Listener Feedback #64

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-192.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-192-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 192 for April 16, 2009: Listener Feedback #64. 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!, the show that covers all your security needs from soup to nuts. And here he is, our chief nut, Mr. Steve Gibson.

Steve Gibson: Chief security nut.

Leo: You are, you know, some would say, and in fact I think you've probably heard this from time to time, that you are a security nut.

Steve: I am fascinated by the technology and the issues that it brings up with security, yes. I certainly know many people conversationally in newsgroups and through email contact who are, I would say, more security focused than I am. But...

Leo: It's not your only job.

Steve: It's not my only job. I just - I love it because it's an area of applied technology which is certainly very interesting.

Leo: Yeah. Well, today we have the question-and-answer segment we do every other show, which means we've got questions from the listeners, 12 good and true listeners.

Steve: Really interesting comments, lots of interesting stuff to talk about, and a bunch of front of show errata and security news and our regular startup stuff.

Leo: Well, let's get right to it. What's the latest?

Steve: Latest is I did close the show mumbling that I may set up a little Conficker honeypot. That's been running for five days.

Leo: Oh.

Steve: So I have my own copy of Conficker and some interesting observations. There's so much interest in it that I've decided - and we haven't done a podcast on it. We really need to do that. So next week's topic is Conficker.

Leo: Oh, good.

Steve: I'm going to attempt to do a complete timeline, a very clear, thorough, technical analysis of it, and really explain how it's changed over time. I mean, the fact that it is changing as rapidly as it is, is interesting, too. And also the fact that in several cases recent security innovations have been incorporated into updates, I mean, within days of them becoming available. There's an amazing amount of technology in there. I mean, none of it's ground shaking. None of it's new. But it's unusual for the kind of authorship we have seen of these things in the past. I mean, there's a lot here.

For example, its update payloads have full cryptographic digital signatures as part of them. So that prevents any non-Conficker authors from commandeering Conficker by tricking it to upload their own payloads because Conficker checks the digital signature of anything it's accepting to make sure that it was signed by its authors. And as we know, that's not spoofable when it's been done right. So there's lots of stuff there.

My own little copy here has been patiently chunking away, chugging away for the last, I guess about five days. It's fun. A number of things have happened. For example, it stumbled into a couple tarpits. And the tarpits it stumbled into are run by the National Center for Supercomputing Applications.

Leo: That's interesting.

Steve: They've set up a large block of IPs specifically to monitor the behavior of worms and viruses and things. And as we remember from talking about tarpitting, what a tarpit is, is Conficker sent out a connection-opening SYN packet, and the responding server or service sent back an acknowledgment saying, yeah, I'd be happy to accept your connection. But, oh, I don't have any available buffer space. So hold on a second. And what that does is that shuts down the connection, but prevents it from timing out. And so for days now an increasing number of connections which my little copy of Conficker has sent out have stumbled into tarpits. There's actually two different ranges that I've seen that have grabbed those connections and never let go of them.

So, now, again, the author is so responsive that, if this became commonplace, we know that he'd update the payload. And it's easy to disconnect those connections. All you have to do is look at how long they've been open versus how much data has been transferred. And if that falls below a certain threshold, you abortively disconnect a TCP connection, which can be done easily enough. But that hasn't happened at this point.

So anyway, next week we're going to talk all about Conficker, and I'll basically give a complete technical explanation. Okay, I mean, it's got many different things it's doing. It's probing my local network for any other machines on the LAN by sending out ARP queries, looking for IPs, so we can talk about that. It's very patiently sending out UDP packets scattered all over the Internet, but carefully avoiding a bunch of Class A networks that it knows it shouldn't waste its time on. It's just doing all kinds of things. So it'll be fun to talk about what I've seen and what the whole industry has seen.

Leo: Would you say Conficker is a well-designed worm?

Steve: I have to be very careful to make sure people don't misunderstand my appreciation of it because, yes, I mean, it is beautifully designed. And I don't want, I mean, I want people to understand that I recognize that it...

Leo: You're not applauding the creator, yeah.

Steve: Yes, exactly. It's a bad thing. I mean, it's causing all kinds of concern. And it's obviously very effective at infecting and holding onto machines that it commandeers, which in no way am I condoning this behavior. But I respect its authorship. So, yes.

So here we are, a couple days from the second Tuesday of April, where we had the standard big monthly update - five critical vulnerabilities, two that were important, and one that was moderate, so a total of eight patches from Microsoft on Patch Tuesday. Everyone needs to do this sooner or later. There were a couple bad ones where there were problems found in the HTTPS protocol on the client side, meaning that if you were induced to - you, a Windows user, were induced to going to a malicious secure website, you could have a remote code exploit against your machine based on the certificate, the security certificate that has been exchanged.

So it's an interesting type of exploit we haven't seen before, I mean, in these details. But fundamentally it's the standard math problem buffer overflow, integer overflow type problem. But it's something you definitely want to get your machine patched against because, just as we've seen with Conficker, where back in October this was fixed, a bunch of machines haven't been patched. We've got some interesting Q&A about that also. And speaking of SSL, many people are wondering, I mean, I'm reading in their

feedback, hey, Steve, whatever happened to the SSL protocol podcast that you promised? And my answer is, it's coming. But this is Security Now!, and so I'm giving priority to things that are newsy and happening now, like Conficker, for example, which is happening now. The SSL protocol, well, that's, you know, something I want to talk about, but it's static technology that we will get to, I mean, literally as soon as something doesn't preempt us with something that is now.

Leo: SSL ain't goin' away.

Steve: It's not going anywhere. Also, for anyone using VMware, there was the first major set of security updates in quite a while for VMware Workstation, both for Linux and for Windows, VMware Server and Player, ESX, ESXi, and ACE. So I was on 6.5.0, that is, Workstation for Windows. Anyone using VMware needs to go over to VMware and make sure they're current. If they haven't updated for a while, you're going to want to because there were some interesting exploits. And in fact one is interesting enough that I've got it queued up for a podcast soon because there are some problems with VMware which have been discovered. And they're not fundamental problems with virtual machines. But as always, if mistakes are made in virtual machine implementation, and those are found, they can be leveraged. So I don't regard it as a huge, glaring problem like we have if a Windows user goes to a malicious website because certainly the cross-section of VMware users is much smaller than all Windows users. On the other hand, many people are using VMware specifically for the security encapsulation it provides. And in this case it's not. So you want to make sure you update VMware Workstation.

Also, many people wrote to tell me, if I didn't already know, and I do, something that I wanted to share anyway. And that is that Phorm, the evil, behind-your-back, intercepting your web connections, and loading your machine with cookies in order to track you technology, which was surreptitiously tested by BT over in the UK, it was on its way back. There was some news about Phorm returning. And the European Commission, the EC, has decided, eh, not so fast. We're going to initiate legal proceedings against British Telecom because we feel that their prior tests, which were undisclosed, involving Phorm violated privacy rights, which are well understood and established. Phorm is saying, we did nothing wrong. Both we and BT consulted our legal counsel before executing these tests, and we think we're going to be fine. Anyway, the EC says, eh, we're not so sure, let's put this to the test. So basically the problem was there was non-consent, there were non-consent complaints raised, and the EC is going to look at those and say, well, we agree that there's a problem with consent, which was not clearly given before.

The other interesting change we're seeing, sort of in the security landscape, aside from of course Conficker's happening, is something we've talked about but never really addressed directly. But one of my favorite security columnists, Brian Krebs, who I've referred to frequently here, who writes a security column for the Washington Post, talked about how one of the newest sort of latest changes is this notion of scareware, which is causing people to visit bogus AV sites and install and register bogus AV software. What's happening is that referral fees turn out to generate tens and in some cases hundreds of thousands of dollars per month for anyone who is able to get people to visit and install this basically bogus AV software.

