SECURITY NOW!

Transcript of Episode #259

Listener Feedback #97

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-259.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-259-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 259, recorded July 28, 2010: Q&A #97.

It's time for Security Now!, the show that covers your security online; your privacy, too. And of course the guy who does this all for us is the great Steve Gibson of GRC.com, creator of SpinRite and many free utilities for security. Hey, Steve.

Steve Gibson: Hey, Leo. Great to be with you again, as always.

Leo: Great to see you. This is going to be a big week because Black Hat and DefCon are going on in Vegas right as we speak.

Steve: Right. Well, actually a little bit after we speak. But this coming weekend.

Leo: Oh, yeah. Hackers don't get up early.

Steve: This coming, yeah, they're late nights and not early mornings. So, yeah, it's - many things have actually been sort of synchronized with this. We will talk today about one of the most newsworthy events, really of many years, which is a weakness has been found in our beloved WPA and WPA2 WiFi encryption protocol. We know that that was created in order to replace WEP, which was not well designed. Unfortunately, it turns out that there's a problem - well, it's not a serious problem, but we'll talk about that. And my point is that it's being disclosed in full this weekend.

Leo: Right.

Steve: And there are a number of other new vulnerabilities that are being disclosed. And in fact the Mozilla folks, cognizant of the fact that they may be in the spotlight, have already said - after actually a very busy couple weeks. They revved Firefox twice since we last spoke, Leo. We left it at 3.6.6. It went to .7 and to .8 between last week and now as they've been fixing lots of things that we'll talk about. But they've said they're, like, watching DefCon and the Black Hat conference and will immediately revise Firefox to fix anything that is revealed there. So this is sort of a new model for our industry is the idea that companies are following the security vulnerability confabs and saying, okay, well, we're ready to deal quickly with whatever arises.

Leo: Very interesting.

Steve: That's crazy, yeah.

Leo: They've got their fingers poised over the keyboard, ready for this. We'll fix it, we'll fix it.

Steve: Right. So it has been a busy week. We can start talking about updates to security. There's been a few things.

Leo: Before you do, I just wanted to mention, I don't know if you saw it, and I know you're very good about not talking about Vitamin D, even though you did a great episode which everybody should listen to...

Steve: You mean The New York Times article on...

Leo: The New York Times on Monday completely confirmed everything you've said. Everything you've said.

Steve: It was interesting to be reading it. And it's like, yeah, any of our listeners a year ago found out about everything that was just mentioned.

Leo: Yeah. Really, really, I mean, I guess that - Jane Brody, who's the health and nutrition writer at The New York Times, I think is very good. I've followed her for years. She wrote this article; it was published on Monday. And if you want a synopsis of everything Steve said, it's right there. And I would recommend you go back and listen to that episode because it was a great episode. And it's available on Steve's site or at TWiT.tv/sn. Just search for "Vitamin D," you'll find it. I wanted to mention that because you deserve credit, and I know you wouldn't bring it up. But you rang the bell on that one.

Steve: Yup. And I've got some other stuff to talk about. I'm going to do - there's been a lot of interest in what I've been noodling around about in the health area. And so we need to do a podcast about my last year...

Leo: Good.

Steve: ...because I'm almost at the end of a year of study of something else that has produced some tremendous results. And it'll be much less of a "this is what I think everyone should do" because one of the things that I've really developed an appreciation for is how different everyone is. And so there isn't any single advice that it's possible to give a broad audience of people. The one thing that doctors get right, I think, is to ask you about your family history because it matters so much. We're just all so different genetically. And that directly bears on the consequences of nutrition and supplements and how our bodies interact with the environment. But with that understanding, I do have a really, really fascinating story to tell. So you and I will have to make some time, maybe as soon as you're done with all your summer travels.

Leo: Yeah, in August, the middle of August, we'll do a separate show. We won't make it a Security Now! show...

Steve: Yup, it will not be security.

Leo: ...but we'll note that it's available on Security Now!. So if you listen to the show, you'll see it. We'll tweet it. We'll put it on the TWiT site and everything. Yeah, I'd very much like to do that with you, Steve.

Steve: You'll be really fascinated, so...

Leo: Can't wait. Oh, now, you're such a tease.

Steve: So we're at 259, Q&A #97 today. And we did have, as I mentioned, people should check with Firefox. Again, I don't know what happens. It sort of seems like if I check under the Help menu, it'll say "Continue downloading an update." And maybe it's the fact that I leave it running for, like, days on end, and it kind of gets stuck or something. But I had to shut it down, manually download 3.6.8 and then run the installer upgrade and then restart it. So it just wasn't keeping up on its own. And, I mean, I was at 3.6.4.

And so these updates have been coming fast and furious from Firefox. And also this pertains to SeaMonkey and Thunderbird. With 3.6.7 they fixed 14 security holes, seven of which were critical. When I looked at the list of URLs for, like, the CVE list that we talked about last week, the common vulnerabilities list, I thought, oh, my goodness. And I didn't want to click on all of them. So I just thought I would take the excellent summary that SANS security newsletter produced and just share that with our listeners to give you some sense for what this is.

SANS assembled this and said: "Mozilla has recently patched several vulnerabilities, some of which may allow hackers to execute arbitrary code on a client's machine. The specific vulnerabilities include several memory safety bugs in the browser engine, some of which may be exploitable for code execution; a problem running content scripts allows an attacker to execute arbitrary JavaScript code with chrome privileges, meaning full browser privileges; an integer overflow vulnerability in the handling of CSS scripts; an integer overflow in the handling of the XUL element; a buffer overflow in the graphics handling code; a problem in Firefox's handling of recursive attribute nodes; a problem with Firefox's method for parsing child elements of a particular tag; and a memory corruption vulnerability in Firefox's NodeIterator interface."

Leo: Whatever that is.

Steve: The old NodeIterator interface.

Leo: Oh, yeah, got the NodeIterator are in trouble, they're on the fritz here.

Steve: Hate those memory corruptions when they happen there, yeah. So just update. Just stay current. iTunes had a remotely executable problem in their ITPC URL. They have, very much like HTTP or FTP or so forth, Apple's iTunes has the URL tag type ITPC, which stands for iTunes Pod Cast.

Leo: Right. In fact, if you try to subscribe on our site to this show, for instance, and you do the dropdown subscribe, it has - you'll see ITPC, it's ://. But what happens when you install iTunes, it registers that URI, and it automatically launches when you click that link. So it's very handy.

Steve: Right. And it turns out that there was a problem in the way they were handling it, iTunes had been handling it, that could result in arbitrary remote code execution. So they fixed it. And again, it's a soup of version updates, depending upon whether you're at 9 or 9.2 or whatever. So whatever you've got, you just want to make sure that it's current. And if you're on a Mac, of course, check for any new software, and it'll find it for you. And I think mine updated, like, over the weekend.

And Google has taken Chrome forward again. Now we're at 5.0.375.125. And Google is, as always, being tightlipped about what they've done. Five vulnerabilities were patched, three they rated as high; although our friends Secunia, who we talked about last week, rated the combined update as "highly critical." There are rumors that Google also reached out and fixed some problems that were actually not theirs, specifically apparently Linux's glibc library had some problems that they took, that Chrome took some sort of preemptive responsibility for. And there's also some rumors that they did something, like to work with a problem in the Windows kernel, but no one's talking. So I'm glad they're on top of it and moving the browser forward as everybody is doing these days - constantly.

So the big news that flooded my own inbox from our listeners was unfortunately again sort of some overblown headlines about WPA2, WPA, the protocol that protects WiFi encryption, being broken. We won't know all the details until it's demonstrated and shown at this weekend's Black Hat conference, which will be happening within a few days. I'm not going to go into it in extensive detail at this point. But we've never really looked at WPA protocol to the same depth that we did WEP. And seems to me that that's a spectacularly good topic for us to tackle in this podcast. So I imagine before long I'm going to want to do a podcast on WPA.

