SECURITY NOW!

Transcript of Episode #659

Never a Dull Moment

Description: This week we discuss AMD's release of their long-awaited Spectre variant 2 microcode patches, the end of Telegram Messenger in Russia, the on-time arrival of Drupalgeddon2, Firefox and TLS v1.3, the new and widespread UPnProxy attacks, Microsoft's reversal on no longer providing Windows security updates without AV installed, Google Chrome's decision to prematurely remove HTTP cookies, the Android "patch gap," renewed worries over old and insecure Bitcoin crypto, new attacks on old IIS, a WhatsApp photo used for police forensics, and an IoT vulnerability from our You Can't Make This Stuff Up department.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-659.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-659-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here with the latest from Drupalgeddon2, the Telegram fiasco in Russia, TLS 1.3, and why you've got to turn off UPnP on your router. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 659, recorded Tuesday, April 17th, 2018: Never a Dull Moment.

It's time for Security Now!, the show where we protect you and your loved ones online through the good auspices, the good offices of Mr. Steven "Tiberius" Gibson, although I might now want to call you "Dr. Smith."

Steve Gibson: Oh. We have that in the show notes.

Leo: We'll be talking about that, I'm sure.

Steve: That's right.

Leo: Steve is the guy in charge of GRC.com, the Gibson Research Corporation. I guess that's the eponymous Gibson Research Corporation. He's also the master in charge of SpinRite, the world's best hard drive recovery and maintenance utility. And for the last 10, 11, 12 years he's been filling us in on what's going on in computing. Hi, Steve.

Steve: Hey, Leo. Great to be with you again. Elaine had a question from last week's audio because I guess I made a comment that SpinRite was - we were talking about bugs and updating, and I said SpinRite was...

Leo: Bug-free.

Steve: I said, like, 14 years old. She immediately put her brakes on because she's listening to all this, she says, wait a minute. Isn't it, like, 30 years old? And so, well, what I meant to say was SpinRite 6.0 was completed in 2004, and so here we are in '18, and we're getting ready, I'm getting ready, of course every one knows, to start returning to and moving SpinRite 6 forward as soon as I get SQRL put to bed. But so it was SpinRite 6.0 that is 14 years ago it was published. And much like the DNS Benchmark, really I was talking about the DNS Benchmark and how I had updated it for the first time in 10 years because I finished it in - its last update was in '08 when I finished it. So anyway...

Leo: Yeah. You're saying the current version of SpinRite is that old.

Steve: Yes, exactly.

Leo: Which is remarkable for any software.

Steve: Exactly. And I didn't have any - there was, like, lots of news. I mean, like lots of news. So it's almost a good thing, a blessing that there was no one huge, dominant, take up half the podcast story because then we wouldn't have been able to get to everything. And there was just lots of interesting things. So I called this episode 659, I just labeled it "Never a Dull Moment."

Leo: That's the truth.

Steve: And, boy. So we do have AMD's release of their much-anticipated and somewhat long-awaited, although hopefully they won't stumble out of the gate the way Intel did, their microcode updates for the Spectre variant 2 problem, which cannot be fixed without hardware fixes in the processor by the operating system working in conjunction with the processor, so that just happened. We have some details about the very messy end of Telegram Messenger in Russia that we've been tracking for the last few podcasts.

The on-time arrival of Drupalgeddon2, I mean, it happened exactly as we anticipated it was going to. And so we've got that. Also Firefox and TLS v1.3. A new and widespread UPnProxy is what Akamai is calling these attacks. Microsoft's reversal on its no longer providing Windows security updates without AV installed policy, which they announced at the beginning of the year, I mean, I remember, we were all like, what? What? So the idea, well, we'll talk about that in a minute. Google Chrome has made a decision which they announced to start as of October, which would be Chrome 70, to prematurely remove HTTP cookies, which is...

Leo: What?

Steve: ...understandable, but, I know, kind of controversial.

Leo: How do you do that, yeah.

Steve: Yeah. So we've also got the so-called "Android patch gap," where Android OEMs have been discovered to be lying about how well patched their phones are. A renewal of worries over old and insecure bitcoin crypto. New attacks on old IIS. A WhatsApp photo that was cleverly used by police for forensics. An IoT vulnerability straight from our You Can't Make This Stuff Up department, and more. So, yes. As I said, never a dull moment.

Leo: Yes. So, yes, he says.

Steve: And some miscellany and a fun note, not a testimonial about SpinRite this week, but someone who's been trying, he was waiting to give one, and finally he got tired of waiting. So anyway, lots of fun stuff.

Leo: You know, sometimes the best testimonial is "I don't really ever have to use it. I just - everything works."

Steve: That's actually kind of what he said. It's like, okay.

Leo: Yeah, haven't needed it. I just SpinRite ahead of time, and everything's good.

Steve: That's right.

Leo: All right, Steve Gibson. I'm going to get the remote control out and turn your brightness up a little bit because you need every bit of it.

Steve: Yeah, I'm a little dim today.

Leo: You need every bit of brightness you've got today.

Steve: A little dim.

Leo: For those not watching the video, Steve's on a big screen, I feel like it's a Star Trek view screen behind me. We've got to...

Steve: Yes, over your left shoulder.

Leo: Yeah. We've got to give him some brightness. Go ahead. You can talk while I brighten you up.

Steve: Ah. Well, so anyway, yes, thank you. Our Picture of the Week is actually about a story we will get to in a little bit, this UPnProxy. But I liked it, this was part of the report that described this particular exploit. And what's happened is that this is fiction meets reality. How many times have those of us who are tech savvy sort of rolled our eyes when the plot of the cyber whatever it is involves the bad guy bouncing around the world and looping around and bouncing off of 19 servers, unquote, whatever those are supposed to be, before making the final connection, and consequently that's a big plot glitch is, oh, there's no way we can track him down because they routed through 19 other locations all over the world. Well, that got a lot easier.

And this picture from this report that we'll be covering in a second shows an attacker, location unknown, connecting to a virtual private server that then hops through three so-called "proxy routers," which anyone looking at the picture will sort of recognize as, oh, I have one of those on my shelf. And that's exactly the point is it turns out that something that we have long warned of, it was our Episode 358 or something. I have it in the show notes, and we'll get to it a little bit later. We warned our listeners to turn this thing off. Well, it's now being abused widely to turn individual SOHO, you know, Small Office Home Office routers, regular residential consumer routers, into basically sort of the grand central of bad guy traffic.

