Five Years of Vulnerabilities

Description: This week Steve and Leo discuss a disturbing new Windows 0-day vulnerability present in all versions of Windows. They cover a very busy week of security news, then discuss the recently released report from Secunia which analyzes the past five years of Windows software vulnerabilities.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-258.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-258-lq.mp3

Leo Laporte: This is Security Now! with Steve Gibson, Episode 258, recorded July 21, 2010: Five Years of Vulnerabilities.

It's time for Security Now!, the show that covers all your security needs. With us right now, the king, our guru of security, Steve Gibson from GRC.com, waving happily.

Steve Gibson: Hi, Mom.

Leo: Steve is the man who discovered spyware, coined the term "spyware," wrote the first antispyware program. He's written a number of great free security utilities and over the last five years has really been edumacating us on security and privacy issues. From GRC.com, Steve Gibson. Hello.

Steve: Leo, great to be with you again, as always.

Leo: Are we in our fifth year now?

Steve: Not quite. Well, we're wrapping up our fifth year. We're at two, since we have 52 weeks a year, and we've never missed an episode, the end of our fifth year would be Episode 260.

Leo: You mean we're beginning our sixth year in three episodes.

Steve: Exactly.

Leo: Holy cow.

Steve: Yes. And what's coincidental is that we started the podcast at the same time that Secunia, the Danish security firm that we've talked about a couple times - actually several times, many times even. They have that neat free utility, PSI, which we have recommended to our listeners, which is free to use and download. It gathers information about a user's installed software, programs and versions, and alerts people to their use of software which has gone unsupported and/or has known vulnerabilities in it. Well, they started exactly five years ago; and, as a consequence, just this last week produced a report of what they have found during the five years they've been counting vulnerabilities, which happens to be the same five years we've been doing the podcast. So we're going to wrap up a very long start of the podcast covering what's happened this week, and boy, a lot has happened this week, by talking about what the Secunia analysis of vulnerabilities over the last five years have been and, unfortunately, why it's not good news.

Leo: Oh, dear.

Steve: Yeah. We won't be done, we won't be running out of material here anytime soon, Leo.

Leo: Although anybody that listens to this show knows that, obviously.

Steve: Yes, it's been pretty clear for a while, yeah.

Leo: Yeah, yeah. The bad guys aren't winning, but they're certainly not losing, either.

Steve: So top of the news, the biggest - and the whole security community is going bananas over this - a really bad new Windows 0-day vulnerability. It turns out this has - it's one of those that's always been in Windows, that no one ever found before.

Leo: Oh, I hate that when that happens because then you figure, gosh, how long? I mean, as we've been vulnerable from day one.

Steve: Well, in this case at least 10 years.

Leo: Wow.

Steve: Because Windows 2000 has it. NT probably does. It turns out there's a subtle error in the way the Windows shell, which is, you know, the desktop system that runs on

top of the sort of the kernel, so the Windows shell, which displays icons and our Start bars and all that stuff, there's a mistake in the way it parses, that is, it displays the icons of .LNK, that is to say, .LNK files, which are commonly known as "shortcuts," so Windows shortcut files. What was found about two weeks ago by a researcher in Belarus was, in the wild, this was being used to attempt to take over the control systems for, like, electric power utilities.

Leo: Oh, no.

Steve: Yes.

Leo: This is more than just hacking passwords here.

Steve: Well, yes. So the particular target was SIEMENS SCADA systems, which are used for, like, major process control, industrial control, nuclear reactor control, electrical power generation stuff. Turns out that these SIEMENS systems have a hardcoded password which was built into the malware that this vulnerability was being used to install. What it was installing was a rootkit which installed two different .SYS drivers: one to hide itself, thus it's a rootkit; and the second to attempt to exploit what was known about the fixed password of these SIEMENS SCADA systems.

So several things are interesting. First, these .SYS files, one of the things that Microsoft did to increase the security of Windows, you'll remember, with Vista, was you had to have signed drivers. So a lot of people bitched and moaned about that because it's like, oh, it's going to be a pain to have to have signed drivers. But that was something that Microsoft said that's going to enhance our security. So you would think that no malware could install kernel-level system drivers. One is actually a filter driver, which filters what the file system is showing in order to filter out the display of these .LNK files. They were signed with the digital certificate from Realtek.

Leo: Wow.

Steve: So that immediately raised a warning flag. What that means is that Realtek's private key with which it signs its valid, good, benign drivers, somehow escaped its control so that bad guys got a hold of that. Well, it turns out that, since this has happened, well, the immediate reaction from Microsoft and actually VeriSign, who was the signer of Realtek's certificate, and with Realtek's understanding and acknowledgement because they were culpable in this, too, was that certificate was revoked. So it was added to the so-called "CRL," the Certificate Revocation List, so that Windows would no longer honor drivers signed with this known, escaped-into-the-wild certificate.

Well, it turns out that just recently someone spotted the same exploit signed with somebody else's credentials, a company called JMicron Technology Group. And then a sharp-eyed researcher, Pierre-Marc Bureau of ESET, he noted that both JMicron and Realtek share the same science park in the Hsinchu - it's the Hsinchu Science Park in Taiwan. Both companies whose private keys have been used to sign these trojans that are carried by this exploit, like physically are in the same location, or nearby. So that's an amazing observation. It's like, okay, well, that - I'm not sure what that tells us, but

it's hard to imagine that that's a coincidence.

Okay. So what we have is a 0-day vulnerability found in the wild. The problem now is that everything I've described about what this is being used for is just one tip of the iceberg. I mean, this just happens to be how this particular exploit, this vulnerability in Windows was first seen. Everybody knows about it now. It's been dissected. Proof of concepts have been created. Our friend HD Moore of Metasploit fame has already updated Metasploit so it's able to demonstrate proof of concept. So all the bad guys now know how to do this. And what the "this" is is what's so troubling because Microsoft's security report - they've acknowledged this a few days ago. They updated it just yesterday, late yesterday, acknowledging that it turns out that, not only will just - okay. I skipped a part.

This is just amazing. It's been propagating with USB thumb drives because it copies itself to any - when it's on a system it copies itself to any thumb drives, and you can't see them on the thumb drive because of the rootkit that is has installed as part of itself. So it moves a set of files onto the thumb drive, which include these .LNK files and the two device drivers and so forth, and you can't see them. You then take the thumb drive and stick it into another system.

Even if it's got autorun disabled, even if they've done everything everyone knows for safety you need to do, it doesn't matter. The act of viewing the contents of the directory, certainly if you've got autorun enabled and it pops up a little window saying would you like to browse these files, which is what so many people do, the point is, when you stick a thumb drive in a computer, you're typically going to look at the files on it. That's, you know, you're going to bring it up in Explorer, in Windows Explorer, in order to see what's there, drag something out of there, drop something in, whatever.