What I can tell you is that this is a problem that arises from the fact that we were attempting, we the industry were attempting to put an encryption wrapper around Ethernet. And the idea being that we have an existing Ethernet network, an Ethernet protocol. And we want to add encryption to that. But because it's sort of a wrapper on top of it, that is, we can't change the underlying Ethernet protocol, but we want to encrypt it.

So in WEP this wasn't a problem because everybody who was on a WEP node had the same key. And one of the mistakes the WEP designers made was that key was directly used to drive the encryption. Which meant that everybody on the same WEP-encrypted access point was using the same key, was generating compatible key streams using the RC4 cipher, which essentially meant that we were all part of one big LAN. And because it was - and we've talked about this before. Because it's radio, everybody can see, hear, and talk to everybody else. So there was no inter-client privacy. That is, under WEP, when you accessed an access point that everybody else was accessing, you were also able to see their traffic.

Well, so the designers of WPA understood cryptography to a much greater degree. And one of the fundamental real guidelines of crypto is you never expose your master key. That is, you don't directly use that key. You use derivatives of that key. And, I mean, that's just now part of common correct practice in crypto.

Well, the designers also said, while we're at it, let's enhance the privacy of users of the same access point. So there's a - the master key that people have for accessing a WPA network, first of all, it is never itself used to perform crypto. But it's used in a negotiation handshake at the beginning when you're setting up your relationship, or the client is setting up a relationship with the access point. The master key is used to derive the keys that you actually use, which are retired sort of for various reasons at different times. Well, the problem with creating privacy is that the Ethernet isn't. That is, Ethernet, remember, which...

Leo: By definition.

Steve: Well, yes. And there's specifically, there's something called a "broadcast" in Ethernet. And there's multicast. And anyone on an Ethernet can, by definition of Ethernet, broadcast to everyone else. So the designers of the WPA protocol had a problem because they wanted to isolate individual users of the access point. But at the same time they had to support all the functionality of Ethernet because they had to be a transparent wrapper on top of Ethernet, that is, to support the underlying protocol.

So what they did was they created a pair of keys per client, the so-called PTK, the Pairwise Transient Key. "Pairwise" meaning it links, it cryptographically protects a pair, meaning your conversation, uniquely your conversation to the access point. But then the problem was, how do you send something to everybody? So they had to have a Groupwise Transient Key called the GTK, which is inherently shared by everyone. And that's the chink in the armor that the Airnet security guys - it's not Airnet. I can't think of their name [AirTight]. I didn't write it down here in front of me. Well, it's easy to find on the 'Net.

The guys who are going to be presenting at Black Hat figured out a way to take advantage of this groupwise transient key. And all we know about it is that they're using the fact that this allows broadcasts to spoof the MAC address of the access point, send a packet to another client on the WPA network, and get that client somehow to reveal its PTK, its private Pairwise Transient Key, which is specifically used for talking to the access point. And that's not something that we want to have happen.

Okay, but understand that what this means, and here's the point of all this, is this doesn't allow somebody roaming the street outside to access anything. What this is, is this is a breach of privacy among clients that are already authenticated on that WPA or WPA2 network. So what it means is, one of the nice things that WPA offers is some enhanced privacy which you'd like to have because you're in the air. You're radio. And we know that radio is a bad start in terms of privacy. So WPA created cryptographic isolation among users of the same access point.

This breaks that, so that one user - and apparently it breaks it badly. I mean, it's like a simple thing to do, once you get this, once you know what the hack is. It's like, oh, 10 lines of code. So what this means, though, is that it isn't - it doesn't allow someone outside, who is not authenticated on WPA, who doesn't have the master key, to get in. It only allows somebody who's already on that access point, who is authenticated, who is now sharing this broadcast key, the groupwise transient key. It allows them to get somebody else's PTK, pairwise transient key. And unfortunately at that point they can play all kinds of mischief. They can, for example, probably do ARP spoofing and insert themselves with a man in the middle or at least do - we don't know that for sure. We won't know the details until we see what these guys have done. But it would have certainly allowed them to snoop anyone else's traffic.

Now, on the other hand, Ethernet sort of always allows that. So hubs have always allowed you to see everybody else's traffic. Ethernet switches are better at isolating that. But they're not guaranteeing isolation. So there's sort of an implied trust with the Ethernet protocol about anybody who's on the same LAN. There's not that much privacy there. And we've talked a lot about how simple ARP spoofing attacks are that allow a person to insert themselves into traffic bound for and from a gateway into other people's streams.

So encryption, WPA, the best encryption we have now for wireless, has been dented a little bit. And once we see the nature, the details of this, we'll be able to get a better sense for how bad it is. But it certainly does not mean that AES is broken, or WPA no longer protects robustly against somebody who does not have the key. This is only a privacy problem among people who are authenticated on the same access point. I learned from a frequent contributor to my Twitter stream who goes by the handle "Captn_Caveman"...

Leo: You're loving Twitter, aren't you.

Steve: I really am. Actually, and I've been meaning to say, I get a great deal of very useful information from the - I don't know if I'm at 13,000 yet, I was approaching it some time ago - number of people who have subscribed to my SGgrc Twitter account. I read everything that is sent because there's not that much of it at this point, which is good. But I really appreciate, I mean, there's a huge number of people who are involved in security and this kind of stuff. And they often run across things before I do.

Leo: I think you're using Twitter in the best possible way, which is a small group. You don't want a million people. You want a small group of people who have the same interests that you do. And it's a conversation between you, of knowledgeable people. And then for those of us on the outside, see, we'll follow that, saying I know where I can go to get great security conversation. I'm going to follow Steve and follow the people Steve follows, which you can also do.

You might look at using the Twitter Lists feature. If you've got 20 or 30 really good security sources that you're following, that you want to share with the world, you can make a list of that and call it, you know, "security sources." And people can then subscribe en masse to that. And that's very useful. I really would appreciate, any time you feel like doing that, that's very useful.

Steve: I guess what's different about what I'm doing is that I'm not following anyone.

Leo: Oh. Well, then, that wouldn't be very useful.

Steve: No. I'm not following anyone. And I recognize that it's a pain for people to send me stuff.

Leo: Well, you don't want direct messages. They have to send you stuff via @SGgrc; right?

Steve: Yes. And so they do. I get it. I read it. So I wanted to make sure everyone knows that, I mean, every single one of those that comes in, I do read, and I try to acknowledge when I can. But it's just - so it's a fantastic source of information for me. Anyway, he was the first person who notified me that Sophos, the well-known security company, had developed a free blocker for this very bad Windows shell LNK zero-day exploit that we talked about last week. So I wanted to point everybody at it.

We talked about Microsoft's temporary fix, which is - in fact we have a Q&A question about it today, which is really a mixed blessing. They say turn off the display of all of the shortcut icons within Windows, across all of Windows. And it's a problem. Sophos.com has a free tool which is very comprehensive and very nice. I tweeted about it a few days ago, actually, the moment after I checked it out from Captn_Caveman telling me about it, and looked at it carefully, and looked at what they had done. They just produced a very nice solution. So it is a workaround until Microsoft fixes it for Windows XP SP3 and later.

But it is probably also exactly what I was hoping for for XP and XP service packs prior to 3, for example, SP2, where several of my machines are stuck. Unfortunately, they do explicitly say that it does not support Windows 2000. So Windows 2000 will remain vulnerable, at least until somebody else comes out with something that fixes it. The Sophos tool will help people who have SP2, which Microsoft presumably is never going to fix, never going to patch. It'd be wonderful if they did because this thing is so bad. And, by the way, worms have started to appear, much as...

Leo: Oh, really.

Steve: ...we expected, yes.

Leo: Oh, boy.

Steve: Yes. The guys at Prevx.com, in their blog, they were the first to indicate that they are now seeing the .LNK viruses and worms are now in the wild, exploiting this. And we can expect over the next couple weeks that it's going to go crazy. So that is beginning to happen.

Leo: Do you think the Sophos patch is preferable to the Microsoft workaround?

