SECURITY NOW!

Transcript of Episode #370

Mark Russinovich & Other News

Description: We begin the week with a visit with our distinguished guest, Mark Russinovich, late of Sysinternals and now with Microsoft. Mark joins us to chat about the release of his second security thriller, "Trojan Horse," and to share some of his view of the security world.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-370.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-370-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. We've got lots of security news, including a zero-day exploit in IE9, IE8 and 9. Oy oy oy. But before we do that, we're going to talk to one of our favorite authors. Mark Russinovich is here, next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 370, recorded September 19th, 2012: Mark Russinovich.

It's time for Security Now!, the show that protects you and your loved ones online and your privacy online. And we've got a great show planned for you today. Let me first introduce our Explainer in Chief himself, Mr. Steve Gibson of GRC.com. Hi, Steve.

Steve Gibson: Hey, Leo. Great to be with you again, as always. Before we began I didn't just double-check that you've got your recorders running, but...

Leo: I am recording this. Because if you're hearing it now, ladies and gentlemen of the jury, then it must have been recorded. So according to time travel precedents...

Steve: I was going to say, that's sort of a time travel paradox.

Leo: Said by Isaac Asimov or somebody, we're okay, retroactively. You know, there's that new movie, and I...

Steve: "Loopers."

Leo: Yeah, to me it's like paradox city. How could Bruce Willis - anyway.

Steve: Yeah. I don't understand why the, I mean, I'll see it, of course, because it's sci-fi. But the premise is that the mob 30 years in the future, which first of all doesn't seem like very far for us to have developed time travel all of a sudden, and then for it to be in the hands of the mob.

Leo: Yeah, that was quick. Those mob R&D departments work fast.

Steve: When they want to assassinate someone, they send them back into the past, into what is apparently our present. And it's like, wouldn't it just be easier to do it the old-fashioned way?

Leo: Well, there's more room for the bodies, apparently, in the 20th - nowadays.

Steve: Ah, or maybe part of time travel is omniscience on the part of the feds or something. I don't know. Anyways, it's interesting.

Leo: I'm sure they'll explain that.

Steve: I hope they've come up...

Leo: But you would think Bruce would know, well, I guess he does know, maybe there was nothing he could do about it, that he was going to - he knows the outcome of this whole thing. Otherwise he wouldn't be there.

Steve: I will say something. And that is that there is something compelling about time travel.

Leo: It is. We love it, don't we.

Steve: There's a special pack of all the Star Trek time travel episodes across the entire set of series. The original ones with Spock and Kirk, then the Janeway ones - Janeway actually was getting herself in all kinds of trouble on "Voyager" - and various ones.

Leo: Well, this is kind of their version of the if-you-kill-your-grandfather-what-happens saga, only in the other direction, I guess. Anyway, it'll be fun. But we don't need to spend time with this.

Steve: No, because we have got something much better.

Leo: Introduce your guest. He's sitting here. He's lurking right next to you.

Steve: Someone much better. Our listeners will know, actually we told everybody last week, so unless someone missed last week they'll know that we have a special guest this week, Mark Russinovich.

Leo: Woohoo!

Steve: Who long-time security and computer insiders know from his work at Sysinternals, where all of us were downloading fancy utilities that were absolutely unavailable in any form anywhere else, just like the best stuff. I remember every so often I'd go over and suck everything down, just in case anything ever happened to the website that would cause them to become unavailable because they were so...

Leo: Good stuff.

Steve: They were so good. They were so important.

Leo: Oh, yeah.

Steve: And then, I don't know, I guess it was last year, Mark dropped me a note and said he'd written a novel. And I said, "What?" He said, "I'd like to send you a copy." And I said okay. Now, I have a review of his second novel, which is the occasion of his joining us on the podcast to chat a little bit about that and how we got into this and all that, sort of the human interest side. But I thought I would quickly share what I wrote publicly about Mark's work. I said:

"Like so many of this terrific book's early reviewers, I've known Mark for many years. Mark is a celebrity of significant note within the computer industry. But I only knew that Mark could write world-class code. I had no idea that he could also write world-class novels. And being artful at one certainly doesn't suggest any strong talent for the other. So being very picky, I worried when Mark sent an early copy of his first novel, 'Zero Day.' I wanted to like it and worried that I might not. So I'll just say that I wasn't the least bit worried, I was delighted, when he sent an early copy of novel No. 2.

"If you haven't yet read 'Zero Day,' you don't really need to. But I loved that Mark told his second story through the eyes of the two protagonists whom he introduced and developed throughout his first work of fiction. So by all means, click the purchase button above; but, if you haven't already read 'Zero Day,' why not begin at the beginning?

"Today, everyone understands that modern 'connected' life requires some concern for online privacy and security. If you know very little about the details of how bad things happen to people online, you'll find Mark's stories compelling from that standpoint. They explain this clearly and intelligibly, wrapped around exciting narratives that bring those details to life. And if, on the other hand, you know your way around computer security, you'll find Mark's stories not only compelling, but also technically perfect.

"I'm so glad that Mark decided to share his imagination and storytelling talent with the world. Once you've read Mark's novels, I'll bet you find yourself recommending them to others, as well. I certainly have."

Leo: Well, that's exciting. And we should mention that Mark will be back on Windows Weekly tomorrow and probably will talk more about Windows tomorrow. But today we'll talk about "Zero Day." Mark Russinovich, welcome.

Steve: Well, and so what I loved about the book, just by way of introducing it to our audience - you know we have a special audience that have been maybe listening to us for seven and a half years. We've covered, as I was reading the book, I mean, everything that Mark discusses, we've done podcasts on. And we've come at it sort of from a dry, technical, this is the way it works, here's the technology side. And as I was reading this, I was thinking this would really be interesting for our listeners because the technology will be intimately familiar, but here Mark actually employs these things in a very interesting plot that's exactly real. And it gives you a chill to sort of see this stuff come to life the way Mark pulls it together.

Leo: You're talking about his, of course, wonderful book, Windows Internals Part 2, now available in paperback. Oh, no, you're not talking about that. Okay. Welcome, Mark. It's good to have you on Security Now!.

MARK RUSSINOVICH: Well, thanks for having me on the show, and thanks - I emailed Steve when I saw that review. I'm thrilled and flattered and honored that he liked the book so much and that he took the time to write a review and share that opinion with everybody else. And it's great to be on the show.

Leo: Well, so I guess my first question is, how did this happen? We all know you as a codesmith. And now you've written two really good novels. What's the back story?

MARK: So, well, it really happened because I had this - I've always had this urge to write a book, a novel, like many people that get involved in reading when they're young, science fiction and techno thrillers. And I would read these stories that were so well crafted and yet built on solid technological grounding, so that I'd read it, and I'd feel smarter at the end. It was like I was going to school but having fun as I was reading a book, and thought it'd be really fun at some point to challenge myself to construct something like that.

And what pushed me to the edge of actually dedicating the time required to craft something was the strong belief, post-9/11 and post-SQL Slammer and Blaster and Code Red, that terrorists would see cyberweapons as an ideal weapon for achieving their agenda, which would just be indiscriminate destruction. We saw with those kinds of worms that people would write them, kids would write them in their basements, let them loose just to see how fast they could spread, without any real kind of malicious payload really involved with them. And yet they would cause so much disruption just in that form.

So that's what pushed me to write the book "Zero Day," what I think is a realistic threat, and also one that I could tell a story that was a techno thriller built on technology and share what a security professional's life is like and what cybersecurity is all about and the kind of risks that we operate with because our systems and our lives are so dependent on computer systems. So that's what pushed me to write that. And I actually finished it in mid- or early 2006. It took me several years to find an agent and then a publisher and then finally get it out the door. So, but that's what was the impetus.

