like, thumbing a ride for a passing alien spaceship. [I'm pretty sure it was Ford Prefect who had the electronic device. Elaine]

Leo: That's right. That's right.

Steve: And we ought to come up with, like, some sort of rubber thumb, like just, you know, you carry it around in your pocket, and it's somebody else's fingerprint on the thing, and you just push it against the screen when you - when something says we want your fingerprint. So, like, this is just a bad - this is a bad trend we're seeing here.

Leo: You could see why people start to figure privacy's dead. You know? I mean, this is just going to be everywhere. And at some point you just throw up your hands and say, fine, take my fingerprint. I mean, just people just give up. Most people don't even know. But even - but those of us who know, at some point, I mean, I just go, okay, fine.

Steve: Well, and our listener Andrew, I mean, he had to fight them not to take his fingerprint. And, you know, not all people, even if you're security conscious, are going to feel like putting up a big fight.

Leo: I'm not a fighter. I always said all right, all right. I would have tried the knuckle thing. And if they didn't, I'd say okay, fine. Which is not probably a good idea. We don't know what they do with that fingerprint database. Who knows. You know.

Steve: Yup. I say give them a knuckle if you can.

Leo: Right to the temple. An anonymous listener brings us the Hard Drive Destruction Headache Story of the Week.

Steve: [Groaning]

Leo: We were talking about how to get, you know, is drilling - you said drill a hole through the platter and so forth. In Episode 173 you guys spent some time discussing secure disposal of hard drives that no longer function. I'm an admin with one of the top security companies in the world. We go through a lot of SCSI and SAS drives a week in

our RAID systems. We have Dell to thank for that because their hard drive firmware requires an update on a lot of our systems, but you have to take the server down before updating the firmware on the RAID arrays. That's not exactly an option. So since Dell doesn't offer a live firmware update - HP does, by the way - we kill disks like it's our job. To dispose of - this is terrible. So they have to shut down, and then the disks die because they shut down? Is that...

Steve: I don't quite - I didn't quite track all that. But I, you know, I believe him.

Leo: To dispose of them we have a large degaussing machine about the size of a microwave. Wow. We shove the entire drive into the machine, hit a button, and after two seconds the drive slides out the side fully degaussed. That's interesting. So I was talking about doing it in the radio station degausser. But obviously if you have a big enough magnet...

Steve: Oh, just wait till you hear what this thing - what the side effects are.

Leo: We had some guys test the disks afterwards to check for data. Not only does it fully destroy the drive, it seems to destroy the heads on the drive. The thing won't even spin up. It probably bends. Everything gets bent. This may be why we get a little bit of a headache after using the machine for a while. Yeah, maybe.

Steve: Ooh.

Leo: Maybe you want to get a lead apron.

Steve: Ooh.

Leo: Can you get hurt from a magnetic field? Is that bad for you?

Steve: Well, MRI uses a very strong magnetic field. But, I mean, the idea that this thing gives them a headache...

Leo: That's not good.

Steve: ...I mean, that's just - that's really frightening.

Leo: That's not good. Maybe it's just - it could be like a low hum or something that's bugging them. I hope that's it. Yeah, wow. So while you guys and some listeners may like to vent by dismembering some drives, for anyone doing any kind of volume destruction, I'd say buy a degaussing machine. Just leave the watch, iPod, credit cards, et cetera, in another room, if you still want them to work afterwards. And bring some

Tylenol. Oy oy oy.

Steve: Oh, yeah.

Leo: Oh, man.

Steve: So just I wanted to acknowledge that industrial-strength degaussing does exist and is clearly effective. It sounds like not only is there data on the drive, there's also extensive servo information, which is always prerecorded on the platters. And the degausser will, of course, uniformly wipe everything. So there's no way, I mean, it's not like just - it's not going to selectively remove the data out of the sectors in between the so-called "sector headers." The beginning of every sector has a bunch of management. Very much like a packet has header data at the beginning of the packet, sectors have sector headers that confirm that the head is on the right track and the sector number and the status, the health of a sector, is this one maybe no good, in which case there can be a pointer to the sector that has been replaced so that the drive then goes and gets the data from the relocated sector. It's all that kind of housekeeping data. So all of that will get wiped out, in addition to some carefully laid down servoing information, which is what the heads read in order to follow the tracks around the drive. That's all gone, too. So, I mean, I'm not at all surprised this drive doesn't even spin up. I mean, it's just - it doesn't know what has happened to it.