Steve: Yes, I do, because it inserts itself into the shell's display of the shortcut. And it is comprehensive inasmuch as, for example, it handles all different vectors for exploitation. And you get to keep your shortcuts. I mean, if you do this thing that Microsoft wants, even using the little Fix it button, suddenly a huge number of icons in your system go white. And so...

Leo: Oh, so this doesn't do that. Oh, that's good.

Steve: No, this allows you to keep the display. What it does is it checks the shortcut on the fly, before Windows has a chance, before Windows gets to it, before it passes it essentially to the shell. It verifies that it's benign and is not going to cause this problem.

Leo: That's great. Good fix. Good workaround, yeah.

Steve: Very nice fix. I wanted to let all of our listeners know that there is something that they can use. Oh, and it installs and uninstalls very cleanly. So once Microsoft, if they do an out-of-cycle patch, if they feel it's that bad, then we'll have a fix more quickly. Otherwise I would hope that, for the second Tuesday of August, that we'll be getting this thing fixed in Microsoft's normal cycle. In which case you can just easily go into Add/Remove Programs and take the Sophos patch out because you won't need it any longer. So as an interim solution, it looks like it's a great idea.

Leo: Excellent.

Steve: And I got a kick out of this. Someone sent me a screenshot - again, this came to me through Twitter - a screenshot of Twitter's own SSL cert, expired. I mean, it happens to the best of us. It happened to me not long ago, we may remember. And the screenshot was a picture of their certificate that showed that it was valid from 5/26/2009 to 7/27/2010. So it had expired on 7/27, and somebody trying to go to https://twitter.com would have received this invalid certificate. So it's like, whoops. I'm sure they've - I presume they've fixed it by now. I didn't check, but I would think they would have.

Also just sort of in browsers-moving-forward news, Safari gets browser extensions. Safari was just updated to v5.0.1. And you can now go to extensions.apple.com, where Apple maintains a list of browser extensions for Safari that add all kinds of cool features to Safari. So Safari has jumped on the extension bandwagon.

Leo: Yeah. Maybe I've been playing with the beta or something. I feel like that's been around for a while, but maybe I'm - I do see the update. In fact, I'm waiting till after the show. I've learned not to do updates that require reboots.

Steve: Oh, actually, it does.

Leo: It's a reboot.

Steve: It forces a full reboot of your machine. And then the last little bit of news in the "oopsie" category is - you may have seen this, Leo - Dell shipped motherboards that were infected.

Leo: Oh. How did that happen?

Steve: Apparently some motherboards, in fact it's four of their servers, the PowerEdge R310, the PowerEdge R410, the 510, and the T410. They contain on the motherboard some flash memory that is like some part of, like, boot process. It's not in the firmware. But, for example, if you run either their Unified Server Configurator or their 32-bit Diagnostics. So it's probably something where like at boot time you can hit F2 or F8 or something, or maybe press a special button, and go into their own built-in diagnostics zone.

Somehow they were shipping replacement motherboards - which of course we know Dell has been doing lately because of the dry capacitor problem - they were shipping replacement motherboards that had that code, their own, like, you know, special diagnostics flash ROM was infected with the W32.Spybot worm. So in the first place it was Windows specific. It would only affect Dell systems that had Windows running on those servers. And they've apologized and said that it affected a small percentage of customers. They've notified them all, blah blah blah. But I also got a bunch of listeners sending that little bit of news to me, so I wanted to acknowledge that.

And the IANA made some news this week by reminding us again that the Internet is running out of IPv4 addresses.

Leo: Yeah. Now, I remember that this was a topic of conversation some years ago and has become - it's come back again. I thought we kind of thought, oh, we dodged a bullet by using all these routers.

Steve: Yes. Well, that exactly. So what has happened is that the worry sort of surfaces every so often, and people come up with solutions around it. I mean, in fact, I think it's in Russia that I read that ISPs, whole ISPs are using NAT in order to solve the IP depletion problem. And, I mean, we know from our own experience what a boon NAT routing is for small offices and homes, where we've got a whole ton of machines behind a NAT router. Now, the Internet purists have never liked the idea of NAT. They've all regarded it as a kludge because the original concept of the Internet with a 32-bit IP address was that, oh my goodness, four billion, we're never going to run out of that.

Leo: How many computers could there be in the world?

Steve: Billion with a "B," you know, it's like we're never going to have four billion machines. Well, actually we still don't.

Leo: No, in fact I think it's something like we're approaching two billion computers in the world. It's not computers that are the problem, is it.

Steve: Well, in fact, that's one of the concerns is that now little things like webcams and temperature monitors and weather sensors and weather vanes and all these little sensors, they all like to have an IP, too.

Leo: I'm holding up a camera here that has a unique IP address, exactly.

Steve: Exactly. So now - okay. So we've talked a lot about, and we will be talking in the future probably a lot more about IPv6 because that's regarded as the only real solution to this problem. IP addresses, as we know, are normally looked at as a set of four bytes. And, for example, there have always been, there have remained up until just very recently, in fact, I think technically today still, 16 of the 256 possible first bytes in the Internet address - like 4.79.whatever, or Google has 8.8 and so forth, and we know that a lot of our home routers are 192.168 and so forth. I use a 10. network where the whole 10. has been set aside as being private and unroutable.

Similarly, there were 16 other numbers, that first byte, that had still been reserved, never been allocated. And those are now, just now, they've been, like, divvied up, where Europe gets this many and Russia gets a couple and we get some. And so they're, like, handing out the remaining top digits of the IP space. And the point of this is that the rate of consumption now, and the projected rate - we never really know exactly what the rate's going to be. But the general consensus is, sort of like the average consensus, is around this time next year, around July of 2011, we're out.

Leo: Wow. At the rate we're going now.

Steve: Kind of at the rate we're going now. Now, again, there is latitude because there are still sort of islands of unused IPs that could be squeezed. I have 64 here at home, Leo. I don't need 64, now that I've just confessed publicly.

Leo: Internet hog. Internet hog. You're an IP address hog.

Steve: Although I only have 16 at Level 3, and I could really use more there.

Leo: I should count them because I bet I have that many, too.

Steve: Yeah, I mean, so...

Leo: We have a lot of internet connections here, though. And you do, too.

Steve: Yeah. I mean, so there are organizations that are still hording them. Although I did read - actually, if anyone's interested, Wikipedia has a very nice treatment. If you look for IPv4_address_exhaustion, they have a great treatment of this whole issue. And Stanford, for example, gave up their big block.

Leo: They had, like, a C block; right?

Steve: Oh, no, no, they had an A.

Leo: They had an A block?

Steve: Oh, yeah, I mean, in fact BBN still has an A block. There have been people who...

Leo: That's how many addresses? 62,000?

Steve: That's 16 million addresses.

Leo: 16 million?

Steve: 16 million addresses is a Class A network.

Leo: Holy cow.

Steve: So, yeah, that's 24 bits because you've got...

Leo: You have three dotted quads to yourself.

Steve: Yes, exactly. So three, the lower three bytes are all yours. But that's also how many are in a 10. network. I mean, I've got one. I don't have - I mean, but lots of people have them. And but remember also...

Leo: But you can have a 10., and I can have a 10. We don't have to worry about conflict because it's not routable.

Steve: Exactly.

Leo: But Stanford's whatever it is, 168 block, they own it all.

Steve: Yes. And in fact remember also that Hamachi, one of the clever things that Hamachi was doing was they were using 5. IPs. Well, that's going to all break soon because...

Leo: So routers have been ready for IPv6 for a while.

Steve: Well...

Leo: No?

Steve: Don't know. I mean, so what IPv6 does - and we'll obviously be covering this in extensive detail, talking about the migration from and what it takes. It takes us from 32 bits to 128. And even though 128 doesn't seem like that much more than 32 bits, remember that this is all that power of two thing. Every bit you add doubles the number of IPs. So the fact is, that's something like 10^38 possible, I mean, instead of, like, 10^9, where we are now, we're at 10^38. So...

