A Mega News Week

Description: This first week of December brought us the early Christmas present of an amazing amount of interesting and important news. This entire episode is chockful of reports and discussion of everything that has happened during the past busy week in security and privacy.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-537.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-537-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. And this was such a big news week, we're just going to spend the whole show talking about kind of a potpourri of big news stories. We'll kick things off with Microsoft's Patch Tuesday, next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 537, recorded Tuesday, December 8th, 2015: A Mega News Week.

It's time for Security Now!, the show where we cover your security and privacy. We wrap it up tightly in a nice double layer of tinfoil, and you're safe forever. Mr. Steve - by the way, tin, not aluminum. Mr. Steve Gibson is here. He is our Explainer in Chief from the Gibson Research Corporation, GRC.com. He joins us every week for the last 10 years. It's amazing.

Steve Gibson: Yeah, yeah. In the show notes for this week, since we're just past the first week of December, I said that we got an early Christmas present of just an unbelievable amount of interesting security news this week. So there is no - we've done two Q&As in a row in order to have time for some questions in the last two weeks. And normally I like to do, like, some sort of a focused topic. But I'm not even sure we're going to get through all the news. So this is just a pure mega news week episode. Lots of interesting things have happened.

Leo: Not what you would have thought. In fact, didn't we say last week we thought it would be slow for the rest of the month? Ha.

Steve: Right, right, right. Not so slow.

Leo: Not so slow.

Steve: So just to give people sort of an overview, of course we just had the earliest Patch Tuesday possible because it's always the second Tuesday of the month, and the first of December landed on last Tuesday, which was our previous podcast. So this is Microsoft's Patch Tuesday. We've got new machinations that Microsoft is making towards forcing people to move to Windows 10, pretty much whether they want to or not. Dell, AOL, Lenovo are all in the doghouse for the things they've added to, well, actually Dell and Lenovo for the things they've added to people's PCs; AOL for just - this is chilling, how long there's been a problem with AOL's desktop.

We have news about Let's Encrypt; a brief little comment on one line in President Obama's Sunday address from the Oval Office; some reactions, some early maybe overreactions from France in the wake of their terrorist attacks; and also Kazakhstan is making some noise. ISIS has an app for Android. Mozilla has made a couple good decisions and has a new piece of iOS freeware aside from Firefox. CryptoWall is back with a worse version. And then a ton of miscellaneous stuff. So like I said, we've got a lot to take care of this week.

Leo: You're a busy, busy guy.

Steve: Yes. And our Picture of the Week is a kick. Martin Chadderton sent this to me. He said, "@SGgrc, didn't know you were branching out, Steve."

Leo: Steve Gibson Ukulele Event.

Steve: For those who are not looking at the video, it's a strange blue LED-illuminated sort of like, I don't know, backyard chunk of a fence.

Leo: A bamboo prison guitar rack.

Steve: Yeah, I don't know what that is. Anyway, I'm certainly not the only Steve Gibson. Because of my Internet presence, when you google me, I am the first few pages' worth. But, for example, I'm not Steve Gibson on Twitter, and that poor guy gets my tweets all the time.

Leo: Oh. Oh, I didn't know that, oh.

Steve: Oh, yeah.

Leo: Whoopsies.

Steve: He's like, uh, no, you want to send it over here. It's like, okay.

Leo: Well, there's a guy, I can't remember, I think it was jim@aol.com, who can't even use his email, of course, because jim@aol.com?

Steve: Jim? Oh. Well, and I heard you correctly noting on something, maybe it was on The Tech Guy on the weekend. You were commenting about the problem of using just a name on a domain.

Leo: Yeah, yeah.

Steve: Oh, it was, it was the military guy, or he was...

Leo: It was the Air Force, yeah.

Steve: ...unable to get his benefits because of the mess-up that...

Leo: Do you believe that mess-up? Apparently somebody had signed up on the same government site and must have mistyped the email address. This guy, the caller thought, well, is it possible for two people to have the same email address? No.

Steve: No.