The act of displaying the icon of the link files executes the malicious code in that new machine. It's regarded as not requiring any specific user action. So in this particular case it's being considered a worm. And something like 9,000 instances of this a day is now being seen in the wild. The point is that everyone who recognizes how pervasive this can be is expecting this to be a big problem. And Microsoft in their most recent update acknowledged something that HD Moore was first quoted as saying. He has apparently figured out how to get favicons to do this.

Leo: Ugh. So websites would do it, then.

Steve: Yes. And so Microsoft has acknowledged that not only displaying these .LNK file icons in Windows Explorer, but now in Office documents, any Office documents are also vulnerable, including Outlook, which is to say email. So receiving malicious email containing one of these can compromise your system. And they also acknowledge websites can do it. You can now have a malicious website that will display, that will leverage this through the defect in the shell. And I'm not sure if it's all browsers. Certainly IE because Microsoft has acknowledged that. Depending upon where the display code is, I would imagine this may be cross-browser vulnerable also. We'll know more certainly a week from now.

The problem is that there isn't anything clearly - there's no real good solution for this. Microsoft has posted a Fix it which makes some changes to the registry and also shows what manual changes can be made. The problem is that the fix that is required, until we actually get the problem repaired, is that all of your link, all of your shortcuts stop being displayed, and you get sort of the generic white rectangle.

Leo: Oh, that? We've seen this before.

Steve: Yes, instead of the normal link that you're expected to see. And many of the icons that people are familiar with are actually shortcuts that they're not really aware of. So they don't always have that little curly arrow down in the lower left-hand corner, which is what you get when you have, like, a manual shortcut created to a file somewhere. It turns out that Windows uses these pervasively to sort of glue things together. So if people do this and then reboot the system as is necessary, suddenly you've got your, like, windows and control panel and all kinds of things are covered with these white rectangles. And now it's not even clear that that solves the problem.

So essentially everyone's holding their breath. Our friend Didier has come up with - Didier Stevens has an interesting tool that he had created. He calls it ARIAD. It stands for AutoRun.Inf Access Denied. This is a filter driver that he's installed that sort of globally prevents autorun.inf files from being able to be used to gain a foothold into your system. And so he talks about this as a means of mitigating the problem.

Now, the other annoyance is that this has existed from the beginning of Windows, as far as anyone knows. In fact, I even read something that referred to it as like the Windows metafile problem, which of course was one of our early topics at the beginning of this podcast five years ago, which existed back in NT. This very likely does, too. Microsoft takes no responsibility for that, even in their summaries of the affected platforms. It's all versions of Windows which are supported by their current security policy, meaning as of a couple weeks ago no longer XP SP2, no longer XP, no longer any Windows 2000. So although those are all vulnerable, apparently they are always going to be.

So we're beginning to see a problem with Microsoft's understandable need to at some point stop back-supporting old operating systems. The problem is that many of these older operating systems are still in active use today. For reasons of their hardware limitations, they can't be updated in many cases. They're just not powerful enough, fast enough to run Windows 7 or Vista. You remember my little Libretto, my little subnotebook Libretto?

Leo: Yeah.

Steve: I brought it up to Vancouver or Toronto a couple times? Just, like, last week I was dusting it off because I wanted to experiment using it as the machine to run Windows' version of Kindle with a big display in front of me when I'm on my stair climber. And it was way behind in security patches. The first thing it did was it said, oh, you need SP3. I installed it; it broke it.

Leo: Oh, dear.

Steve: SP3 can't run on that. And then I remembered, oh, yeah, I've tried this a few times.

Leo: That's frustrating.

Steve: And I keep forgetting. And then my own main machine is still back on SP2 because it doesn't work if I install SP3. And of course we've heard reports about that all along, and apparently that's still the case. So all of those machines and all of the Windows 2000 machines that are still around are never going to get this fixed. And this is a big problem. So it can get you through the Internet, through opening documents, through Internet Explorer at least, maybe other browsers, from surfing to malicious websites, from displaying favicons when you go to websites that are malicious. It turns out also through the WebDAV interface, and Microsoft also acknowledges now through fileshares. So this is, I mean, this is a brand new big problem. No one knows when Microsoft is going to get it fixed. Microsoft, I mean, people are speculating that this is bad enough they'll do an out-of-cycle patch, just push it out because they have to. Who knows.

Leo: I thought they did.

Steve: There isn't...

Leo: Responding to an avalanche of criticism about the latest 0-day exploit, Microsoft has posted, oh, that quick and dirty patch is what they put out.

Steve: Right.

Leo: Got it, got it.

Steve: The Fix it is the only thing that they've got.

Leo: So they need to fix - they really need to fix these libraries.

Steve: Oh, and they absolutely know. I mean, I'm sure they're not happy about this. And what I expect to be reporting a week from now, and probably two weeks from now, is what has happened with this exploit over the course of the next week or two because it's expected that the bad guys are going to jump on it fast.

Leo: Oh, boy.

Steve: And do as much damage, unfortunately, in whatever time they're given before this gets fixed. And we know that lots of Windows systems will never be fixed. It'll just...

Leo: Like that SCADA stuff that has the hardwired password.

Steve: Yes, yes.

Leo: Geez, what a bad idea.

Steve: Yes, Microsoft's security advisory says, under the topic "how could an attacker exploit the vulnerability": "An attacker could present a removable drive to the user with a malicious shortcut file, and an associated malicious binary. When the user opens this drive in Windows Explorer, or any other application that parses the icon of the shortcut" - which is to say that it displays icons - "the malicious binary will execute code of the attacker's choice on the victim system." This is Microsoft saying this.

Further, "An attacker could also set up a malicious website or remote network share and place the malicious components on this remote location. When the user browses the website using a web browser such as Internet Explorer or a file manager such as Windows Explorer" - that is to say in the case of a network share - "Windows will attempt to load the icon of the shortcut file, and the malicious binary will be invoked. In addition, an attacker could embed an exploit in a document that supports embedded shortcuts or a hosted browser control (such as, but not limited to, Microsoft Office documents)."

Leo: It's kind of an infinite number of vectors, it sounds like.

Steve: That's why there's such a concern here is that this is just, I mean, it is a malicious hacker's dream come true to find something like this. And the best thing Microsoft can do is, as quickly as they can, get this fixed across all of their OSes. The fact that it's ubiquitous means this is code originally written for NT that never got changed. It's been there. It's like, hey, if it's not broken, don't fix it. Well, turns out it always was broken. So now they have to fix it on all their platforms.

And it is troubling, now that we've got as many older machines as we're going to have that are never going to get patched, that are going to have outstanding serious vulnerabilities like this. I mean, this begins to be a real problem, the fact that big problems like this are coming up in really old Microsoft operating systems that Microsoft will no longer fix, it will no longer patch. And it's not clear that even, for example, Didier Stevens' filter tool - what I'm hoping is, well, I was going to say it's not clear that even it will be able to deal with other than the .LNK execution exploit.