So essentially what's happened is viruses happened. The AV industry then responded. Then awareness was raised so that everyone who's using PCs now is aware of the virus problem, and we've worked on educating people about how to avoid being taken over by viruses. And then almost, in retrospect, almost obviously, what's then happened is fake antivirus tools and warnings and so forth have occurred. So people are now being

confronted with pop-ups, for example, that say this system is acting like it has a virus, please check to see, you know, click this link to have your system scanned. So that will install something which then beats on them to register until they finally do. And affiliation fees are, like, on the order of 50 percent in these cases. So there's a strong incentive for the people who want these affiliate fees to do whatever they can to generate the scareware warning because there's real money in it now. So unfortunately we know that, where there's strong economic motivation, those things tend to happen more than when there isn't. And now we have that for this kind of - sort of this new class of scareware.

Leo: Yeah.

Steve: I also wanted just to comment, I was listening to you and Paul last week talking about, among other things, cellular connectivity. And he was talking about the experience he was having with his EVDO card, which runs on Sprint or Verizon. And I just wanted to chime in that, I mean, I've been an EVDO user, as you know, Leo, for years. And, I mean, it really is a spectacularly functional system. It is completely usable bandwidth, unlike, unfortunately, what you get with the iPhone in most locations, where if you don't have 3G it's just painful. But this little EVDO card, and now it's not even a card, a PCMCIA card, as I have had, but of course they have a little USB dongle that you just plug in...

Leo: Yeah, I use that just because it's easiest to move it from computer to computer, so, yeah, very convenient.

Steve: Yeah, it's just a spectacular solution.

Leo: Oh, I love it. I'm a huge fan. We can actually stream video with it, it's that good.

Steve: No kidding.

Leo: Yeah, when Dane was - when we were covering Roz's arrival in Hawaii, on her trip across the Pacific, I sent Dane with a laptop, an EVDO card, and a camera, and we got streaming video of her arrival via EVDO. It was amazing.

Steve: It's great.

Leo: Yeah, yeah. And it's getting better. They're really upgrading these services as we go.

Steve: Yeah. Well, because it's popular, and it's profitable. I mean, I did also hear you make a - I think it was Paul who mentioned the fact that there are total bandwidth caps on those.

Leo: Yes.

Steve: They say unlimited Internet, but they also say in their terms of service that it's for web browsing and email, not downloading movies.

Leo: Exactly.

Steve: And so they absolutely do, I mean, I've had this long enough, I've never run across any kind of a limitation because I just use it, and I don't have a need to download movies when I'm in laptop mode. But...

Leo: Oh, five gigs goes fast, believe me.

Steve: I know of many people who have run up against the cap and have had their provider say, look, sorry, we're cutting you off. I mean, often the accounts are just canceled. It's like, sorry, you violated our terms of service. That's it.

Leo: I really am - we're judicious. We don't use it except when we need it. Streaming video would use - and by the way, it's up and down, total of five gigs. So streaming video would eat it up pretty quick. So we have to be a little judicious in our use. But it is convenient. I carry it with my little Netbook so that I have always-on access wherever I go. It's really great, yeah.

Steve: Right. And I had a short little interesting SpinRite anecdote to share because it involves the Mac, and SpinRite not being the sole solution. I discovered this when I was going through the Q&A postings for today's episode, from Rabbe Sandelin. His subject was "Interesting Dual Rescue Operation." He said, "I have twin nieces who one day called me. Their old iBook had refused to boot. They were devastated, as many important documents and pictures were on it. I have one of the better Mac recovery tools, and it sort of saw that something was on the disk, but could not recover any of the files.

"So I bought SpinRite, removed the drive from the Mac, and popped it in a PC laptop. SpinRite warned about a drive about to physically die at any minute. Then it went to work and finished two days later with reporting some unrecoverable sectors and quite a few repaired ones. I pulled out the drive and connected it via USB to my own Mac. No luck. It would still not mount. I was getting desperate. So as a last resort I once again fired up my Mac recovery tool." Which he doesn't name. I wish he had.

Leo: Well, there's only a couple of choices. It's either Alsoft's DiskWarrior, probably is that, or Micromat makes a program called TechTool. There are really only the two. We don't have a huge choice.

Steve: So he said, "Once again I fired up my Mac recovery tool, and now it could find all the files on the disk."

Leo: Aha.

Steve: "SpinRite obviously had been able to repair it, although it still had some problems mounting on the Mac. I'm now a very happy SpinRite owner, and I also have two very happy nieces, who also now are aware of the importance of making backups. Thank you very, very much."

Leo: So that's a case where you don't look at the file system. SpinRite looks at the underlying guts of the hard drive...

Steve: Physical sector of the hard drive.

Leo: ...fixed whatever was wrong there. And then the Micromat or the DiskWarrior, whatever tool he was using, which doesn't operate, I mean, they say they do, nothing like...

Steve: Clearly they don't.

Leo: Nothing like SpinRite.

Steve: They didn't do what SpinRite did.

Leo: No. But once SpinRite got those sectors readable, then they could recover the file system and get things back to normal. Yeah, that's not uncommon.

Steve: Exactly. So I thought that was, you know, good to share with our listeners, an interesting hybrid solution.

Leo: A good one-two punch. Same thing happens in Windows, though, where you have file system level tools. You don't do file system. You need a lower level tool to recover it. The file system level tool can then take over.

Steve: Yeah, although with NTFS it seems to be a robust enough structure that we're seeing fewer problems for whatever reason.

Leo: I'm with you. You don't really need those tools. Someday I'd love you to take a look at ZFS, which we've been all excited about here at the TWiT Cottage, and you know we did an interview with Sun about it. It's the Solaris file system. You will not believe this file system. I don't know if you're into file systems at all. But it's incredible. I mean...

Steve: I'm into everything that's got to do with computers.

Leo: I know you are. It's next generation. You'd be very interested. Does things like it has built-in rollback, lot of redundancy. I mean, it's a rock solid - it's basically like a RAID 5 in a file system. It's amazing what you can do with this thing, lot of virtual hardware and so forth.

Hey, before we go to the questions - and we've got some great ones. I see you've put together 12, including a...

Steve: We have our dozen interesting questions and topics and anecdotes and things, yes.

Leo: All sorts of good stuff. Steverino, you ready for your first question, my friend?

Steve: Ready.

Leo: Ready. From Phil in Montreal. Phil in Montreal asks: "Running Windows isn't professional?" Last podcast, about GhostNet, you mentioned at the end of the podcast that running Windows is a bad idea. In fact, you said that they should run other OS or embedded ones that have not been targeted with virus or attacks. Doesn't this same argument go against what you preach? Isn't this security by obscurity? Why do you assume that other operating systems would be better? Who's to say there aren't other security holes? Seems rather bold of you to say that anything else is better than Windows. If all the airport terminals switch from Windows to a embedded Airport OS 2000, who's to say that hackers who love to crash those terminals aren't going to continue? By the way, I don't think it's hackers crashing those.

Steve: No.

Leo: Windows does a perfectly good job all by itself. That was me editorializing. Plus, why do you assume that non-Windows programmers would be better than others? Seems if the programmer creates buggy software on Windows, he or she will do the same on any operating system. I'm not a Visual Basic programmer, and personally I call it Very Bad, not Visual Basic. But your last remark about saying you get what you pay for, oh dear, oh dear, oh dear, Steve. We can't all program in Assembly. Software costs would be five or ten times more expensive and longer to program, compared to people working on Visual Basic or other Rapid Application Development (RAD) tools. And just imagine how much more it would cost when you factor the cost of training on another OS and an API that is not common like Windows.

Windows does have its flaws. But the assumption that anything else is better than Windows seems wrong to me. I've used Linux, BeOS, Mac. And coming from the VIC-20 and the Commodore 64, I can honestly say I've crashed them all. Well, it's pretty hard to crash BeOS, but okay. They are all flawed; and a bad programmer will

always be a bad programmer, no matter what platform he is working on. And many times it has nothing to do with the programmer, it has to do with time, pressure to do things faster than the competition, especially when the competition is international, hint hint. Sorry if this comes out mean or insulting, but I really don't think those comments were correct. Your opinion.