Leo: And so this guy must have mistyped his because it's just a mess. And of course the Air Force has no way of resolving this. So what the guy's going to have to do is create a new address and just - I think he can change his address on his account and just do that. And I don't know what the other guy's going to do.

Steve: Your advice was great because you explained that, if you did use something like jim@somedomain, you would immediately start getting spam. And I've watched GRC's email server, I mean, I've looked at the packet layer, and random servers connect to mine and just do an alphabetic name attack, essentially. They just go from Abigail to Zeke, right down through every name you can imagine, just hoping to get lucky. They have no reason to believe any - there's never been a jim@grc.com, but he's trying to receive mail here.

Leo: Yup. Same thing at Leoville. Just goes through all the lists. It's incredible. Well, let's go to Kazakhstan, Steve Gibson.

Steve: We'll get there in a few. First, because Microsoft's Patch Tuesday is today, and they don't always release them, well, they don't release them a day early, they release them somewhere in the morning, I never have time now to dig deeply in. But while the deep dives have been interesting in the past, the resulting admonition is always the same. Update soon.

Leo: Do it, just do it, yeah.

Steve: Yeah. So this month we've got a bunch, 12 patch bundles, and lord knows how many individual vulnerabilities are fixed within each bundle. Eight of them are critical, so two thirds of them are critical. The other four are important. The critical ones are remote code execution vulnerabilities, which, as we all know, that's like the worst. In Office, Uniscribe, Silverlight, they called it the "graphics component," that's something different than Silverlight, a graphics component. So that was in the title, and as I said, I didn't dig any further. DNS, of all things, apparently someone found a remote code execution vulnerability in that and reported it privately to Microsoft. And JavaScript, or JScript, as Microsoft insists on calling it, and VBScript.

So those are all the critical problems, although - and then also critical problems which may or may not be remote code execution because they didn't elaborate in the title, for both of their browsers, both the Edge and the IE browsers. So there's a bunch of problems. You certainly want to get them fixed. But those problems are dwarfed by Adobe's update to Flash, also today.

Leo: I'm getting that from Microsoft right now.

Steve: Yes.

Leo: So it's not just - you don't have to necessarily go to Adobe to get it.

Steve: Correct. And in fact, I think - I've never been very impressed with Firefox's update. It's supposed to, Adobe's supposed to - you can give Adobe the ability to update itself. It may be...

Leo: Which you should; right?

Steve: Oh, yeah, because it's absolutely time to do that. We know that both IE and Chrome proactively take responsibility for their users in fetching and installing the latest updates. But for Safari users and Firefox, you may need to be a little more proactive. So what Adobe said was "Adobe has released security updates for Adobe Flash Player. These updates address critical vulnerabilities that could potentially allow an attacker to take control of the affected system." How many? 78.

Leo: Oh. Saving up, are we.

Steve: Merry Christmas.

Leo: Wow. So now, the update I'm getting from Microsoft is for IE, but will that update Flash in general? Or is it like Chrome and Firefox, where it just updates it

within the browser? Right? If you do the Firefox update, you still want to do a general Flash update.

Steve: Yes. And in fact the version numbers that IE updates to is different than the version number that Firefox updates to. So there's not quite synchronization. But you can go to, I think it's - just search for "Adobe Flash update." You'll get a link that you can use to check your version.

Leo: It's a tester; right.

Steve: Yes. And mine was behind on Firefox, and so I updated and then restarted Firefox, and now - although Flash is - I've set Flash in the add-ons for so-called "click to play," which is absolutely what everyone wants to do. We've talked about how you can do that over in Chrome. There's the setting there. And in Firefox, what that does is it shows a little Lego block. That's the icon that Mozilla chose. And so it's just a sort of a gray panel with a Lego block saying there is a Flash object here, which we didn't fetch, and we're not rendering, unless you explicitly say that you want to do that. And then when you click on it, you get another dialogue, in the case of Firefox, that says, oh, you sure you want to do this? And you can say yes or no and so forth.

So that click-to-play is crucial because any advertisements that you do display, great to go have the browser fetch it. Then it's going to see that it's trying to mess with Flash and then say, whoa, okay, hold on, that's a bridge too far. So again, 78 potential critical vulnerabilities...