Leo: Avtech [ph] is telling me that that's 340 trillion trillion trillion.

Steve: Yes. That's a number I've seen.

Leo: That's a lot.

Steve: And you divide it by the number of people on Earth, and we all get to have several trillion trillion. Just for ourselves.

Leo: So Stanford, you can keep your A block.

Steve: Well, so what's going to happen is this will begin - people are going to begin to get more worried about this. ISPs are going to, like, look at the amount of IPs they have.

They may begin to push v6 compatibility. The problem is Google did a study not long ago, I think it was in '08, that found only one percent of the Internet was ready for IPv6. It's really not yet, Leo. And in fact I'm going to have to ask Level 3, my connectivity provider and the datacenter, do I have IPv6 addresses? I probably do, I just don't know it. Because I would imagine someone like that is way on top of this and following along. But it did hit the news this week that we were running out. And like around next summer, next September, I mean, that is to say 2011, rather, September, maybe July-September, then we begin to have a problem.

Now, again, there's still elasticity. People will rummage around and find more IP addresses. But even when I signed up, when I did my Level 3 setup, this is now, what, maybe four years ago, I had to fill out, they made me justify my allocation of 16 IPs, which was easy because of the stuff GRC does. But so they were already beginning to get more responsible. It's not just like, oh, yeah, here you go, you can have a C block. We've got them coming out of our ears. Not so much anymore.

Leo: Interesting. So a year is not a lot of time, really, if we're going to have to make that conversion.

Steve: Oh, no, it's not. It's not. And then lastly, there had been some dialogue over in the Security Now! newsgroup at GRC over how I kept talking about Episode 260, as five times 52 is 260, and navely believing that there were 52 weeks in a year. Which I sort of seem to remember from elementary school.

Leo: Yes.

Steve: But the fact is, when you take 365.25 - which we know is the number of days in a year because every fourth year has an extra one, it has a February 29. So you get the 365.25. If you divide that by seven days in the week, you do get 52.179 weeks per year.

Leo: So what do we do?

Steve: So, well, we multiply that by five because we're coming up on the end of five years. And that gives us 260.893 weeks.

Leo: Okay.

Steve: So 260.893. So, okay.

Leo: Okay.

Steve: I guess we have to round up. And so it's more accurate to say 261 weeks for our first five years.

Leo: Five years. So next episode will not...

Steve: Not be, yes.

Leo: ...be our fifth year.

Steve: We will not be beginning our sixth year. We will be ending our fifth year with Episode 260, beginning our sixth year, technically, and I guess we could figure out what hour it is on...

Leo: I bet the folks at Entertainment Tonight don't have to deal with this in their audience. I bet they don't get email saying, well, you know, technically...

Steve: That's why we have so much fun.

Leo: I know. I love it.

Steve: So much fun with our people.

Leo: So next episode, which is our 260th...

Steve: Is the last episode of...

Leo: ...concluding our fifth year.

Steve: Yes.

Leo: And in two weeks we will celebrate...

Steve: [Vocal fanfare]

Leo: ...our beginning of our sixth year. Hard to believe, Steve. I mean, I'm amazed that we've been going that long. We are now approaching how long Tech TV lasted. It only lasted six years.

Steve: And do you notice that we seem to be getting busier with security stuff?

Leo: Yeah, yeah.

Steve: I mean, it's going upwards.

Leo: No fear of running out of material, that's for sure.

Steve: No. I have a fun note from a listener of ours, Bill Cox, who's in Vancouver, whose subject line - actually this email just bounced through my sales account this morning when I was updating my mail. What caught me was the subject was "SpinRite on an island." And he said, "Dear Steve, like most people that write to you, I'm a longtime SpinRite user and longtime Security Now! listener. Never thought I'd have a "SpinRite saves the day" story, though.

"A couple of weeks ago I was working with my staff at a client office which is located on a small island near Vancouver. Our business is professional accounting, and we charge out our staff by the hour. There were four of us networking together, peer-to-peer. Of course, as fate would have it, the staff person who was hosting our shared data resources had their four-month-old computer" - which says "new" - "their four-month-old computer suddenly give them a Blue Screen of Death.

"Phoning Dell technical support suggested all kinds of things relating to completely powering down, removing the battery, et cetera. After every change, an attempt was made to reboot, and each time a BSOD appeared. At one point the tech support even suggested that we reinstall Windows. A little hard to do without a functioning hard drive."

Leo: Reinstall Windows and a new hard drive was probably what he meant.

Steve: Yeah. "Eventually they said they would rush courier a replacement computer to us. The problem was, being on a small island meant that 'rush courier' would take about 30 hours. Not to mention the fact that it didn't have - that new replacement machine wouldn't have our irreplaceable data. As I did the math, I realized that the four of us together charged out at $900 per hour. Therefore, a 30-hour wait..."

Leo: $27,000.

Steve: A 30-hour wait, yes, "would cost thousands of dollars. Of course we couldn't charge the client for our faulty hardware. But still, the four of us sitting around, far from the office, represented a huge amount of lost revenue to that degree. Finally, I thought of SpinRite. I downloaded it on my computer, transferred it to a USB stick, and ran it on the BSOD machine. It took about four hours on the first sector."

Leo: Holy - well, now we know where the problem lies.

Steve: "And the projection was that it would take the better part of a year to complete. However, once done with the first sector, obviously where the problem was, it went through the rest of the hard drive in minutes. The result was we got the data off the bad computer and used another computer as the main data store. Of course we also began backing up regularly now just in case. However, we used that previous problem computer for the rest of the week without issue."

Leo: Wow.

Steve: "Thank you for rescuing us while we were 'stranded' on the island. I appreciate that this product just works without any fancy bells or whistles."

Leo: Isn't that neat.

Steve: And ending on "Yours truly, Bill Cox." And I did want to just mention also that this is something we see a lot. People go crazy when SpinRite starts saying it's going to take a year. But what it's doing is it's looking at how much it's gotten done and how long that has taken, and it multiplies that by the remaining number of sectors it has to do. Sort of, I mean, that's the only thing it can do is say, well...

Leo: It's the best thing to do, yeah, yeah.

Steve: ...assuming that the rest of the drive is in the same condition as what it has seen already. But if you start off early on in the drive with, like, where the problems are, then once it gets past that, often its projection just drops dramatically as it's able to see that, oh, look, this is going much better than I thought. And so it was only four hours, rather than a year.

Leo: Well, that's a good thing because I calculated out at $900 an hour that would be $7,884,000 that they'd have to bill their client. So it's probably a good thing. See, that's a good $80 purchase there. That SpinRite saved their client a lot of money.

Steve: And they can use it over and over and over.

Leo: Yeah, that's right. Now, Question 1 for you, Steve. You ready?

Steve: Yup.

Leo: Glenn Edward, Nottingham, Maryland asks, "What are the odds?" Dear Steve, when I first heard that Microsoft was going to drop its support of XP SP2, I thought, as many others probably did, I could live for some time with an unpatched version of Windows - I just want to say that again. That should ring warning bells - an unpatched version of Windows and perhaps take a chance on applying SP3 later if it became necessary. Worst case would be to start looking for another used PC that could handle SP3. Like some of yours, mine cannot. SP3 was troubling on XP.

So what do you think the odds were that within a couple of weeks of the official SP2 patch cutoff, the worst-ever Windows worm would surface? It's almost as if the bad guys had been sitting on this thing for months, perhaps even a year or so, until Microsoft began cutting off XP and Win 2K support. Is it my imagination, or have PC attacks become more intense these days? Thank you. That's an interesting conspiracy theory. Do you think they waited?

Steve: This is the, I have to say, Leo, this is the least over the top of a number of theories that I received. Yeah. Some people thought that maybe Microsoft - I did read someone saying that Microsoft always knew about this and left it in there and waited to spring it on the world by, like, leaking this out.