Steve: [Sighing] Well, you know, I'm normally - I normally work to be PC, as they say.

Leo: Yeah. You use a lot of Windows.

Steve: Politically correct.

Leo: Oh, that kind.

Steve: Yes. Windows is a steaming pile of crap.

Leo: Okay.

Steve: It is. Look what we put up with.

Leo: Yeah.

Steve: I mean, it is just unbelievable what the Windows community puts up with. Now, what this author of this post doesn't appreciate is that I wasn't talking about Linux or Be or Mac or any consumer operating system. There's a whole 'nother class of operating systems, RTOSes, Real-Time Operating Systems, and for embedded applications, which are a whole 'nother class of bulletproof and solid. So when I see a marquee system in Vegas with a Blue Screen of Death or a Windows dialogue, I mean, what's funny is there'll be, like, you have to click OK. But there's no mouse. There's no way, I mean, I guess you can climb up on a ladder. No, I'm just kidding, of course, because it's not a touchscreen.

But, I mean, the idea that a kiosk in an airport or a big screen in Vegas has Windows underneath it is appalling to me because that says that these people who created this are so far away from the way that kind of a turnkey system could be built with a low-volume embedded system with a real-time operating system which is fundamentally vastly more robust than this ridiculous second Tuesday of the month cycle that we're in now. I mean, I hear you laughing in the background. But, I mean...

Leo: I'm with you. I'm with you. You sing it, sister.

Steve: We've been bent so far away from what is reasonable. And we've gone kicking and screaming, one insult after another after another. Old-school people, when this

whole auto update started, said oh my goodness, no, I want control of this, I'm going to decide what goes in my computer or not. And now, I mean, and IT got pissed off because they were sending updates all over the place, and they began lumping them up in groups. And, I mean, where we are is ridiculous.

Now, I take my hat off to Microsoft. I salute them for somehow managing to keep this massive Hindenburg called Windows aloft as long as they have. I mean, it is becoming unbelievably cumbersome and burdensome, even for Microsoft to understand their own creation. And it's a consequence of evolution. Again, they're still running programs from the early '80s and carrying all of that technology forward, which is not an easy thing to do. And they're only slowly removing those old features from their newer systems. And we talked about, for example, the eventual loss of 16-bit Windows support. So, I mean, I understand that this is not an easy thing for them to do. But where we are today is just - it's an atrocity. It's just - it's ridiculous.

And then, for example, you mentioned last week, Leo, that the electrical power grid of this country has been taken over, and essentially there's spyware that's been installed, apparently, the news reports say, by China and Russia. I haven't reported much on that here because not much is known, I mean, not much is known publicly. I'm sure that our intelligence community has much better information about that. But again, what you find when you look is that these systems are running Windows. Somebody built some nuclear reactor control system on top of Windows. Which is just like, oh, my goodness. It's inexcusable.

So when I read this posting I just thought, okay, wait, time out. Let's have a little reality check about what it is that we're all dealing with and how ridiculous this is. I mean, this is ridiculous. But it's what we've got. And so that's what we're using.

Leo: Yeah. Okay. I'm trying to - I also want to be politically correct here. So I want to defend Microsoft a little bit. I'm kind of, you know, my visceral reaction is yes, I agree with you. But the issue is that Microsoft needs to be in that position because they're a business operating system, so they have to support the legacy hardware and software that they've accreted over time. I mean, in order to make it a better operating system they need to cut bait and start over, don't you think?

Steve: No, you're absolutely right. For example...

Leo: It's a business problem they have.

Steve: I've continued to study computer instruction set architectures for the last few months. And actually I'm finding myself feeling really interested in the PowerPC, which I think was a really spectacular piece of work. And it's sad that we've seen its arc sort of diminish, as it has over time. But Intel is where they are today because they're still supporting an instruction set that basically still runs 8080 or 8008 instructions and have dragged it all forward. If they were to start from scratch today, they could design a spectacular chip, because they know how, which would be far more powerful and require much less energy, much less heat, much less drive space. It would be much less expensive. They're paying an awful price for their backward compatibility several decades back.

But we use the Intel chip because of the compatibility. I mean, that's the benefit for us.

And just as we do with Windows, for its compatibility, the fact that it runs - anything it ever ran, it still runs today, while Microsoft attempts to bring new technology into it. I mean, we grumble about all this .NET stuff that's having to be loaded now. Well, that's like the next, the next way of talking to Windows, the next API layer, while they're still supporting the old ones. So, I mean, I really do see that, too, Leo. But I just - this note sort of said, wait a minute, let's understand how bad the situation has become. And some of the other notes that we're going to be talking about in our Q&A today highlight additional aspects of this. It's just ridiculous. But...

Leo: So you're saying there's a reason why we're seeing all these security flaws in Windows. It's, at this point, it's a can of spaghetti. It's unfixable.

Steve: Well, you've heard me often defend the programmers, as one myself, recognizing how strangely difficult it is to write code which is absolutely bulletproof. It's just - it's amazing how difficult it is. But this is not an insolvable problem. I mean, we've got such a ridiculous amount of power now in contemporary processors that it would be possible to essentially run a protected emulation layer around everything in order to prevent these kinds of problems. There are things we could do. So I'm just saying.

Leo: I think that's where Microsoft is actually moving. I think Hypervisor in the hardware and the virtualization that Microsoft is promoting, I sense, and I'm not an expert on this, but from talking to Paul Thurrott, is that the future, Microsoft feels that the future of Windows is totally virtualized. And that does solve a lot of these problems, doesn't it, because it isolates stuff. It puts it away out of the core.

Steve: Right. I just, again, I never rant. I don't think I've ever ranted before. But I just - it was sort of a wakeup call for me. It's like, wait a minute, let's just - yes, we're going to move forward. We're going to keep patching on the second Tuesday of the month. We're going to put up with this, I mean, with this huge, bloated OS. And again, I accept what Microsoft has done. But I just wanted to stand back for a minute and just say, hold on a second. This is ridiculous. This is horrific. And what's happened with Conficker and with hospitals being brought down and with identity theft and, I mean, all the things. And in the license agreement that you check it says we're not responsible for any of this. You bear the full responsibility for your use of this. No other industry ever has gotten away with that except the PC software industry. That's just phenomenal.

Leo: And yet, I mean, does NASA use it for launching rockets and things? I mean, it's used in some really pretty mission-critical situations, I think.

Steve: You mean Windows?

Leo: Yeah.

Steve: It's used foolishly because...

Leo: [Laughing]

Steve: Oh, it is, because you've got tools like Visual Basic that allow monkeys to program.

Leo: [Laughing] I love it. Steve's in a fine fettle today.

Steve: Okay.

Leo: Moving along. Next question.

Steve: Okay, I'm going to calm down now.

Leo: You know, right on.

Steve: It's how I really feel. And I...

Leo: It's important to say this.

Steve: I don't normally share it. And I'm not going to make this the rant podcast. But if this was, like, okay...

Leo: Well, I do get a lot of heat from it. I mean, there are people who, oddly enough, there are people who feel about computers and their operating systems the way they do about Mom, apple pie, you know, it's this kind of ownership of it, this very strong ownership of it. And so I think that people who get het up about this and feel hurt about this are people who kind of, you're attacking my operating system. It's just a piece of code, folks.