So I thought this was a great picture because it demonstrates that, yes, what once was sort of fanciful and it's like, okay, well, maybe super advanced hackers could pull this off, but it's not really going to happen in the real world, no. Now, I mean, you, too, can do this from the comfort of, I guess, your couch, or your mother's basement, or wherever you happen to be. So anyway, sort of a fun picture we will get to.

And Leo, for the first - this actually, I was going to number this zero, except we don't have zero - our show notes items are not numbered. But it actually, believe it or not, is the case today, April 17th, I guess as a consequence of the fact that April 15th fell on a Sunday, that must be why...

Leo: Yeah, and Monday was like Emancipation Day in Washington D.C. So it'll be Tuesday, yeah.

Steve: Ah, okay. So in the U.S., for those who are not in the U.S., our so-called Internal Revenue Service, the IRS, this is our tax filing deadline date for the 2017 calendar year. And one of the headlines I got a kick out of said that the IRS's e-filing system is - wait for it - "overtaxed."

Leo: Ha ha. That just sounds like a clever headline writer because what I saw was that the IRS didn't know why it wasn't working.

Steve: They don't, no.

Leo: So it may not be overtaxed. It may be something else.

Steve: Under attack, yes. Yeah. So basically our U.S. e-filing system, which one would expect to be heavily used, has not been working well all day. And as we know, it is extremely difficult nowadays to keep a system online for which there's any reason for bad guys to want to have not be online. There are so many ways now with DDoS amplification attacks and the ready availability of things that can attack in order to launch these attacks, that, I mean, as we've been talking about...

Leo: Could be some 15 year old in Columbus, Ohio; right?

Steve: Yes, yes. It doesn't have to be a nation-state mounting an attack against the IRS in the U.S., and probably isn't. It's just somebody who says, hey, you know, this is the time that lots of people are going to be filing their taxes at the e-filing website. So let's just take those guys offline. And if that's the case, I mean, we don't know. But I guess some IRS person was giving testimony in front of Congress, not a big high-profile issue, just some meeting somewhere, and one of the congresspeople said, "So, do you know that the e-filing system is offline right now?" And he's like, "Oh, well, yes, we're looking into that, and we expect it to be back up later today." Which apparently they have no idea what's wrong. Oh, and the other...

Leo: It's been eight hours, at least last time I checked.

Steve: Yes. And it says that it's a "planned outage."

Leo: No. That's not true.

Steve: No, no, I saw a screenshot.

Leo: That seems stupid, if you plan an outage on tax filing day.

Steve: Wouldn't that be bad planning?

Leo: Oh, man. I wouldn't put it past them.

Steve: It literally said "April 17, 2018 Planned Outage." Which basically means it wasn't planned, but the message was planned to appear and declare that it was planned.

Leo: Unbelievable.

Steve: So, yeah.

Leo: Unbelievable.

Steve: Clearly not planned.

Leo: We didn't plan this.

Steve: Okay. So we have AMD having last week published the updates for microcode for all of their chips since 2011. So that's dating back to - you know how everybody's got these code names for their chips. These are the first Bulldozer core products introduced in 2011. So from Bulldozer on there are now somewhere - which isn't to say that it's actually in anyone's ADM chips yet, but supposedly. So those patches are available. They were supposed to be released last Tuesday for the Windows 10 v1709, the Fall Creators Update, which is where we still are, the most recent official version of Windows 10. And do you have news, Leo? Because I know you and Paul and Mary Jo were talking last Wednesday about when the Spring Update, whatever it was going to be called, Spring Creators Update?

Leo: Well, so one thing, first of all, it doesn't have a name. It's 1803. The other thing is that Paul and Mary Jo said, you know, no one at Microsoft said it was going to be Patch Tuesday. Everybody just assumed it was going to be Patch Tuesday. So Microsoft never said it's coming out then. So they're not late, in other words.

Steve: Right.

Leo: Although they did say there is...

Steve: There was no promise made.

Leo: There was a delay. Its internal code name is Redstone 4. And according to Paul, the last time I saw, they've put out a new RTM. They don't like to call it RTM, but they put out a new RTM for it.

Steve: A hopeful RTM.

Leo: Yeah, hopeful RTM. And so it'll be soon. It'll be soon.

Steve: Okay. Well, so aside from that, it was supposed to be the case that last Tuesday's Patch Tuesday existing version of Windows 10, which is 1709, that that added the mitigations and the Spectre variant 2 for the AMD chips. Which is to say they had provided those to Microsoft. And just as Microsoft has incorporated the Intel microcode patches into an earlier release of Windows, that was supposed to have been done for AMD. Now, I have a laptop with - and I forgot what it was now. It's an AMD 64, something 5,000, M45000, I don't remember now what it was. But I think it was only, like, 2013. So I would have expected it to be swept up in that.

I did the update. I checked, and it's not showing this as fixed. However, there are developer guidelines now that have also been published which enumerate the changes in the chips, the CPU ID bits, which can be queried to determine whether it's got the updated functions. So the point of all this is that probably tomorrow I will, as I have been recently, return to InSpectre and add support for these new functions which are now documented in the developer docs, which will allow my InSpectre app to tell users whether their chip has been updated. And presumably Microsoft won't update the firmware unless they're also updating the Windows OS to support it.

So anyway, I guess it was last week that we talked about the final, for Intel, on the Intel side, the final list of CPU IDs which had Intel's updates and, controversially, those that did not. And I did then rev InSpectre to Release 8, which it is now, with knowledge of that. So there's another line in the little summary screen at the top of InSpectre telling you whether microcode updates are available, which is different from whether they are actually in effect for your chip. So that allows you to see whether there's hope if you're on the Intel side. And I haven't yet found the same thing from AMD. I'll see whether they've got, by CPU ID, a list of which ones do and don't have those available.

What I do have now is the ability to determine whether it's actually in place or not in the hardware. So I plan to be updating InSpectre, it would probably be Release 9, to incorporate that additional information. So for what it's worth, AMD is finished that. They did it all at once. It's supposed to be from Bulldozer on, which was 2011. So Microsoft will probably be incorporating those. Oh, I'm sorry, Microsoft has said they did, although I haven't seen it. So hopefully I'll get some tweets from people saying, yeah, ever since last Tuesday, InSpectre has been saying that my system is all patched against the Spectre variant, although I haven't seen that. I haven't looked actually since. So I will.

But remember, separate from this, we still have the Ryzenfall, Masterkey, Fallout, and Chimera vulnerabilities which came to light last month. Those are considered less dangerous and not as big a problem, but those are yet to be dealt with by AMD, who has at least acknowledged them and said that they would be getting to it. So, progress. And hopefully on the Windows side those using systems that are no older than about seven years and who are using a recent enough version of Windows that Microsoft will patch them, we'll be able to get those microcode updates. So, yay.

