Windows Autorun-around

Description: Steve and Leo discuss the inglorious past of Windows Autorun. They explain how, until recently, disabling "Autorun" never really worked, how Microsoft hoped to fix it while bringing minimal attention to the problem, and how Microsoft's documentation of their recent fix still "got it wrong."

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-187.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-187-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 187 for March 12, 2009: Fixing Autorun. 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 talks about security, now.

Steve Gibson: Yay!

Leo: Yeah. And here he is, the star of the show, from GRC.com, the Gibson Research Corporation, the creator of SpinRite, the discoverer of spyware, and man about town...

Steve: Doo-to-doo.

Leo: ...devoted cabernet drinker, Mr. Steve Gibson.

Steve: Yes, we've got a whole ton of really interesting security news. And we're going to talk about Windows AutoRun and AutoPlay this week. Remember I mentioned it a couple weeks ago. Actually it was part of - this came up because of the February updates that

Windows did where they fixed the fact that it was broken. And it turns out that they still haven't got it right. Apparently the technology is working, but they forgot to mention something really critical in every page that I have found on their site that talks about how to configure it properly. They still don't explain that correctly. So today we're going to. And it's important because...

Leo: Now, I know - yeah, okay, I was just going to ask because we're spending a whole show on AutoRun.

Steve: Yup.

Leo: Why?

Steve: Well, it's probably one of the first things that a security-aware person does when they want to bolt down a computer. And what's interesting is the actual back story behind why Microsoft fixed it. Because there was a patch for it which was only available in Vista and Server 2008. You had to manually install it. There was an update, but you had to go manually get it from Microsoft's site, so nobody did. Well, believe it or not, the Downadup/Conficker worm...

Leo: Oh, no.

Steve: Yes, started exploiting Autorun in order to spread itself. And so even users who had turned it all off were still getting infected due to this bug that Microsoft knew about, but didn't figure was important enough to push out. And one of the reasons is they were literally afraid that, if they updated everybody and fixed the fact that it was broken, that people would be more upset that things that used to work no longer did, even though it's what they said they wanted. So go figure. Anyway, so we've got a great show today.

Leo: It sounds very interesting. Sometimes we get very granular on this show. And I think this is one of those granular ones.

Steve: Well, yes. We're going to be down in bits because, in order to specify the configuration, you need to understand the way hex bits are merged together to create a composite value. Microsoft did not make this easy. So anyway, we've got a whole bunch of stuff to talk about.

Leo: You said a mouthful. Microsoft did not make this easy.

Steve: Yeah.

Leo: Well, we'll talk about it in a second. We'll also get updates on the security news. There is some, and...

Steve: Tons of that.

Leo: Tons of it.

Steve: Tons, baby.

Leo: So I came in today, and you know we have the new Skypasaurus. Have you see the Skypasaurus behind me, Steve? This thing is...

Steve: No.

Leo: We built - Colleen built this.

Steve: Oh, is that those four screens that I saw?

Leo: Yeah. Colleen built this. It's four - because we were trying to figure out how can I do TWiT and MacBreak Weekly and Gillmor Gang, the shows that have multiple panelists, how can I get video from them all. And I wracked my brain. The only thing we could come up with is, well, we need four computers running four instances of Skype. And we place four separate calls. And then we route them all through the TriCaster. And that's what we did. It's Colleen - there are four mini ITX cases with four 17-inch screens on one giant multi-screen mount.

Steve: Now, this is not the reason that on the Gray-Haired Computing that we did, it's not the reason that Ray's audio was a little crispy?

Leo: Well, it is, in a way, because that was the first - that was the trial Skypasaurus. And we almost - I almost abandoned the whole project because of that. But Colleen updated drivers, we messed with it, we got it to sound - actually sounding...

Steve: Oh, yay.

Leo: ...just as good as you sound. And so that's much better now. So, for instance, if we do another Gray-Haired Computing segment you'll both be side by side on Skypasaurus and like that. But I came in today, and Skypasaurus had rebooted. All four Windows instances. That's how I know there's been a patch.

Steve: Ah, yes. We are on this side, or the other side, some side...

Leo: Of Patch Tuesday.

Steve: ...of Patch Tuesday, the second Tuesday of March. And there was, as usual, a bunch of stuff. I wanted to start, though, by asking our listeners to do us a favor.

Leo: Oh, good. I love that, yes.

Steve: There is some voting we need.

Leo: Uh-oh. Uh-oh. Are you running for beauty queen again?

Steve: No, no, this is Best Security Podcast.

Leo: Oh.

Steve: It turns out that there is going to be an announcement at April's, that is, this year's RSA conference.

Leo: That's the big one.

Steve: That's the big one. Remember, that's where I ran into Stina from Yubico and discovered the YubiKey at the top of the escalators, when she was sort of looking around forlornly, wondering how she could come to the world's attention. That problem got solved.

Leo: Is it in San Francisco again this year?

Steve: Yes. I think it's the Moscone Center. I'm not going to go up this year. It's like, eh, I did it, I saw what was there.

Leo: I'll accept on your behalf.

Steve: Oh, that'd be good. Anyway, so the URL is strangely named SocialSecurityAwards.com. It's got nothing to do with Social Security except it's podcasting and blogging, which are social events, social venues. So that's why they called it SocialSecurityAwards.com, all one word. The annoying thing for our security-conscious listeners is you must enable scripting in order to do this.

Leo: Well, that's not very socially aware of security.

Steve: Yeah, I know. They use some monkey program.

Leo: They probably use - they use cookies to keep you from voting more than once, probably.