Leo: Oh, come on, no.

Steve: And it's like, to me that completely stretches credibility or credulity. It seems unlikely in the extreme.

Leo: It's a variant of the thing that the antivirus companies make the viruses so that they'll sell product. Both, I think those are bogus theories, they really are. Nobody's doing that.

Steve: Yeah, and Microsoft, much as they definitely want to get us to upgrade and move forward, they're certainly far more damaged by, I mean, in terms of reputation and people thinking, okay, that's the last straw, now I'm moving to Linux, that's it, or to Mac, thanks anyway. But so I just - I don't see any way that it makes sense. The one thing that sort of feeds this sort of thinking, frankly, is a lack - because most people are not coders, most people haven't been there - a lack of appreciation of how absolutely feasible it is. And this is one of the things that I preach on this podcast is how feasible it is for these kinds of things to exist for 10 years and never be seen. I mean, it really is possible.

Leo: Oh, absolutely, sure.

Steve: I mean, it just, you know. And so we're wringing these problems out of our systems. I desperately wish that Microsoft would just stop changing Windows. Of course it's completely antithetical to their business model to do so. Thus the whole pressure to upgrade moving forward. If they would stop messing with it, then over time it would get stable. But that's just not going to happen.

There was one question, I think it was on one of the Q&As that we were unable to finish a couple weeks back, someone said, well, why is it that Windows 7 is so much better than Vista was? And it's like, well, remember how bad Vista was? Vista was a real change from XP, and it was a security catastrophe. And 7 is just sort of like giving a fresh coat of paint to Vista. They didn't really change anything because they were scared to. And so they sort of, like, fixed the things that they messed up with. So by no means is 7 anything like the change from Vista that Vista was from XP. And Vista's change from XP was, I mean, we've had podcast after podcast about the disaster that it was. And we haven't for 7 because...

Leo: That's true.

Steve: ...there really hasn't, I mean, yes, it's got - we're doing vulnerabilities that are common to all of these, much like this LNK shell exploit is because it's been in there for 10 years. But nothing Windows 7 specific because there really isn't anything Windows 7 specific.

Leo: Right. I mean, frankly, Windows 7 is Vista.

Steve: Yes.

Leo: I mean, it's not a service pack, but it's Vista polished. It's improved. It's got all the fixes in there. And of course it would be better.

Steve: They cleaned up the UAC a little bit so it's not bugging people to death, and they don't have to turn it off. And, yeah, they did some next-generation UI things. But the core, which was dramatically enhanced for Vista from XP, they've pretty much said, okay, we're not going to change that now.

Leo: Yeah. Oh, I have to read another question. Okay. Let me move on. Question 2, Stephen Conway in Dublin, Ireland found, demonstrated, and proved, and got a bug fixed in LastPass: Steve, Security Now! is a beacon of sanity in a world gone mad. Wow. I really enjoy listening to educated, balanced, and reasoned guys discussing important information. Thank you. I, too, am a SpinRite owner, and like every week you have a spin on SpinRite, I have many I could add, mostly boringly and predictable. Family member: "Oh my god, my computer won't boot. I've lost everything." "Wait, give me a day or two." I'm sorry, I'm making him sound like a leprechaun. He's not. Later, family member: "Wow." Me: "Back up your data." Anyway, not the reason I'm here today, Steve.

I previously wrote and send you a long, frustrated note, but skip that now. To give quickly the full picture regarding the invalid password from LastPass, I've attached their explanation. After many emails and videos of the error, I could prove that my password was correct and there was an issue on their servers. I've actually had that happen, too. So I'm glad to see that he noted it. Actually it hasn't happened lately, but it came and went for me, and I thought, why? It's valid.

Steve: Well, and you're about to find out why.

Leo: I must say the support from LastPass was extremely good. They really responded to my many emails and followed up the problem, and this is a free service. Yeah, he's not paying for the premium. The customer service turned a negative situation into a positive one. Take care, Stephen. And the reply sums up what had happened. "Stephen, we believe we've resolved the issue and added automated checks to ensure it doesn't reoccur. We use multiple datacenters and database servers linked by replication, but one of the servers didn't have correct data. As a result, unfortunately yourself and one other user would intermittently hit the 'bad' server and get the invalid password error." I'm going to add myself to that list. I just didn't complain about it because it didn't happen every time; right?

Steve: Right.

Leo: "This is why it would sometimes work for you, sometimes not. I say this is unfortunate because the invalid password error would happen only to you and one other user out of over 700K users. Thanks for being persistent to help us resolve the issue. Wow. So two people complained, and they fixed it.

Steve: Yup.

Leo: "Again, we receive about a dozen 'help, it won't let me login' requests a day, and every single one of them ends up being mistyped passwords." Not in my case, I cut and paste. "And so perhaps you could understand our initial skepticism. In any case, we're very sorry for any inconvenience. Let us know if you encounter further issues. Thanks, LastPass." Wow.

Steve: So what he did - and I did find, I went back and found this lengthy email of frustration, you can imagine, because he's, like, he's sure he's doing it right. And they're saying you're probably just not. And he's like, no, I'm sure I am. And then the other thing is that apparently what they have is, because they're using replication and distributed datacenters, sometimes the routing of his authentication would go to a server which correctly had his data, and sometimes it wouldn't. So he was also having to deal with the fact that sometimes it worked, and sometimes it didn't, which hurt his credibility further. But he stayed on it. He made videos of what he was doing. He refused to give up.

Leo: Thank you.

Steve: And he showed them that, okay, it's really not working, and I really need it to work. And they said, oh, it really does look like it's really not working.

Leo: Right.

Steve: And then they scratched their heads and dug in and found it and fixed it. So props to Stephen for pursuing it and to the LastPass guys for listening to him - and, yeah, he gave them no choice - but for also getting on it and fixing it for all of our sakes. Because that would be pretty annoying if it didn't work.

Leo: Yeah. Well, it's funny, because it was happening to me. And these things happen to me, and I'm just used to it. This is kind of one of the things I think that happens to sophisticated or longtime computer users is you put up with crap.

Steve: It's like Ctrl-C. I'm so conscious now that Ctrl-C doesn't always work. And I realize how much accommodation I have done of that.

Leo: Because that's normal with computers.

Steve: Yeah.

Leo: It's often the newer users who become very frustrated. And that's why I have a lot of sympathy for new users or inexperienced users because I forget that we're just kind of inured to the fact that they crash and they fail. In fact, it's much better now than it used to be. So we feel like, oh, this is great.

Steve: Yeah, it's way better. I mean, Windows used to be just locking up all the time.

Leo: Oh, yeah. Exactly. So, but I'm always grateful for the user who is persistent and who says, no, I'm going to fix this. And I do encourage that, and we benefit from that. So thank you, yeah. Because I was getting that error, and I know - see, I was second-guessing myself. I was thinking, well, I must have mistyped that. So what I did is I put the password in a text field in my Evernote, and I would cut and paste it. And sometimes it would work, and sometimes it wouldn't. So I knew there was something weird. And it is fixed now. It hasn't happened in a long time.

Steve: And for any of our other listeners who may have encountered this as well, we've got good news. It looks like it's fixed.

Leo: Yay. Question 3, Rodney Morton in Round Rock, Texas - which is just around the corner from Dell, I believe - was warned about a Security Now! PDF by McAfee. Okay, I'm not going to laugh. Hi, all. As a long-time listener I was surprised to receive a "site advisory" message when saving the PDF version of the transcription for Episode 255. I did note that my McAfee "Total Protection" had completed an automatic update just prior to my saving the SN-255.pdf to my system. Being security-conscious and aware of the Adobe woes, I thought I'd make you aware. Not that McAfee is 100 percent infallible, as I'm having some licensing issues with those folks for not wanting to use the words I really had in mind.