What I'm hoping is that soon we'll end up with some third-party gizmo of some sort. I'd write one if - I guess if I had the time. I'd rather not because I hope Microsoft will fix this soon. But some sort of a third-party add-on that blocks this pervasively. Maybe once we know a little bit more about it - I mean, this is just all breaking right now. As we know a little bit more about it, it may be possible to come up with a blanket solution that can be applied to these versions of Windows that are never going to get fixed.

Leo: Wow.

Steve: Yeah.

Leo: That's really scary. Not good. I guess it's pointless to moralize at this point. But how could this happen? It's a dumb question. Never mind.

Steve: No, and there has been dialogue like that, Leo, people scratching their head that something this significant has escaped Microsoft's attention for a decade, more than 10 years. And remember when Ballmer was jumping around making all the noise about XP and how it was going to be the most secure OS Microsoft ever produced, and they were just taking time off, and they were going to go back through all their own code. That's all nice sound bites for people who are not coders. But as we've said on this program, as I have said, I've been amazed at how you can stare at code that is wrong and not see it. It takes...

Leo: That does, it shows you how hard this is to fix.

Steve: Well, yes. It tells you that the concept of reexamining written code for security problems is fundamentally flawed. The concept is flawed. It doesn't work. You cannot look at code and see what's broken, even if you're looking for it. Most of the time programmers are just happy that it seems to work, and they move onto the next thing. But in a forensics mode you're going to look at it and go, okay. I am trying to find a problem here.

But what happens is you buy into what the code is expressing. In understanding it, you get compromised. You get biased because you look at the code. You go, oh, now I see what it's trying to do. And you go, yeah, yeah, yeah, I get it. But it's so interesting then to have a debugger, to be stepping through it and have it malfunction. And you'll go, what? Wait a minute. I just looked at that. And then it's like, oh, you slap your head. It's like, whoa, now I see. But it's weird, I mean, you have to have your face rubbed in it in order to break the assumptions that the code brings with it about the fact that it's working correctly.

So the concept of Microsoft going back and rereading what they wrote before, it's like, okay, well, good luck with that. And here we've seen it. It just, you know, we keep seeing problems, in some cases that are very old, that have been there for a long time, that presumably lots of people have looked at, went over it again and said, yeah, it looks just fine to me, and then bang. Now we have all versions of Windows vulnerable.

Leo: You think these kinds of vulnerabilities exist in other operating systems undiscovered, buried treasure for bad guys?

Steve: I really do. I think that we're seeing this because Microsoft is still the big target. We have all, all listeners to this podcast have seen a relative shift of target towards Adobe recently. And look at the goldmine that has been for the bad guys. So Reader and Acrobat and those various Adobe tools, and Flash, they've been around for a long time, too. No one was looking at them hard. But they presumably had all the same problems that have been moved forward in time.

Only when the bad guys really recognized Adobe as, first of all, a large profile because it is highly installed. In fact, Adobe Reader's installation share in Secunia's analysis, that's one of the cool things about their tool is that that provides them with an anonymized inventory of what stuff people have installed. So Reader is installed in 91 percent of those Windows systems where PSI, Secunia's tool, is in place. So the bad guys look at a 91 percent install base - it's not 100. That's Windows. But 91 percent...

Leo: 91's okay, yeah.

Steve: That's pretty good. You're going to get a lot of people. And that's exactly what we've been seeing with all these Adobe problems. So I really do believe that - we've talked about how difficult it is to write solid, secure code. It's much more difficult to make it secure than it is to make it work. And most of the time programmers stop with a piece of code when it works because they're under pressure, they're behind deadline, management wants it done. They move onto something else when they've got this thing working. Getting it working doesn't mean it's secure. It just means it works. But it's very different to have it able to defend itself.

And so obviously links are able to be displayed. They've been displayed for 10 years. Turns out there's a way of deliberately changing the icon code so that the common link displayer in all versions of Windows will run that code rather than display the image of the icon. And so, yeah, it works; but it can also be abused. And there's enough difference between those two thresholds of it works, and it works perfectly, that is, it cannot be abused, that I imagine any sufficiently complex software system that's very involved, that's inherently dealing with data coming into it, new stuff, it's probably got vulnerabilities. And what we're going to see by the end of this podcast is that the rate at which vulnerabilities are being discovered is skyrocketing. It is not getting better; it's getting worse. On that happy note...

Leo: Speaking of Adobe...

Steve: Speaking of Adobe, exactly. They blogged, their security guy blogged this last week that they have been and are working with Microsoft now to use some of Microsoft's sandboxing technology for a future version of Reader. Adobe recognizes just what I said, that they've got a problem in that their software is too exploitable. And so it totally makes sense for something like Reader, which is a reader, to be in a sandbox. When you load a PDF, you want it to display on your screen. It doesn't need to reach out into your file system and change the registry or do any of a number of things that a non-sandboxed application can.

Remember that any application running under Windows has a tremendous amount of power. Normally we have applications that are operating in our best interests, and they're benign. But when you run someone's application you're inherently trusting that they're not wanting to do anything bad to you. And for the most part that's the case. That's not the case where you've got malicious content which is able to abuse the content interpreter, in this case the Acrobat PDF Reader, and cause it to misbehave.

So even though Adobe had the best of intentions, their product is so complicated that you could give it something malformed and cause it to misbehave. And we've been talking about that a lot lately, for example, with that /launch feature which allows PDFs to cause executables to run in people's machines. Adobe didn't intend that. They even have a warning dialogue which comes up to tell you that's about to happen. But it turns out they had a mistake in that so that the malware was able to change what the warning dialogue said in a way that Adobe didn't intend. So, yes, it worked; but it could also be abused.

So the idea of having Reader sandbox itself is fantastic. The idea would be that in Windows there's a very sophisticated system of permissions. And so Reader would

deliberately reduce all - the first thing it would do when it starts up, before it even thinks about loading the PDF file that you've asked it to view, is it would itself strip itself of every possible access right to Windows that it doesn't need. It would be nice if programs did that preemptively; but that's a lot of work, and it requires a lot more testing, and it might make the program a little more fragile. But the idea of programs sandboxing themselves by voluntarily relinquishing rights that they don't need, I mean, that's a fantastic concept. Nobody does it.

But so that's the notion of self-sandboxing which Adobe has now said they're going to do. So that's a really good thing. I can't wait till - they haven't said when. They haven't said what future version of Reader. But they're working on it with Microsoft.

Leo: It's a great idea. Maybe more programs should do that.