Steve: They do that, yes. And so immediately I said, oh, well, I've listened to other security podcasts, and I really do like mine best. So, hey, I wanted to be fair.

Leo: That's fair.

Steve: I went to Social Security Awards, and all you get is this big black type on the screen: JavaScript must be enabled in order to proceed. It's like, okay, fine. So I enabled it for SocialSecurityAwards.com, and it still wasn't happy with me because there was something monkey or other, Vote Monkey or something, that I also had to enable.

Leo: See, I don't have to do any of that because I'm not running any of that stuff.

Steve: Because you have no security. That's fine.

Leo: I have no security.

Steve: But that, I mean, if that helps you to vote for Security Now!, I'm all for that.

Leo: Now, it's going to ask for the name, podcast name. That's Security Now!.

Steve: Security Now!.

Leo: The URL is TWiT.tv/sn.

Steve: That's exactly, hey, I filled it out correctly, Leo. That's what I put.

Leo: That's kind of the homepage for it: TWiT.tv/sn. And that's where all the shows live. And that's probably the best place for them to go to find it.

Steve: Yes. So TWiT.tv/sn for the URL.

Leo: And then of course the reason.

Steve: There's no prompting. It's not multiple choice. Our listeners are going to have to fill that in. You only - there's five opportunities, five things, because there's four different

blogs and one podcast. The podcast is the top one on that form. And all I did, since I am not reading other people's blogs...

Leo: Oh, I read Brian Krebs. I want to vote for Brian Krebs's blog.

Steve: I would, too. As a matter of fact, I refer to him in today's podcast because he had a great column about the Tigger trojan that we'll be talking about.

Leo: Yeah, so, I mean, I'm not going to tell people how to vote on this. But I'm going to say blog name is Security Fix, and the URL is blog.washingtonpost.com/securityfix. And Brian really floats my boat. I don't know. They want a reason. Now, I don't read a corporate security blog. You know, that really should - Brian should be the best non-technical security blog.

Steve: There's some sort of a limit to the reason length because I basically typed in a small book about why Security Now! was the best thing. And then when I tried to submit my vote it said...

Leo: They don't care.

Steve: ...that's invalid. So I shortened it, and it still didn't like it. So finally I just said, "Steve needs more hair." And then, you know, it liked that one.

Leo: I'm going to put Brian's in the non-technical because he's really a good non-technical security blog. I don't know who I would say technical. I'm not sophisticated enough to read a technical security blog. I certainly read a lot of the stuff, the security websites. I'll find a good one. Corporate, don't know.

Steve: Anyway, so to our listeners, SocialSecurityAwards.com. I won't say to vote for Security Now!. I would just say vote for your favorite security podcast.

Leo: But I'll be glad to accept when we win.

Steve: And Leo will happily accept when we win. That would be great. And then...

Leo: You know what, Steve, maybe we can get you up here. If you win, I think you should come up.

Steve: And after you've lowered all your security down so that you're completely vulnerable during the voting process, you can bring it back up right where it was before and turn off the monkey vote or whatever the hell that thing was.

Leo: They have to, come on, now, well, maybe you - you're good at doing stuff without scripts. But seems to me, if they want to kind of make sure only one vote per person, that kind of thing, a script is the best way to do that. Don't you have to use JavaScript to use cookies?

Steve: No. No. JavaScript is a horrible idea that came along way after cookies came along.

Leo: Oh, okay, okay.

Steve: No. No. Cookies are part of the fundamental HTTP protocol. HTTP or HTML? HTTP. It's the transport layer.

Leo: So in the GET and so forth you can set and get cookies.

Steve: Yeah. My guess is that they're doing things like probably using Flash cookies in order to be extra sneaky, in order to hook a little bit deeper in so you just can't delete your cookies and vote again. I mean, I only voted once. It's funny, too, because then I wanted to go back in order to be able to cite what the other blogs were. And it wouldn't even let me to the page. It said, "Thank you very much for your previous vote."

Leo: You've voted. You've voted. Stop it.

Steve: Done. And it probably logs your IP. I mean, who knows what it does. I don't care. I only voted once. But if all of our listeners would do that, I think we'd have a good chance, so.

Leo: I think we...

Steve: I'll get up off my knees now and stop begging.

Leo: Okay. What else is in the news?

Steve: Well, we do, as you said earlier, we have our monthly Windows Update drama. The bad news is there is still no fix for the very bad Excel flaw that we spoke of last week which is being actively exploited in the wild. Microsoft did not fix that this time. The general murmur out in the security community is that this is so bad that as soon as Microsoft can, even out of cycle, that is, they should not - given that we now know we're not going to have it for early March, they really don't want to wait another four weeks until the second Tuesday in April because this thing is, I mean, it's a problem we know about. It's becoming widespread in its exploitive spread. And Microsoft knows about it. They've acknowledged it, but they haven't fixed it. And essentially all it takes is somebody who's got Office installed to open mail and get tricked into clicking the link.

The act of displaying a deliberately maliciously formed Excel page can take over your machine, cause code to be executed remotely. The proof-of-concept technology is out and floating around the 'Net, so it's as bad as anything can be. And we didn't get a fix this cycle.

What we did get was the standard monthly critical remote code execution fixes. Turns out our old friend the Windows Metafile is back. There is a parsing bug in WMF and EMF, the enhanced metafile parsing, where during the handoff, as the GDI is getting involved and accepting parameters from the user mode down into the kernel, during that user mode-to-kernel handoff there is a problem with the metafile processing, parameter handling, that allows a malicious metafile to do bad things to you. So it's important. And I would say - I mean, they're all important. This one is as important as ever, that absolutely will require a restart of your machine. So you're going to want to do that.