We've been tracking, because it's sort of interesting, for the last few podcasts the fate of Telegram in Russia. As we know, Russia said we're not going to allow any encryption that we cannot decrypt. Telegram said, sorry, we're not going you the keys to the kingdom. Russia went through several rounds of various court actions in order to make this compulsory. Telegram stood their ground, said sorry, nope. And so Russia then late last week got the final machinations finished to require that Telegram get blocked. That is, Telegram's domains. Apparently in an effort to - and I guess it's sort of they were playing cutesy because, I mean, this is a losing battle on Telegram's part. They moved, Telegram moved a bunch of their IPv4 IP addresses deliberately into net blocks being used by Amazon's AWS and Google's cloud platforms. As a consequence, Russia, using a rather blunt instrument, blocked 15.8 million IPs...

Leo: Oh, man.

Steve: ...on those Amazon and Google cloud platforms.

Leo: Oh, lord.

Steve: Yes. And I have them in the show notes. I mean, it is a massive block. So in network terminology, if you have a network with a /16, that says that the high two bytes is the network, and then the low two bytes are typically .0.0, meaning that all addresses with any of the lower two bytes are part of this block. Well, this isn't quite that bad. It's a /15. But there's three /15s and a /14, meaning that basically four different networks, each one being specified by two bits plus the highest order bit of the third byte, have all been blacklisted. That is, just blacked out.

So that ends up being 15.8 million IPs. Which, unfortunately, because many, many, many other Amazon and Google services were occupying this huge region of IPv4 space, all kinds of Russian retailers and non-Telegram services, credit card processing, it just created a huge, I mean, and is still a huge upheaval. There's been a tremendous - this happened yesterday. And so it's been a tremendous problem in Russia because they were just going to say no, we're not fooling around here. We're blocking all of this.

So in addition, Russia's telecommunications regulator asked Apple and Google to pull Telegram from their app stores, you know, iOS and Android. They said pull the apps. They also requested the side-loading site APK Mirror to cease serving Telegram, which would probably be the first alternative for Android users should Google comply, as I would imagine they would, and pull Telegram from the Play Store, if they can do so for Russia's view of the Play Store. And also the telecommunications regulator for Russia also urged VPN providers to prevent Telegram messages from getting through.

So right now there's a mess over there. I don't know what Telegram's position will be. I mean, they ought to just give up. I mean, they should have seen the writing on the wall. There was some comment that I encountered where Telegram said, well, they're considering doing a peer-to-peer messaging system, but no time has been set for that happening. And The New York Times in their reporting noted that the ban on Telegram would put the Kremlin in a slightly awkward position because many inside the government, including those in President Vladimir Putin's press office, use Telegram themselves. So Russia's Foreign Ministries announced its intention to move over to the Viber messaging app. Viber claims that it is completely encrypted, as well, but presumably not so much. Or I don't know, maybe we'll go through the same dance again. But it's been interesting to watch this.

As we know, this happened with Telegram in China, where Telegram is now blocked in China. Now it's happened in Russia. And the problem is that someone trying to run a service in direct opposition to the government that controls telecommunications within that space, they're going to lose that battle. So I guess I'm somewhat at a loss to understand what Telegram thought they were doing except just it's not expensive for them to fight Russia, so I guess they've decided, well, we'd rather fight than just go quietly. So, fine. Still, Telegram is gone from Russia, essentially. Unsurprisingly.

And we've also been following from the start what has been called "Drupalgeddon2." Remember that Drupalgeddon1 was a very bad SQL server exposure that Drupal suffered years ago. Now we've got essentially what is regarded as a 25 out of 25 in the NIST's ranking, so the highest level of critical rating. Remember that they gave a one-week notification, the Drupal team did, one-week notification that on a Wednesday they were going to be making public the details of patches for both the 7 and the 8 series, as well as the 6 series of Drupal, even though it had long since stopped being maintained because there were still some version 6's on line, and this was that bad.

So the problem with patching is, especially with something like Drupal, where it's possible to analyze it and figure out what was done, is that the next day, the day after, on Thursday, Check Point Research came out with just, I mean - and it wasn't like any great explosion of surprise. They said, okay, here's what happened. Here's what was done. Since it was patched, it was in the public. It was available to everyone. And so that produced full details. Immediately afterwards GitHub began hosting proof-of-concept demonstrations. And now many security outlets are reporting that Drupal sites are 1000% predictably under attack.

So we have a remote code execution, an RCE for unpatched Drupal 6, 7, and 8. So essentially, if you've got a server running Drupal, and you haven't patched it, it's going to get found, and it's going to get taken over. Probably you'll notice that it starts running really slowly because what people want to do these days is run crypto mining, cryptocurrency mining on a strong Internet-connected machine. So if you start noticing things start going slow, you need to deal with it.

What we know now is that Drupal had insufficient input sanitation on Form API, so-called FAPI, AJAX requests. And as a result, an attacker was able to inject a malicious payload into the internal forms structure, which would have caused Drupal to execute it without any sort of user authentication. And so by exploiting this vulnerability an attacker would have been able, and can, is able, if you haven't patched 6, 7, or 8 in the last couple weeks, to carry out a full-site takeover of anyone using Drupal.

So on last Friday, the day after this Thursday announcement that this is happening, in what they considered a public service announcement, and this of course was Friday the 13th, which really was for these guys, Drupal published: "This Public Service Announcement is a follow-up to" - and then they've got the number of a previous release - "Drupal core RCE (Remote Code Execution). This is not an announcement of a new vulnerability. If you have not updated your site as described in" - and then again the original announcement - "you should assume" - get this. This is Drupal saying: "...you should assume your site has been targeted and follow directions for remediation as described below.

"The security team is now aware," Drupal writes, "of automated attacks attempting to compromise Drupal 7 and 8 websites using the vulnerability reported in" - and again, this is SA-CORE-2018-002. "Due to this, the security team is increasing the security risk score of that issue to 24/25." I don't remember what it was, but obviously a little lower than that. Still, like right at the ceiling. "Sites not patched by Wednesday, 2018-04-11" - so that was the Wednesday a week before - "may be compromised. This is the date when evidence emerged of automated attack attempts." That is, the same day the patch was announced.

"It is possible targeted attacks occurred before. Simply" - and then here. "Simply updating Drupal will not remove backdoors or fix compromised sites. If you find," they write, "that your site is already patched" - I had to do a double-take on this one. "If you find that your site is already patched, but you didn't do it, that can be a symptom that the site has been compromised." Meaning that the attackers are closing the back door behind them after they already get in to keep anybody else from coming in and pushing them out.