And then I had started working on "Trojan Horse" a couple years before "Zero Day" [inaudible] in case "Zero Day" did well, then I wanted to have another one ready to go. I finished it after "Zero Day" came out. It was kind of the reception to "Zero Day" encouraged me to push through and get that one out the door. And I've been working on a third one, as well.

Steve: Whoa, wait. You just said you've been working on a third one?

MARK: Yes, working on a third one.

Leo: What, is that in between writing Windows Internals? How do you find time to do all that?

MARK: Well, Windows Internals, as you showed, Sixth Edition Part 2 is going to be out, I think, next week. RTM and Microsoft Press announced that earlier this week. So it's now off to the publishers and Amazon.com to get out there. But that's my last rev of the Windows Internals book. And that one I actually finished several months ago. And I've been working with Dave Solomon and Alex Ionescu, with contributions from some other people. So it's been kind of a low-level background activity, working on the book for the last few years, on the Windows Internals book series.

Leo: It's funny, I would have thought it would be the other way around, the novel would be the - you go home and go up to the attic and spend an hour each night working on it.

MARK: Well, actually the novel is that way. But the novel comes in more dedicated spurts than the book did. And the book, the book research for the Windows Internal book and some of the original writing for the book started many years ago, around the time of Windows 7 RTM, as I was writing magazine articles and blog posts and researching and just being familiar with what the product was and researching areas that I wasn't directly involved in. So that has been kind of ongoing for a long time. But the novel work is more - I need to dedicate serious time in more shorter spurts so that I don't lose my train of plot and thinking and being immersed in it.

Leo: Is it like programming, writing a novel?

MARK: It is kind of like...

Leo: What you just described sounds like a programmer might say that. I don't want to lose the thread of my - you're juggling many balls when you write a program.

MARK: It is totally like a program. In fact, I've experienced the same kind of context switching overhead - and there's a programmer term for you - when I'm working on a Sysinternals tool, and then I am pulled off to do other things and return to it a week or two later, it's, okay, I need to get back in the mindset of what this tool is and the flow and the architecture of it to figure out how to evolve it.

Leo: Now, you have comments, you have comments in source code to make that possible. What do you do in a novel? Do you have comments?

MARK: Yeah, I've got notes of things that I make as I go along to keep track of what my thoughts are and where I think things will go, things that I'd like to include. So I do have some of that to help me get back into it. But it's still - it is massive context switches. And even switching between writing and coding is a big context switch. So I try and minimize the number of times I do that.

Steve: For what it's worth, having read both novels, I feel strongly that there is an important social good that you have accomplished. I mean, it really - those books are technically accurate. They give anyone who is familiar with what's really going on in the security scape, I mean, a deep chill because what you paint we understand is absolutely possible. And, I mean, I really did get a sense of almost foreboding. And that's a useful thing to be able to give people, for example, decision-makers in government who don't really get it, don't understand what's happening because what you've portrayed is technically, I mean, it is happening at, like, right now. And frankly, I'm very impressed that you wrote "Zero Day" six years ago because, I mean, it was contemporary last year. I mean, it was - for that to have been already five years old is impressive. You were looking into the future back then.

MARK: Yeah, and I was actually concerned in that time gap that something would happen and the book would become obsolete.

Leo: No fear of that.

MARK: But you said that...

Steve: Yeah, I mean, we had Stuxnet happening at the same time.

Leo: It got more germane. It got more topical.

MARK: Yeah. I mean, I actually did, I complained to the publisher, why is this taking so long, it's going to become obsolete. They were like, no, it'll just become more topical. They're putting a positive spin on it. But absolutely, I think I wanted to send a message to everybody because everybody's involved with cybersecurity. Anybody running a small business, even in your home, you've got cybersecurity as one of the kind of responsibilities for keeping your own data secure, keeping your identity secure, keeping your business up and running, keeping your customers' data secure, keeping our national infrastructure secure. And you've seen with the Cybersecurity Act of 2012 and the debates in Congress and the partisan politics that we've seen going on with that, there's a lot of people that don't get it.

So I think that there's this antiregulatory philosophy that a significant portion of our politicians have which I think that, if you look at some of the industries that we've regulated, it's hard to argue that the regulation was unnecessary and not beneficial. You look at food, for example, or water, or the financial, the regulations we've got there that we're not all better off because of some regulation. And yet they'll sit and argue, no regulation necessary in cyber sphere...

Leo: But isn't the concern that the government, unlike food and water, that our governmental officials just seem to lack a basic understanding of technology? I think people are afraid that they're going to write something - look at SOPA - that makes no sense technically.

MARK: I think that is a concern, and it's a valid concern. But I don't think that that's a good reason to say, well, we're not going to do anything about it, and let everybody - and just have it be cooperative and voluntary and let people do what they want to, especially when the nation is depending on these systems for us to continue to operate well. So we outsource so much of our critical, national critical infrastructure to private industry, and yet say, well, you can voluntarily have security best practices and voluntarily share information with us and voluntarily - and I just don't see that as working. It's not in their best interest to spend money on something that they view as maybe low risk, or, well, if it's going to happen to us, well, it's going to happen to everybody, so why should I encumber myself with being the best at it. The free market pressures that people say will influence people to do the right thing I don't think really are there.

Leo: Congress recently decided not to regulate. But the President a couple of days ago proposed an executive order that would add some cybersecurity. Have you looked at his proposed executive order?

MARK: Yeah, it is pretty watered down. It is focused on, again, their voluntary sharing and voluntary adherence to cybersecurity principles.

Leo: It's not enough.

MARK: I think that - yeah, I don't think it's enough. And I think that one of the - a lot of the language is vague, so it's really open to interpretation. But I think one of the theories about what this executive order is really aimed at is not for the President to come out and issue an executive order, but rather to scare Congress back into talking about a bill and getting a bill through, which is the right way that this should happen, not just the President issuing something. So I think it's - somebody's - I've read articles that people say looks like it's potentially a bluff, just to get people back at the table.

Leo: Was the Cybersecurity Act sufficient, in your mind? Was it well written, well crafted?

MARK: Well, I think that the original Lieberman version was. I think that the one that, after McCain got his hands on it, became way too watered down. And that one, if you look at it, is basically volunteer versus regulation. And I'm not saying, by the way, when I say "regulation," that it's just purely regulation. I think we need to have incentives through tax breaks and other ways of positive reinforcement for people doing the right thing, not just the negative side of it, too. But the Republican version of it is definitely, I think, more close - it's closer to what the executive order looks like. And I think maybe that the Obama administration figured, okay, maybe this is a first step. Let's just agree, let's just establish what we can agree on, and then we can build from there rather than just not have anything. So that's why you saw Lieberman say, okay, fine, we'll go with this one, and then it still fell apart.

Steve: I guess as a consequence of the way the Internet sort of grew organically and the way computing and personal computers sort of grew organically, but I'm noticing this sort of, I don't know, a schism between the - or as a consequence of the amount of damage that an incompetent programmer can actually do. And I note, for example, by way of comparison, that attorneys and medical doctors have to get substantial additional education and then pass tests and essentially become certified. And programmers don't have anything like that.

But at the same time it's sort of gone from a casual hobby into something that is really a potent tool for good. But if code is written incorrectly, sloppily, casually, a lot of damage can be done. And of course all the license agreements say that there's no responsibility on the part of the producer of the software, which is another odd aspect to this computer industry that has persisted from the beginning. What do you think about the idea, I mean, not that I'm wanting to impose regulations and the same sort of MD degree and law degree on people. But something, it feels to me like somehow we need something to begin to tighten down the quality of the software being produced because it's become - it's gone from not really mattering much to being national security and nation-state level.

MARK: Yeah, and I think you're absolutely right. One of the things we do at Microsoft is people have to go to SDL training, Software Development Lifecycle training, which includes the threat modeling aspect of it. Not just the threat modeling, but then what kind of tools do we have available to us to make sure that the code is more secure, the tools that flag improper use of variables and uninitialized variables and then why you - the defense in depth things that we apply to our software. And Microsoft tries to help the industry in general by publishing SDL training publicly. And there's a number of companies adopt it.