Leo: Amazing.

Steve: ...that can allow an attacker to take control of your system. I think you want to keep Flash updated, just on the off chance that you use it for something. By the way, I did see, someone tweeted me the news - and thank you, whoever you were - that there's a beta.speedtest.net which does not use Flash. Speedtest.net was one of many bandwidth-testing sites, but you had to lower your shields and allow it to run Flash because it was a Flash-based test. They have an HTML5-based test. I also saw someone say, although I didn't have a chance to follow it down because I was furiously putting all this together last night and all of this morning, that Adobe themselves are officially encouraging HTML5 authoring over Flash.

Leo: Yeah, this was the big news last, or, yeah, I guess it was last week.

Steve: Oh.

Leo: So they are now - let me see if I can find the story, just so I don't...

Steve: Now, last week...

Leo: Basically they're deprecating Flash. But we talked about that.

Steve: Yeah, exactly. We talked about they had renamed it from Flash, whatever it was, studio, to Content Creator or something, I don't remember what it was. We talked about it last week.

Leo: Right. I think that's what I'm talking about.

Steve: So maybe that...

Leo: Yeah. Yeah. Basically, if you're using Adobe Creative Cloud, they're telling you don't - you're not going to be coding in Flash.

Steve: Right.

Leo: You're going to be coding in something else from now on.

Steve: Right. And they're saying we're not abandoning Flash, for those who for whatever reason need to keep using it. But you're right, its days are clearly numbered. And, for example, the advertising whatever, the IAB is also saying use HTML5, don't use Flash. And as we said last week, the fact that you can't run Flash on iOS, period, means that...

Leo: Yeah, that was the nail in the coffin.

Steve: Yes, yes. Especially when you look at the Black Friday sales through iOS devices.

Leo: Oh, yeah.

Steve: Clearly, advertisers want their ads to operate in mobile platforms. So that's a really nice side effect of Jobs making a decision that he absolutely will not allow Flash to run on his iPhone, and then later the iPad.

So speaking of absolutely refusing to run something, many users of Windows 7 and 8.1 are absolutely refusing to upgrade to Windows 10. Microsoft, however, is not taking that lying down.

Leo: I saw this story. I was kind of shocked.

Steve: Yeah. So several things are going on. There is a really neat tool, which I've just loaded after learning of it, called GWX Control Panel. GWX, of course, is the abbreviation for Get Windows 10. GWX is the thing that Microsoft has been installing in people's

machines since, what, early summer. Remember the whole "reserve your copy," like as if they were going to run out. And it caused people concern. They thought it was malware, what's all this. And then people have been discovering that 2GB of Windows 10 binary has been downloaded into their pre-Windows 10 machines without their knowledge or permission, Microsoft just saying, well, you know, we're going to get you sooner or later. We'll send Windows 10 to you so that it's just a button-click away.

Anyway, this guy Josh Mayfield has GWX Control Panel. It used to be called, it was formerly known as "GWX Stopper." But he's renamed it as it's become more capable. He just recently updated it on November 24th so that it had the opportunity, or the feature, of running continuously in the background because what his users of previous versions, where it just checked on demand, they were reporting that their endeavors to say no, I don't want Windows 10 were being reenabled. Which is to say Microsoft was flipping these switches back on to override their explicit request not to get Windows 10.

So with this update - and by the way, this is free. He does have a PayPal donate button. And I'd drop him a couple bucks if you think it's worth it. I'm very impressed with it. I just gave Wikipedia a bunch of money because they've been asking, and I use them so much that I wanted to support Wikipedia. This guy says only about one in a thousand downloads ever pay anything for it. So it'd be nice to support him, if you think it's worth it.

So this runs in the background. And since the update he's been getting much more feedback from his users, confirming that Windows is trying everything it can to ignore these settings. And Microsoft themselves have said that, starting, like I think they said this month, and in fact I carefully scrutinized that block of today's Patch Tuesday downloads to see whether they had snuck in what they had said they were going to. And the idea was they were going to move this from an app in your tray, which you can say no thanks, or it keeps annoying you and so forth, they were going to actually move it into an optional download category of Windows Update.