Steve: Yeah. Well, and I think part of this is that I've been spending a lot of time looking at history and looking back at the fundamentals. And I have remembered that there are alternatives, I mean, not for Mom and Pop, not for you and me. I'm not complaining that I'm on Windows. I mean, this is where everyone is. It's where I need to be. But there are really robust, small, fantastic operating systems that should be used for things like kiosks and shuttle systems. I mean, that's what they use are these really good operating systems which are not anything that consumers touch. But there is a whole different way for computers to work than this disaster of barely functioning and stumbling along and weird things happen and people don't know why they can't print anymore or their Windows Update doesn't update anymore, or one of their two screens just doesn't work anymore, I mean, things are just falling off because it's barely functioning. And...

Leo: We've kind of come to accept that, haven't we. I mean, we kind of have come to assume that's just the way it is.

Steve: Yes, look, that's my point, look what we put up with. We put up with something that is ridiculous.

Leo: You're saying it doesn't have to be that way.

Steve: It's all our fault, Leo. It's our fault for visiting that website. It's our fault for clicking that link.

Leo: Right, right.

Steve: It's our fault for not rebooting often enough.

Leo: You know, I do say this on the radio show. That's the tagline of Call For Help on the radio show. It's not your fault. And I think, you know, we put - there's a huge burden on users to be security experts, to protect themselves. And it's only because the stuff that we're using is so poorly designed.

Steve: Yeah.

Leo: Okay. Question two. Dan Rector in Rochester, Minnesota - no, is that, yeah, it is question two, page eight, but question two - wants a page of Steve's software picks: Steve, first of all, thanks for the work and dedication you do in producing Security Now! each and every week. I've been a listener since show one. Could you create a page, if there isn't one already - if there is, I haven't found it - that has links to or at the very least lists the software you've found over time and have become things you use all the time or are your favorites, tools like Taskbar Shuffle, allSnap, Image for Windows - which we mentioned the other day. I often hear you talk about these programs when listening to the podcast, and it plants a seed. When I have a need for one of these programs or am installing on a new computer, it takes quite a while to search the transcripts to find the reference to the program. I know what he means. I mean, I'd love that, too. I don't know if that's something we should do, or you could do, or...

Steve: Well, I've made - I stuck it on my to-do list. I will get to it when I can. I just wanted to post the question because so many people have asked for that. And I don't want to get into this mode of, like, Steve's Pick of the Week sort of deal.

Leo: Yeah, yeah, yeah. We do that already on Windows Weekly. We have quite a few of them, actually, yeah.

Steve: And my problem is, what you tend to do, then, is to feel like you have to come up with something.

Leo: Right, you force it.

Steve: I want to be driven by the excellence of what I find, rather than the need to find something. So but it absolutely makes sense for me to have a page where I can say, oh, and I've added that to my favorite software page on GRC.com. I don't have that yet, but I'm going to put that together with the stuff that I've talked about so that there will be a place where everyone can go to go through that. And, you know, I'll use it myself when I'm setting up a new system. It'll just be easy to go click click click click click click click and suck all those things down.

Leo: I mean, we have - that's kind of what the wiki is for, and it may be that somebody would like to volunteer and do that on the wiki, as well, wiki.twit.tv. Anybody can edit, create pages, add content. And if you've already been keeping such a list, it would be a simple thing to paste it in and then keep it up to date. You get help from the community, as well.

J.T. Aaron in Houston wonders if Steve isn't way too trusting. Steve, you're way too trusting. He says: You talked on a recent show about installing, trying, liking, and then recommending a brand new Firefox plug-in. How do you know if a new plug-in just released is a security threat? Especially when the new cool app is not from an established company? Great shows, by the way. Good question.

Steve: It is a good question. And I think I agree that I'm probably too trusting. It is certainly the case that I take a look at sort of the motivation, the site where the plug-in came from, try to get some feeling, as soft and fuzzy as that is, it's certainly not scientific. But get some feeling for where this came from and for why, what the user designed it for. Often their sites will say, yeah, I was struggling with this for some time, and I decided just to write my own sort of thing. Now, it's absolutely the case that there could be a security problem with a plug-in. That is, an inadvertent problem as opposed to something malicious. On the other hand, established companies have those just as often as guys working from their bedroom and publishing these. So I don't think there's any reason to believe an established company's plug-ins are going to be in any way more fundamentally secure than something that an individual writes.

And again, it is the case also that things that have very low yield tend not to be targets. I mean, Windows is a much bigger target than the Mac because it's what 90-something percent of the world is using. And as we'll find out later in this podcast, a big chunk of the world isn't using legitimate copies of Windows, and those are even a bigger problem. So it's the case that it seems very unlikely that, were there to be a problem in my hierarchical tab tree organizer, that some malicious software is going to target that because the chance of someone using that is diminishingly small, even among Firefox users, who are still in the minority of all browser users. So I agree with J.T., I think I tend to be too trusting. I also think that the actual target surface is small for these, relative to the whole browser or the whole operating system that have much larger attack surfaces.

Leo: If you were going to do it, how would you go about that? Would you put a network analyzer on it and stuff like that? I mean, how would you test it?

Steve: Well, yeah. You can't. I mean, the presumption is that it's non-malicious intent, that is, that there might be a mistake made. In which case, I mean, who knows where the problem is, what particular set of coincidences of traffic could cause there to be a problem, and what the result would be. I mean, probably what would happen is it would become unstable. It would be crashing; and you'd go, oh, I think I want to remove that from Firefox. So you'd take it out because there was a buffer overflow that was producing a denial of service attack, that is, denying you the service of your browser. And certainly that happens. We know that there are poorly written add-ons which crash your browser. So what do you do? You take them out. So here's a poorly written add-on which works for some subset of people until it crashes them. Well, during that little Window of opportunity, maybe that crash could be turned into an exploit. But before that has a chance to happen you've removed it because you decided, well, this is buggy software. So the bugs which created the opportunity for an exploit you've removed because you say, okay, this thing's not ready for primetime yet.

Leo: All right. Moving on. Taylor Schreck - no relation - in Rochester, Minnesota - I made a little joke, a little funny there - in Rochester, Minnesota shares some thoughts on Conficker: Hi, Steve. I'm a few episodes behind, so I

apologize if you've already discovered this. In the episodes I've listened to recently you've commented on how amazing it is that it's taking so long for computers to be updated with critical security patches. I agree with your assessment that the corporate review of Microsoft patches may be partially responsible. However, I read a blog post this morning that brought up another probable factor. Many people cannot install updates.

Here's the relevant excerpt, quote, "Relatively few of the infected computers, about 4 percent, are in the U.S., according to a report issued by SRI International in March. About half the Conficker infections were Chinese computers, at more than 10 times the rate of U.S. infections. That makes sense, Wisniewski said, because there are now more web-connected computers in China than anywhere else. There's also a high incidence of pirated copies of software in China, meaning users there cannot keep their machines up to date with security patches." I just wanted to provide that as food for thought. Thanks to you and Leo for the work you do on Security Now. It's been a great way for me to learn and stay current. That's a good point. If you don't, well, is that true? If you don't have a legitimate copy, you can't update?

Steve: Yes. And I remember when that change was made. And I thought, oh...

Leo: That's a mistake.

Steve: ...goodness. You are forced now to install the Genuine Update or Windows Genuine Verifier or whatever they call it. And it's like - or Genuine Advantage, that's it. And I love it, too, because when you agree to this, it brings up a dialogue, and it says, when you're done, we'd like to show you some of the many benefits of Genuine Advantage. And it's like, uh, no, thank you.

Leo: Many benefits to us.

Steve: Exactly.

Leo: To Microsoft. Yeah.

Steve: So I remember thinking, oh, goodness, now we're not going to get the updates on all versions of Windows. You've got to pass the Genuine Advantage, which I've heard derisively referred to as Genuine Disadvantage.

Leo: Right.

Steve: But it is the case that those machines which are running Windows but not able to be updated for this reason, they didn't get the fix in October. They didn't get fixed until Conficker infected them and then closed the backdoor behind it.