It would be great to see that, at least starting with people that are developing the systems that are at the heart of things like our electrical grid or communications systems, that those people would have to have some certification in SDL and maybe - and probably have it renewed every year or two years, as well, just to make sure that they are at least aware that this is a way to look at their software to make sure that it's more secure and more resilient to attack. I think - I totally agree with you.

Steve: Where would you - you sort of touched on this before. But I'm wondering where would you split the responsibility for the trouble that we're seeing between the technology suppliers and the technology consumers? That is, how much of the responsibility is on the software authors, and don't users have some responsibility for their own conduct?

MARK: I think I would put, yeah, it's hard to put the blame on the consumer because the consumer assumes, right, when they buy software that it's being developed properly and it's not going to have flaws with it. So I find it hard to put the burden on them. But I also find it hard to put the burden on the software provider in that scenario, too, because they're sitting in a market where it's one of those - I've got certain competitors. If I spend too much time and energy on this stuff, I could fall behind on features and being competitive. And so what if it's secure if people aren't buying it because the company next door has all the cool features everybody wants, even if it's insecure. Those guys are playing this risk-management kind of situation while it's unlikely to really come back and slam us in the face.

And so if you look at what the government does, they've got this program called FISMA which has now evolved a bedrock where they'll say we do have certain requirements for the software that we're going to deploy our applications onto and run government workloads on top of that include things like making sure that you have two-path replication for your administrators and a whole number of other things that don't go as deep as the software developed using software security development lifecycle, but at least hitting some of the outside, very visible aspects of having a secure environment. In that case it's the consumer, in the government's case, which has leverage, which is the money and the dollars required that they're willing to spend on buying solutions. And so unless we have all consumers be that way and have certification and auditing, which the government has, then I don't see a way to change that dynamic between the consumers and publishers of software that people are using, like in a dentist's office.

Steve: Yeah. So I guess there will, from what we can see, always be a tension between the suppliers and the consumers, but also a tension within the developer side between new and features and spending more time on security, but not having as many features. People talk about how nice it would be to have a closed system which could inherently be more secure. The problem is, though, then they want - oh, but I need this and this and this. And it's like suddenly they push it away from being closed. And as soon as you do that, you open it up to exploitation.

MARK: Yeah. And we're seeing actually, as we move to the cloud, and we've got all these startups, agile software development bringing it on as fast as you can. And you know that you're sacrificing something there.

Steve: Yeah.

MARK: It's good enough to run for now. We'll move on to the next thing. But at some point it becomes a house of cards that you're playing with. So, yeah, I don't see a good way out of that dynamic without the kind of leverage that government's put in place that really cares. It's like paying taxes or eating broccoli. That's what security boils down to. It's sort of paying insurance; right? So unless you really believe that you're going to - that you're at risk of something bad happening, you're just not going to pay that price.

Steve: Yeah, for example, we advise people not to use the same password across multiple websites. And that's now becoming sort of standard, if you really want the best security, this is what you need to do. But wow, that's much more difficult to manage and maintain over time than saying, oh, I'm not going to worry about that, I want the convenience of just using one password everywhere. So again, it's exactly that kind of a tradeoff of convenience versus security.

MARK: Yeah. And very few people are making that tradeoff right now with passwords, despite the fact that you see these huge password breaches from one account surface that enables the attackers to get into a whole bunch of other related ones. That's still not stopping people from doing that risk calculation of it's unlikely to happen to me, so I'm just going to continue operating the way I am and cross my fingers.

Steve: Right.

MARK: The other thing, too, I wanted to point out about this regulation aspect, in that some of the arguments that McCain will make and some of the people against regulation and even government [indiscernible], they'll say the free market will take care because, if there is a problem, then there'll be a lawsuit, and that's the way that the free market will fix it. But I wouldn't want to bank our national security and infrastructure on, well, if it falls apart, well, then we'll sue the people that created the holes because by then it's too late. You've already - the damage is already done. You're not going to redo or fix things with a lawsuit and putting the company out of business after the fact.

Steve: Yeah. Okay. So here's a big, wide-open question that I think our listeners would find interesting, which is from your perspective, and this is completely wide open, what major trends of any kind do you perceive, like in the way the industry's moving, the way security's changing, the way attitudes are changing, development is changing, sort of what's - where are things going?

MARK: Well, the bigger trends, I think we're right in the middle of the third disruption in the computer industry, the first one being the mainframes, the second one being client-server, and this one being cloud and mobile. So that's one that's affecting everybody and the way that everybody thinks about software, from enterprise developers to ISDs to consumers. But underneath that, as far as security goes, I think that what we're seeing - and I've been a proponent of this form of security, the security technique, the security mechanism since shortly after 2000, when I started to really focus on what my software company, Winternals at the time, could do from a security perspective, and that is whitelisting. Back then whitelisting was something that nobody used. Windows and UNIX had some whitelisting capabilities, but very, very few people used it. And that's been the case up until very recently.

And people I don't think are really aware of this, but now whitelisting has become one of the key security features of the modern client platforms. When you look at iOS, for example, Apple's ecosystem, it's a complete whitelisted ecosystem. The whitelist, you can only run the software on the phones that have been approved by Apple and curated by Apple. Apple is essentially creating their whitelist in their Apple store. And that has made those platforms - Android's got one. It's not as well curated, so we've seen a problem with that. And then Windows Phone's got a curated whitelist, as well, and Windows 8 does, too, that those whitelists, you see the dramatic impact on the security of the system by having that whitelisting in place. Even if there is - and the sandboxing that goes with the whitelisting, as well. So I think I feel somewhat vindicated because I've always believed whitelisting would come back and become one of the primary tools in a cybersecurity posture or platform. And we're seeing that with the cloud platforms really adopting it and seeing the dramatic effects of that being in place.

Steve: And that's really interesting, too, because it does parallel the same kind of evolution that we've seen elsewhere. We've talked several times on the podcast about how the very first deployments of firewalls were default open and blocking only specific things that were known not to want to be made public. And it took a while, but we finally reversed that model in firewalls where it's default block, and then you selectively open availability for those services that you do want to allow through. And it was only after making that switch, although it's arguably more difficult, you're going to perhaps false block when you don't intend to. But that's better than having everything open by default and blocking only the things you know you want to prevent.

MARK: Yeah, no, that's a great parallel there. And we see the mirror of that in cybersecurity, too, with the blacklisting approach of antimalware. And just what I think is hard to argue not being a complete failure. I mean, the fact is, when I give a talk on security and Sysinternals tools for troubleshooting security, I have a fake piece of malware, which it's a piece of malware that I created, and it is malicious in the sense that it's a demo piece of malware, but it is completely unknown to the blacklisting antimalware solutions. Now, if I tried to deploy that in a system that was employing whitelisting, it would be totally ineffective. It would get blocked. And very similar to what you were talking about with firewalls, where for a long time we operated with a blacklist approach with firewalls, and then switched over to whitelisting and realized that's much more effective. I think the same thing is happening with antimalware. The places where it hasn't caught up are desktop systems and even server environments.

I don't - listing is not mandated as part of bedrock, and I believe it should be, or as far as software that's operating our national critical infrastructure. There should be policies in place for what software is running on those systems and stopping any other software from operating on those systems. And that would go a long way to keeping those systems more secure.

Steve: Yup. So you have...

Leo: Well, I - go ahead. I didn't mean to interrupt you, please.

Steve: No, I was just going to say - I was just going to wrap up by saying, so you do have a third novel to tease us with at some point in the future.

MARK: Right, I do, it's called - I've been working on it, and it's called "Rogue Code." It is, see, if you look at the first book, the theme was cyberterrorism. The theme of the "Trojan Horse" was state-sponsored cyber espionage and spear phishing. And the theme of this third one is insider threats in systems now.