We're going to be talking a little bit later about some serious trojans and worms which are still today managing to proliferate based on a patch that was issued in October of last year, October of '08. So we're now at, what, T plus five months. And people are still not patched. So I can't - it's inexplicable why that's the case to the degree that it has been because in this case we're talking about 11.5 million instances of a really bad worm infecting people, although it's becoming increasingly clever in the way it both survives and spreads, which we'll be talking about here in a minute. But I just want to say I think it's important. Rebooting is a pain, but you want to do it every so often. Certainly balance the risk versus the reward. But a restart of your machine will be required.

We talked a couple weeks ago and then again last week about the flaw in Adobe Acrobat and said that the most recent version of Acrobat would be patched on the 11th. Well, that's yesterday for the people who are listening to this on Thursday. It has been patched. The patch exists. And that's only for version 9. I'm still using 8, myself, and I'm happy there. So I went to their site, and sure enough, the update for Acrobat 9 is available as of the time we're recording this on the 10th. But there's no available patches for the prior versions. Remember that this is something which is also actively being exploited. This was a zero-day flaw, that is, it was found only after exploits were already taking advantage of it. Then Adobe figured out what was going on, said whoops, we've got a problem, we're going to get this thing fixed for version 9, the most recent version, on March 11th. And it'll be a week later for the prior versions. So I'll be keeping an eye out for when the update for my version 8 is available, and I will certainly apply it.

Leo: Why don't you just update to 9? I mean, is there some reason that you...

Steve: No, I just haven't.

Leo: I mean, I guess that's what they figure is that, well, update to the latest version, that'll fix it.

Steve: Okay. Yeah.

Leo: Is there something you don't like about 9? I mean, is there something we should avoid because 9 has...

Steve: No, I just haven't gone there. I have no need to. Maybe you're right, this going there, I mean, who knows what the story is. I don't even know if they'll charge me for an update from 8 to 9. You know, Adobe tends to be...

Leo: Oh, I see. You're not using the Reader, you're using the full Adobe Acrobat.

Steve: Correct.

Leo: Ah. So you don't want to pay for the update.

Steve: Correct.

Leo: But if you're using Reader, you should just update to the latest Reader.

Steve: Yes, absolutely.

Leo: Because that's free.

Steve: Because that's free, yes.

Leo: Although there are people who say - and that's why I was asking, because there are people who say, you know, they've always - because every time they update Reader they add more stupid features.

Steve: Oh, I know. And I did read something that was not confirmed on the 'Net that non-Adobe PDF readers may also be subject to the same problem.

Leo: I saw that, too. Foxit might have the same problem.

Steve: Yes, Foxit may well have - and you know...

Leo: I've been telling people use Foxit instead. And now I'm going, oy yoy yoy.

Steve: Yup.

Leo: Why would it have the same problem? Did they copy code from Adobe?

Steve: Without looking at it in detail I couldn't guess, although - oh, the other thing I

wanted to mention that was important is, when we first talked about this, I said that one short-term workaround is to disable JavaScript for Reader, that unfortunately - now, talk about adding things to it. Like I just want to open a PDF. I don't need JavaScript in my PDF reader. But they all have it. And it turns out that that was the way the original exploit was being leveraged into remote code execution. So at that time disabling JavaScript was believed to be a weak, yet sufficient for the current version of exploit, solution. Well, there's a way around that. As we expected, disabling JavaScript doesn't - we knew we didn't cure the underlying problem, but it only might solve the problem with this particular approach of exploitation. It's now the case that non-JavaScript exploits exist for this bug. And given that Reader may not be actively updated, this is something that could bite people. So it is the case that disabling JavaScript no longer protects you.

Leo: What a mess.

Steve: Yeah.

Leo: Big mess, yeah.

Steve: It's also Mozilla product update time. There are multiple vulnerabilities in all of the Mozilla products - Firefox, well, Firefox, Thunderbird, and SeaMonkey. In the case of Firefox, 3.0.6 and prior have the problem. And I'm using 3.0.7 now, so everyone should be who's using Firefox. Thunderbird 2.0.0.18 and prior are vulnerable, and SeaMonkey 1.1.16 and prior. And Mozilla's site has updates beyond all of those. So it's possible to update yourself to, in every case, a secure version. And you're going to want to do that. Also we haven't heard from Opera for a while, but Opera has got multiple vulnerabilities.

Leo: [Muttering]

Steve: So version 9.63 and prior are vulnerable. You want to be using Opera later than 9.63. And finally, one we've never talked about, but I thought there were some users of it still because it's popular, and that's Winamp.

Leo: Yeah.

Steve: Winamp uses an open source sound file parser called Libsndfile, L-i-b-s-n-d-f-i-l-e. Turns out that there is a sample processing problem that involves integer processing overflow in this Libsndfile file, and it's necessary to update to Winamp after version 5.55. So if you are a Winamp user, and I imagine among our listeners there are some people, just wanted to give you a clue that version 5.55 and prior are using the vulnerable version of this Libsndfile, and you should update. And updates are available from Winamp.

Leo: It's always scary when an exploit affects data files because everybody who listens to this show, anyway, knows to avoid executables.

Steve: Right.

Leo: And of course you back up data files. So you don't think, oh, a JPG, a PDF, an MP3. Those are harmless.

Steve: Yeah, or an Excel spreadsheet.