Steve: So this was an opportunity just to talk about false positives. Because they occur all the time. And it's no one's fault. Frankly, what the antivirus companies are doing is phenomenal, in my opinion. I'm so glad that's not a business I chose to pursue because it's just - it is so difficult. Anyone who is offering software or now even non-software content like PDFs encounters this. I get a report, oh, maybe a couple a year, someone will say, oh, you've got a virus in, like, in Securable.

Now, I haven't changed Securable in four years, since I first wrote it. It's been sitting there unchanged. And so I doubt that I have a virus in Securable. And sure enough, Greg normally fields these things for me, and he'll say, well, did you try updating your virus patterns, or report that you think you have a false positive? And then they come back the next day, oh, yeah, it went away now. It's like, okay, yeah. So this just happens.

The reason I thought this was worth mentioning was just sort of to remind people that the job that's being done is herculean on the part of antivirus. The idea that they're looking through a rapidly escalating volume of binary-ness. I mean, it used to be K, now it's megs, and hundred of megs of data, on the fly, looking for patterns that match some that they have in this huge and growing volume of possible match patterns. I mean, so I don't even know how the software does this. When you think about what it's doing, that it's scanning files at that speed, looking for any of thousands of possible pattern matches of random binary data that happens to be sort of the "signature," which is just a run of bytes that is known to sort of be reflective of a possible virus, I mean, it's just incredible that they do as well as they do.

So I am never annoyed or upset when a false positive occurs. We explain it to anyone who has used our content, that it's probably not us. We'll check it. But it's very likely that this is just, I mean, statistically, statistically it has to happen. You have to have some likelihood that some particular confluence of bytes in, for example, in this case a PDF, will by chance match a signature that is also a similar confluence of bytes that occurs in some virus somewhere on the planet. It's just going to happen.

So hats off to the AV guys. I think they do a fantastic job. Like I said, I don't want that job. And you've got to be sensitive enough not to miss something, but not too sensitive so that you're generating false positives at a rate that then annoys people more than the benefit you're providing. And that's a fine line which I think they do a really great job of walking.

Leo: You're kinder than I am, but okay.

Steve: Well, I'm a developer. I recognize...

Leo: You get a lot of false positives. I'm going to ding them a little bit because I think what happens is different companies use different virus signatures, and different companies use shorter versus longer virus signatures.

Steve: And have different heuristics, certainly.

Leo: And different heuristics. And I suspect what happens here is that sometimes, in order to improve the speed of the scans or the size of the downloads, they shorten the signatures to the point where they're more likely to get false positives. And it has been my experience that some companies get more false positives than others. And you've been dinged many times by McAfee; right? It's not the first time McAfee's dinged you.

Steve: I don't even really pay attention to who, so...

Leo: Okay. I seem to remember this happening a few times before from a particular company.

Steve: Well, yeah. Anybody who's providing content will be hearing from people saying, oh, you got a virus in that file. I mean, it happens all the time. It's like...

Leo: Yeah. It does happen. It's never happened to me. And I just don't know why, but I think it's something about - I don't know. It's just I think that you could have fewer false positives, but at a consequence - the size of the signature file, or perhaps the speed of the search, or perhaps your heuristics. But I don't think this is a heuristics thing, but maybe it is. Heuristics might not maybe be tuned. But you're kinder than I am, and you're the expert, so I'm not going to say anything. Moving along. Bruce Harrison, Durban, South Africa...

Steve: You're not going to say anything more, you mean.

Leo: Anything more. Good, thank you for correcting that. I shall zip it for the time being. Bruce Harrison in Durban, South Africa, Question 4, brilliantly wonders whether AES just became less secure. This is the encryption technology that I think in the past we've agreed is the state of the art.

Steve: Yup.

Leo: Greetings, he says. Now that Intel have added the AES instruction set to their chips going forward, does this mean that cracking AES just got easier for the bad guys? Thanks for everything you do for the security community. Warm regards from South Africa, Bruce. So I didn't even know this. So they've added this into the instruction set.

Steve: Well, yeah. We talked about this last week.

Leo: Oh, okay.

Steve: The Intel Core i5 and i7 chips have a vocabulary of new instructions which TrueCrypt v7 has begun using.

Leo: Ah, okay.

Steve: And so this accelerates the functioning of the AES crypto algorithm because one of the reasons AES was chosen was that it lent itself to efficient implementation in hardware. So Intel jumped on this and said, well, let's do some custom AES instructions which literally - where one instruction replaces a big block of instructions otherwise. TrueCrypt gets a 4-8X gain in performance. But that also means that brute-force cracking gets a 4-8X gain...

Leo: Oh, it does.

Steve: Well, yeah. Because as far as we know, the only attack against full-strength AES is brute force. And remember that, for example, a 256-bit key, 256-bit AES uses 14 rounds of encryption, meaning that the same thing is done 14 times. And fewer rounds of AES have now been analyzed, I think like seven rounds, or eight. They're able now, cryptographers, to sort of track the migration of the bits through each round, up to about that point. And then after that they lose track. So it is the case that cryptographers who designed AES understood that, and they chose 14 rounds for 256-bit keys, I think it's 10 rounds for 128-bit keys, and maybe 11 for 192-bit keys because AES can run at 128, 192, or 256.

So what Bruce noted is that, well, anyone who's attacking AES in different ways, who would be attacking it by actually using it, which is what a brute-force attack does, also gets accelerated by virtue of these instructions in Intel. So for those of us using AES, it's a benefit to us, for example with TrueCrypt, because v7 will now run faster, if you've got one of the supported Core i5 or i7 chips. But, similarly, somebody trying to use brute-force cracking does have a speed gain.

Now, the fact is, 256-bit keys are, I mean, really even 128-bit keys are so much more strong than is feasible, if they're good keys, if it's like a random 128 bits, so much more strong than it is feasible to crack that this still isn't a problem. Having a 4 or 8X gain means, okay, now it's only one eighth of a bajillion years.

Leo: Now, it's only halfway to the end of the universe instead of all the way.

Steve: Yeah, instead of a whole bajillion, it's only one eighth of a bajillion. It's like, okay, fine. Good luck with that.

Leo: So that's interesting. I assumed maybe it was symmetric, or asymmetric, that it helped with creating a key, but not with reversing that or something like that. But it is symmetric.

Steve: It's a great observation that Bruce made.

Leo: Yeah, yeah. Good. Lee Elliott in Columbia, Missouri has thought about the new Windows LNK shell vulnerability and virtual surfing: Steve and Leo, I've been listening for a few years. I'm caught up with listening to, if maybe not fully understanding, all of the episodes. Join the club, by the way, Lee. This Windows shell vulnerability has me a little freaked out. I'm looking at a bunch of "white page" icons right now on my Windows 7 machine. This seems a bit Draconian. I guess he applied the Microsoft workaround.

Steve: Fix, the temporary fix, yes.

Leo: Assuming that I'm not vulnerable to a sneaker net attack, would it adequately protect me to do all my surfing on a Linux virtual machine? Of course this would mean not opening documents, et cetera, outside of that virtual machine that might have an offending shortcut, and I don't have any network shares. Basically, I'm trying to avoid inadvertently surfing to a malicious web page. Or am I misunderstanding the threat, or the protection that surfing from a virtual Linux machine might provide? Hey, that's a great suggestion. Lee Elliott, Columbia, Missouri - SpinRite owner, Carbonite user, Audible listener. Right on.

Steve: Okay. Absolutely, doing your surfing in a Linux virtual machine is about the best thing I could imagine for protection, better even than surfing in a Windows virtual machine because a Windows virtual machine will be a virtual machine known to be vulnerable. You would be counting on the virtualization to protect you, which is probably a good bet. But, gee, if all you really want to do is surf, then Linux is going to boot faster. So just use a nice Linux running in a virtual machine, and it doesn't have the shortcut problem at all.

So by essentially switching to Linux for your surfing, by virtue of running it in a virtual machine running on top of Windows, you have complete containment of surfing. So you have the security of just in general being on Linux, which is not being attacked to the same degree that Windows is, so there's a bonus there. And you have virtualization, so there's a bonus there. And you're in an OS that doesn't have the LNK shell shortcut problem. So that's just - that's a huge win. Absolutely. I would recommend that. If that's something that you want to do, you're completely safe from this particular problem - and probably lots of other ones that we don't know about yet.