Leo: Yeah, yeah. And there's also a lot of - I'm surprised, 4 percent seems like such a low number. I am actually shocked that it's so low in the U.S. I guess we're doing our job, we're getting the word out. But I think there's also a lot of people in the U.S. who choose not to update. And there are a lot of people in the U.S. who can't update because their updates are blocked. I get this call a lot. People had a bad update, and they haven't been able to update ever since. A failed update will block future updates; right?

Steve: We've got that in a coming question.

Leo: Oh, you're way ahead of me. Well, then, let's move along. Nick Antonizick in Las Vegas, Nevada wonders about "Mitigating the Buffer Overflow Threat." Dear Steve and Leo: First, thank you both to the tenth power for the Security Now podcast. It has become my favorite source of information and entertainment. Because of you both, I am always looking forward to Thursday nights every week. That's when the show comes out. I have a question regarding buffer overflows: I operate my computers from limited user accounts. I also force high-risk applications to operate under Sandboxie. And he includes Firefox, Foxit - the PDF viewer we talked about - image viewers, and office applications in that list. So if an application is victim to a successful buffer overflow attack, and the application is contained inside a sandbox in a limited account, is the injected hostile code constrained or confined in any way?

As I examine the process stack, even from a limited account, over half of the processes running the system are system processes. I'm guessing, if the hostile code is injected into a system-owned portion of the stack, that any precautions I take will not provide any protection or containment at all. Likewise, if the hostile code lands in a limited portion of the stack, it will not have much authority to modify the system. Am I correct? And when faced with the practicalities of implementing or suffering a

buffer overflow attack, is hostile code more likely or less likely to be injected into a system-owned area of the process stack? Thanks again for a great show. As always, I'm looking forward to hearing Thursday's episode.

So what he's saying is, I take the precautions that you guys have recommended, particularly the limited user and running Sandboxie. But there are still escalated code running on my machine. What happens if that's where the malware strikes?

Steve: Right. I think what Nick doesn't understand, and I just sort of wanted to make sure that our listeners understand, is that even though a sandboxed program can see both system processes and its own limited account processes - and he's certainly right about that. If you use a process viewer from within the sandbox you can see those. What the sandbox is doing is preventing modification to the system. So what the sandbox can't tell, can't see, is that when a process in the sandbox makes a modification to a file, it's actually sort of it's caching the modification so that the actual file is not modified, but what happens is a copy of the file is brought into sort of a holding area, and that copy is modified. Then if this application checks to see if its modification was successful, it's actually checking - it's sort of redirected, and it's checking that modified version, not the real one. So something malicious can think, ha ha ha, you know, I've got the guy now, and be making changes to the registry, to files on the hard drive, I mean, to in-RAM processes, to anything, and it thinks it's succeeding.

Well, this is actually all a charade that the sandbox creates that prevents things in the sandbox from making permanent changes. They make them only locally to their own copies. And so when that thing terminates, when you reboot your system, when you shut down the sandbox, those changes are flushed, and no permanent changes have been made. So it really doesn't matter whether something thinks it's trying to modify system processes or perform process injections or do anything it's doing. It's all been carefully orchestrated so that those changes are simulated for the sandboxed environment, and nothing actually has changed. There's no rights of any kind that escape that out into the system externally.

Leo: Good. So you are safe. What about if you do a process viewer, you'll see there are system processes running, if you're not running Sandboxie, there are system processes running. Is it the same for them? Are they not accessible by malware? Can malware not leak into them?

Steve: Correct. I mean, and that's exactly the question he was asking was...

Leo: Even without Sandboxie.

Steve: Yes, does it really - oh. Without Sandboxie, no. I mean, the problem is there are all kinds of ways, for example, of performing a privilege elevation attack where, even though you're in a limited account, you jump to some piece of code in the kernel that has the side effect of elevating your permission. Then you come back. Now you have full admin permissions. And then the changes you make that would normally not be permitted by that account are permitted.

Leo: Right, right. So that's why these exploits are an issue, because even if you're running as a limited user you can get in trouble.

Steve: Yes. I mean, you're not supposed to be. But there are privilege escalation exploits which get around the whole limited user...

Leo: To make it clear, those require that there be a hole in the operating system.

Steve: Yes.

Leo: There is malware that doesn't require that, that you run an application that does stuff.

Steve: Correct.

Leo: If you run that as a limited user, generally it won't be able to elevate its privileges, and you're safer. But if there's a hole in the operating system, all bets are off. Doesn't matter what you're running as.

Steve: Well, yes. Or if you're a victim of a social engineering attack, where something says, "Hi. We're Happy AV. We need you to authenticate your admin account so that we can install our system drivers." Well, you've just given some bad thing complete access to your system.

Leo: Right. And we should also mention, we've said this several times, but just so people know, in Vista and OS X nowadays you don't have to run as a limited user because even when you're an admin you're really not an admin. You're always a limited user, and you have to escalate using User Account Control or OS X's equivalent before you're able to do anything anyway as an administrator.

Steve: Right.

Leo: You have to give it an administrator password. Moving along to the next question. This comes from Robert Harder in Monterey, California. Robert asks: Why do all CDs, or why do some CDs stall the whole system? Thanks for the great tidbits we learn about the down-and-dirty on hard drives when we listen to Security Now!. I have all the episodes way back to #1 in iTunes. But what I really want to know is why optical drives have the power to bring a computer to its knees? On both Macs and Windows, and for many years, computers seem to really choke and stall when CDs or DVDs are inserted or have bad parts or whatever. What's wrong? How come something like a bad disk can bring the whole machine to a crashing halt?

Steve: I saw this, and I just chuckled to myself because this is one of the continuing

annoyances I have with Windows. I hadn't experienced it as much with the Mac. And I was going to ask you, Leo. Is it the case with the Mac as much as it is with Windows?

Leo: I'm trying to remember.

Steve: Because with Windows, I mean, if you do anything involving a CD drive, it literally - your UI locks up. It's just everything waits.

Leo: And that's because these are not asynchronous, I mean, synchronous reads; right? They're asynchronous in the operating system or...

Steve: It's because the system is as I described it in question number one. It is ridiculous.

Leo: Well, remember Windows did not have CD-ROM support. It was added after the fact.

Steve: And that's the reason. It's the heritage. It's the fact that we - okay. We know Windows has never been comfortable with the idea of removable file systems.

Leo: Right.

Steve: It didn't have them in the beginning, and it has never really had them done right. It's ridiculous that having the CD in sort of an unknown state - and CDs take a long time, and an increasingly long time also in the case of DVDs - to sort of get themselves up to speed and "seeked" and logged in and all happy. Meanwhile, nothing else, I mean, literally the whole system comes to a halt while you wait for the CD to decide if it's good or bad or what condition it's in. And it's purely a function, there's nothing, nothing from a technology standpoint that enforces this, except just the legacy of design which has been dragged kicking and screaming forward to where we are today, and this annoyance, which just, who knows if it's ever going to go away.

Leo: These are called blocking applications. It is possible on the Mac to have that happen. I mean, the beach ball - they call it the Beach Ball of Death sometimes, where the little waiting, lurking, spinning thing...

Steve: The little spinning color wheel...

Leo: ...just starts and will not stop. So I don't think OS X is immune to this, either. But a good operating system should handle this kind of stuff. What, do they get in endless loops or something, or they're waiting for a read, or they're just hung up until the read completes, or...

Steve: I mean, it's definitely the case that it's easy to take proper operation for granted. Operating systems are super complex. There's a phenomenal amount of synchronization and interlock going on. And the problem is that the designers from a decade ago didn't anticipate some things that we have today. And so the result is a kludge. It's no one's fault except the fault of evolution. I mean, that's - our own DNA has all kinds of gunk in it that we no longer need. And that's just a function of history. So Windows is the same way. It's evolved over time. And there are things that just - that were not a big problem, that have become a larger problem as we move forward, that sort of never get fixed. And this is one of those. Just sort of it's something that annoys me all the time about Windows. So when I saw this, I said, yes, Robert. Boy, do I agree with you. This is just ridiculous. And there's no good reason for it except heritage, except legacy.