Leo: Or an Excel. That, at least, because there's macros, you go, well, I know that's got some executable code. But, c'mon, an MP3, there's no executable code in there. How could that be harmful? So these are - I think these are really serious. People ask me all the time, if I back up my data - because I tell them, you know, back up, reformat, reinstall so that you'll get rid of everything - if I back up my data, I'm safe. And I say, yeah, if you get the data only. But technically that's not true, is it.

Steve: Not so much anymore. I mean, as I do the research every week, and I write all this down, I just - I think, my goodness. It's just - it is never, I mean, literally never-ending.

Leo: You kind of have to admire the tenacity and, frankly, intelligence of these hackers to find an exploit in Winamp or Reader that they could take advantage of with a data file. PDF even, because PDF is kind of a programming language. PostScript is really a programming language. But come on, MP3? That's ingenious. Let's face it.

Steve: Well, and somewhere somebody was writing code to parse and process the samples in an MP3 sound file. They weren't thinking about security. They were thinking about getting the darn thing to work so that sounds come out. And it turns out that, as a consequence of that, if you give it a deliberately specially crafted sound file, an MP3 file, it will cause a hiccup in the processing that allows you then to, like, cause the rest of the sound buffer to be jumped into. So you have this special set of samples which causes this integer overflow, which causes the execution of the rest of the buffer. So you literally are putting a program into the sound file with a header that gets this vulnerable version of the library to execute the following code. And as soon as you do that, it can bring in some more code, take over your machine, go off to somewhere malicious, and install backdoors and trojans and worms. And, I mean, it's just the reality of computing today.

So really the only thing we can do is hope that vendors and developers continue to function in as responsible a fashion as possible and do their best to keep us safe. But it's just - and the other thing, too, is that what's really changed from the beginning days, where this was done as a curiosity, is unfortunately, as we're about to learn in a couple of other points I'm going to bring up here, next stories, is that it's big business. I mean, now this is big business. This is infecting and taking over people's machines for profit - not just to see if you can, or because you can, but because you can get paid to do it.

Leo: Somebody in our chatroom sent me a link to Foxit's page. They do have an update today. But ironically they say, "We have received a number of inquiries about the latest Adobe vulnerability. And people say, is Foxit Reader subject to the same

kind of vulnerability? It was caused by a buffer overflow in their JBIG2 decoder. We use our own JBIG2 decoder, and we are not vulnerable in the same way."

Steve: Great.

Leo: So instead of crashing, you get an empty image display when you get that buffer overflow. So good news. But there is an update. They did update their JBIG2 Reader. So clearly they took a closer look at it when they saw this Adobe vulnerability, and they found some stuff to clean up.

Steve: Good. In other news, as of the beginning of this month, all of our government's top level .gov domain servers are now running DNSSEC.

Leo: You mean they weren't?

Steve: No. They had never been before. No, DNSSEC is a complex and annoying system to set up. There's a lot to it. And our own .gov top level domain had not been using DNSSEC. It's now - all is in place as of February 28, the end of last month. So that's a good thing. I mean, it doesn't mean - that doesn't help us for, like, the .com and the .net and the .org and all the other top level domains. But at least the .gov top level domain servers can now offer signed and authenticated records. So anybody who wants to ask them for verifiably nonspoofable signed records can get them from our top level domain .gov servers. And that's, you know, it's a step forward. It's not clear that DNSSEC is going to end up being widely deployed soon, or maybe ever. I know "ever" is a long time. But this thing has been - the DNSSEC spec that we talked about at length in a podcast not too long ago has been around for a long time. So it's been available. It's there. It exists in all the current versions of the DNS servers. It's just that no one takes the time to do it because it's like, eh, well, you know, nobody else is, so we're not going to bother. Well, now the government is. And so that's at least one small step forward.

Leo: Did you mention that one of the patches that Microsoft issued yesterday was to fix a Kaminsky-type flaw in IIS? Or in their DNS server, rather?

Steve: No, I didn't.

Leo: Yeah, there still was a Kaminsky flaw in there. I'm going to call it a "Kaminsky flaw."

Steve: So a spoofability problem.

Leo: Yeah, a man-in-the-middle issue.

Steve: Right.

Leo: So they still were working on that, I guess.

Steve: And speaking of Brian Krebs, he had a nice little write-up - I ran across a reference to a new, an interesting trojan. It's called the "Tigger" trojan. And so in his write-up he explains that what's interesting about it is it is the most tightly targeted trojan we've really seen. More than a quarter million Windows machines have been infected.

Leo: [Whistling]

Steve: And this thing specifically targets employees and clients of E*TRADE, ING DIRECT, Vanguard, optionsXpress, TD AMERITRADE, and Scottrade.

Leo: Wow. Everybody.

Steve: In other words, the stock market guys, the people who are doing stock market stuff. It uses - it's interesting. It uses a privilege escalation exploit which was patched in October. So once again, five months ago this thing was patched, but it's still infecting these people. Maybe their corporate policy is, well, we'll get around to it when we can. It's hard to account for the fact that here we've got people doing financial services, both employees and clients apparently that have these accounts and this software on their machines, which this thing is working to target. But even running under a limited user account, which normally protects you from these kinds of exploits, won't protect you because it takes advantage of this privilege elevation fault which, if it's not been patched since October, allows it to install this trojan on your machine. And then apparently it has code in it, they've analyzed it, where it is deliberately doing malicious things if it happens to land in a machine owned by an employee or a client of any of those stockbrokers.

Leo: Wow.

Steve: Bad news.

Leo: I guess they didn't have enough money, they probably couldn't fix it. Too busy doing other things.

Steve: Well, and the worm that just keeps on giving.

Leo: Let me guess. Koobface? Conficker? Downadup?