Leo: I love it.

MARK: Which I think...

Steve: Good, good.

MARK: ...if there's any weak spot in any system, you can have the best technological defenses in place. But if you have an insider, a malicious insider, that is very hard to defend against. And social engineering, of course, a slightly weaker form of the same thing as an insider threat, but also extremely hard to defend against.

Steve: Very cool. Well, Mark, thank you very much for joining us. And...

Leo: We'll see you tomorrow. And actually LouMM, who is in our chatroom and I guess a colleague of yours, is going to run over with a Heil PR 40 microphone for you to borrow for tomorrow. I think he's already linked you. But really great to have you, and I appreciate, boy, we've been fans since the Sysinternals days.

Steve: Yeah, I was going to say, thank you so much for all your contributions through the years, to be able to have those tools. And they did not disappear when Microsoft sucked you up.

Leo: Thank goodness, yeah.

Steve: I remember when that happened, everyone was like, oh, my god, we're going to lose Sysinternals, no. Microsoft's got Mark now. And it's like, they're still around, and they're getting better all the time.

MARK: Business as usual. Still that's my other hobby is the Sysinternals tools. Still working on those. Thanks for having me on the show. It's been fun.

Leo: Nice to meet you, Mark. Really appreciate it.

MARK: And nice meeting you, Leo.

Leo: Take care, bye bye. Mark Russinovich, Russinovich.com. And then Sysinternals is still on the Microsoft.com site if you just Google "Microsoft Sysinternals."

Steve: And people can...

Leo: I should have asked him if he's updated. We'll ask tomorrow if he's updating them because I think, I don't know if there's a Windows 8 version.

Steve: I remember looking at one of them not long ago, I needed something, and it was there, and it was current. It was at least Windows 7 current.

Leo: Good, good.

Steve: And it was like, oh, thank goodness, this stuff is still around. So, yeah, just some of the best tools there are.

Leo: Yeah, Part 2 tomorrow. We're going to take a break, come back with more Steve Gibson and security news.

Steve: Yup. We had a very, very busy week. This was nominally a Q&A week.

Leo: Right.

Steve: But I thought with Mark and with so much news to talk about, once again we just don't have a chance to get to questions. So I did download 289 pieces of email this morning, but you have another week to send more stuff in to GRC.com/feedback, and we will do that next week. Today, for the second half of this podcast, we'll catch up on the week's news because there was a lot that happened.

Leo: Excellent.

Steve: I did find, I ran across a really neat note from someone named Philip Cooke that I just wanted to briefly share. He had a success, not surprisingly I guess, with SpinRite. He said, "A week ago I started my day with a Blue Screen of Death, advising that I had an unmountable boot volume."

Leo: Ugh.

Steve: "Efforts by a Dell tech only led him to the conclusion that we should reformat the drive and lose all my data. Nothing would recognize the drive, and all of the chkdsk commands in the book could not even see it or result in anything but the same blue screen on every reboot. A Maxtor utility that I ran from a downloaded file advised me to return the drive for replacement. After getting estimates ranging from $400 to $2,700..."

Leo: Huh-ho.

Steve: Which is, unfortunately, it's typical because they often - it's like a manual process to do this. "...[T]o recover my data and trying numerous other tricks recommended by online chats, et cetera, I was fortunate to come across SpinRite. At first the glowing testimonials seemed just too good to be true, and I will admit that I thought they may have even been fake. So I invested the $89, downloaded the file, and fired it up.

"At first I thought that it was going nowhere 'cause after four hours it still said 2 percent complete. I figured I would leave it running over the weekend. And imagine my surprise when I came back this morning, saw the message that it had completed. It booted up, ran chkdsk, and then started Windows. All I can say is wow. Thank you for taking the time to create this program. It's bad enough losing data, but I also saved the hours it would have taken to recreate my desktop, links, et cetera. Needless to say, I am impressed. Philip Cooke." So...

Leo: Yay.

Steve: Yay. Thank you for sharing that, Philip, with me and our listeners. So, okay. Well, Mark is not involved in IE security.

Leo: That's an important thing to say right upfront.

Steve: Yes. There is a serious, all abuzz this week is a, I mean, Microsoft warning, sending out emails warning about a new zero-day IE exploit that was found in the wild. It was discovered by a researcher monitoring some servers that were known to be used by bad guys. He discovered this on Friday, and it has since been found in the wild. The Rapid7 guys who manage the Metasploit framework have - they dove in over the weekend and have already updated Metasploit to demonstrate this.

Microsoft has no really good answer at this point. This affects all versions of IE that are current, that is to say, not Window 8 and IE10, but IE9 and earlier, across all versions. Apparently the exploit that's in use now is aimed at XP, but there's nothing that prevents it from being used on Vista and 7. And in fact exploits have been developed, I think the Metasploit framework instance is even more effective than the one that's out in the wild. So what the one in the wild is doing is installing the Poison Ivy trojan that we've talked about many times, the so-called RAT [Remote Access Trojan]...

Leo: I like the name.

Steve: ...the remote takeover trojan. Now, Microsoft's only response has been - they're not telling people to switch to Chrome. They really can't say that.

Leo: [Laughing] That would be a good answer. Hey, you know, you might just want to use Chrome for the time being.

Steve: Yeah. They're telling people to install EMET, the Enhanced Mitigation Experience Toolkit. The problem is that's not always effective, either. And it can represent problems in corporate settings and in the enterprise where it conflicts with other things. So everyone's sort of holding their breath. The real solution for our listeners has probably already been taken, which is no one is using IE for their main surfing all the time anymore. They're using it periodically, when necessary, to run Windows Update, if they're running Windows Update through their browser, or only when necessary.

Hopefully people have already taken the advice Microsoft can't give and switched to Firefox or Chrome, and then you don't have this problem. This is enough of a problem, and this next second Tuesday of October is far enough away, that is, the 9th, that we're - and Microsoft did react to this immediately. I was impressed with how quickly they were on the ball with this, when you consider this was only discovered on Friday, and I was getting mail Monday morning, two days ago, saying there's a problem. Unfortunately, we don't really have a good solution.

So October 9th is their next opportunity for their regularly scheduled in-band update. I don't know if they can be ready in time. Maybe they'll be ready sooner. So we'll see. But really the only thing you can do is stay away from IE, or I guess you can crank the security all the way up so that IE won't run scripting. That is one of Microsoft's recommended mitigation measures. Of course...

Leo: Should probably use it anyway; right?

Steve: Yeah. Increasingly, things don't work on the 'Net. In fact, you can't even do Windows Update if you follow Microsoft's advice for making IE secure because it requires an ActiveX control and scripting in order to work. So just don't use IE. It's just - it's got to be your...

Leo: Even IE8, even IE9, even IE10, even...

Steve: Yes, yes. No, no, not 10.

Leo: 10's not out yet.

Steve: 10's not out, and Windows 8 is not out. And it is not - the betas...

Leo: Are not vulnerable. Oh, okay.

Steve: Yes.

Leo: Well, that's good news.

Steve: So whatever this is - and there are very little details. I've not bothered to go, you know, this is the exploit du jour. So I can't spend much time figuring out...

Leo: Yeah. Nobody has time to read about all the flaws in Internet Explorer, it's...

Steve: There'll be another one tomorrow.

Leo: ...a full-time job.

Steve: Now, LastPass has just added an interesting service. They call it the LastPass Sentry service, which is, interestingly enough, opt-out for all LastPass users who are at the paid level, either premium or enterprise users. So if you're just using the LastPass completely free, this is not available. But if you're a LastPass premium, if you've given LastPass some money and are a premium user, then what LastPass is doing for you, and by opt-out I mean that you're in now unless you tell them you explicitly don't want this, is they've made a deal with a group called PwnedList that are - this PwnedList group are aggregating all of the publicly leaked usernames and passwords. They currently have a list of 24 million of these.