And so this redefines Windows Update from patching the current version of Windows to upgrading you to Windows 10 because Microsoft, for whatever reason, is desperate for us, you know, to get everybody over to Windows 10. And then, sometime in 2016, the plan is that they're going to move it from an optional update to a recommended update, to again further up the ante. And that means that users who don't look through the list of recommended updates, and most users don't, you just say, oh, yeah, fine, I want all of my monthly updates, it'll be enabled by default. You'll click yes, and you'll be downloading the permission for your system to be updated to Windows 10.

Now, you will be told before this happens. So it takes more than just downloading this update. So there will be a chance to say no. But essentially Microsoft is flipping all of the defaults in the direction of getting Windows 10. And of course one of my trademark concepts on the podcast is I call it the "tyranny of the default" because defaults tend to be what people use, and they rule the day. So Microsoft really, really, really, really wants everyone to move. And from their standpoint, I totally get that it is a huge burden on them to continue backporting all of the changes that they're needing through multiple versions of Windows.

My problem is that Windows 10 is something I actively don't want. I mean, I absolutely don't want it. So it's not like it's something that's like, okay, yeah, fine. I mean, I absolutely don't want it. And so the idea that Microsoft is pushing something on people which we've already talked about, the various controversial aspects of it. I know Paul rolls his eyes; but it's like, okay, Paul, you're welcome to your opinion, and I am to mine. And I know a lot of people are with me. And it's like saying, no, that's not what we want.

And so there is freeware to turn off all of this excessive communication that Windows 10 does back to the mothership. And so my problem with them pushing it this hard is that it's really something I don't want, and they're making it really hard not to get it by mistake.

Leo: You're safe because you're not using 7 or 8; right? Or are you?

Steve: Right, I'm still, no, I'm happily on XP still.

Leo: So don't worry. They're not going to force you.

Steve: No, but in fact you and I are talking through Windows 7 right now because I have Windows 7 machines all around me, just not - and I would be using Windows 7 on my main system if it were easy to switch to it, but it's not. Microsoft has never made changing versions actually work.

Leo: Well, here's the good news. Microsoft's never made it so easy to go to Windows 10. Yeah, actually the thing that's even more disturbing, and Paul and I have talked about this, and he's just as disturbed, is there seems to be some number of people, it's hard to confirm, that are actually getting upgraded whether they want to or not. They're actually being moved to Windows 10. My suspicion is it's kind of along the lines of what you just talked about.

Steve: Defaults.

Leo: They're just saying, yeah, I want updates, and getting it by accident, although...

Steve: The dialogue...

Leo: ...it seems that it should warn you a few times, you know we're upgrading your operating system.

Steve: But again, remember what Microsoft has demonstrated is they want it installed.

Leo: Right.

Steve: I mean, that's what they're showing us. And so it's not going to give you multiple opportunities because it really wants to override the user's choice. I mean, if it's flipping the switches back on, and Josh confirms, now that he has a monitoring tool, he said starting the beginning of this month, December 1st, he started getting a flood of reports from people saying, "I had turned that off, and it's back on again." And apparently several times a day it gets flipped back on. So he's now digging in. This is just recent, so

he's digging in to figure out what's going on.

But really I could recommend this GWX Control Panel. I have it installed on my Win7 now. It's very nicely written. You can get it as an installer or just a standalone, if you don't like installers. And it shows you, oh, just it's neat. It shows you whether the directory where Microsoft stages the Windows 10 files exists yet or not. So, like, have they snuck the binaries in behind your back? And a bunch of other information. So it's super nice, GWX Control Panel.

Leo: Nice.

Steve: So now a series of disturbing add-ons by OEM vendors of machines. We've of course now for several weeks been talking about Dell's disastrous inclusion of a certificate which included the private key in all of their systems that were recent and that had been upgraded. They responded and fixed that. However, they didn't actually address the main problem. LizardHQ.org, back at the end of last month, took a look at the disposition of the so-called Dell Foundation Services after that patch was applied.