Steve: Yup, it is the multi-named worm - Downadup, Conficker and also Kido. It's known by all three names. It was discovered, okay, in November of '08 by a honeypot. It was found in a honeypot that Symantec was managing and monitoring. Since then this worm has managed to infect at least 11.4 million PCs.

Leo: Whoa.

Steve: 11.4 million machines. Now, this is according to a census, not from an AV company where it's like, okay, they want to inflate that. But this was a census carried out on compromised Internet addresses by SRI International. So a neutral party said 11.4 million machines infected. Now, get a load of this. We're now at major version C of this. What happened was the original - one of the reasons this thing has been hard to contain is that they use an algorithm in the worm to determine what domain name to go to based on any given day. And so typically the way - and by the way, this installs a botnet. So you've got a big botnet, a whole large number of machines infected. Well, they need to go somewhere to get themselves updated and to receive instructions and various specifications for how to function.

So the first thing somebody does who wants to shut them down is they get a hold of one of these, they look at the domain names that are built into it, and then they go to the registrars, people like Microsoft, for example. It's called the "Conficker Cabal." There's Microsoft and a bunch of registrars that are all working together, and a bunch of AV firms, to try to control this problem. So the idea is you cut off command and control so that you shut down the domains that the worm is trying to go to and prevent it from updating itself, prevent it from mutating or getting more instructions or even new sets of domains. So because this is the way it's always been done, the designers of this new worm Downadup/Conficker/Kido, they said, okay, we're going to use a sophisticated algorithm which is going to be much more difficult for anyone to reverse-engineer and figure out, which will determine - which will essentially set up a large list of domains, but without revealing what they are.

So the original version of this, basically it was able to deal with 250 different domains. So it was necessary to reverse-engineer the algorithm, figure out in advance what domains this worm would be going to in the coming days, and then beat it to the punch by going to the registrars and getting them to preemptively issue - basically take those domains out of service. So the C version, which is out just recently, uses a new algorithm to increase this number from 250 domains to 50,000. So we're now looking at the worm able to, in the future, generate 50,000 domains. And it isn't only going to one a day. It's going to many.

Leo: But they have to register them, too, though. I mean, it's not like they can just spawn domains, can they?

Steve: Well, this thing, as I understand it, what it was checking was it was checking at 250 domains a day before. Now it'll be checking 50,000. So the idea is...

Leo: Oh, I see. So it's hard to figure out which domain they're going to use.

Steve: Well, and you're got to cover all of them on an ongoing basis.

Leo: Ai yai yai.

Steve: I mean, it really is a problem. Based on an analysis of traffic, that is, people looking at incoming requests to the known domains, the stats are that three million IP addresses - right now, three million IP addresses are contacting those domains each day. And that number has been stable over the past two weeks. So right now there are still - historically, 11.4 million PCs infected with this. Right now three million PCs are actively contacting these bogus domains. I mean, these are wacky domain names that no regular user is going to be contacting.

Leo: So these are - they're basically botnets.

Steve: Yes, this is a botnet.

Leo: They're creating a botnet at that domain.

Steve: Yes. Well, it's a botnet that is updating itself and mutating by using these - by essentially downloading updates to itself at these domains. And so it's really, they've escalated this cat-and-mouse game to the point that it is necessary, in order to block it on a given day, you need to prevent accesses to 50,000 domain names. You miss one, and these things are able to contact that one that you didn't block.

Leo: Can they tell from looking at the code what the domain names will be? I mean, is it algorithmic? It must be.

Steve: I don't know. I can't say definitively. I haven't looked at it. But, I mean, certainly that's what it's doing in order to do it. I just don't know what it's basing it on. And it seems to me somebody who gets the code and dissects it should be able to figure out the next set. The problem is it's just a problem of numbers. They realize that each day having the worm check a different 250 domains is - that's blockable.

Leo: Right.

Steve: Each day having the worm check 50,000 domains, that becomes a real difficult problem, to go and register, preemptively register 50,000 domains, and have that be a moving target over time. So, I mean, you can really see how this thing has escalated.

Now, interestingly, what happened with the B variant, which of course came between A and C, the B variant added a trick. And as I said at the top of the show, it's the thing that caused Microsoft to say whoops, because the B variant spreads through open network shares and also weakly protected systems by trying 240 common passwords. It basically is able to use peer-to-peer technology within a LAN in order to use network sharing in order to spread. And it's also able to propagate through USB memory sticks by infecting the autorun.inf file of a USB memory stick.

Leo: Well, now, that's convenient. We're talking about Autorun today.

Steve: Well, exactly.

Leo: Yeah.

Steve: So the problem is that, if you had this thing on your system, and you inserted a memory stick, it can copy itself to the memory stick, alter the autorun.inf, or create one if there isn't one. Then you go to a different Windows machine and stick this in. Well, if the owner or corporate IT, for example, had configured Windows Autorun so that USB sticks, that is, removable drives would not autorun, it turns out that feature of Windows was broken until February. Microsoft knew about it, but they did not push out the patch for it. You had to go get it manually, which few people did. They only pushed them out for Vista and Server 2008. So what we're going to talk about here in a second is the nature of their fix and why, believe it or not, Microsoft still hasn't got it correctly figured out. Their own documentation misses a critical feature which can cause this thing to even now still auto execute network and USB.

Leo: Okey-dokey.