And so what LastPass is doing is making a daily check of their paid LastPass users' account email addresses against this master list. And LastPass will proactively notify any of their paid premium and enterprise users if at any point their LastPass account email appears in the PwnedList, which is very cool. They have interesting future plans because of course the first thing I thought was, well, that's nice, except here we've recently been telling people don't use one email address for everything because we know that that could be a problem. That was essentially what bit Honan with his problems.

So many of us have deliberately custom or differing email addresses. And but that's not our LastPass account email. In fact, we may explicitly have, for security, the high-value email is different than others. So we would like to know if those are leaking. Well, they say that they're working toward providing local verification of users' entire database of LastPass data against public leakage. To do that, that would mean that there would be an agent which was added to the LastPass scripting, the JavaScripting which is running in our local browser since, I mean, I haven't thought this all the way through.

They would be, I mean, I guess they could hash everything and send hashes up and then check that. Or our own machines could be checking against a list through a service that they provide, which is what I'm guessing they would do, is they would take all of the email addresses that they see, well, email addresses and usernames that we have in our locally stored LastPass in-browser database, protect that so that our security is preserved, and then presumably they would provide an API in their servers that allowed our browsers to check those in a secure way against this master PwnedList. So it wouldn't be just the LastPass master account that was being checked, but all of the email addresses and usernames that we use with LastPass. So that's very cool.

Oh, and they're also saying that they're working - that their plans are at some point to work toward increasing the frequency so that it's much more frequent than once a day, more towards something closer to real-time.

Leo: Wow, that's neat.

Steve: So, very neat. Now, Symantec - this really comes perfectly on the heels of what Mark was talking about with his novels. And he's off the line now, so I'll just say to our users again, I mean to our listeners, they're really good books. I mean, I can't imagine anything more interesting to the listenership of Security Now! than what Mark wrote because it is everything we have talked about, set in a - here's the way the stuff would be applied and how it escapes detection. It's really neat. And as I was reading book No. 2, "Trojan Horse," I was thinking, wow, this is just so perfect for our podcast listeners. So it's really - it's fun.

But speaking of nation-state scale stuff, which is clearly one of the focuses Mark has had from his perspective, Symantec just produced a 14-page paper which I posted a link in my Twitter feed yesterday. And we are now - I've got this in the show notes. And, Leo, you have a person who is posting the show notes somewhere. Is this - I've never...

Leo: On the wiki: wiki.twit.tv.

Steve: Okay.

Leo: Every show, theoretically, on the wiki has show notes. But it's all volunteer. And so I had been posting stuff up there. I've given him all the notes for the past year's worth of episodes, and I think he's getting them all up there bit by bit. So I'm very grateful to our volunteers.

Steve: Well, I did have a number of people, or maybe one person multiple times...

Leo: Probably that.

Steve: ...tweeting me, asking me, couldn't find some stuff that I had referred to in the last week or two. So I do want to explain that I produce notes with links to everything in them. And we're now, since Leo's got a neat volunteer who's going to be moving those into the wiki, I would recommend to everyone, take a look at the TWiT wiki in order to find these. But also my Twitter feed has it, in this case. Anyway, it's a 14-page...

Leo: He's still catching up, I think. So it looks like he's got quite a ways to go still.

Steve: Maybe he could start on the most recent ones and work backwards. If that makes sense.

Leo: I will suggest that. I don't know where he's putting them, now that I look. Anyway. All right, so we'll see what's going on.

Steve: Okay. So this is gripping. And again, I tweeted it because it's a fantastic, another fantastic sort of real-world, bring-this-down-to-reality look at what's going on. And Leo, I think on page 9, if you want to put that onscreen, there is an amazing graph that Symantec has pulled together. I'll just read their overview because it gives you sort of a chilling sense of what is actually going on. And this is not a Mark Russinovich novel, though it is just like one. They said:

"In 2009 we saw the start of high-profile attacks by a group using the Hydraq" - and then they said "(Aurora)." And we remember Aurora being referred to as what was - I think it was the Google attacks, and maybe the RSA attacks were the Aurora trojan horse. "Symantec has monitored this group's activities for the last three years, as they have consistently targeted a number of industries. Interesting highlights in their method of operations include the use of seemingly an unlimited number of zero-day exploits; attacks on supply chain manufacturers who service the target organization; and a shift to 'watering hole' attacks."

This is the first time I had seen that term. We've talked about phishing attacks, where someone is, like, spear phishing, where you know who you want to compromise, so you send them emails containing links or documents which will directly lead to their machine being taken over. A watering hole attack is Symantec's term, and I think it's going to catch on because it's a great term, where you know who you're trying to target. But rather than going after them, you are able to anticipate the websites they are likely to visit.

Leo: Like a wildebeest, which returns again and again to the watering hole on the desert veldt.

Steve: Exactly. So the predator lays in wait at the watering hole and attacks at that point. So they say the "watering hole attacks compromising certain websites likely to be visited by the target organization. The targeted industry sectors include, but are not restricted to, defense, various defense supply chain manufacturers, human rights and nongovernment organizations (NGOs), and IT service providers. These attackers are systematic and reuse components of an infrastructure we have termed the 'Elderwood platform.' The name 'Elderwood' comes from a source code variable used by the attackers. This attack platform enables them to quickly deploy zero-day exploits. Attacks are deployed through spear phishing emails and also increasingly through web injections in watering hole attacks.

"Although there are other attackers utilizing zero-day exploits, for example, the Sykipot or Nitro or even Stuxnet, we have seen no other group use so many. The number of zero-day exploits used indicates access to a high level of technical capability. Here are just some of the most recent exploits that they have used." Then Symantec enumerates four that we've talked about over time: Adobe Flash Player Object Type Confusion Remote Code Execution Vulnerability, Microsoft IE Same ID Property Remote Code Execution Vulnerability, Microsoft XML Core Services - remember when that was happening a few months back - and Adobe Flash Player Generic Remote Code Execution Vulnerability.

Leo: There's so many. How can we count them all?

Steve: Oh, god. It says, "In order to discover these vulnerabilities, a large undertaking would be required by the attackers to thoroughly reverse-engineer the compiled applications. This effort would be substantially reduced if they had access to source code. The vulnerabilities are used as needed, often within close succession of each other if exposure of any of the vulnerabilities is imminent. The scale of the attacks, in terms of the number of victims and the durations of the attacks, are another indication of the resources available to the attackers. Victims are attacked, not for petty crime or theft, but for the wholesale gathering of intelligence and intellectual property. The resources required to identify and acquire useful information, let alone analyze that information, could only be provided by a large criminal organization, attackers supported by a nation-state, or a nation-state itself."

So in this 14-page report which, again, I recommend our listeners take a look at, I think anyone would find it interesting, Symantec details the structure that they have tracked down over three years and how the specifics of the attacks which might look disparate on the surface, you might not easily note that these things are connected, they found the connections and built a connectivity graph showing how all of these pieces spread over the years are associated with each other. And they've also noted, based on the time, the windows during which the attacks were deployed, when the zero-day vulnerabilities were found, and when backtracking from the next attacks backwards, what they've been able to deduce is that, shortly after a zero-day vulnerability is discovered and patched, the entire platform immediately deploys the next one, as if they have an inventory of these things.

Leo: Isn't that amazing. Wow.

Steve: Yes. So, I mean, here we are, from our perspective, talking about, okay, what happened this week and what happened last week. It all just sort of seems like salt coming out of the shaker, bouncing around chaotically without any connection. But at least in this case Symantec, by looking carefully at these and noticing things like common variable names and common deployments, they've got - they got a Shockwave Flash file which there appear to be automated systems in place for, like, compiling exploits into this Shockwave, this generic Shockwave Flash package that allows them to quickly - and again, this is all about windows of opportunity. We understand that there are moving targets, that there are people looking for malicious connections and malware, so it's all about time, how quickly can you get in and suck things out before the window is closed, before you're discovered, and you then need to come at it in a different direction.