Leo: I'm a mess.

Steve: I mean, the drive has a headache, in addition to the people who are using this thing. But boy, I tell you, if a machine was giving me a headache, I would seriously wonder what other radiation besides magnetic it's putting out because I don't think a magnetic field can give you a headache. But...

Leo: Well, we have hemoglobin; we have iron in our blood. Maybe it's pulling all the blood to one, you know, like one side. Like [sound effect]. That would give you a headache over a period, you know, if all the blood is pulled to one half of your head. I don't know. I'm sure, again, I love talking about stuff like this, Steve, because invariably we've got somebody really smart who's listening and says, oh, yeah. Well, I know why that's happening [muttering].

Steve: Well, and there have been science fiction stories where super strong magnetic fields have killed people by pulling all the iron out of them.

Leo: Right.

Steve: You know, all the iron in their blood gets yanked out.

Leo: And there's a lot of quack science about this, you know, the orgone machines and all this stuff, which is all quackery.

Steve: Yeah.

Leo: But in the early days of electricity, that's what - that's a lot of the stuff that people did was, like, medical treatments with magnets.

Steve: Well, and there are still people, yeah, who will pass magnets over you and believe that it's helping you somehow. It's like, okay.

Leo: Oh, I don't think so.

Steve: Good luck with that.

Leo: Yeah. Hope it helps. Randy Hammock, Lake View Terrace, California, with our last question of the week. It is our Hard Drive Destruction Tip of the Week. Seems that most of the drives I've had use glass or ceramic platters. So I just take the drive outside and toss it on the sidewalk. After a single toss, I pick it up and shake to see how much it rattles [laughing].

Steve: Isn't that great? I love that.

Leo: If it doesn't sound like sand rattling around, and it almost always does, then a hammer strike or two will render the platter pretty much destroyed. So are a lot of drives using glass platters these days?

Steve: You know, I was wondering that myself. And there must have been a change since I have last been opening drives because I've looked inside a lot of drives. But mine are, like, early first-generation IDE drives. I have a huge inventory of them that I used for developing and testing SpinRite. So, like, during SpinRite 6 I ran it on every single one of these old drives I had in order to see how it was behaving. But as far as I know, back then they were all metal platters, not glass/ceramic.

Leo: Well, I told you that story about when Patrick slammed the thing with a hammer, it went - we thought it was metal, and it went, like, everywhere.

Steve: Right, right. So anyway, so yeah, toss the drive on the sidewalk. And if, I mean, literally, as he says, if it sounds like sand, you know your job is done.

Leo: I love that. I love that. Steve, our job is done.

Steve: Ours is, too.

Leo: All we have to do is tell people that they should go to GRC.com for many good

reasons. Wizmo is one. Lots of really great free utilities that Steve writes just because he loves to do this stuff and give it away. Of course there's one that's not free that you must have, SpinRite, the world's best disk maintenance and recovery utility. That's at GRC, Gibson Research Corporation, GRC.com. While you're there, of course, you'll find the Security Now! forums there. You can ask questions, securitynow.com/feedback. And you'll find - I'm sorry, GRC.com/feedback. And you'll find the Security Now! shows, the 16KB as well as the full 64K versions; transcripts of each and every show so you can read along as you listen; and show notes, too, with links. So it's a really great place to go. GRC.com.

You can, of course, subscribe to the show in iTunes. I encourage you to do so. Just go to the iTunes store. I know it says "store," but it's still free, don't worry. We don't charge you. I think a lot of people - not our audience. They know better. But I think a lot of people go to the iTunes store, they find a podcast, and they see a button that says "Subscribe," and they think it's going to be a charge of some kind. It's kind of a flaw in the setup. No, it's absolutely free. Just search for TWiT. You'll find all of our fine shows, including Steve. Just look for the mustache on the cover. No, actually Dick DeBartolo's has a mustache, too. But yours is more...

Steve: Yeah, he's got a mustache that could take over the world.

Leo: "Viva Zapata!" All right, Steve. It's great talking to you. We will talk again, believe it or not, Christmas Day.

Steve: Christmas Day, yes.

Leo: Amazing. The man never sleeps.

Steve: I'll talk to you then, Leo.

Leo: Have a great Christmas, and we'll talk to you on Christmas on Security Now!.