Steve: I did want to share a little, before we get into the main content here, a fun little note. This is actually not a success story, but rather a listener of ours who wanted to share with our listeners how he's using SpinRite added to what he called his "tools of hard drive paranoia." He said: "I've been listening to Security Now! for a little over a year and own a copy of SpinRite. I have used it to recover some of my friends' computers, but have not had a critical issue of my own. I now have a single internal drive, a front-loading removable SATA bay, and my Drobo. I run SpinRite on my internal and backup drives quarterly, give or take. I do a full backup manually every weekend, which I store offsite, and run Carbonite on my system drive. And every disk in my Drobo has been tested by SpinRite prior to being installed, as well as the spare disk I keep around for replacement if any of them should fail."

Leo: This person listens to a lot of the TWiT network, I think.

Steve: He does. "It is easy enough to set SpinRite running before I go to sleep, and every time so far wake up to 'No problems detected.' I just thought I'd toss out my total backup strategy. I thought it might be nice for other listeners of Security Now! to hear how SpinRite can be used in connection with other programs to protect them from data loss." And you'll notice that his friends are having problems because they're not doing anything in terms of preventative maintenance. But he's using SpinRite in a preventative maintenance mode. Every quarter he'll let SpinRite have the drive overnight and just dust it off and keep it running correctly.

Leo: So that does make sense to do that?

Steve: Oh, absolutely. Oh, yeah, yeah. We keep hearing, I mean, the reports we get of, like, critical distress are because SpinRite wasn't run until the system would no longer just - it wouldn't even come up anymore. And then SpinRite was able to fix it. Had SpinRite been run, it would preemptively prevent this kind of problem because it's able to

see sectors and detect sectors which are becoming problematical before they become completely uncorrectable, unreadable. And it's able to work with the drive to say, okay, here's the data you want. Give me a new sector to put this in, and we're going to take that existing sector out of service. So, I mean, it really, truly is a preventative maintenance tool.

Leo: That's very cool. That really was your intent, more than a data recovery tool, was a maintenance tool. Or maybe not. I shouldn't put words in your mouth. I always thought of it as a maintenance tool.

Steve: Well, it is, except I don't expect people to buy it that way.

Leo: Right, right, right, right.

Steve: No one's going to buy it typically...

Leo: Until they need it.

Steve: ...until they need it. Unfortunately, it can be too late. And so everybody who then discovers it as a consequence of having it save them in a time of need, then they have it, and so they use it quarterly, and they never have problems again. So, but it's much more difficult to say, oh, buy this because it'll prevent problems. I mean, it really will, and it does. But that's a tough sell, which I recognize.

Leo: Hey, we just got a big box in the mail. The new Mac Pro is here. This is what we're going to use for our new streaming setup - $5,000 worth of Nehalem processors. But look at the corner; look at the corner on this box. It came a little - it's crumpled. So I'm a little nervous. We're going to do - right after, those of you watching live, we're going to do, right after the Security Now! ends at about 1:00 o'clock Pacific Daylight Time, we will do - which is 4:00 p.m. Eastern - we will do an unboxing, and I'll set this thing up, and we'll see if it boots. Always an adventure. You never know what's going to happen. All right, Steve. We've seen that Microsoft did it wrong. Is it still doing Autorun wrong?

Steve: Well, the technology appears to be correct. Their documentation for it is not complete. And it's not complete in a way that's going to probably get most people. Okay. So a little bit of background here. As I said before, this was all a consequence of a problem that Microsoft realized they could not leave up to the user to go and fix because users would not. They recognized there was a problem with Autorun not preventing running, which was the nature of the problem, is literally you could do all the configuration correctly, and it just was broken. Quoting from the CVE, the Common Vulnerabilities and Exposures database, they said, quote, "Microsoft Windows does not properly enforce the Autorun and NoDriveTypeAutorun registry values, which allows physically proximate attackers to execute arbitrary code by, one, inserting CD-ROM media; two, inserting DVD media; three, connecting a USB device; and, four, connecting a Firewire device. Then they have, five, allows user-assisted remote attackers to execute arbitrary code by mapping a network drive; and allows user-assisted attackers to execute

arbitrary code by clicking on, six, an icon under My Computer/Devices with Removable Storage; and, seven, an option in an Autoplay dialogue related to the autorun.inf file." I mean, it's just, like, really bad.

And US-CERT, the Computer Emergency Readiness Team, says, quote, "Malicious software such as W32.Downadup is using Autorun to spread. Disabling Autorun as specified in the CERT/CC Vulnerability Analysis blog is an effective way of helping to prevent the spread of malicious code. The Autorun and NoDriveTypeAutorun registry values are both ineffective for fully disabling Autorun capabilities on Microsoft Windows systems. Setting the Autorun registry value to zero will not prevent newly connected devices from automatically running code specified in the autorun.inf file. It will, however, disable media change notification messages, which may prevent Windows from detecting when a CD or DVD is changed. According to Microsoft, setting the NoDriveTypeAutorun registry value to hex FF, quote, 'disables Autoplay on all types of drives,' unquote. Even with this value set, Windows may still execute arbitrary code when the user clicks the icon for the device in Windows Explorer."

So this has been a big problem. And the problem is that corporations depend upon disabling Autorun by group policy, where you just blanket all of the machines on the corporate network with a, okay, do not run programs from when CDs are inserted, when drives are mapped, when removable drives like a USB thumb drive is stuck into the machine. Do not run. And Microsoft has provided that functionality forever in Windows, and it's always been broken. So what happened was, when Downadup, the Conficker worm, began to spread this way, Microsoft last month thought, uh, whoops.

Leo: Yeah.