"Some attacks in the past have applied the patch as a way to guarantee," Drupal writes, "that only that attacker is in control of the site." So it's hard for me to imagine that somebody listening to this wouldn't have also been listening to both of our previous two podcasts where the urgency of this was made very clear, even when it was still a week away from being known. But somebody would have been very ready.

So what they are reporting is that it looks like these automated attacks are closing the backdoor behind them, patching this so that they alone are there. Therefore, if your site appears to be patched, and you didn't do it, that's additional reason to worry. And I don't know for a fact that they're installing cryptocurrency mining. But that's what people are doing these days. So if you suddenly see that your CPU utilization has jumped up, that's a good reason to suspect also that this has happened.

So this unfortunately is now the model for vulnerabilities being discovered on the Internet. It was discovered. They got the patches ready. They preannounced to everyone, get ready for a patch for which we expect to have exploits immediately follow. That happened. The exploits happened. Now they're underway, and sites are being taken over. So I hope, if by any chance you are a Security Now! listener and you skipped a couple weeks of announcements, and you somehow didn't already know that your Drupal site needs to get patched, don't wait any longer.

Leo: And assume you've been hacked.

Steve: And, yes, you really do. At this point it's not difficult to find you, to check your version and to insert an exploit, if the backdoor hasn't been closed by somebody already beating somebody else in. Yikes.

So I performed the following test just now, this morning, in preparing these notes, and it all works. Firefox has begun bringing up support for TLS v1.3, but not enabling it by default. This is a very cool thing for any Firefox user. SSLLabs.com is Ivan Ristic's very cool SSL, now TLS testing facility. We normally talk of it in terms of testing sites, that is, testing like GRC.com, Google.com, Apple.com, whatever, Amazon.com.

But the second item on Ivan's testing menu is check your browser. You can also use SSLLabs.com as an individual to check the strength of the crypto that your browser is using. When you do it with Chrome, you will find it's already supporting TLS v1.3. When you do it with Firefox, you will find TLS v1.2. So again, that's SSLLabs.com, and then you choose Test Your Browser over on the upper right, the second item down.

So with Firefox - and I updated my Firefox, I'm at 59.0.2, which is the latest, and that was on a Windows 10 machine - you'll see that your browser supports v1.2. Go to about:config, put "about:config" in the URL bar of Firefox and hit Enter. That will give you this huge list of things you can tweak. In the Search area, you can just put in "version.max." That'll weed it right down. I think I had two items in there when I had version.max. And you will see that it is likely set to 3. Set it to 4. That won't hurt anything.

Set it to 4. You don't need to restart Firefox. And if you had opened another tab, like if you just opened another tab to do about:config, go back to the SSL Labs tab, refresh that. And you will now be greeted with the fact that your browser is running TLS v1.3. So just changing, under about:config, and then search for version.max. The whole thing is security.tls.version.max. Change the 3 to a 4, and your Firefox will now be persistently and from then on operating with the very latest version of the Transport Layer Security, TLS v1.3.

So Akamai is calling this UPnProxy, and of course we recognize the first four letters, UPnP. I'm speechless. Years ago we talked about this, and we were stunned that UPnP, that Universal Plug and Play, aka Universal Plug and Pray, protocol which was only ever intended to be a function or a feature on the inside, on the LAN side of consumer routers. And even then it was a worrisome idea. This was Microsoft's solution, essentially for Xbox to be able to make itself available behind a NAT router, the idea being that it was a zero configuration solution. Any time you hear the words "zero configuration," that's when you should start worrying because, if nobody has to configure anything, then the bad guys don't either.

And so the idea was that, with no configuration, for example, an Xbox on your home network would be able to find the router, talk to the router, doesn't need any router admin login passwords or anything. It's just able to say, hi there. I'd like an outside line, please. And the router says, oh, that's why I'm here, and opens up a port or multiple ports, however many the Xbox wants. I mean, essentially, Universal Plug and Play is an invisible, unprotected, insecure, zero authentication protocol that completely defeats the router's NAT firewall, the beauty of NAT being that only outbound connections are allowed, and incoming traffic is only allowed back in if it matches something that first went out. It's just it's a perfect firewalling solution, which Universal Plug and Play completely subverts.

Okay. So it was bad enough, right, when the Universal Plug and Play service was exposed on the LAN. Bad enough. As we covered years ago on Security Now! Episode 389, it came to our attention that many routers had not bothered to restrict it to the LAN, and also had it available on the WAN. Which, I mean, words - there are no words. It's unbelievably insane. So it was so bad that I dropped everything I was doing at the time and added a new test to GRC's ShieldsUP!, which, Leo, you'll remember at the time. I called it "GRC's Instant UPnP Exposure Test." And I want to remind everyone about it so that everyone can make sure that anything that they've done since then hasn't caused this to be reopened for them because there are many routers that currently are still doing this today.

So just go to GRC.com under Services, I think it's the second item in our top-level menu. Under Services you'll find ShieldsUP!, the first thing on that submenu. Select that, say okay, and there's a big orange box that I haven't touched in all these years. Click that, and in a few seconds you will be able to confirm, with everything coming up hopefully green, that your router, wherever you are, is not making Universal Plug and Play service available to the Internet.

Leo: I can't believe that after all these years we still have to tell people that.

Steve: Leo, when you do the test - and you're doing it right now. When you do it, it will show you the count. This morning it was 53,922 open UPnP ports found.

Leo: Wow. Wow. Where is that number? Oh, here it is.

Steve: So click that big orange thing.

Leo: The big orange button, yeah, yeah, yeah.

Steve: Yeah. Click that. And now it's running the test for you. And now it ran the test for you.

Leo: Good news.

Steve: And you're green, doot de doo.

Leo: We're green, look at that. Wow.

Steve: And let's see. So what is it, five...

Leo: That's a lot of open routers: 55,922.

Steve: Okay, same number I had this morning.

Leo: That's good news.

Steve: That's good news. Let's hope that it doesn't increment in the next 10 minutes while the listeners to this live podcast are checking theirs to see what's going on. And I'm noticing an increase in traffic at GRC, so I know people are listening to it and running the test right now. Okay. So here's what's happening. Because there are so many, an unbelievable number of routers exposed, Akamai did a test using their network resources. They have detected more than 4.8 million routers that expose various UPnP services through their WAN interface. That number should be zero. Zero. I mean, it's an absolute mistake. There's no - it's just amazing to me that this is still happening.