Leo: I'm going to jump back a little bit just because, I don't know if you noticed, I missed question five, Casey Clingan.

Steve: Yes, I noticed.

Leo: In Hattiesburg, Mississippi. He says that people never cease to amuse: Hey, Mr. Gibson, let me start by saying that I really enjoy your weekly podcast, Security Now!, with Leo Laporte. It's always very informative. Lately you've been discussing the newest version of the worm known as Conficker and the importance of always staying up to date with the latest Windows updates in order to make your PC as secure as possible, though we all know that Windows PCs are never really totally secure.

Well, as I've been listening I've noticed that a great deal of the time those who get infected or hacked by worms and viruses like Conficker are those who do just the opposite of what I just said. Now, to be honest, in the back of my mind I have been saying to myself, come on, who is really dumb enough to deny Windows Updates? I mean, for me, every time that little balloon in the task bar appears I get excited, like I've got a gift. All right, so I'm easily amused.

Well, as the title of this post says, people never cease to amaze me. I noticed the other day as I was using one of the computer labs on my college campus that auto updates were turned off. Needless to say, the first thing that came through my little mind was, what idiots. So as any responsible geek would do, I proceeded to correct the issue. I came to find out that the machine I was using hadn't even updated to Service Pack 3. Yes. It didn't even have Service Pack 3. I was totally at a loss for words. Needless to say, I then immediately proceeded to Microsoft's website, downloaded and installed all available updates. This leads me to wonder how many other computers on this campus are in the same predicament? Anyways, all this to say you were indeed correct about the fact that many Windows machines are running unsecure and on outdated software. Thanks again for your helpful info, and please continue to keep us updated on everything security.

That's a case, I think a common case, of neglect. Machines that are on big networks that nobody's responsible for just get neglected.

Steve: Yeah, and computers in a lab would be a good case. You can imagine, I mean, we don't know specifically and when auto updates were turned off and why. We know that Microsoft has them on by default, prompts you, bugs you until you turn them off. And it's

difficult to have them off. But something somewhere deliberately said I want auto updates off on this machine. Maybe they were in the middle of something, they didn't want to be forced to reboot. I mean, we just don't know. But it certainly is the case that in this instance there was this important system, which is arguably very important, was disabled.

Now, you might say, oh, well, certainly they're on a big private network behind a big university routing system. They probably don't have public IPs. Incoming traffic is probably heavily filtered and blocked. That may be so. But one of the things that Conficker is now doing is sending out ARP probes across the entire subnet where it's located. So even if that machine was protected, if there was any other instance, for example, of a machine being outside the network, getting infected, which is then brought into campus, that machine can infect across the entire sub-network through this next-generation LAN technology that Conficker has that we'll be talking about in detail next week. So it really is the case with state-of-the-art malware that things can get you even when you believe it's safe to depend upon further exterior resources, like the fact that you're behind a router, and all the machines in your own network can be trusted. If one stops being trustworthy, then the rest of your network can go down.

Leo: Moving to Jesse in Madison, Wisconsin, who says, "I know why Windows machines don't get patched": Steve, I'm sure that you have been reading the stories about how many Windows computers aren't yet patched for Conficker. I think you know why computers aren't patched, even though the default Windows settings might even be set to automatically install. I think "I" know why, he says. I was helping my mom with her laptop, which is running Windows Vista Home Edition. I noticed that Windows Update hadn't installed any patches since [fanfare] November. I confirmed her settings. It was indeed set to automatically download and install updates. So I ran Windows Update manually. It failed. I didn't write down any error messages, but the gist of it was it couldn't find or download any updates. This is bad. I Googled for hours to see if anyone had seen this problem and if there were any solutions that worked. I found hundreds of forum postings with people having this problem. No one had a surefire solution that worked for me or other commenters on the forums.

I tried many things to fix the problem. I won't bore you with the details. But be assured, as a Linux user I am not afraid to get into the guts of the system. I even ran SpinRite. There's a little happy face there. In the end, the only solution, reinstall Windows. Luckily, my mom only used the computer for browsing the Internet and checking her email, so the reinstallation was relatively painless. However, if I hadn't been around to help her, I'm sure she would have never even, not only not fixed the problem, she may have not known. Her computer would have just been another drone in a botnet army. Or worse, her identity might have been stolen. Most people are no more computer literate than my mom. So if Windows is failing to update itself for a significant portion of the population, this could explain why so many Windows computers are not being patched properly. Thanks for the show. Wow.

Steve: And that's similar to what you said you deal with on the radio show all the time, Leo.

Leo: Yup. Yup.

Steve: I've seen, I've had it happen to me. I've had systems where one particular security patch won't take. I'll try it over and over and over. It just says no, sorry, can't install that. And here again I salute Microsoft for doing something as difficult as this is. I mean, this is not an easy thing to do when you think about how complex Windows has become, how many individual components it has, how they're all interlocked and interlocking, I mean, dealing with managing the problem of keeping it up to date, it's just a phenomenal job. And the whole sort of almost-on-the-fly updating where you're bringing in new code, you're somehow arranging that next time you boot the new code will be running, and it will replace the old code. You also need to guarantee that you can roll back these changes if they hurt you so that there's undoes on all of this. I mean, this is a huge problem. But it's also a problem of their creation.

So it's the case that Windows Update is complex and delicate and fragile. And unfortunately it breaks. At the same time, we now depend upon it more every day because of these evolving threats from malware and worms like Conficker. We have to have it working. So when it breaks it's not optional to have it working or not. It's like, oh my god, this guy reinstalled Windows is the only thing he could do after spending a great deal of time struggling to keep the current installation. He had no choice.

Leo: Yeah, I'm going to have to start telling my listeners on the radio show, check to see if you're getting updates. Because the class of calls I get is I have an update that won't finish. So every time I reboot, I start my machine up, it says, okay, we've got to do this update, and it never does finish. It happens all the time, you get an update that is incomplete. Something went wrong. And Microsoft has a fairly lengthy page in its knowledge base on what to do if Windows Updates breaks. And there is no one fix. There are a lot of different things to try. You clean out - there's a folder, temporary folder where updates are stored. You clean that out. You might have to clean the registry by hand. It's a mess. Who would have ever thought that we would be in a position where we would need to update this operating system, or any operating system, so often?

Steve: Yes. Yes. That's exactly the problem. It's like, okay, throw some cold water on us and wake us up. It's like, wait a minute, look at the degree to which we're just putting up with nonsense.

Leo: I can imagine that this is costing Microsoft a huge amount of resources to keep up with that they never anticipated.

Steve: Well, and any surprise that they were so reluctant to get themselves involved in security? It's expensive. It's difficult. I mean, it is a whole 'nother class of hard.

Leo: Jonathan Issler, Mount Airy, Maryland. Is that the same Mount Airy? No, I don't think it is, that Andy Griffith was from Mount Airy? It was in - wasn't in Maryland. I have a mug from there. Anyway, he wonders about the blocking of HTTPS traffic, secure HTTP: Steve, I recently had an issue providing support for a school because their IT director had blocked all HTTPS traffic on their network. Okay. I'd like to hear the rationale for that. In particular, this user was unable to go to GoToMeeting because the site automatically redirects users to HTTPS, as many security-conscious sites do. The IT director said allowing HTTPS access for certain sites is difficult, and

asked us to find a different way to provide the support. I cannot possibly understand why an IT director would be blocking all HTTPS traffic on a network that people need to do work on. What are your thoughts? I love Security Now! most of all of the TWiT podcasts. They definitely keep me sane during a three-hour daily commute. Wow. Thanks, Leo and Steve. Wow.

Steve: Well, he said this was a school. And the short answer is the IT director can't easily monitor and filter HTTPS because it's encrypted and secure.