Leo: In fact, if I were you, I would just throw out the Windows and run Linux.

Steve: Yeah, exactly.

Leo: Just a thought. Nathan Hartley, Lansing, Michigan, Question 6. He notes that OpenDNS filters for DNS Rebinding. He is quoting the OpenDNS settings "Suspicious responses," "Block internal IP addresses," and it explains "When enabled, DNS responses containing IP addresses listed in RFC1918" - I think that that's the private IP addresses that they're talking about - "will be filtered out. This helps to prevent DNS Rebinding attacks. For example, if badstuff.attacker.com points to 192.168.1.1" - which is internal to your network - "this option would filter out that response." It's that cool.

Steve: Isn't that really cool.

Leo: And it does all three of the private addresses - the 10-dot, the 172.16, and the 192.168.

Steve: So I didn't know about this. I jumped over to my - I just hadn't noticed it before. I jumped over to my OpenDNS account. Now, sadly, this option is not enabled by default. So they have left it off. But I realized that I can add testing for this to the DNS

Benchmark that I'm working to finish right now. That is - and we're going to be talking about rebinding attacks probably next week, unless the upshot of the Black Hat and DefCon conferences...

Leo: We might have more to talk about.

Steve: ...is such that we have to hold that one off for something even more fun and interesting and hopefully not dire. Because I want to really explain in detail what that is. But what's brilliant about this, and I appreciate the OpenDNS folks having this notion, is there is no reason why a remote DNS server should ever serve you a private IP. That is, like an IP within your own network. You're asking for public domain names. And so, by definition, Amazon.com or Google or whatever can never be a nonroutable IP because you're asking for the IP in order to send packets out to it. So if it's nonroutable, they can't go anywhere. And so the only thing that can happen is mischief. And so I think it's a tremendous idea for DNS servers to not allow those nonroutable IPs.

Now, what I'm going to do at GRC, I already have a sort of a pseudo DNS server that I built some time ago, which is the way my versioning system works; the way, for example, when you run the DNS Benchmark, it asks for the IP address of DNSBench.version.grc.com. It actually asks for it as an IP address in a single packet. And in a single packet I respond with the latest version of the utility. So I'm using DNS sort of as a communications means.

So I realized that I could test DNS servers to see - like OpenDNS, for users to verify that it was or not filtering. Because you would ask your DNS server for some funky domain name at GRC, which would return an IP like 192.168.1.1. So, for example, you would ask your DNS server for that domain, the IP of that domain. It would ask GRC. GRC would return a private IP on purpose. The question is, does your DNS server forward that to you, or say, eh, don't think so? And so OpenDNS has the option of not doing so.

So I just wanted to let all of our listeners who are OpenDNS users know that under the Security tab, where you're configuring your network, on the Security tab the last checkbox of three is not enabled by default. But by all means, turn that on, and you've got immediate rebinding protection.

Leo: Mine's turned on. And maybe I just thought to turn it on. I don't know.

Steve: Okay. Mine wasn't. And I don't think I would have turned it off.

Leo: Right, yeah.

Steve: So I was assuming it was not on by default.

Leo: It's probably the case. Hey, can I ask you something, though? I'm a little scared because I just logged in to see this in OpenDNS, and I've got "Malware botnet activity detected on the TWiT network today at 2:43 a.m. UTC," which is just now. And it says an IP address. What would that mean? That would mean an attempt to access a botnet from my network?

Steve: A malware botnet...

Leo: Botnet activity detected.

Steve: Activity.

Leo: That's what it would sound like to me, like something on my - because what OpenDNS is looking at, DNS requests from my system.

Steve: Yes. So that would mean that something in your network has asked for domains that they've identified as, like, botnet control. So that's not good.

Leo: No. And you know what, this is another reason why OpenDNS is fantastic. All of our DNS requests come through there. And it's just notified me that it saw some suspicious activity on the network. Now I'll have to figure out exactly what system it came from. They do give - I think they give me more information. I'll have to look at it.

Steve: Cool.

Leo: Yeah. Isn't that interesting.

Steve: Very nice.

Leo: Yeah, nicely done.

Steve: And I did want to mention just one thing I forgot to say about the IP depletion thing. The best thing that ever happened to end-user security was NAT routers. We've talked about that so much, that one of the things - the Internet purists who believe that, oh, no, NAT is fundamentally evil, it's like messing up the packets, you're rewriting packets, you're changing ports around, that's just wrong. Every machine ought to have its own IP.

And what that means, though, is that any machine is directly accessible to any other. And it's like, okay, well, the good news is we now know how insanely insecure that would be. And so there's no way that, even if NAT is no longer necessary, I imagine we will still end up with hardware, little hardware firewalls at our borders which protect our LAN, rather than just having all the packets that want to wander in off the Internet able to directly come in and probe all the machines on our network. I mean, that would be the alternative, and that would be nuts. I mean, I'm delighted with the security that a NAT router inherently provides. I don't want to see that go away.

Leo: Right. Hugely valuable. And it doesn't obviate the need for other security. But, boy, it's great that it's there to begin with.

Steve: Right.

Leo: Moving along. Let's see. Ray Garrett in Miami, Florida wonders how much damage the shell LNK exploit could really do as long as your UAC is turned on. Steve, how much damage - well, I just said that - assuming the user doesn't click on a UAC prompt elevating the malware to an administrative level? I'm assuming it has no way to install a rootkit on the machine, right, because UAC would stop that, or embed itself deep into the bowels of the operating system. It can only perform the same actions as a limited user would be able to perform.

Are there any known problems with the UAC that would allow the malware to elevate itself to administrator without explicit permission through a UAC dialogue popup? It seems to me UAC would severely limit the damage that can be done using the new Windows shortcut vulnerability. Well, that seems sensible. What's the case?

Steve: Well, I guess my feeling is that another way of asking this question, or sort of flipping it around, would be to say, well, if we know that the shell LNK vulnerability is only able to execute under the permissions of the current user, which is what we do know about it, then does that mean we're comfortable having malware running as us? And I would say - I would use an expletive here [laughing]...

Leo: Heck no.

Steve: ...in front of the word "no."

Leo: Yeah.

Steve: So we're glad UAC is there. And we're glad that for most things that are asking permission, they do so, and we have to give it to them. But there's just so many ways that something could lodge itself in our machine as us and then, like, wait for permission or wait for us to reboot as an admin or wait for us to do something. It's like you just don't want anything to get a foothold because footholds are bad. And so I would never suggest that we don't care that, oh, our machine's encrusted with malware; but look, we're a limited user, so it can't do anything evil. It's like, oh, just give it time.

Leo: [Laughing] But it does bring up the point that, if you're using Windows Vista or Windows 7, you're probably a little bit safer than if you're using previous versions of Windows which didn't have UAC.

Steve: Absolutely. Microsoft, one of the painful yet useful things Microsoft has done is to slowly march forward with tightening Windows down. And it always causes conflicts. It causes problems. And people complain, but then Microsoft negotiates back a little ways or does whatever they have to or makes it a little less noisy. But, yes, we're really moving forward. And that's a good thing.

Leo: Yeah. Yeah, it is. Let's see. Question 8, Paul in Ottawa, Ontario with a LastPass TNO Rebuttal: Hi, Steve. Just getting caught up on Security Now! episodes after some vacation time off. Couple of points you might be able to clarify about LastPass for me. One, it's all nice that LastPass folks explain how your passwords are encrypted and saved. But it's one thing to say this is how it's being done, another that it's actually being done that way. Is there a defined way to know for sure? I'm not saying that LastPass would be up to no good. But hypothetically speaking, let's say someone buys LastPass as a company, changes the code to the browser plug-ins that would allow them to get your login information. You'd think everything's okay. You'd get a notice that the plug-in needs updating to support new features or something. Isn't that a potential threat?