And Leo, their whitepaper that I've linked to in the show notes has toward the end a list of routers which are today, as a consumer benefit, they posted the list of routers they have identified which are still doing this. There are a bunch of ASUS routers, unfortunately. And there are some of my favorite Ubiquiti routers, not the one that we've chosen, but some of the wireless routers still have this available. So if you page down through that PDF, Leo, that you've got onscreen right now, you should find, I think, toward the end is their list. They fully document this for anybody who's interested, and then they show the various routers which they have identified which are exposed.

So the point is that, when routers do this, you can normally disable it. You can normally turn off, and it should never be on - it shouldn't even be an option. But hopefully you can turn off Universal Plug and Play on the WAN interface. There is no valid reason for having that exposed. So for some reason a lot of ASUS routers do offer it, frighteningly.

Leo: Yeah, sometimes you need it for outbound traffic. Famously, this was created for the Xbox by Microsoft. That's who made this so that the Xbox could create an Xbox server, and you could play games with people, and they could have inbound access. But that's not WAN access. That's a very different thing.

Steve: Correct, correct. So anyway, I just wanted to make sure. So what's happened is, because there are millions of SOHO routers with UPnP services exposed, and because Universal Plug and Play can be used to create a NAT mapping, not only are you able to map from an inside IP and port to an outside IP and port, you can arbitrarily - basically it's known as packet rewriting. You rewrite the destination IP of incoming packets. Normally they would be rewritten to an IP destination inside the LAN. So, for example, that's where the Xbox would be. And so it would say, ah, packets coming into this port on this router get rewritten to 192.168.1 dot whatever the Xbox is.

You can, however, establish packet destination rerouting to any IP you want. What's happening is these routers are being used to bounce incoming traffic back out. In other words, with enough of these routers, it's possible for a bad guy to do exactly what we see in all of the fictional cyberattack scenarios where traffic is routed around the globe five or six times, bouncing off of proxy servers. Well, this turns SOHO routers into proxies which are able to be used trivially to route public traffic from one UPnP router to another to another to another to another in order to hide the origin of the traffic.

And there's nothing to prevent multiple bad guys from all doing this simultaneously on any given user's router. Meaning that your router with UPnP exposed becomes a little Grand Central Station of malicious traffic, bouncing off of your WAN interface in order to obscure and hide whatever these bad guys are doing. And of course the problem is, when this gets traced back, it gets traced back to you, to your IP or the one you had at the time. So it's better not to have to explain to the authorities that you weren't the one who was originating this traffic. Just better to have this shut down and not have an open router.

So use GRC's quick Universal Plug and Play test to verify that no response is coming from the UPnP service port on your WAN interface. It takes five seconds to do it and know that you're okay. And if you're not okay, then absolutely, I mean, change routers. Update your firmware. Turn off Universal Plug and Play on the WAN interface if that's an option. And, boy, you certainly have my endorsement in scolding any router manufacturer. I don't know what ASUS is thinking. But as I recall from the Akamai document, there was like a huge block of ASUS router models that have Universal Plug and Play exposed, so that can't be a mistake. That's a policy decision, which I just - it makes me scratch my head.

In January of this year, when the Meltdown and Spectre attacks became known, Microsoft gave us the first mitigations to those attacks that they were able to in the January updates for Windows. And somewhat puzzling at the time, and certainly controversial, was their decision to announce, well, the announcement of their decision and the decision that they would no longer update Windows unless a specific registry key was present, which their AV solutions and other AV solutions could create in order to assert that they were not going to crash people's machines, cause blue screens, and so forth. And I remember you and I, Leo, were like, what? Just kind of scratching our heads, and I heard you talking to...

Leo: It was kind of a funky way to do it.

Steve: It's like weird, yeah. And normally, because you had Windows Defender or Security Essentials or something, you were kind of probably going to be okay. But there were instances where Windows 7 might not have had something enabled, and suddenly Windows Updates would stop, and you wouldn't get them anymore ever, or so we believed. Well, turns out that there was a lot of back pressure on this policy, and Microsoft learned that that had not been such a good idea. So, quietly, the March update for Windows 10 happened even if that key was missing. And last week this April's updates happened, even if that key was not present for Windows 7 and 8.1. In other words, that's no longer true now. Windows 10 and 7 and 8.1 are all now ignoring the key, whether it's present or not, and going ahead and doing updates.

Microsoft, of course, now has to kind of backpedal and explain what, what, what? And so now they're now saying, well, we've now been able to verify that no one's AV is actually causing a problem. Or everyone's AV is now no longer causing a problem or some nonsense. Anyway, basically this is gone, and I just sort of wanted to correct, or I wanted to update everybody with where we stood and the fact that this was now happily a non-issue; that everybody, no matter what version of Windows you're using, whether you've got a registered AV or not, you are getting Windows security updates. Oh, and Microsoft said in their notice that this change, in other words, undoing what we did in January, this change has been made to protect user data. Okay, right, yeah.

Okay. So this is a little bit controversial in my mind. Google has announced that, starting with Chrome 70 - which is slated for still a ways away, toward the end of October 2018 - that their Chrome browser is going to begin deliberately ignoring the requested expiration time on cookies delivered to the browser over HTTP. Now, as opposed to HTTPS. In other words, this is another pushback by Chrome using their market dominance and their position to make things more troublesome for non-HTTPS, non-TLS-connected websites. So starting with Chrome 70, any website trying to present a persistent cookie, like a cookie with an expiration date set way in the future, will have it capped at one year. And their longer term plan is over time to proactively reduce HTTP cookie life down to as little as a few days.

So I guess I have mixed feelings. This is clever because it's going to create some inconvenience for sites trying to create statically persistent session cookies so that you can stay logged on without having to reauthenticate and re-log on. Typically that's done with a cookie. And most sites just say, oh, you know, you're logged on until you log off, and leave it at that. They do so by setting an expiration far in the future.

Now, the reason I have sort of mixed feelings is that Chrome is also deliberately breaking the HTTP standard. I mean, they're just saying they're going to deliberately ignore and violate a longstanding standard. So I guess I understand it, but it makes me feel a little queasy. We all remember the danger of HTTP cookies because that's what Firesheep made very famous back in the day when it was easy to - like when Facebook and Snapchat and all the various services were not yet using HTTPS all the time. You would typically use that briefly to log in, to protect your username and password. But then, somewhat paradoxically, they would drop you back down to HTTP, but your cookie was there so that anybody sniffing the traffic could grab the cookie and immediately jump online impersonating you, essentially acquire your logged-in session for their own.