And interestingly, some of their advice for, for example, defense contractors, is you really need to look at your suppliers because what they're seeing is they're seeing that the one or two steps away suppliers, who have relationships with the contractors they're actually targeting, the suppliers who presumably have somewhat less stringent networking security, maybe sloppier management of their own websites and so forth, they represent points of entry into the network that then allows them to piggyback in on the relationship the supplier has with the contractor. I mean, and this sounds like science fiction. But there's a map of this in this PDF. So it's just, I mean, this is going on. And so there is reference to China. This does sound like a nation-state that has a formal program assembled. And what's bizarre is this is a chunk of Mark's book. Even though...

Leo: Oh, really. How interesting. He called it.

Steve: Yeah. I mean, again, I read this three months ago in his book. And I'll say again, I am amazed that he put together "Zero Day" in '06 because Stuxnet was happening just a couple years ago. It's like, whoa, okay. Which really...

Leo: He didn't have prior knowledge, I don't think; right? But it just - it was - you think?

Steve: No. No, no, no, I don't think so. I think that...

Leo: He just saw it coming.

Steve: Well, and you've heard me do the same thing. If you understand the technology, you know what's going to happen. I mean, you can just say, okay, this is going to happen. And there have been a number of times when that has come true. And so he gets it, too. He understands the technology. He realizes where the weaknesses are. And I thought he did a good job of sort of characterizing at the legislative level the tension that exists. The shuttle software, the U.S. shuttle program, had to be absolutely bug free. And we can do that at an incredible expense. Software that's being produced commercially, eh, you know, it can get updated.

Leo: We'll fix it in post.

Steve: Yeah. The cost of making it perfect goes exponential. You hit the hockey stick where, to make it incrementally better, you've got to spend amazingly more money. You will get something for it, but is it worth it? And then there's of course ever-present time pressure and competition, who eats your lunch because they're producing sloppy code faster, yours is better, but they're getting the sales that you're not. So it's not a perfect world.

Anyway, I'd really, if somebody wants to have charts and graphs and numbers rather than generalities, Symantec has put together an amazing piece of work. Oh, it looks like it's on - it's Fig. 6 on Page 7, Leo, is a graph of what they've actually found of the way all of this ties together. And they've put together a beautiful paper. So I wanted to recommend it to people.

Speaking of foreseeable problems, for the last couple months BMW has had trouble. Theregister.co.uk, in their typical inflammatory but factual fashion, they had a post recently titled "Got a BMW? Thicko thieves can easily nick it with $30 box." And they said, "BMWs and other high-end cars are being stolen by unskilled criminals using a $30 tool developed by hackers to pwn the onboard security systems. The new tool is capable of reprogramming a blank key and allows non-techie car thieves to steal a vehicle within two or three minutes or less. Onboard diagnostics (OBD)" - which is a term, an acronym we're going to be hearing in the future. "Onboard diagnostics bypass tools are being shipped from China and Eastern Europe in kit form with instructions and blank keys, says a news report linking the release of the tool to a spike in car thefts in Australia, Europe and elsewhere during 2012. Would-be car thieves need to grab the transmission between a valid key fob and a car before reprogramming a blank key, which can then be used to either open the car or start it, via the OBD system."

Okay, now, that's one instance. There's a different one which is unrelat- well, it's related, but not identical. Back in July Motor Authority magazine carried a story. They said, "It's every car owner's worst nightmare: You wake in the morning, grab your keys, and head to the parking lot, only to find that your car is no longer there. While new technology such as chipped ignition keys and Near Field Communications (NFC) key fobs have made cars more theft-resistant, they haven't made cars theft-proof.

"In fact, as Piston Heads points out, European fair trade rules have opened a back door of sorts for car thieves, one that allows them to create their own NFC fob to steal a car. We're not experts - and if we were, we wouldn't publish the info online - but it appears that all thieves need to snatch your ride is a diagnostic device that also reprograms blank NFC fobs.

"Break into a car via conventional means, access the diagnostic port" - which is typically located under the steering column - "and you can program a new blank key in a matter of minutes." And this works on BMWs right now. "While BMWs seem to have the highest incidence of theft via this method, models from Opel, Renault, Mercedes, Volkswagen, Toyota, and Porsche are also reportedly susceptible to fob-cloning theft. While Britain's Society of Motor Manufacturers is working to make access to key reprogrammers more difficult, doing so may conflict with the EU's competition rules, which allow independent facilities to access all data available through onboard diagnostic ports."

Okay, so that was July. So our update of September is, they said, "In July we brought you news that car thieves, in Great Britain anyway, had gone high-tech, stealing new cars via the use of NFC key reprogramming devices. Instead of relying on old-fashioned methods to steal certain new cars, today's thieves just need access to the car's diagnostic port, a blank NFC key, and a key reprogrammer.

"BMW models built between 2007 and September of 2011 are the cars of choice for these thieves, and the Bavarian automaker has just announced a software fix that will eliminate the chance of NFC key theft on X5 and X6 models. Per Auto Express, BMW dealers in Great Britain will upload the revised software to owners of affected vehicles at no charge." Well, isn't that nice. "While that solves the..."

Leo: Your car's gone. By the way...

Steve: We have an update for you. If you can find your car, we'll happily give it to you.

Leo: Find your car, yeah.

Steve: No charge.

Leo: Oh, boy.

Steve: "While that solves the problem for owners of X5 and X6 models, it won't do anything to resolve the issue on other BMWs. The company advises that a software upgrade is in the works for its other products and is expected to be ready within the next eight weeks. In the interim, BMW is advising owners to park their cars in a locked garage or under the watchful eye of closed-circuit cameras." And then in a sort of a strange, yeah, well, this would happen note, they said, "Even after the software updates re installed, expect to see a high number of break-ins of BMW vehicles."

Leo: Why?

Steve: "Since the modification is transparent, thieves won't know..."

Leo: They won't know, yeah.

Steve: "...which cars have been updated and which ones haven't. In other words..."

Leo: You should put a sign in the window. "I've got the new firmware. Move on."

Steve: "In other words, even after the fix, BMW models will still be seen as targets of opportunity, so park appropriately." Now, I have a link in the notes I'm not going to dig deep into, but it is very disturbing, about the onboard diagnostics. This was a presentation that Rob Vandenbrink gave to a SANS group, a SANS security presentation at SANSFIRE 2012. Turns out that there is a set of standards, international standards for the networking technology that is across all cars. It is a CSMA/CD, the standard sort of Ethernet Carrier Sense Multiple Access Collision Detection, which there are lots of tools for, that uses a serial protocol at, well, I think it's like 115K baud. But it's open. It's documented. You can give it commands. It tells you whatever you ask it. And it's ubiquitous.

So when I hear you say, Leo, that Ford is really, really, really taking this seriously, I'm glad. And I have said to people, I'm glad I have an older Beemer" that doesn't have any of this stuff in it because I don't want it. Not probably ever. But that's just - it's a better way to operate. We're going to - apparently we're going to learn these lessons all over again. So, I mean, like for example it's mandated that all new cars have to have tire pressure transmitting sensor systems, and that's RF, and that's a way into these systems because people that have engineered them haven't been willing to spend a lot of time, and they've been in a hurry, and same old routine again on our cars, which are becoming rolling networks, essentially, of small computers. So I have a feeling we'll be talking about these things in the future. And I'm glad Ford is really taking it seriously.

In a surprising development, Google has added the DNT technology to the latest developer build. Do Not Track will be in Google's Chrome browser by year's end. Google's spokesman Rob Shilkin said that the Obama administration had asked the entire industry to adopt the Do Not Track technology, and Google was complying with that request and the consensus that arose around it. There was sort of a - I kind of got this sense, reading the whole thing, they weren't that happy about it. But they were the last browser without it. So they decided, okay, we'll put this in and let our users decide.