Steve: So but the mistake they had made was when they found this problem - and they knew about the problem much longer ago, last year this came up - they thought, well, the problem is, if we fix this, then things that people are doing now which is in contravention of their stated desires, meaning that network shares will still run, for example, well, maybe they're depending upon that, even though they told Windows they don't want that. And so if we go and just fix this in a security update, it'll change that behavior. So we're only going to do that automatically for Vista and Server 2008. Anybody on earlier machines, well, we'll hope they upgrade to Vista. Hmm. So...

Leo: That's the solution.

Steve: So then when Downadup...

Leo: You really ought to upgrade. You ought to buy a whole new version of Windows. That'll fix it.

Steve: Yeah, just hold on for Windows 7, there you go.

Leo: Oh, geez [laughing].

Steve: So they said, okay, well, that strategy is not working. So we're going to have to push this out to everybody. So in February they did that. The problem is that it is, because of the nature of the way this was done, it ends up being extremely complicated because then they said, well, the problem is, if we push this out, and the behavior changes so that it's now correct, that may break things in a way that people don't want. So we're going to add another registry key to the already convoluted registry key that we'll talk about in a second, and which is still not documented correctly, called Honor Autorun Setting. Which they will default to a 1, meaning true, meaning yes, honor the Autorun setting which we have now fixed so that it really works. But in doing so it may have broken some things. So you now have the option of turning that off, if you want the pre-fixed behavior which sort of worked, but not really.

Leo: Okay.

Steve: Okay. So what we have now is we have a key in Windows, in the Windows Registry, which is called - I'm looking for it here in front of me, and I can't find it. Oh, there it is. I've said it many times, NoDriveTypeAutorun. What this means is it's saying do not autorun for specific drive types. And unfortunately, the types that you don't want to autorun for are encoded in bits in the value of this registry key. So, for example, the 1 bit in the value disables Autoplay on drives of unknown type. And it's not clear why, but the 80, the hex 80 bit does the same thing. So, like, this is a 1 byte that is an 8-bit long value. So the first bit and the last bit both have the same definition. And they are always both set to 1, if you want to disable drives of unknown type.

And I don't know what unknown type drives are because all the other bits pretty much cover all the types I can think of. For example, there used to be the 2 bit, that is, the second from the lowest bit, stood for NoRootDirectory. But that's apparently been deprecated. They no longer use that bit for that. But they didn't assign it to anybody else. They just said, well, we're just not going to have that bit defined that way anymore. And I'll explain a little bit more about how these bits are addressed in a second.

But the hex 4 bit, which is unfortunately the third bit from the right, the least significant bit, that stands for, if it's set, you disallow removable drives. Now, that's the key bit, for example, for a USB. And it turns out that Firewire is also obviously a removable drive. So USB and Firewire drives are disabled if the hex 4 bit is set. Fixed hard drives are disabled by the hex 8 bit, which is the fourth bit from the bottom. Network drives, that is, drives over network shares, and this is key to what was broken before in the previous, the pre-patched version. You could tell it you wanted nothing to execute, and network drives still would. Now they won't. But you need to set this bit for that to be true. CD-ROMs are governed by the 20 hex bit, RAM disks by the 40 hex bit. And as I said before, talking about the 1 hex bit, the 80 hex bit also disables drives of unknown type.

So this is really complicated. The good news is, if you just want them all disabled, that is, all bits on is a hex FF because that's a value of 255, which is what you get if you add 1, 2, 4, 8, 16, 32, 64, and 128, meaning those are the decimal values for each of the bits. You add those all together, that's 255, which is one less than 256, which is the total number of possibilities of bits in a byte. So if you set it to FF, Microsoft says that disables everything. Unfortunately, they're wrong.

Leo: Oh. You'd think they'd know. It's their operating system.

Steve: You'd think they'd get it right, yeah. Well, okay. So the problem is there are two places in the system, well, at least two, two or more, where this NoDriveTypeAutorun registry key can be. They only talk about it in the registry under HKEY_LOCAL_MACHINE. And it's HKEY_LOCAL_MACHINE\software\Microsoft\Windows\CurrentVersion\Policies\Explorer. And under there you will find NoDriveTypeAutorun. And this is what they talk about. They completely forget to talk about the CURRENT_USER branch of the registry. It's mentioned nowhere. And it overrides any setting you have in the LOCAL KEY branch of the registry. So you can follow their instructions, go there, set this key under HKEY_LOCAL_MACHINE and all the other stuff, software\Microsoft\Windows\CurrentVersion\Policies\Explorer, to FF, and think, okay, I got it. And you don't. Because if this key also exists under the CURRENT_USER, and the same subtree under the CURRENT_USER key, it takes precedence.

Now, I thought, okay. Is it the case that LOCAL_MACHINE could override the setting by bit? Are the bits OR'd for disabling where, like, so LOCAL_MACHINE setting would be a policy that takes precedence over CURRENT_USER? Anyway, I did a whole bunch of experimenting, and I've confirmed that that's not the case, that bits are not AND'd or OR'd or anything. If the key exists under the CURRENT_USER tree, it completely replaces anything you have specified under the LOCAL_MACHINE, which is the more global-applied key.

Now, the reason people may have this thing under their CURRENT_USER is the very popular Tweak UI little applet for Windows. Tweak UI has - one of the settings is to make it very simple to disable or enable Autoplay drive types. And if you've ever used Tweak UI or anything else where you've explicitly enabled and disabled, then those changes are always put under the current user. Which means you will have a NoDriveTypeAutorun registry key. And nothing that you do following Microsoft's instructions under the HKEY_LOCAL_MACHINE registry will have any effect at all.

Leo: Okay.