So anyway, I think it's - I wanted to explain this to everybody, to tell our audience that this is something that Chrome has decided to do, probably for the best. But still annoying that they're going to be ignoring this standard. I don't know what kind of timeframe they expect for shortening this to a few days. It certainly will upset people who for whatever reason want to stay with HTTP, want to be able to have persistent sessions with HTTP-issued cookies. They just won't be able to do that in the future for more than a couple days, eventually, apparently. So it'll be interesting to see how this evolves.

A German security firm, SRL (Security Research Labs), did some careful looking at a large number of Android mobile devices, primarily smartphones, and discovered that OEMs of Android phones were deliberately misrepresenting the completeness of patches for their devices. In Android you're able to look at the so-called "security patch level" as a certain date. It's presented as a date. And the clear statement that is making is that your phone patched up to this date incorporates all of the known problems earlier than that. Well, it turns out it's not even close to being true. So in an interview with Wired magazine, the researchers at SRL, at Security Research Labs, said: "Sometimes these guys just change the date without installing any patches." They said probably for - I know, I know.

Leo: [Indiscernible anguish].

Steve: Probably for marketing reasons, they just set the patch level to an almost arbitrary date, whatever looks best.

Leo: Oh, that's terrible. Yesterday. Yeah, we fixed it yesterday.

Steve: Yeah, oh, we're all - don't worry.

Leo: Don't worry about that.

Steve: You've got, oh, yesterday. We're updated.

Leo: That's got to be some crappy phones, though. I can't imagine.

Steve: Okay. So here it is. They enumerate them. And if you follow the link, Leo, in the notes you can get the detail because they have a nice little red-colored chart. But 0-1 missing patches was Google, Sony, Samsung, and Wiko Mobile.

Leo: Well, I wish they'd say whether it's 0 or 1. That's kind of annoying.

Steve: I know.

Leo: There's a big difference between 0 and 1.

Steve: Yeah. On the other hand...

Leo: I've got to say Google is zero; right?

Steve: Yes. On the other hand, HTC, Huawei, LG, and Motorola are 3-4.

Leo: Yeah, that's not good.

Steve: No. That is to say, they're claiming they are current, yet they are not. Three to four missing security patches later than the date they said they are current to. And then the worst at 4-plus were people I'd never heard of: TCL and ZTE.

Leo: Chinese companies both. In fact, all of them, I don't know about ALPS, but TCL, OPPO and ZTE are all three Chinese companies.

Steve: Yeah, yeah. And I don't know how to...

Leo: Huh?

Steve: What were you going to say?

Leo: I just said wow.

Steve: Oh, yeah. And also OnePlus, Nokia, and is it pronounced Xiaomi?

Leo: Xiaomi. Another Chinese company. Another Chinese company.

Steve: Xiaomi. I've heard of them, sure.

Leo: Big, big Chinese - maybe the number one phone maker in China, yeah.

Steve: So Xiaomi, OnePlus, and Nokia, those are 1-3 missing patches. Meaning none of them have zero. They were all missing at least one.

Leo: Yeah. That's ridiculous. That's ridiculous.

Steve: Yes. And they said: "Specifically, the above" - that is, that table I was reading from - "focused on security patches for Critical and High severity vulnerabilities that were released in 2017," still missing from their phones.

Leo: You know it's sad, Motorola's on here. Used to be a Google company, but now it's owned by Lenovo. And I have to think that maybe because it's owned by a Chinese company it, too, is not getting updated.

Steve: Yeah, yeah. Now, there is some good news. We've discussed previously that Google is aware of this problem, that is, because they're the main driver of this. They have a project underway called Treble, which is rearchitecting Android to disentangle the OEM-level customizations from the OS code. Because right now it's necessary, essentially, all of this stuff has to pass through the OEMs and be sort of backported into the stuff, into the OEMs' own code blob, which then needs to be pushed out for their phones. And it's unclear if it's just lack of concern.

Essentially, what we believe is that OEMs are unhappy because all they want to do is sell hardware. They want to sell DVD players, just consumer electronics, and just like sell them and forget them. And so they're complaining about the burden of this constant updating patching of the devices they've sold, which consumes too much of their resources because, as it is structured today, it's involved to get these things patched.

So Google's Treble project is, in recognition of this serious significant overhead, is restructuring Android to separate the OEM junk from more of the OS stuff, which will reduce the burden on the OEM for these kinds of ongoing fixes. So Google's responding, and we can hope that, as we move forward, we're going to get this whole process sped up some.

Two bits of miscellany, then I'm going to continue. The first is, Leo, "Lost in Space."

Leo: Okay.

Steve: Did you see it?

Leo: I only watched the first episode.

Steve: Okay.

Leo: And I have mixed feelings about it. I downloaded the whole thing for our trip, so it's on my iPad. They spent a long time getting that girl out of that ice in the first episode. That just kind of went on and on and on. But I liked it.

Steve: Yeah.

Leo: I didn't hate it. What did you say? I feel like it's a mixed bag. It's not great.

Steve: Yeah. Lorrie and I - yes, I agree. Lorrie and I watched all 10.

Leo: Wow.

Steve: So we did Friday, Saturday, and Sunday.

Leo: Holy cow.

Steve: So I've seen the whole first 10 episodes. I hope there's more. I hope that...

Leo: You liked it enough that you want to see more, okay.

Steve: Yes. I would rather watch it than "House of Cards," and that got, what?

Leo: Well, that's pretty good, yeah.

Steve: Three seasons?

Leo: Yeah, yeah.

Steve: No, it was great. I will say, and this is not a spoiler, I'm never going to spoil anything. But, boy, Dr. Smith is annoying.

Leo: Yeah, yeah. Well, he was kind of annoying in the original.

Steve: Yes. He was like a fly in the ointment.

Leo: But at least he had something going for him in that one. This one they've really made Smith kind of not so good.

Steve: Yeah. Parker Posey we've talked about. And, yikes. So be prepared to be annoyed. On the other hand, I mean, I was thinking about it. It's engaging that she, Dr. Smith, is so annoying.

Leo: Right.

Steve: I mean, you just keep wanting something to fall on her, but nothing does. But really cool robot. Neat robot. And an interesting back story there. We learn about, you know, anyway, I'll just say I like this.

Leo: I think people who dislike it the most are people who were real fans of the original because it's nothing, nothing like the original.

Steve: No. And I think that's probably good.

Leo: Yeah. It was a cartoon.

Steve: Waving your arms around, "Danger Will Robinson, danger." And being attacked by salad monsters, it just doesn't really - that's not going to do it. But anyway, I just wanted to follow up on that. We liked it.

Leo: Yeah, it was entertaining.

Steve: I hope we get another season of it, yeah.

Leo: Yeah. Mixed bag.

Steve: Yes. And it won't surprise anybody that there will probably be another season. So without giving away any spoilers, I'm sure Netflix is hoping for more, and I am.