Steve: Yes. In fact exactly three years ago a researcher at Microsoft, a security guy, David LeBlanc, did a series of blog postings titled "Practical Windows Sandboxing," where he discussed exactly this. It wasn't the notion of a third-party sandbox container, like we've talked about using virtual machines, we've talked about using Sandboxie in order to sandbox things that don't expect to be sandboxed. But what David was exploring was the idea of applications that would sandbox themselves. The problem, of course, is no programmers ever assume they've made a mistake. So they go, well, all those other people have problems.

Leo: They should do it.

Steve: Exactly, they should sandbox themselves. But look, our code's just perfect. Uh-huh.

Leo: That's what Java does, doesn't it? I mean, that was one of the security models of Java is all programs in Java are sandboxed.

Steve: Yes, yes. And we've also seen, for example, that newer systems, Android has this notion, the iPhone OS has this notion of not giving programs global access to the system. In the case of, for example, the iPhone OS, a program is given a branch to the file system, and it can't explore anywhere but within its own branch. Now, users complain that that means there isn't a global file system, and they can't, like, store and load and save things between programs. But, yes, that's both - that's an inconvenience, but a huge security win because you've inherently sandboxed a substantial aspect of what a program can do. Does it limit you? Yes, in this case. But the upside is potentially much better security.

Leo: That's, I think, going to be - and we'll talk about this I'm sure in the body of this show. But that's the kind of global thinking that we need. I mean, it's clear that these Band-Aids are never going to keep up.

Steve: Yes. I think, I mean, I would imagine every listener of this podcast, having spent the last six months even just listening to this, is beginning to get a little dizzy. And it's

like, okay. And I ranted about this a few months ago where I said, okay, we need a different solution. We need a different approach. Clearly, and as you said, in the body of this we're going to be looking at the escalation of this problem. It's not getting better. It's getting worse. And, I mean, it almost seems like there's more attention coming from the "mal" community of finding and exploiting these problems. So we need a different approach. Something has to change.

Leo: All right. What's next on the menu of security flaws?

Steve: In addition, well, no. We have some good news, a bright spot on the horizon courtesy of the TrueCrypt folks.

Leo: Oh, this is good news. I did see this, yeah.

Steve: Yes. A couple days ago TrueCrypt v7.0 was released. One of the things that I think was really interesting that Intel has done in their more recent Core i5 and i7 processors is, due to the extreme popularity of AES, the Rijndael cipher, we did a whole show on exactly how it functions, how it takes 128-bit blocks of data at a time and maps that into a completely different 128-bit result, thus giving us a very strong symmetric cipher.

It turns out that the algorithm is so clean that it lent itself to specialized instructions. And so the Intel Core i5 and Core i7 processors have a set of, I think it's six instructions which essentially perform like a macro of the fundamental AES round. There's another set of instructions which are used for key generation. But most of the time is spent, after you've set up the key, is spent doing the actual, the bit scrambling. There's like a block shift and a block add and some block mappings.

One of the things that's so nice about the AES Rijndael cipher is that it's clean to implement. Well, Intel leveraged that into instructions which dramatically accelerate over what software can do by somewhere between four and eight times. So I mention this because with TrueCrypt v7.0 they now support hardware-accelerated AES cipher if you're running it on one of these supported Core i5 and i7 processors. On their site they list the sub-model numbers of those i5s and i7s which support it. And they're called the AES-NI instructions, which stands for New Instructions. And because the cryptographic rounds take up most of the time, as opposed to key generation, TrueCrypt does not bother using the AES new instructions which are used for key setup, only for doing the rounds. But they report a four to eight times improvement in performance.

So, I mean, even though it's fast as it is, in my own - people may remember my own sort of crude measurements of using a system with and without TrueCrypt. I couldn't really see any difference. The encryption overhead was lost underneath the overhead of the hard disk performance. So it wasn't slowing things down at all for me.

The other cool thing they have done is they've created the notion of "favorites." You're able to sort of teach it about, for example, USB drives, thumb drives or larger physical spinning hard drives where, in your own environment, you want the drives' contents to be secured, that is, encrypted. But you don't want to have to deal with the need to enter in a long nightmare secure password. And we all know what those are about from our discussion of LastPass two weeks ago, what it means to have a secure password. And so they allow you to add specific drives of your choosing to the so-called "TrueCrypt

Favorites," and automount those volumes. Which is sort of cool.

So it means, for example, you could have a TrueCrypted USB thumb drive on your keychain. And I do, and I'm sure that a lot of our listeners do because you absolutely don't want to let that thumb drive out of your control if you've got important stuff on it. The idea being, though, that you might, for example, have a machine at home and a machine at work, and you use a thumb drive for transporting files back and forth. Well, you can use TrueCrypt installed on the machines at each end and teach them about this thumb drive. And then it is automatically mounted and decrypted with, as you'd expect, lots of cautions. And TrueCrypt has carefully designed this so that it's still secure within the bounds of automounting. I mean, even that, people could say, oh, I don't want my precious crown jewels automounted. It's like, fine, we're not making you do it. But in some cases where you, for example, you really do have physical control of a computer, you could train it to automount drives of your choosing just to make it easier to use. And so I think that's nice.

They've also added large sector support. Hard drives, as we know, are beginning to incorporate larger physical sectors because it's more efficient for them in terms of storage as densities get up. Western Digital famously has a 4K physical sector hard drive as opposed to the normal half a K. The 512-byte has been the sector size for all time. Well, TrueCrypt could support mountable volumes on larger sector size drives before now, that is, before v7.0. But they could not support where you encrypt the whole drive, where the OS and everything, the whole drive encryption still needed 512-byte sectors. That's changed so that the whole drive encryption can now run on sector sizes of 512, 1K, 2K, and 4K. So that's one addition.

And they have had to, until now, until v7.0, in order to get hibernation file encryption to work, they had to do some messy things, essentially hooking into Windows and modifying some internals in an aggressive fashion. With v7.0, they're now using the official, provided by Microsoft, hibernation file encryption API which exists in Vista, Windows 7, and in Server 2008. The API is not in XP, so people using XP will - it'll still work. It'll just use it the way it was. So they're sort of cleaning things up where they're able to. And so TrueCrypt v7.0 is available now and looks like a nice move forward for those guys. They've done a lot of good stuff.

Leo: They really are keeping up with the Joneses.

Steve: Yeah, they are. And I ran across a sort of an interesting page. I feel like I'd seen it somewhere before. But someone in Twitter, Chris Gohlinghorst, whose Twitter handle is @oihorse, he sent me a mention about a site called wpacracker.com. And you should take a look at it, Leo. It's just www.wpacracker.com.

Leo: I usually stay away from sites with the word "cracker" in it.

Steve: Yeah. This is safe. And it's fun. I saw that the email address for inquiring was moxie@ something, thoughtcrimes, I think, .com.

Leo: Ah.

Steve: I thought, oh, it's our old friend Moxie Marlinspike, no doubt.