Leo: Right.

Steve: So his answer is disallow it. Force all connections to be standard HTTP, which much less technology can be brought to bear on for filtering and monitoring actions of users within the school. So we know that it's absolutely possible to filter HTTPS, but it requires much more expensive systems, and it requires proxying connections and putting custom root certificates on all the web browsers that are going to do it. We've talked about how this is done in enterprises often. In this case the school IT just said, well, we're not going to go through all that. We're just simply going to deny HTTPS because we can't see what's inside, and our policy apparently is we want to be able to see everything that's crossing our network. I'd be surprised if it weren't just that simple.

Leo: Wow. Yeah, I think you're exactly - that's probably exactly right. But you can't use Gmail, I mean, there's a lot of legitimate stuff you'd want to use. Is there a...

Steve: You can't even log in to Gmail because it forces you to do a secure, if only briefly, to do a secure connection to log in. So you're right, I mean, it really does limit you. On the other hand, the school policy might be, sorry, you can't do anything that requires that kind of security.

Leo: Right. We don't want you doing that anyway.

Steve: Right.

Leo: Would there be a way that they could allow GoToMeeting only to have HTTPS? Is there some...

Steve: Yeah, certainly. Given that GoToMeeting servers are on relatively fixed IPs, they could certainly make an exception...

Leo: Just allow that IP, okay.

Steve: ...in their blanket block, in their blanket traffic filter for that range of IPs, yes.

Leo: Number ten, Zurahn in Ontario, Canada wonders about Conficker. Who isn't? We're all wondering about Conficker. This is going to be a good episode next week when you cover this in great detail.

Steve: Yeah.

Leo: He says: Recently, considering the fervor surrounding Conficker, I thought of something that seems too obvious to work, but I'm not sure where the issue is. If I understand correctly - this is a whole category of questions we get. "What did I miss?" we call this. If I understand correctly, the Conficker worm generates a list of domain names which it checks for updates, the most recent one the April Fools update, 50,000 domains a day, and some Internet service providers have been pre-registering domains to prevent the updates. Legality and ethics aside, would it be possible to go a step further and not only register the domain, but use it to create a rogue update for Conficker that tells it to destroy itself? Whether or not this is possible, I'd really like to hear why. Could you do that? I mean, it is illegal.

Steve: Legality and ethics aside, yes. The first, I mean, I'm glad he said that because you're right, we've discussed many times the idea of white hats going in and leveraging the worm against - or the virus or the trojan or whatever against itself and using it for "good," unquote, as opposed to evil. And remember we had the one story about the BBC who - I think it was the BBC that used a botnet and demonstrated that it worked, sent spam, did a denial of service attack against a willing ISP, and then modified all of the bots' screensaver to inform their owners that their system was infected and please go here to find a cure. I mean, that was a controversial thing to do, and arguably everything that the BBC did was against the law.

Was it unethical? I don't think probably. And probably maybe not even illegal, depending upon what country you're in and who wants to form a complaint. But, and I referred to this earlier in the show, one of the things that Conficker does is very clever. And that is, it specifically blocks this kind of effort, not only being taken over by good guys, but by other bad guys who would like to commandeer the Conficker worm army that's been built. And that is, I mean, exactly as Zurahn says, you've got 50,000 domains. The worm's going to check every day for a small subset of those. So you could potentially set up your own server at some of those domains, and Conficker would, statistically, some Confickers would contact that domain. In which case you've got a connection to it. Why not do something?

Well, the reason is that the authors are on the top of their game. They have a requirement that any packages coming into Conficker contain a valid digital signature, signed by them. And because this is public key technology in a digital signature, even reverse-engineering Conficker, all we could get - and we have determined all we can get, we'll be talking about this next week - is the public key. There's no way, and this is how public key technology works, asymmetric cryptography, there's no way even from having the public key for us to know what the private key is. The author of Conficker, or authors, have the private key. So anything that they want their worm to update, they package up, and they sign with their private key, and they stick it out on the Internet on these prearranged servers for it to be discovered by the worm. The worm discovers it, downloads it, and then uses its public key contained in its own code to verify the signature before it allows it into the system.

So, I mean, it's the same way, frankly, Windows Updates work. Windows Updates are signed by Microsoft's private Windows Update key. That prevents Windows from being spoofed and us accepting any malicious Windows Update packages. Conficker does exactly the same thing. So, I mean, it's using state-of-the-art cryptography to protect itself.

Leo: Wow, that's kind of amazing, yeah.

Steve: Yeah.

Leo: So you couldn't do this. Conficker would say no, you're not allowed, sorry.

Steve: It'll say sorry, that doesn't look like it came from us.

Leo: Wow. We're going to take a break and come back with Gerco Dries in The Netherlands. He's worried about information leakage using VPNs.

Steve: Great question.

Leo: And Brad has a cookie management scheme he'd like to - another one of those questions, you know, what am I missing? Gerco Dries in The Netherlands is being bothered by information leakage when using VPN software. He says: Hi, Steve and Leo. I first wrote to you about this a month ago or two, but you either decided not to discuss it on the show, or you might have missed it in the daily torrent of feedback. I decided to mention it again just in case you missed it. I think it's an important question. When using any kind of VPN - Virtual Private Network - software, any kind known to me, anyway, on a laptop, I find that some information always leaks to the network you're connected to. When waking up or booting a computer running any operating system out there, usually programs like an email client or Skype or Gmail notifier or whatever start up and immediately try to connect to their respective services. This is before the VPN has been established. And at that point you're leaking information about who I am, my email provider, for instance, what programs I use. This could enable an attacker on the network to figure out what attacks to use against my machine. Do you have any ideas on how to counter this type of information leakage? Isn't it just a problem of what starts when?

Steve: Well, it's such a great question. And I immediately put it into the feature list for CryptoLink.

Leo: Oh, good.

Steve: CryptoLink will have essentially a hooking intercepting driver which installs at boot time. And so, I mean, this is just a perfect example of why I'm excited about doing my own and why I'll be enjoying having a protracted development period which is interactive like this, so that people who say, hey, here's what I need, hey, what about

this, and what about that, I will be able to incorporate that wish list into the product. And so, I mean, it's there now. It's going to have it, this notion of - and you'll be able to configure it so that, until you establish the link, no traffic flows out of the interface other than what's minimally necessary, which is basically just establishing the interface's IP address. But no protocol traffic. So that's a great question. I don't know of any other VPN that addresses it. But it's one more reason why I've decided I'm going to write my own for everybody.

Leo: So it is really an issue of kind of saying don't start until I'm started.

Steve: Well, yeah. The idea is that, if you installed a shim down in the network layers, down in the so-called NDIS layer, CryptoLink's driver will install itself between the NIC and the rest of Windows, the whole driver stack. And it's easy enough for it to simply block, just like a personal firewall would, to block any and all traffic that is not running through the VPN. So you'd be able to go somewhere, boot the machine, confident in knowing that none of the other junk like Windows Update, for example, that wants to get on the network and see what's going on, can establish, can leak any traffic at all, if that's the way you've configured CryptoLink. It'll only be running through - traffic is only allowed running through the VPN, even before CryptoLink starts, since that driver will be down there preemptively blocking any traffic.

Leo: Perry's saying in our IRC chatroom that Windows does allow you to start a VPN before you log in, which would presumably be soon enough to prevent that kind of thing.

Steve: I wouldn't know without, well, before you log in...

Leo: Like on boot-up?

Steve: I don't know what services would be running. Certainly Windows Update does not require you to log in. So system-level services that aren't log-in required would still be, could still be a problem.

Leo: Interesting. Well, I'm glad you're addressing that. That's great.

Steve: I'm going to. It was a great question. It's like, oh, yeah, there's a great additional feature, yes.