I did get, as I mentioned at the top of the show, a nice note that I wanted to share. And I didn't know what "Overcoming SSE" was. This is Mike in Dundas, Ontario, on the 15th of April, so that's two days ago, on Sunday. He said: "Hi, Steve and Leo," addressing it to both of us. He said: "I've been waiting a long time to drop you guys a note. I decided the trigger for my correspondence was to be a miraculous save using SpinRite. That's why I titled this document 'Overcoming SpinRite Story Envy.'"

Leo: Ah, SSE.

Steve: So that's SSE, SpinRite Story Envy. He says: "I, like many, many others whom I have heard on this podcast, I purchased," he wrote, "a copy of SpinRite as a thank-you for the invaluable service you both provide." He says: "I've been listening to Leo for quite some time, from very early when he spent a lot of time in Toronto." And of course you and I were there.

Leo: And you did, too, that's right, yeah.

Steve: Yes. It was in Toronto that you proposed this podcast to me, in fact.

Leo: I got on my hands and knees and proposed to Steve.

Steve: So he says: "Thought I would give this new Security Now! podcast a listen." He says: "You had me from the very beginning. I guess I am a 'SN0dder,'" he says, S-N-0-D-D-E-R.

Leo: He likes his acronyms.

Steve: Yeah, a "Security Now zero-day-er."

Leo: Oh, I like it. Oh, a SN0dder, yes.

Steve: S-N-0-D, a SN0dder.

Leo: I'm using that. Hello to all you SN0dders.

Steve: That's right. He says: "However, I've finally given up waiting for a drive to have trouble because I don't think it will ever happen to me personally." He says: "I practice Steve's Hard Drive Hygiene..."

Leo: Exactly.

Steve: Okay, he arranged not to do SHDH, which was Steve's Hard Drive Hygiene protocol, "...to the point where I too have a dedicated SpinRite machine, and my daughter uses 'SpinRite' as a verb." So he says: "Just wanted to say thanks, and that you guys are the best."

Leo: Wow.

Steve: So, Mike, thanks for sharing.

Okay. We've known for about five years that the original SecureRandom function, which was provided by JavaScript, was not random, or not as random as we hoped. We have known for five years, since about 2013, maybe even 2012, that it actually only provided about 48 bits of entropy. So there was a scramble around, we covered this at the time on the podcast, a scramble around to improve the JavaScript library. There was a...

Leo: It is Java or JavaScript? I'm sorry.

Steve: It was JavaScript.

Leo: Script, okay.

Steve: Yes. And so the concern is that there were at the time browser-based bitcoin wallets, and also some wallet apps that were using some early JavaScript libraries, even if they were standalone non-browser based. So essentially what has been found by researchers is that those early web browsers' JavaScript, which offered the so-called SecureRandom function, were only providing about 48 bits of true entropy. We want to have, like, 256; right? Forty-eight, I mean, that's still a lot because 32, after all, is 4.3 billion.

But several things have happened in the meantime that have sort of created a trifecta. We've got first an inherently low-entropy private key because the SecureRandom generates both the bitcoin address and the private key used to protect your access to it, so an inherently low-entropy private key. Second, in the last five years a huge increase in brute-force processing power, which is to say brute-force cracking power driven by all of the GPU and ASIC design for hashing fast. And then the significant increase in bitcoin valuation, which has moved bitcoin from an, eh, I really don't care if I even know where my wallet is, to oh, shoot, where did I put that? Or what was my password? I know you can relate to that, Leo.

Leo: Absolutely. I've had the "oh, shoot" moment, yes.

Steve: So what we have is means, motive, and opportunity for there to be a renewed interest in attacking bitcoin resources, which are not as secure as they really should have been then. But since then it's gotten easier to attack them, and there's much more motivation to attack them. And as we've learned, the protection that they have is much weaker than was believed.

So for what it's worth, the researchers who are looking at this have said, if you have had your bitcoin for a long time, if you may have generated it back in the early days when it sort of just didn't matter, and you were screwing around, and you thought, oh, what the heck, and you used a web browser, like a browser-based wallet, even if you subsequently moved to something much more secure, the point is the original entropy being low means that there are now, and researchers know this, there are people working on cracking older bitcoin addresses and their private keys.

And then, finally, if you have a substantial sum in a bitcoin wallet which you have had for a long time, and whose entropy, as I've just been explaining, you have reason to distrust, then it is probably worth creating a new bitcoin address and transferring your balance from the old one to the new one and move into one with guaranteed known high entropy. So I just sort of wanted to pass that on as a public announcement.

I know exactly where mine was synthesized when I first talked about it. It was a Windows-based wallet on a version of Windows with a known cryptographically secure source of entropy. So I have every reason to believe I'm okay. But if those three, if those multiple things fit you - you had it for a long time, it may have come from a JavaScript source, and you've got more money in there than you would like to lose - worth probably moving it to a new bitcoin address, freshly created with a full set of entropy bits rather than a lower number.

Leo: Or if you forgot your password, here's a chance to try to brute-force it; right?

Steve: And there you go, exactly.

Leo: It's a silver lining.

Steve: That's a very - I hadn't flipped it over like that, Leo. That's a very good point, indeed. And along the lines of things that people didn't bother attacking once, that they're now coming back to attack with new motivation? It turns out that, as we know, malicious cryptocurrency miners are looking around everywhere for any still-exploitable places where they can install and run their mining software. And the devices must be connected to the Internet. And optimally they will be as fast as possible. And as we have been discussing, this of course places public Internet servers among the ideal set of targets.

So now another old and long since known bug. It hasn't been patched because it's too old. But that doesn't keep it from being a problem. It's a bug in Microsoft's IIS v6. IIS v6 was the one that shipped with Windows XP and Server 2003. So, old. But the WebDAV service was known and has been known to have a problem. A pair of Chinese researchers a little over a year ago discovered that an attacker can craft and send a malicious PROPFIND request to an IIS v6 server that has WebDAV enabled. And that PROPFIND request contains an oversized IF header, which is one of the fields in that query. When the IIS WebDAV controller reads the request, guess what? Because it's oversized, it won't surprise you that a buffer overflow occurs, allowing attackers to deliver and execute code on the targeted server.

Now, due to the server's age - this was 2003, right, and Windows XP? Even though today, get this, even though today IIS v6 accounts for 11.3% of all IIS server installations, so one in nine of IIS servers are still IIS v6. The code is well past end of life and will no longer, obviously is not going to be updated. So Shodan, a search under Shodan shows that there are a little over 600,000 - 600,000 - publicly accessible IIS v6 servers on the Internet. The good news is WebDAV was not enabled by default. So most of them, most of those 600,000 publicly accessible IIS v6 servers do not have WebDAV enabled.