Leo: Oh, boy. So what does this do?

Steve: What it does is, for a fee, for a fee ranging between $17 and up, I think I see in my notes here $40, but I think it's possible to end up spending more, what they've done is they've put together a large WPA cracking facility. Basically...

Leo: It's a cluster.

Steve: A cluster, exactly, a large cluster which will do in 40 minutes what a strong state-of-the-art personal workstation could do in five days. And so the idea is, for as little as $17, using half the cluster, which takes 40 minutes, or $35, twice that, essentially, for the full cluster, which takes 20 minutes, and with your choice of English or German dictionaries.

Leo: 136 million word dictionaries.

Steve: Yes.

Leo: Wow.

Steve: Big, big dictionaries. Now, that's the standard. The extended has an additional, not overlapping, an additional 248 million words.

Leo: Oh, geez.

Steve: They will pound on a packet capture from a WiFi sniffer. So, and you're able to literally submit, like, a Wireshark packet capture file which contains packets, and they will then work on cracking the encryption by passing those packets through their 136 and optionally an additional 284 million word dictionaries and try to tell you what the password is. Now, you pay whether it succeeds or not. And they run through Amazon payments. Then they, oh, and the extended dictionary crack is $40 as opposed to probably 17 for the half cluster. And so you pay in advance, hope for the best, and they'll let you know in, like, 40 or 20 minutes, depending on how much you pay, whether they were able to figure out what the password was.

So this tells us a few things. This means that, just as we were saying two weeks ago, you definitely want to be using non-dictionary-based passwords for this kind of reason. Now, in their FAQ, one of the questions is, well, wait a minute. The Church of WiFi has Rainbow Tables for a thousand of the most common ESSIDs, but apparently only has one million word dictionaries for each. So what that means is, remember that - and we've also covered this in the past. The nice thing about the WPA encryption is that it merges the SSID of your WiFi network into the password you provide to create the key, specifically to prevent Rainbow Table attacks.

A Rainbow Table is - essentially it's a table of the results of using different passwords. So, for example, you could take - and this is what the Church of WiFi has done. You could take a million word dictionary and run them through the algorithm to create the key for all of those words. Then you use those keys to quickly see whether you can decrypt the WiFi traffic. So in order for that to be the case, because WPA incorporates the ESSID, what they've had to do was limit to some number of ESSIDs.

Now, for example, we know that access points have default ESSIDs. For example, you plug one in from Linksys, and it says Linksys, or D-Link or Netgear or whatever. That is, those are - and you can imagine those are the first ones anyone is going to try. So if you had never changed your ESSID, and you were using words in a dictionary, then you're much more vulnerable to the Church of WiFi's Rainbow Table attack than if you had changed your ESSID.

So this further says that, not only do you want to use a good password, and we know what that means, it's really, really valuable not to leave your WiFi node named whatever it came out of the box. Whatever it came out of the factory is going to be in organizations like the Church of WiFi's Rainbow Table system. You're still protected if you've got a really good random password. But renaming your access point to something off the map is definitely a good thing, too. And I thought it was just interesting that this is how people are spending their time. It's like, okay. Well, good luck. No listeners of ours are going to be using words from the dictionary, I hope. So that would be a good, again, just a reminder not to do that.

Winamp, for anyone using Winamp for playing their media, I just wanted to give people a heads-up that there is a Flash exploit for the - it's not actually, it's not an exploit in Flash. It's Winamp's parsing of the Flash VP6-style FLV content. So if you play an FLV, a Flash Video File, through Winamp, version prior to 5.58, and if it were malicious, that could take over your computer. So anyone using Winamp make sure that you are updated to v5.58, and you'll be safe from that.

Leo: We're actually big fans of Winamp here because they feature the network, and they sponsor the bandwidth for your show, as a matter of - come to think of it.

Steve: Oh, thank you.

Leo: Yes, thank you, Winamp. Through - I guess AOL owns it.

Steve: Oh, okay. Mozilla got caught by surprise.

Leo: This is a bad one.

Steve: Yes. And this is also a cautionary tale we're spending a moment thinking about. Something called Mozilla Sniffer was uploaded to addons.mozilla.org and added to the list of optional add-ons for Firefox on June 6th of this year, so last month. During that time it was downloaded about 1,800 times, per Mozilla's counter. On July 17th, so after more than a month, it was discovered to be sending to a remote server all the form data from any page that anyone who had installed that logged into. So it was malicious spyware of

the first order.

Leo: Wow.

Steve: So the good news is it had only been downloaded 1,800 times. It was flagged "experimental," so anyone who was using it would have had to have seen all those cautions that Mozilla puts up saying we're not vouching for this. We haven't looked at this. We haven't checked it out. Use at your own risk. Unfortunately there was major risk. And so certainly what Mozilla wanted everyone to know is, if you did ever use this thing called Mozilla Sniffer, and I wasn't able to determine, because it's gone now, I wasn't able to determine what it was, what benefit it was supposed to be providing. Presumably it was billing itself as something that someone would want for some reason.

Leo: They kind of gave it away with the name "Sniffer."

Steve: Yeah.

Leo: Sniffing your passwords.

Steve: Yeah. And so it was sending back all the form data. So, like, anytime you logged in it got your username and login credentials, and of course the URL of the page that you were logged into. So, not good. It has been blacklisted. So even if it hasn't been removed from people's machines, Firefox will stop using it, will alert its user that they've got a blacklisted add-on installed and that they should remove it. So that's good.

Leo: Yeah.

Steve: The last thing in - is this the last thing? Oh, no, it's not.

Leo: You were right when you said this was a big day for security news. Oh, my god.

Steve: Yeah. I want to discuss this in detail in two weeks because it's an interesting type of attack that we haven't discussed in the past. It's been around and has been known for a while. And it's sneaky. And it will make for a great detailed coverage in two weeks. It's called a DNS Rebinding Attack. And it's in the news now because someone named Craig Heffner is going to be presenting at the Black Hat conference at the end of this month his presentation titled "How to Hack Millions of Routers."

The good news is it's in the news today, and all the routers which are vulnerable hopefully are scurrying right now to get themselves fixed before his presentation. Because he's not only going to present how this works, but offer proof-of-concept code because he's annoyed that this problem has been around for so long and has not been fixed. Popular router models from Netgear, Linksys, Belkin, Dell, and both the FIOS and DSL routers provided by Verizon are vulnerable, including routers running the third-party firmware DD-WRT and OpenWrt.

In testing, 30 different routers, half of them were vulnerable. So not all routers are, but half were. So I would say at the very least, once this becomes public, there will be some proof-of-concept sites that are benign. You'll definitely want to be making sure that you're not a victim to this. Apparently NoScript has some DNS Rebinding Attack prevention technology in it which I will track down as part of, two weeks from now, the complete presentation on what is DNS Rebinding.