Okay. A bunch of people tweeted this. And we'll have details probably next week. Do you remember, Leo, a couple years ago, that there were two hackers, one of whom was on the beach in Indonesia, communicating with a friend of his. I think we were imagining him sipping on umbrella drinks while he was reading the TLS CBC at RFC.net.

Leo: I remember that, yeah.

Steve: That was Juliano Rizzo on the beach, and his partner Thai Duong. They're back. They were the people who figured out BEAST, which was the Browser Exploit Against SSL and TLS. That was a man-in-the-middle attack which they crafted by taking advantage of a weakness in the cipher block chaining, which is CBC, employed in SSL, in order to crack into secure connections. So they now have a new attack called CRIME. That stands for Compression Ratio Info-leak Made Easy.

Leo: That's a retronym.

Steve: Compression Ratio Info-leak Made Easy. And I love it because what that says is that this is a classic side-channel attack. They've come up with a way, and it's not public yet, they're putting their paper out today, tomorrow, and Friday, that is, September 19, 20, and 21, at this year's Ekoparty in Argentina. They said that the new attack works much like the BEAST attack. Once they have a man-in-the-middle position on a given network, meaning that they're inline in the communications path, they are able to sniff HTTPS traffic and launch the attack.

Their current implementation requires JavaScript running in the browser. Rizzo was quoted, Juliano was quoted saying, "By running JavaScript code in the browser of the victim and sniffing HTTPS traffic, we can decrypt session cookies." Now, we all know what that means because session cookies are the way persistent authentication is created in browser-client sessions, so that allows impersonation. That's much like what Firesheep was doing with Firefox some time ago. So "...we can decrypt session cookies. We don't need to use any browser plug-in, and we use JavaScript to make the attack faster, but in theory we could do it with static HTML." Rizzo also said that both Mozilla Firefox and Google Chrome are vulnerable to the attack. However, the browser vendors have developed patches for the problem that will be released in the next few weeks.

Now, I saw elsewhere in researching this that browser vendors have stated they're no longer vulnerable. So I don't know who's right. But any browsers that support either TLS compression, which is a standard, or Google's SPDY - SPDY, of course, offers compression, as well. Basically what these guys are doing, we've talked about side-channel attacks on crypto. The idea is by changing the data being sent, or sending their own, with and without compression, the content is leaked by the amount of compression it gets.

So, for example, we know that completely random data won't compress much, or at all. Pure entropy, absolutely random data, there's no pattern that a compressor can use in order to represent the same thing more densely. On the other side, a string of 10 A's takes up a lot of space unless you encode it as there will be 10 A's following, in which case it compresses extremely well. So the point is the ratio that you get of compression is set by the contents. So by tweaking the contents, it must be that these guys are looking at the difference in compression and then reverse-engineering what the unknown data is by subtracting out what is known. So a very clever attack. I'm guessing about most of this, but that must be, if they're called it Compression Ratio Info-leak Made Easy, that's what it would have to be.

Now, you need TLS compression or SPDY in this HTTPS link. So that would require support at each end. Both are still relatively rare. Some guy said, I read, "My calculator doesn't have enough zeroes to the right of the decimal point for me to tell you what percentage of traffic on the Internet is subject to this attack at the moment. Meaning it's too far off to the right.

Leo: Nothing, yeah, zeroes.

Steve: Nothing. So not a big problem, nothing to worry about. If anyone is worried, and you're a Firefox user, you can disable SPDY by putting "about:config" in the URL address and then hitting Enter. That brings up the massive configuration settings for Firefox. And then in the search bar put in "spdy," and that'll give you a nice little block of settings. And I found mine said network.http.spdy.enabled=false and .enabled.v2 is false and .enabled.v3 is false. So I had mine all turned off. I don't remember why. I think because there were some concerns about it earlier.

Leo: You were worried, probably. You had talked to Mark Russinovich, maybe.

Steve: Yeah. So anyway, I will probably have confirmation that this is the problem. It doesn't sound like a bad attack. I will try to determine what's going on here between one story that says the browser vendors will soon have this fixed and then others that say they already have had it fixed. My Firefox hasn't updated recently. I'm 15.0.1, which is probably current. So maybe that had it fixed, or maybe that's why I've got SPDY turned off. Maybe that's what the point of 0.1 was, because mine was all off. So maybe other people will find that, too. We will see. And I don't know how you fix this. Maybe you pad the compression with pseudorandom data so that it's not deterministic. That would block this. Anyway, we'll see what they suggest. But again, this is a very clever hack using the fact that different data compresses by a different amount to reverse-engineer the unknown portion from what is known, which must be what they've done.

And finally, before we get into a quick little bit of miscellany, our old friend John Graham-Cumming was in the news with his most recent blog post: blog.jgc.org. Our listeners will remember that we had John on about his neat techie book of interesting wacky tech locations scattered around the globe. And John has been a participant over at GRC's newsgroups for years. And what happened was there's been news, I haven't been talking about it a lot because it's sort of always in the background, of the depletion of the IPv4 address space.

One of the Twitter feeds I monitor is a big - unfortunately it shows a big atomic bomb mushroom cloud glowing red to remind us that we're running out of IPv4 space. And there was a recent announcement that in Europe the last one was gone. They were down, I think it was that RIPE was down to one final network. And rather than giving people huge allocations, they were now giving them a thousand, like out of the 16 million IPv4s in this remaining /8 network. So being very, very stingy about them. And John somehow said, uh, you know, what about 51.0.0.0/8, the 51-dot network? What's going on there?

Leo: Who owns that, Steve?

Steve: It's registered, yeah, it's registered to the U.K. Government Department for Work and Pensions.

Leo: I saw this.

Steve: And, you know...

Leo: How many addresses is that, Steve?

Steve: That's 16+ million addresses. And they're not - they say it's in use. But it's not public. So they're using it like a 10-dot network. They're using it as their own privately routed nonpublic sort of LAN in the same way other large organizations use 10-dot. It's exactly the same as a 10-dot. I chose to use 10-dot for myself, although I hardly need 16 million IPs. And they're saying, well, we like - we want to keep it. And so...

Leo: No.

Steve: I mean, they can't. It's like, it's wrong. They're saying, well, 80 percent of it is in use. Okay.

Leo: Just replace it with a router. I'm sorry.

Steve: Well, all they have to do is change the 51 to 10.

Leo: Yeah.

Steve: All they have to do. I mean, yes, many times. But still it is a publicly routable block that is not being publicly routed. Well, John, as we've talked about before...

Leo: This is like some sort of spy agency or something; right?

Steve: Well, he launched - remember that he launched the petition to get Turing's reputation, like, fixed because...

Leo: And won. He got an apology from the Prime Minister, yeah.

Steve: Yes, yes, a formal apology over the way they had been treating Alan Turing - posthumously, obviously. Well, he's launched another one. There is now a petition in the works to bring to light and to bring pressure on - I'm sure that he's not real popular with them right now - to bring pressure on this Department for Work and Pensions to give up their 51-dot, huge, I mean, okay, that's one - that's more than one 256th of the entire Internet. So is it 16 million, or is it more? It's going to be 2^24.

Leo: Oh, that's a lot.

Steve: Yeah, that's more than 16 million. That's two to the - I think I was doing - well, no.

Leo: That's trillions, isn't it?

Steve: No. 2^24, okay. Here's a little math. Oh, yeah, I was right, 16 million.

Leo: 16.8 million.

Steve: So that's a huge block. And they can't keep it because it is...

Leo: It's needed.

Steve: Yes, we need it. And it's not, well, I mean...

Leo: And they don't need it.

Steve: As soon as it - exactly. They're not using the public routability of it. They're using it like a private network, their own little private network. All they have to do is change all of those 51s to a 10, and everybody will be happy.