But any servers that were using Share Point portal do have it enabled, so there are still plenty of them. And as a consequence of all of this, again, and bad guys now having a new motivation to find servers, there is a campaign running at scale, meaning Internet scale, trying to find those servers and install Electroneum cryptocurrency mining on those machines. There are security firms tracking a campaign that is apparently being very effective. And so Electroneum is the cryptocurrency being mined by this campaign, installing itself into IIS v6 servers that are unfortunate enough to have WebDAV enabled. And there's potentially, who knows how many, I think I saw something like 65,000 somewhere. So a substantial percentage of that 600,000 potential publicly accessible IIS servers. Yikes.

And I was initially a little confused by a story about how a photo on WhatsApp of somebody's hand which did not show their fingertips was used as a new source of crime forensics. It was covered by the BBC and picked up by Bleeping Computer. The South Wales Police Chief Dave Thomas said that, although the scale and the quality of the photograph proved a challenge, the small bits were enough to prove that the person whose hand was shown was the dealer of the drugs that were depicted in the picture.

So over WhatsApp somebody was offering some illegal drugs with the palm of their hand showing the various samples of these various pills. And although the picture wasn't enough to identify the person because even in the photo you could not see the fingerprints, what somebody cleverly realized was that they could see a lot more. If you scroll down, I think there is a picture in their story. Or maybe, oh, I think it was the BBC's coverage. So if you can find the link to the BBC story, they show the picture, where you could only see a little bit of the person's hand. But because they had suspects for the crime and knew who it probably was, what they were able to do was use the photo as a further source of confirmation.

And what I was reminded of was our discussion about Tor, where as we have noted several times in the past, when traffic goes into the Tor network, you never know where it's going to come out. And Tor is so popular now, and there are so many nodes that can be weakly linked, that if you didn't know where someone's traffic was connecting to, you'd be hard pressed to figure it out. But if you suspect what the two endpoints are, it is very easy to confirm the communication once you know what it is, even though you've got Tor in the middle stirring things up and confusing things. So in other words, confirming a suspicion is not something that Tor protects.

And similarly, using a photo which is insufficient to identify someone can still be used to confirm with sufficient exactitude in order to close the case. And in this case, there were 11 convictions that resulted essentially from the fact that the photo that itself didn't identify someone was enough to confirm law enforcement's suspicion. So I thought that was sort of an interesting twist.

And, finally, we will wrap up this week's podcast with one from our You Cannot Make This Up department. So get this, Leo. An unnamed casino located somewhere in North America - the casino is unnamed because this is a report from the casino's security forensics company that of course wants to leave their employer, their contractor, unknown. This unnamed casino located in North America had 10GB of its internal network data, including all of the casino's high-roller database, exfiltrated to a location in Finland. That occurred through a newly installed, Internet-connected, aquarium thermometer.

Leo: At least the fish were comfortable.

Steve: Oh, my lord. Nicole Eagan, the CEO of cybersecurity company Darktrace, told attendees at an event in London last Thursday how cybercriminals hacked this casino through its Internet-connected thermometer installed into an aquarium in the lobby of the casino. According to Eagan, the hackers exploited a vulnerability in the thermostat to gain a foothold into the network. Once there, they accessed the high-roller database of gamblers and additional information, then pulled it back across the network, out the thermostat, and up to the cloud. So that was a very busy thermostat for a while.

Leo: It got really hot.

Steve: And of course - yes. And this, of course, is a perfect and classic demonstration of the crucial need that we have often talked about on this podcast for network isolation and segmentation; that you really want to keep the security of things you can't vouch for or that may be suspicious, like your fish tank aquarium thermometer, which you just have to have on the Internet, after all, to make sure while you're traveling that your fish are comfortable. The good news is we are beginning to see WiFi routers with multiple isolatable guest networks. And I think that's a great thing in this evolution.

I was configuring a network the other day, it was actually an ASUS router, and I'm going to go back and make sure that it doesn't have its WAN port exposed after today's podcast. And I must have looked at it when I was scrutinizing it, but I'm going to make sure. But it offered four isolated guest networks with options like "allow guests to interact." And so you would turn that off if you don't need the various IoT things within your home to talk to each other, yet you want them to talk to the Internet.

And so I would, moving forward, look for routers for your home that support multiple isolatable guest networks because I think this is going to be a trend. And think in terms of, not visitors, I mean, yes, also visitors, but give a couple of your router's guest networks to your IoT devices. Let them have their own place to play, not on your main network. And you can imagine that this casino really wishes that they had done exactly that. So very cool stuff. And as I said at the top of the podcast...

Leo: Such a great story.

Steve: ...never a dull moment.

Leo: Never a dull moment. It's the perfect name for this show. We're going to close the book on Episode 659. You can watch this show, we do it live in front of a live studio audience every Tuesday about 1:30 Pacific, 4:30 Eastern, 20:30 UTC. You can watch at TWiT.tv/live, and join us if you do in the chatroom at irc.twit.tv. After the fact you can get your own copy of the podcast for your collection. Steve's got them at his website, GRC.com, the Gibson Research Corporation. If you go there you can download it. He's got transcriptions, a giant mug - good lord, that's huge - and a whole lot more at GRC.com. While you're there, don't forget to pick up a copy of SpinRite, his bread and butter and the world's best hard drive recovery and maintenance utility. If you use it right, you never have to use it, which is kind of a paradox.

Steve: Ooh. R-I-T-E. If you use it "rite," yeah.

Leo: Never have to use it. You can also get a lot of freebies there, and all sorts of information. Steve, that site is just jam packed. It's like the back of a Dr. Bronner's Peppermint Soap bottle. You could just read it for days. GRC.com. We also have copies of audio and video, so you can see Steve's giant mug in space. All you have to do is go to TWiT.tv/sn, or get your on-demand versions by subscribing in your favorite podcatcher. That way you'll get every show.

Steve: And Leo, we should note to our listeners that you are off to Japan.

Leo: I am, on Thursday. So either Jason Howell or Father Robert Ballecer, I actually don't know, one or the other will fill in for me for the next couple of weeks. I'll be back May 7th. So we can resume this ongoing colloquy.

Steve: Cool.

Leo: If you have questions or comments or suggestions for Steve, he's on the Twitter, @SGgrc. Or you can go to GRC.com/feedback. Thank you, Steve. See you next week.

Steve: Thank you, my friend. Have a great vacation, and we'll see you in three weeks.

Leo: Three weeks.