But so in brief, what happens is you go to a malicious site, obviously not knowing that it's malicious. Now, the good news is, if you're a NoScript user, or you've got scripting controls of some kind, then you will not be running the script probably that this malicious site offers. The problem, of course, is that we now, we're constantly seeing instances where bad guys are installing bad script on good sites. So, for example, if they're using some SQL injection vulnerability to get some malicious script installed on someone's Facebook page, and you go to their Facebook page, well, then, you're going to run that script.

So it's not enough to say don't go to bad sites or to assume that NoScript will protect you because we're seeing instances all the time. In fact, there was one we talked about a month ago where an advertising banner was benignly being presented, but it contained malicious JavaScript in the advertising banner. So you go to a site that gets scripts to run as JavaScript. In going to that site your browser had to get the IP address of that domain, obviously from that site's DNS server. If the site that you go to has control of its DNS server - any good high-end site does, for example, GRC. I run my own DNS server. So I'm able to - I'm providing DNS for GRC, which is then being echoed by Level 3.

So you go to a site that has control of its DNS server. What happens then is the script which is running from that site is, due to the sandbox that exists for JavaScript called - and we've talked about this also before - the same origin policy. Same origin policy prevents that script from being able to run against any other sites. So it keeps it local. What happens, though, is this script makes another query out to the same domain. And it's been set up with the DNS server for that domain to the second time return the IP of your router.

So what happens is, and it's not uncommon for a DNS query to return multiple IPs. It's done, for example, for load balancing. If you look up the - if you use, like, NS Lookup, a command line utility in Windows, or actually in all kinds of, I mean, Mac has it, and Linux, and UNIX, you use NS Lookup to look up an IP, like for Google or for Microsoft or for AOL, you'll get like a set of four or five. And if you use it again you'll get a rotated set of those. So the idea is they're giving you multiple IPs that can be used for accessing them for load balancing. And it's rotating that list. So this notion of getting a different IP back is not that uncommon.

What happens, though, is by having the script make a second query to the same domain, it now believes that your router is part of the same domain that the script is running in, which gives it access despite the same origin policy to your router. If you've got default login for your router - and apparently half of the routers that were tested did, that is, the Linksys, Netgear, Belkin and so on - then not only does it have access permission to your router's IP, but it can log in and of course perform all kinds of mischief - open ports, redirect your DNS to malicious DNS server so that you have spoofing problems and so forth.

So this has, again, caused a huge buzz in the security community. We'll be finding more about it in detail in a couple weeks, at the end of the month. And I'm going to be talking about the history of it, mitigation that has been done, how things have been created, what NoScript is doing to try to deal with this, and what users can do. But in the

meantime, if by any chance you are still running a default username and password on your router in the belief that it's on your side of the network, so why bother changing it, here's an example of why we can't even leave default username and passwords for equipment in our own LAN, the way they came from the factory, any longer. It's just not safe. There's just too many ways around these things.

Leo: It's amazing.

Steve: In the news also, I got this from the SANS security newsletter, I just wanted to - a little heads-up on webcams. If anyone has still not, has been intending to but hasn't yet covered their webcam over with a piece of opaque tape, a German man was arrested, an unnamed German man arrested in Germany for spying on 150 girls through their webcams. Apparently they began to complain, some of the girls complaining about random erratic operation of their computers that caused the computers to be looked at by someone who knew what they were doing, who discovered a webcam spying trojan had been installed. The common vector appears to be ICQ chat client, which was used in order to install these since it was found in every instance.

The communications was then backtracked. It installed a trojan which was able to turn on the webcam. And the communications was backtracked to this person, so they were able to then acquire his equipment and determine that the number was 150 that he had been spying on. So unless you need your webcam, just cover it over with a piece of opaque tape, and just peel it off when you want to use it. Hopefully we're going to have shutters installed by the manufacturers before long. That would be a good thing.

And my final bit of good news is that the v2 of Microsoft's Security Essentials is now in beta as of a couple days ago. It adds, from Microsoft's blog which describes it, a better, smarter protection and cleanup engine. So it's just more better. For some reason it says it can turn the Windows Firewall on. It's like, okay, that's good. Apparently they just gave it the ability to do that, and it didn't have it before. Sounds like a good thing. It also integrates, they say, more deeply with Internet Explorer to provide better protection against web-based threats.

And it's now getting itself involved in network filtering. People were complaining, AV vendors who were, well, who had a problem. You may remember that with Vista they added - Vista added technology that prevented kernel hooks from functioning, which was a problem for the AV vendors because they wanted, they needed to be able to hook the kernel in order to, for example, monitor traffic flowing. And firewall vendors were in the same boat. So Microsoft added something that they call the Windows Filtering Platform API to provide a sanctioned means for allowing that kind of functionality without needing to hook the kernel.

So Microsoft Security Essentials, moving ever forward into the territory of firewalls and AV vendors, as I think everyone expects them to over time, they've now added that functionality in v2. So it'll be doing a much better job of protecting against network-based attacks. Microsoft is, I mean, this is what Microsoft does. They did this with the Windows Firewall. When they first came up with it, there was a large, active industry of firewall vendors. And Microsoft came along and said, oh, well, we're just going to add a little firewall here. It won't bother you. Don't worry about it. And we're leaving it off by default. So it's like, okay, fine.

Well, that was the way it was for a few versions. And then SP2 of XP turned it on by

default. And now it's of course become an intrinsic part of Windows. And I think we're going to see the same thing with Security Essentials becoming an ever more aggressive and useful AV replacement for the third-party add-on products. People still run third-party software firewalls. People will still run third-party AV tools. Microsoft is just trying to say, okay, you know, we're going to offer one, too, for those who want it. It's certainly better than not having it at all. And of course I agree. If anyone's interested, you can get that through the Connect service. Microsoft Connect is connect.microsoft.com. I have it. I haven't yet begun to experiment with it. And once it's becoming more official, I'll have better and more detailed coverage.

Leo: All right.

Steve: In a little bit of errata, I just wanted to note the news in, I think it was E-Commerce magazine or site or something. Amazon announced that sales of eBooks have outstripped the sales of hardcover books. They announced what was called, and I'm quoting from this story: "Amazon has announced a dramatic upswing in eBook sales. For the first half of 2010 it sold three times as many Kindle books as it did in the same first half of 2009. For the full second quarter, it reported sales of 143 Kindle books sold for every 100 hardcover books sold. So of course it's not saying - they're not comparing it to softcover books. Obviously they're still selling tons more of that. But it's now selling more than hardcover books. So...

Leo: Isn't it amazing. I would have never thought that. I mean...

Steve: eBooks are happening.

Leo: Yeah. I thought it might be the younger generation, but our generation would never adopt these paper-free books. But, you know, you and I both read eBooks like crazy, so...