Leo: It'll be a little messy.

Steve: Be a little messy.

Leo: But that's all right. I wonder if there are other blocks like that out there. Do you think? Do we know? Because that's just such an egregious example.

Steve: I know that HP had, like, it had 14 and 15, even recently. And but maybe they can make a convincing case for their using it. So I just wanted to make a little miscellaneous category. "Revolution," the new J.J. Abrams future power outage global sci-fi series started on Monday, and the jury is out in my case, in my instance. I read a couple very negative reviews. I'm less negative about it. We'll see how it turns out. It's too early to say.

Leo: I like the premise. I love dystopian future, the world is, you know...

Steve: Yeah. The acting seems fine. The people are interesting. We were teased at the very end. I mean, there is a definite, okay, what is going on...

Leo: Kind of Hunger Games-y in the plot, it seems to me.

Steve: Yeah. Yeah, that's a very good point.

Leo: Somebody said, hey, that "Hunger Games" movie, that's real big. What can we do that's like that? What have we got in the bin?

Steve: Yeah. Hey, J.J., you know...

Leo: Hey, J.J., can you crank something out?

Steve: Yeah. And lastly, for anyone who is interested in what we've been talking about recently in multifactor authentication for their own websites, I ran across an implementation of Google Authenticator written in HTML on GitHub.

Leo: What?

Steve: Yes.

Leo: Wow. JavaScript or HTML? Must be JavaScript.

Steve: Don't know what it's in at that end. But probably if you Google "html5-Google-authenticator," or maybe not even put the dashes, and it is at GitHub, you'll find it. And I just thought it looked nice. And so anyone who's interested in dropping that into their own website to allow for Google Authenticator-compatible authentication...

Leo: Wow, that's awesome.

Steve: And I'm sure we're going to see a lot of that. But I just wanted to point our listeners at it.

Leo: That's neat.

Steve: Yeah.

Leo: That's it?

Steve: That's it for today.

Leo: That's all she wrote?

Steve: That's it for today. That's our news. And we had Mark.

Leo: That was great.

Steve: And we will do Q&A next week. So by all means, if you've got any questions, GRC.com/feedback.

Leo: If you're just tuning in late, go back and listen to the beginning of the conversation. And Mark will be back for Windows Weekly tomorrow, which is a coincidence. But I have a feeling we'll talk more about Windows. I don't know. Maybe we'll talk about the books. I don't know. Don't know.

Steve: And I'm jealous he's going to have a good microphone for that, for Paul's podcast.

Leo: Yeah, thanks, Lou. Lou's running it over from the other side of the campus. Steve is at GRC.com. That's where he keeps SpinRite. He hides it there, the world's finest hard drive maintenance and recovery utility. Hey, the Ford Motor Company has 19.0.0.0/8, according to Sidera.

Steve: Wow. I wonder about these companies that have such massive, I mean...

Leo: Well, they have a lot of employees, and they're all over the world. But do they need it publicly routable, is the question.

Steve: Yeah, exactly. And once upon a time it was easy to do. I mean, we're going to go through a period of anxiety. The rebuttal, not surprisingly, from the U.K. group, this U.K. Government Department for Work and Pensions, their rebuttal was, hey, IPv6. That's what it's for. Go use that.

Leo: Right. Yeah. Well, they're right. I mean, we need to move.

Steve: Yeah. Sooner or later we won't have...

Leo: But we don't need them to kick us in the butt to do it. I mean, come on, guys.

Steve: And then the question is, in order for an organization like HP or Ford to give up their IPs, first of all, Leo, you are 100 percent right. They do not need publicly routable IPs. I mean, really only servers need publicly routable IPs. Everybody else can come out of a smaller pool of NATed IPs, which is, for example, what ISPs are doing now, which is what we all do in our home networks. We've got one IP publicly, and a bazillion inside our homes. So that scales in a hierarchy beautifully.

Now, of course there are Internet diehards that are - hopefully they're not dead yet, I was going to say turning over in their graves to hear me. But they're, like, moaning because they bemoan the whole notion of NAT. The original purist concept was one IP per machine, and every machine will be accessible by every other. Yeah. Well, that was before firewalls and before nation-state-supported crime rings of very, very good hackers began to happen. But my point was, if a company did want to give up some of their excess space, what they would need to do would be to move their allocation all - sort of compress it to one end of their network block. Essentially, they would, for example, if Ford was - was it 17? Don't remember what number it was.

Leo: Yeah, what number, yeah.

Steve: Anyway, I know that HP, for example, has 14 and 15. If you took - or say the U.K. Department for Work and Pensions. They've got 51.0.0.0. There's no way they have, they need 16 million IPs. They couldn't have 16 million machines in the

Department for Work and Pensions, no matter how bloated their bureaucracy is. So all they would have to do would be to move those, if they didn't want to switch to 10-dot, move them all to one end. So that right now, for example, there might be 51-dot, and then rather than 0, they might be using 0 and 1 and 2 and just sort of have come up with a very, oh, look, we've got 16 million IPs, we'll use 51.1 for this location, 51.2 for this location 51.3 for that location. And the idea being that, if the squeeze that down so they're only using, for example, 0, then that would free up 51.1 through 255. And they could keep their little 51.0 network, which is a small fraction of the total 51-dot Class A network.

They would essentially have a Class B network. And that would be a compromise. It would free up the bulk of their allocation. And of course that scales. They might have 51.1, .2, and .3, but be able to cram all of their allocation down into, like, three Class B networks. And then, again, release their allocation for the balance. So I think we're going to see some back-and-forth and some tension as people resist the move to IPv6 just because it's not easy. It does require equipment and firmware and routing upgrades and so forth.

Leo: General Electric has 3.0.0.0/8.

Steve: Yeah.

Leo: IBM uses 9.0.0.0/8 for internal IPs, supposedly. So there's a few out there.

Steve: Yeah, well, but once upon a time, Leo, 4 billion. We're never going to use 4 billion.

Leo: We're not going to use all those. No sirree. Steve Gibson is at GRC.com. That's where SpinRite is, and of course your chance to ask questions for next week's episode, GRC.com/feedback/8. No, no /8. He also has lots of free stuff there, including SpinRite, the world's - oh, I said that. Oh, ShieldsUP!, Shoot The Messenger, DCOMbobulator, all those other free things. Password Haystacks, all of that stuff. GRC.com. And 16Kb versions of this show in audio for the bandwidth-impaired; text versions, transcriptions by the great Elaine. We have the video and the high-quality audio over at our site, TWiT.tv/sn. But you're still putting show notes at your site, right, Steve? GRC.com?

Steve: I have not been doing show notes.

Leo: Oh, okay. Okay.

Steve: For a long time.

Leo: We'll get our wiki guy on it. We'll get him up to date.

Steve: That would be great. And the transcripts that we have really come in handy because, as I was reading about the new CRIME attack, the Compression Ratio Info-leak Made Easy, I thought, Juliano Rizzo. Wasn't he on the beach somewhere developing the...

Leo: And the nice thing is it's text search; right? That's the...

Steve: Yeah. So, like, I went to GRC.com/sn, which bounced me to /securitynow.htm. I put - I think I might have put "beach" into the search box, and up came...

Leo: Lo and behold.

Steve: Oh, no, I think I put "Rizzo" in because I knew his name. And sure enough, there were three hits on that, and one took me to Elaine's transcript from the time we were talking about the BEAST attack.

Leo: Fantastic.

Steve: So it's easy to find those things here.

Leo: All right. We're going to sign off. Coming up, This Week in Google, Jeff Jarvis in-studio with us. We will see you next Wednesday, 11:00 a.m. Pacific, 2:00 p.m. Eastern time.

Steve: Yup, for a Q&A.

Leo: A Q&A. Steve Gibson. Thanks for joining us.

Steve: Thanks, Leo.

Leo: See you next time on Security Now!.