Secondly, if the plug-in uses SSL to communicate with LastPass, how can I check the certificate? Third, also in reference to some websites not allowing special characters in passwords, I'd question the use of such a website for the simple reason they may not be hashing your login credentials. If the password is hashed before it gets stored in a database, it wouldn't matter what characters are in it. That's a good point. Your thoughts? Paul from Ottawa.

Steve: Well, this was a good question. And many people said, okay, Steve, you've explained the technology of LastPass. You've explained how it is that they're able to hold our data and not have access to it. How do we know that's what they're doing? And that's a very good question.

Leo: Yeah.

Steve: Because you can't...

Leo: It's not open source. You can't review the source code; right?

Steve: Correct. Well, correct. The plug-ins are not open source. The scriptlets are. And they have arguably done everything they can to be open kimono with us. I mean, they've created a page where you can look, you can exercise their code, see that the code that they provide on this page executes exactly the same way. But so people are saying, and I think this is more of a theoretical argument, or I'm going to take it that way, it's like, yes, but how can you absolutely know?

And the answer is we can't. I mean, I'm running Windows. I'm assuming Microsoft is on my side. Lots of our listeners are running SpinRite, and they're assuming I'm on their side. Or they're running all the little freeware stuff that I've written. And there's an implied trust when you're using someone's software. Our systems are not designed to protect themselves and their users from the software that runs on them. They're just not. They were designed at a time when we inherently trusted the software we were running. They were designed, the architectures were created before the Internet and before security was an issue.

And even systems that always had some security, like Linux, I mean like UNIX from day one, where you had the notion of a root user, and security was bound into it from the beginning, unfortunately the need of convenience has softened those borders. And Microsoft's own evolution has moved more of the system into the kernel, where it's causing much more havoc than had they kept it out in user space, which was their original security model that was a lot stronger theoretically than where they are today.

So, yes, theoretically LastPass could go to the dark side, change the way plug-ins work, and capture all of our usernames and passwords. I don't think they will. I hope they don't.

Leo: Pray they don't.

Steve: Yeah. It just, I mean, I guess my point is...

Leo: Could you, with Wireshark or something - I guess you really couldn't spot that kind of stuff.

Steve: You definitely could, if you were insanely concerned, intercept the SSL traffic in Microsoft's library before it gets encrypted; and always monitor it; always decrypt it yourself; always look at it on the fly; always verify that nothing else is happening; and, like, create your own overlord to, like, impose itself between your archive and theirs. And I guess my feeling is, boy, look around you at all the other stuff you trust, with much less, I think, with much less reason to trust it. How many of us are running freeware that we just found on the 'Net somewhere from people we don't even know at all?

Leo: True.

Steve: I mean, at least everyone listening to me has some idea who I am. And so you might say, gee, I really believe Steve's not going to play any games with his software. But I run a lot of stuff that was written by people, I have no idea who they are. And compared to the level of trust that I think LastPass folks have reasonably established, I'm very comfortable with using their solution.

Leo: Last question. I think this one's a quick answer, too. From Robert Sylvester in Warwick, Rhode Island, my old stomping grounds, wonders about Sandboxie. Steve, doesn't the use of Sandboxie (which is a sandboxing program) or Windows Steady State (which is the program that lets you reinstall Windows every time you reboot, or kind of reset it to a known good state) prevent permanent problems with remote code execution via the LNK and PIF file vulnerability? I always assume that, if you don't save anything or expose private data, you're always safe. P.S.: Paid Sandboxie sandboxes USB drives, so that would help in preventing the vector, anyway. Yes?

Steve: I don't think so.

Leo: Okay.

Steve: The problem is, and this is - I chose this question because it teaches us, it reminds us something important about security, which is we need to be conscious of what it is that is being protected. So, for example, in the case of Sandboxie, Sandboxie - and we did an episode on this some time ago. It very carefully limits what the programs running under its management are able to do. It filters their access to the operating system, preventing them from doing things. But it still uses the operating system. It's assuming that the operating system itself is benign.

And what we have with the .LNK problem is the operating system has an error. So Sandboxie could be written or updated, much as the Sophos guys did, to intercept a defect in the operating system and protect the user. But today I'm sure it doesn't. So I'm sure you could run, if you had a browser-exploitable .LNK problem, and you ran that in Sandboxie, it would have the operating system render the image of the shortcut because the operating system does, and you'd get exploited, even in Sandboxie, because that isn't what Sandboxie was designed to prevent. That's just something outside of its purview completely.

In the case of Windows Steady State, well, you'd have an infected machine until you rebooted. And you don't want that, either, because who knows what kind of mischief things could get up to between then and now - between then and the time that you reset yourself. So, yes, Steady State, much like booting from a CD, would - you're not making permanent changes. But I'd be very uncomfortable letting malware rummage around in my system, and on my network especially, even if I knew I was going to be expunging it when I restarted the system. So, much better to shut this thing down and not let it get a foothold. Again, "foothold" is sort of the key.

Leo: Right. It's your beachhead, and don't give an inch. Steve Gibson is the man in charge at GRC.com. That's his site. You can get 16K versions of this show for the bandwidth-impaired, transcripts, and all the show notes at GRC.com/securitynow. If you want to leave a question for our next Q&A episode, two episodes hence, just go to GRC.com/feedback. And of course if you want to subscribe to Security Now! you can go to TWiT.tv/sn. We've got audio and video versions available.

We also invite you to watch us live because I watch the chatroom, and we often feed back questions from the chatroom into the show. And the live stuff is done at live.twit.tv. This show is Wednesdays, that's when we record, at 2:00 p.m. Eastern time, 11:00 a.m. Pacific time, that's 1800 UTC at live.twit.tv. Steve, thank you for doing this.

Steve: You guys have been posting the podcast earlier, haven't you.

Leo: Who knows. You're asking me? I used to have something to do with that. That was back when it was just a one-man show, or a two-man show. But now that it's a 12-man show, I have no idea.

Steve: For what it's worth, I have been noticing that it's been going up sometimes later in the day on Wednesday.

Leo: Yeah.

Steve: So I just wanted to let our listeners know that...

Leo: My instruction is that, as soon as it's done, put it out. Don't hold onto it.

Steve: Why not, yeah.

Leo: Yeah. And so because our staff is so efficient and has gotten so good, I think, at editing - and I don't know if it's Tony that does this. I think it might be Eric or Dan. We have three editors now. And then JammerB, John is the one who puts the feed information out. And I just told John, you know, if it's done, if it's up on the server, why hold back?

Steve: Yup.

Leo: So that might be what's going on. Don't necessarily count on it. We guarantee, barring major technical snafus, which we've had in the past, that it will be out on Thursday. But, yeah, if it comes out Wednesday, hey, why not?

Steve: Yeah. Look for it.

Leo: Thank you, Steve. Great to see you. We'll see you next week. Oh, what are you going to talk about next week?

Steve: Next week I think we're going to cover in detail the neat hack of DNS Rebinding, which has been around for a while, unless DefCon and the Black Hat conferences bring something to light that we really have to talk about instead.

Leo: And I don't know if I warned you ahead of time, but I will be out of town next week. Tom Merritt will be helming the show.

Steve: Oh, okay. I didn't think we were losing you until...

Leo: Wait a minute. No, no, I'm - no, you're right. I will be here. You're right. I'm taking a red-eye.

Steve: I was tracking you, so...

Leo: Yes, you're absolutely right. We're leaving after the show. I'm taking a red-eye, which is such a good idea.

Steve: And the week after, too, you're not leaving until the evening, I think, on Wednesday.

Leo: I think I'll be okay.

Steve: Yay.

Leo: We're going to keep up with our never having missed a show in five-plus years.

Steve: 5.179 or whatever it is.

Leo: Steve, we'll see you next time...

Steve: Thanks, Leo.

Leo: ...on Security Now!. Bye bye.