Steve: Yeah, we do. And in fact I forgot to mention, in the past month - so that was in the second quarter, in the full second quarter of this year, 143 Kindle books for every 100 hardcover books. Over the past month alone, 180 Kindle books for every 100 hardcover books.

Leo: Oh, wow. Oh, that's interesting. So it's ramping up fast.

Steve: Yes, it's accelerating very quickly.

Leo: I think, if you point at one thing, it's the drop of the price on the Kindle. Well, actually two things. And then the fact that you can read Kindle on almost anything now.

Steve: Yes. And I have to say, Leo, I briefly had an order in for a third iPad because...

Leo: You're crazy.

Steve: ...I decided to try using the iPad with my stair climber. And it was wonderful. I mean, it was, you know, in landscape orientation, much bigger, much brighter than - I had been using my Kindle DX, and I was disappointed, as I think I mentioned to you, with the DX2 with its supposedly 50 percent greater contrast. It does seem now to be better than the first DX. I think maybe it had to get warmed up or something. And I don't think the technology changed. I think its refresh algorithm changed. I see a little more twitchiness as it's changing the page. There's like some extra flutter going on. And I think that they're just managing somehow to pull - remember that it's an electrophoretic process that pulls black particles back away from the front of the screen. I think they're just somehow shaking them up a little bit more and pushing them further back because it's not that the dark is darker, it's that the white is whiter. And I think it's just, I mean, which sort of says they could upgrade the original Kindle DX with a software fix.

Leo: Ah, just the software, yeah.

Steve: Yeah. And in fact even the non-DX Kindle, the regular Kindle. But anyway, so what I did was it finally occurred to me, it's like, okay, if the iPad is better - oh, I know what I did. I purchased the external VGA connector for the iPad, and it didn't work. Because I think it only works to export specific video, like presentation video, when you're using Apple's presentation deal. It's not sort of a generic video exporter, from my own experimentation. So I thought, okay, well, that didn't work. And so I thought, well, I'll just try a Windows machine, and that's where I use my little Libretto now, and a big VGA screen propped up on a tripod. And I'm in heaven. I have a little RF clicker that I hold in my hand that I'm able to just snap through the pages of Kindle for Windows. And so, yes, it's been a nice upgrade for me. I have...

Leo: A SpinRite story.

Steve: ...a short little SpinRite story from Darren. And I had, oh, I called it the "Magic Touch," quoting from him. He said, "Dear Steve, here's one SpinRite testimonial, not overly dramatic, but it's mine. Some time ago my wife called me at work one day to say there was an error message on the computer when she turned it on, and it wouldn't boot. Having only enough computer knowledge to be dangerous, I told her it would have to wait until I got home and check it out." So he wasn't going to try to have her do anything over the phone. "Upon arriving home I soon realized that my magic touch would do nothing to revive the computer. Not worrying for a moment, I slipped in my copy of SpinRite and proceeded to run a scan on the hard drive. About four hours later SpinRite was through doing its magic. The computer booted up perfectly, and I haven't had one problem with it since. However, I do now run SpinRite occasionally for maintenance. Thank you for this wonderful program." And Darren, thanks for the report.

Leo: Yay. Love that. All right. We're done on commercials. So if you want to run right into our topic of the day, I'd love it. Got about half an hour. Can you do it in half an hour?

Steve: Oh, I can because I've touched on several...

Leo: Five years in half an hour.

Steve: Several of these things. Well, it's five years of summary and some interesting conclusions. So this is from Secunia, the Danish company, the security company that provides PSI. And as a consequence of PSI, but also using the CVE - CVE is the Common Vulnerabilities and Exposures list which is - Mitre.org hosts it. And it's an industry-wide sort of general database of vulnerabilities. Everything that we talk about on this show and a bazillion more that we don't ever have time to talk about because they're just random obscure programs that don't have much exposure to the world, they're all assigned a CVE number. So that database is a huge repository of these kinds of vulnerabilities and exposures.

The Secunia PSI tool, and Secunia as a consequence, monitors 29,000 products. And what they have seen is, over that entire 29,000 product base, there really isn't a clear trend towards more or fewer problems. Which is sort of interesting. When you stand back, the view from 5,000 feet is, okay, pretty much the same. But it turns out, if you look at the top 50 installed programs, it's a whole different story.

Leo: Oh, interesting.

Steve: It's really interesting.

Leo: Which shows you that people are attacking stuff that's popular.

Steve: Precisely. I mean, that's exactly what it says. It's that, well, I mean, look at Adobe, as we were just talking about. Adobe has a huge install base. In terms of the top third-party programs ranked by vulnerabilities during the year 2009, so the full previous year, by vulnerabilities, interestingly enough, and this doesn't mean, okay, this is just number of vulnerabilities. We're not talking about classifications and so forth. But Firefox was ranked number one in vulnerabilities. And it has a - I thought this was interesting - among this database a 56 percent installation share. So well more than half now of Windows users who are also using Secunia's PSI tool - so again, these are smart, security-aware users who are even clued in to Secunia and PSI. But 56 percent of them have installed Firefox.

Number two, that was 96 CVEs, that is, from the CVE database. Second down, with 84, is Safari, that has a 15 percent installation share. Down from that with 70 is Sun's Java Runtime Engine that, interestingly, has an 89 percent installation. And this really follows something you said a while ago, Leo, that you were more aware than I was that Java's Runtime Engine is really well established.

Leo: I think it comes with most operating systems, if I'm not mistaken.

Steve: In Windows systems. So it doesn't yet come with Windows. But...

Leo: Oh, it doesn't, okay.

Steve: But it's certainly required by many popular Windows apps that just sort of install it as part of themselves being installed, if you don't already have it installed. And equal to the Java Runtime Engine, with also 70 vulnerabilities during the year, was Chrome, Google's Chrome browser, with 30 percent installation base within this population. Then one fewer vulnerability, 69, was Adobe Reader, with 91 percent. Then the same number of CVEs, probably because it's the same code base, is Adobe Acrobat, that had 8 percent installation base.

Then at 59 vulnerabilities, but 99 percent installation share, more than anything else, was Adobe Flash Player. So, and then the same number, 51 vulnerabilities, was Adobe Air. And that has - Air has 41 percent installation base. I was surprised by that. It's also well installed. And then dropping a little bit from 51 to 48 CVEs is iTunes, that has a 43 percent installation share. And then at the bottom of the list of the top ten is Mozilla Thunderbird, that has a 10 percent installation share and 36 CVEs.

So aggregating all of this data and looking at what we've seen, of the 50 most prevalent programs, 26 are from Microsoft; 24 are non-Microsoft tools from 14 different vendors. The highest level of installation of course was Internet Explorer because it's pervasive. It's in every version of Windows. And all of this is just for Windows platform. As I mentioned earlier in the show, I'm going to keep my eye out for and find some numbers for comparison with Mac and also with Linux and UNIX, and also open and closed source because I think those would be some numbers worth looking at, just sort of for curiosity's sake.