Steve: So bottom line is, I did create a short little URL, a little SnipURL to Microsoft's page which explains part of this story, the part that they do explain. And so that's SnipURL.com/snautorun, as in Security Now! Autorun. And if you put that into your browser right now, Leo, it's SnipURL.com/snautorun, for people who are listening and just want easy access to this page. It's also support.microsoft.com/kb/967715. And that explains the part that Microsoft explains. It completely forgets to talk about the fact that any presence of this key under CURRENT_USER overrides the key under HKEY_LOCAL_MACHINE.

Now, I assume most users just want to disable everything. It's certainly possible due to this bit-level granularity Microsoft designed into the design of this NoDriveTypeAutorun registry key. It's possible to deliberately enable specific behavior. If, for example, you wanted not to allow fixed drives, removable drives, unknown drives, RAM disks, but, for example, you for some reason wanted to allow CD-ROMs, or you wanted to allow network, network shares autorun, you can go in and design your own value for this key to specifically not disable those. I imagine probably most listeners just want to know that they've got everything disabled. So setting this value to FF will do that. And I would recommend, however, setting it in the CURRENT_USER branch of the registry, not the LOCAL_MACHINE. Or set it in both. But definitely CURRENT_USER because if anything ever came along and did put a more permissive value under CURRENT_USER, it would completely override what was already there under LOCAL_MACHINE, and you would not

get the protection that you're expecting. So that's the whole story on this mess.

Leo: So the CURRENT_USER overrides everything else. It's like - you'd think it'd be the other way around, that the higher level one would override the lower level one. But I guess you could have - that way you have per-user settings, I guess.

Steve: You have per-user settings, exactly. And so if it's not specified under CURRENT_USER...

Leo: Then it goes up.

Steve: ...then the LOCAL_MACHINE, then the global settings specify. Now, what's interesting is the defaults that Microsoft has for this. XP, Vista, and Server 2008 have a default setting of 91 in hex. Hex 91.

Leo: Hex 91.

Steve: Yeah. So that's XP, Vista, and Server 2008 have a 91 setting. What that means is, if you dissect these bits, then unknown drives and network drives are disabled. Except they weren't until you patched it because...

Leo: It just ignored that setting.

Steve: Exactly. It ignored that setting. And the default explicitly allows removable drives, fixed drives, CD/DVD-ROM, and RAM disks. Now, that's the normal behavior when you get a brand new XP out of the box. You stick in a CD, and it launches the CD. You stick in a thumb drive, and it launches anything that you have in your thumb drive. Unfortunately, as we now know, worms are taking advantage of this, copying themselves. I mean, it's very much like the old days of floppy disks and the so-called "sneakernet" where viruses would infect a floppy and just wait around for you to stick that floppy into a different machine, and jump from the floppy into the machine. That's how viruses proliferated prior to the Internet existing. What's interesting is that Windows 2000 and Server 2003 have a hex 95 as their default. And it disables unknown drives, network, and removable drives.

Leo: Which is something you would really want.

Steve: Which is really what you want. So essentially Windows 2000, Server 2003 did by default disable unknown drives, network drives, and removable. But Microsoft deliberately made this more permissive under XP, Vista, and Server 2008. They by default allowed removable drives to autorun rather than not. 2000 and Server 2003 would not run removable drives. So this problem would not have really existed had Microsoft kept that security higher. But they decided, well, for whatever reason, we want removable drives to have Autorun enabled by default. So they changed the 95 to a 91, which changes the 4 bit in the hex value, which governs the enabling or disabling of

removable drive Autorun. So that's the whole story. We've all got, if we've been patching our machines, we've got the technology working. It's now necessary to make sure that you've got FF bytes under...

Leo: That's every bit, and that means they're all disabled, every possibility.

Steve: Every bit set, everything disabled, yes. But you want to make sure you do it in CURRENT_USER, which Microsoft unfortunately doesn't even talk about, because otherwise it's ignored. If you change it in LOCAL_MACHINE while you have a more permissive entry under CURRENT_USER, the CURRENT_USER one takes over.

Leo: If somebody wanted to be industrious, you could just write a little registry, just a little reg file that would set this, that would create the key if it doesn't exist and set it to FF. That would be...

Steve: Yes, actually it's trivial to do that, to do a little registry file. And because it's easy, such a registry file would instantiate the keys if they didn't exist, and would overwrite them even if they did. And so you'd want to set them both to just FF.

Leo: Simple enough.

Steve: Yup.

Leo: Very good, Steve. Again, you can find that discussion at SnipURL.com slash - what was it?

Steve: SNautorun.

Leo: SNautorun. Which is Knowledge Base article 967715. But the best thing to do is go to GRC.com. They've got show notes there. We also will have them on our wiki, wiki.TWiT.tv. Steve's got a transcript of every show, all 187 of them, at GRC.com. He's also got 16KB versions there. And while you're there, pick up a copy of SpinRite if you don't already have it. Be proactive. Don't wait'll you need it. Get it now. And also lots of other free stuff like ShieldsUP! and all his free utilities and Wizmo, which I always love.

Steve: And more good stuff coming soon.

Leo: Coming soon, yeah. Can't wait to see CryptoLink.

Steve: I'm working hard on the DNS benchmark that I think is really going to be popular.

Leo: GRC, short for Gibson Research Corporation, GRC.com.

Steve: And I will remind our listeners that next week is a Q&A Listener Feedback episode. So by all means, I really love receiving feedback and knowing what you guys are thinking and what questions you have. That's GRC.com/feedback.

Leo: There you go. Thank you, Steve. Have a wonderful, secure week, and we'll see you next Thursday...

Steve: Thanks, Leo. Talk to you then.

Leo: ...for Security Now!.