Leo: Well, the best software is really developed in that kind of collaborational environment. I mean, that's one of the things that's really changed nowadays because of the Internet, because of Web 2.0, is you can have this iterative software design situation where people are giving you feedback as you work, and it's great.

Steve: Well, I've been doing a lot of that, thanks to the newsgroups that I run at GRC.com. This DNS benchmark owes many of its features to ideas that people have had.

I mean, there is a tradeoff because it tends to be - I have to guard against people saying, oh, but what about this; and what about that; and, hey, I'd like to have this and so forth. I mean, you can end up running around in circles. And so I have to control myself not to endlessly be adding features.

One of the things that I'm going to do with CryptoLink is do the UI last, that is, deliberately have a temporary interim user interface so that I don't invest in UI design until all the features are there that I want to have there. Because what I've noticed over time is one of the most expensive things to do is for someone to say, oh, here's a great - how about this idea? And I'm thinking, oh, that's fantastic, but I don't have anywhere to put the button. So, I mean, an amazing amount of time gets spent in, like, reengineering, rejiggering the UI in order to accommodate great ideas. So I've decided I'm going to deliberately forestall the UI side. There will be a UI, but it'll just be just enough to exercise the product and have it all working. And my intention is to have, to very quickly get something going, and then have a timeline of other features, and just add feature after feature after feature until it's feature complete. At that point we'll let everyone play with it, see if there's anything I've forgotten. And when it looks like it's stable, I'll put the UI on it, and we're done.

Leo: Cool. Very cool. Last question. This comes to us from Brad Beyenhof, San Diego, California. He's got a cookie management scheme he'd like to run by you: Steve, you mentioned in Episode 190 about the two extremes of cookie management - the one, "let every cookie in" crowd; versus the two, "scrupulously inspect everything" crowd. I used to be in that second group, but I think my current system nicely fits between the two. It's very no-fuss but still very restrictive.

In Firefox, I have the browser set to accept all cookies, even third-party cookies [gasp]. However, it is also set up to remove cookies every time the browser is closed. To allow for persistent logins on the sites I use most, I have added my most-used domains to an "Allow" whitelist in the Cookie Exceptions dialog. So what this means is all cookies are accepted during a session. No sites get broken for a refusal to accept cookies. But all cookies from domains I haven't specifically whitelisted get thrown out when Firefox closes, so there's no persistent tracking by unknown sites. I think this sounds like a good system.

Steve: It does.

Leo: What makes this whitelist so easy to administer is an extension called Permit Cookies. It puts an icon in the status bar. You just click the icon to change the default cookie exception rule for the site you're currently visiting. Oddly, the copy on the Mozilla add-ons site won't install because its maxVersion doesn't extend to the current Firefox, but you can get it from the author's website with no problems. Apparently it works. What do you think? That seems like a good idea.

Steve: It's a really nice idea. I'm aware of people who use the "keep cookies until I terminate my browser" option. It is right there in the user interface. There's Allow First-Party Cookies, Allow Third-Party Cookies, and then underneath that is a dropdown box where you're able to choose the option Allow Until the Browser Is Terminated, some logic or some statement to that effect. And so what it does is it allows, it holds the cookies in memory, never writes them to disk, so your system is fully functional until you terminate. In which case it flushes all of those cookies out.

I did pursue the Permit Cookies add-on because I've become [clearing throat] admittedly something of a Firefox add-on junkie. And it's exactly as Brad said. If you put "permit cookies" into the Find Add-ons dialogue built into Firefox, it'll say that nothing is there. But there's a link that says, like, find all versions or something to that effect. If you click that, it will take you to the page. And if you click the author's name, it takes you to the author's page, which is sort of a different name, it's like Gloria's something or other [Gorgias' Firefox Extensions]. And he's done a bunch of different kind of add-ons. Down toward the bottom is Permit Cookies.

That one - and he acknowledges the fact that there's a version problem, that his latest one on his site installs. Permit Cookies is a very small add-on. It puts a little "C" down in your toolbar. And what I like about it is, if you visit a site which you have whitelisted, or in this case greenlisted, the little "C" turns green. So if I go to Amazon.com, it's green. It knows that I have got Amazon.com in my whitelist saying I'm going to allow persistent cookies of whatever kind. And the same thing for eBay or for other sites you visit. When you go to a non-allowed site, the little "C" is just gray or white, not green. And then you're able to click on it, and it pops up a dialogue if you want to change that site's permission to allow persistent cookies.

So it's another - I would recommend this for people who like the idea of having that kind of control. Allow all cookies, first- and third-party cookies. Flush them when you leave Firefox so they don't persist across startup sessions of Firefox, which means you're not going to be tracked more than across your current session, and then whitelist the sites where you want to keep cookies permanently. That's another nice solution.

Leo: And of course somebody is pointing out in our chatroom Flash cookies, but that's another topic for another day.

Steve: Ah, yes. Yup.

Leo: Because we are out of questions and out of time, Mr. Gibson. Always a great pleasure. Next week, Conficker, the ins and outs of the most famous worm of our time.

Steve: I think it probably is. I mean, we had Code Red, and we had Blaster back in those days. This one has really had the industry chasing its tail. And it's becoming, it has turned out to be extremely difficult to deal with. And one of the interesting things is that the authors are tracking the anti-Conficker work closely.

Leo: Wow.

Steve: That is, everything that is done to try to thwart it, they respond - he or they; he, she, or they, the authors - respond to directly. So they are - it's not something that they just sort of put out into the world and forgot about. This is a project that they have been pursuing for six or seven months, and all leveraged from one particular Windows exploit. The problem is, this is not the last exploit we've seen. We're seeing them all the time. This is a worm because it allows, if a Windows machine is not behind a NAT router so that its ports are directly exposed to the Internet, it allows other instances of the worm

to infect unpatched machines. And that's how these machines have become infected. That's what I'm going to do next, by the way. I deliberately manually infected my test machine that I've been watching it on for a while because it is behind a NAT router. The next thing that I'm going to do is to set up a clean, virgin build of XP and put it out on the 'Net and see how long it takes for it to get taken over automatically.

Leo: Minus the patch that Microsoft put out in November or October, whatever it was.

Steve: Precisely.

Leo: Yeah. That'll be - I can't wait to hear more about this.

Steve: Next week.

Leo: We will dissect it all. Now, if you want to know more about what we just talked about, you can find a transcript, 16KB versions of all the shows, show notes, and more at Steve's site, GRC.com. That stands for Gibson Research Corporation. That's where you'll also find SpinRite, that great program we always talk about, the hard drive maintenance utility that is just - there's nothing better. Just the king of the hill, has been for years. And of course a lot of free stuff that Steve gives away, useful tools like Shoot The Messenger, ShieldsUP!, DCOMbobulator, Unplug n' Pray, Wizmo. It's all at GRC.com.

We also have show notes at wiki.twit.tv. They're created by the listeners, which is always handy, usually with lots of links in there. We have a FriendFeed room now called TWiT Conversations, if you're on FriendFeed it's TWiT-conversations, that people partake in during the live taping, and you can comment after the fact, as well. And of course the live show is every Wednesday afternoon at 2:00 p.m. Eastern, that's 11:00 a.m. Pacific or 18:00 UTC at live.twit.tv or twit.am, if you just want to listen to the audio. And that way you can listen, comment in our chatrooms. We have many of them on Stickam, on Ustream, on IRC, and on FriendFeed now so that you can comment. And we monitor them all and try to feed the comments back into the show. So we always appreciate it when you do that. If you aren't listening to the show every week, you might want to subscribe. In iTunes you can get it automatically by going to the iTunes store and searching for TWiT. You'll find all the TWiT shows there, including this one, Security Now!. They're free. You get them automatically the minute they ship. Security Now! comes out next. Thank you, Steve.

Steve: Thanks, Leo. Always a pleasure. Talk to you next week.

Leo: Next week we Confick together on Security Now!.