So the high installation point was 100 percent, Windows Internet Explorer. The low in terms of this 24 non-Microsoft programs was Cyberlink's PowerDVD. And even though it was low, it had an installation level of 24 percent, so nearly one out of every four machines has PowerDVD in it. So what this says is that those 24 non-Microsoft applications, coming from 14 different vendors, have a market penetration of no less than 24 percent. So it ranges from 24 percent up to nearly 100 percent.

During the two years from 2007 to 2009, during which time Secunia was looking at all this, the number of vulnerabilities in these top 50 programs, so the ones that are most installed in people's machines, those vulnerabilities typically doubled from 220 to 420. So during those two years we saw a doubling of vulnerabilities. And so that's through 2009. So far during the first six months of 2010, we are already at 380 vulnerabilities. So we're at 89 percent, year-to-date, as of now, of all of 2009. So if we extrapolate, if we assume the rest of the year is going to go like it has so far, we would be at 760 vulnerabilities this year, up from 420 last. So it is, I mean, not only, I mean, it's not just a line pointing upwards. It's a hockey stick. I mean, the rate at which vulnerabilities are being found is increasing.

Of the types, Secunia ranks them in five different categories, from supercritical, then to highly critical, moderately critical. They only had 1 percent in the supercritical category. But they did have 50 percent of the vulnerabilities ranging between high and moderately critical. And interestingly, 80 percent of these are remote attacks. Only 20 percent were local non-remotely exploitable attacks. And of course we've been talking about the great danger of having the bad guys able to reach into our systems from far out.

And finally, of course, the conclusion is that, if you look at the chart of Windows vulnerabilities versus third-party vulnerabilities, it turns out that Windows, first of all

Vista - and Windows 7 is not included here at all because that was released in October, and so there just isn't any usable data. But XP and Vista had no essential difference in the rate or the severity of vulnerabilities. They were essentially the same. Essentially the same. And I expect that we're going to see the same thing with Windows 7 because, as we know, it's sort of just a repainted Vista.

And so Microsoft has been managing essentially at a constant rate the level of vulnerabilities, whereas unfortunately - and our own experience bears this out. Look at what has happened with Adobe in the last year.

And to a lesser degree the third-party applications are beginning to be where people are turning because they represent lower-hanging fruit. Microsoft has spent a huge amount of time securing themselves, automating update and patch management. All of Microsoft's programs are covered within the Microsoft Update umbrella to keep them current.

And we do see that third-party providers are late to the party. I mean, here's Adobe finally - first saying we're going to do quarterly updates, then that doesn't work out very well, like not even for a quarter; and now saying, okay, we're going to be doing them monthly because we obviously have a problem; and now finally saying we're going to sandbox Reader, which is the biggest source of ongoing problems that we have. So that's the lay of the land.

Leo: So, yeah, I guess we did kind of touch on this in the beginning part about what, you know, what the future looks like and what we can do and whether it's hopeless and all of that. Very interesting.

Steve: Yeah. I think that, I mean, it's not surprising to me that we're seeing this growth in third-party exploitation because, as I was saying earlier, getting this stuff right is so difficult. No doubt Microsoft is spending a huge amount of money now to do only as well as they are, which is they're spending all this time and resource, and we really know they are, and they're only managing to hold even. I mean, they still have problems like we spent the first half hour talking about with the nightmare LNK problem.

Leo: But it's not getting worse.

Steve: Right. They're not getting worse. But they're investing all of this and just holding even. What's happening is third-party vendors are not investing to the same level, and it is getting worse.

Leo: Yeah, and I think it's almost like the bad guys have discovered they're an easier vector of attack. I think we talked about this some years ago, that as Microsoft becomes more aggressive...

Steve: Yup, we predicted this, Leo.

Leo: We predicted it, yeah, that third parties would become the next vector.

Steve: Yup.

Leo: Plus the lack of regular patching from third parties kind of opens them up, as well. People don't check. They're always checking Windows Update. It's automatic now.

Steve: Yes.

Leo: Very interesting.

Steve: Yeah. So I think what we'll see is, this stuff takes time. I think third parties are going to have to get a clue about managing updates. I myself just added, for the first time ever, no one has seen it, or people have seen it, but it hasn't been officially released, the DNS Benchmark has an integrated version-checking facility in it which I wanted to get all up in place and dusted off and proven because certainly CryptoLink will, as well. I absolutely want to be able to say to people, in fact I even have a facility in CryptoLink where, if I ever discover anything really bad, and people want to enable it, their version of CryptoLink will stop functioning until they get it fixed.

Leo: Oh, that's interesting.

Steve: So it will preemptively protect them from...

Leo: You'll have a beacon of some kind.

Steve: Yes, actually, I have that technology now.

Leo: I think that's an interesting approach. Because that's what you want. You want some way of forcing people to either update or pay attention or just at least warn them.

Steve: Well, there will be several ways of having it operate. But yes, I mean, if, for example, if Reader, if a real problem was discovered in Reader, wouldn't you want it to preemptively pop up something and say, wait a minute, I'm vulnerable right now.

Leo: Yes. Stop using me.

Steve: Yes. Are you sure you want to open this document? I'm not going to force you not to. But I now know that there's a problem with me, and I'd seriously think you ought to fix me first.

Leo: So you'd install a kill - I guess it's a kill switch.

Steve: Well, it would be optional. In this case I'd probably have it default on, and then - and always be overwritable. But the idea would be that, in the case of something really bad, again, I don't think I'm going to make a really bad mistake, but who does? And so in the event of something really bad being discovered, I would be able to, if people wished, to prevent them from exposing themselves to something that I don't know is wrong ahead of time.

Leo: Right.

Steve: And seems like a good idea.

Leo: Seems like a very good idea. And most people have too much ego to do something like that. That's the problem. They don't want to say, yeah, I got - I might have a problem here.

Steve Gibson is the man in charge at GRC.com. His SpinRite software is available there. Great program. Must-have program. If you've got a hard drive, you need SpinRite. Go to GRC.com. Also for 16KB versions of the show. There are show notes there, transcripts of every show going all the way back to Episode 1: GRC.com. And Steve, we'll see you next week.

Steve: We'll do a Q&A next week. And then the week after, in-depth look at DNS Rebinding Attacks, how to prevent them...

Leo: Yeah, if you want to get a question to Steve - how to prevent them? Go ahead, I'm sorry.

Steve: No, no. Go ahead.

Leo: I was just going to say, if you want a question to Steve, it's GRC.com/feedback. GRC.com/feedback. Okay, Steve. Thanks a lot.

Steve: My pleasure, Leo. See you next week.

Leo: See you next week on Security Now!.