It turns out that it still, right now, starts an HTTP server which listens for connections on port 7779. They fixed this so-called "service tag leak" previously by removing the JSONP API. That's the JSON with Padding sort of convention for passing information back and forth API. But now there's this web server running on port 7779 which offers a SOAP service. SOAP is a protocol that runs on top of HTTP, which is S-O-A-P, stands for Simple Object Access Protocol. And it's been around now for years. And it's sort of a - it's a simple way of using the web connectivity to do way more than just web page stuff, to basically use it for any kind of client-server transactions.

So it happens that over the SOAP service, which is running on this web server, which is started by Dell Foundation Services by default, listening on this port, after all of the recent kerfuffle, you are able to perform a complete WMI - that's the Windows Management Interface - enumeration of the system, which allows anyone who can connect to that port to query for the system's hardware, installed software, running processes, installed services, accessible hard drives, file system metadata, filenames, file sizes, dates, and more. Basically, it is a powerful sort of scriptable API to give you complete access to the user system. You can do pretty much anything you want through the Windows Management Interface.

And this is where I remind people to, first of all, to sort of take a breath because hopefully we're all behind our own border router. We're behind a NAT router, and that's preventing an open port on any system in our LAN from being visible externally. But of course that also assumes that there have been no holes punched through the router which Universal Plug and Play makes trivial to do. For example, famously, the Xbox uses UPnP in order to do port mapping through a typical consumer router so that it's able to get unsolicited incoming packets over to the Xbox. There are legitimate reasons for doing that.

The problem is, as we talked about years ago, when UPnP first surfaced, and I said, oh, this does not look good, because there was no security model with it at all. It was just there, and anybody on the LAN could probe for Universal Plug and Play service and get essentially low-level access to the port mapping in the router. So hopefully everybody is behind a router and has disabled Universal Plug and Play, which does then transfer to you the burden of mapping ports manually that the UPnP interface would otherwise do for you automatically.

Unfortunately, there's no middle ground. You either have it on or off. And if it's on, you have no control over it whatsoever. And you can't even see in the router's browser-based interface what UPnP has happened behind the scenes. The UI doesn't show you those things. So there's not even a way to manage it. It's just it's always been a disaster. On the other hand, it turns out that this LizardHQ group, who found this port 7779, I guess I'll call it a vulnerability because it's really bad, turns out that our friend the Shodan search engine finds many vulnerable hosts on the Internet.

So somehow there are Dell systems running the Dell Foundation Services, not behind any kind of NAT or firewall. It's probably the case that Dell Foundation Services does open ports through its local Windows Firewall so that it can be accessed from the outside. But they probably aren't able to access through someone's NAT router, and we know they can't if you've got Universal Plug and Play disabled. On the other hand, it is accessible through the LAN because your router won't protect Intranet access among devices. So potentially, in a large corporate environment, this could be a problem.

So, boy, you know, just what we're seeing is we're seeing our OSes finally getting bolted down, where, I mean, it took a long time for Microsoft to get the clue about how to make their systems secure. It took until Service Pack 2 of XP, after they had 98 and Windows 2000 out on the consumer side, to finally turn a firewall on in order to foreclose all the open ports that they had that caused NIMDA and Code Red and MS Blast Worm, all of these problems that we had fun explaining in the early days of the podcast. That's finally calmed down.

Unfortunately, none of those lessons have been learned by the OEMs, who are now essentially repeating all of those mistakes by saying, oh, well, we're going to add Foundation Services, which probably nobody even wants, but it's there, running on everyone's newly purchased Dell machine, creating this kind of vulnerability behind everyone's back. Not good. Oh, boy.

And here's one. Actually, I'm going to do this a little out of order because I'll stay with the corporate faux pas. Lenovo is back with another problem.

Leo: Come on.

Steve: And actually hauntingly similar.

Leo: Aw.

Steve: Yes, yes. Now, this is the Lenovo Solution Center. Lenovo is in a panic right now, telling everyone to turn it off, stop running it. Because it turns out, when you run the Lenovo Solution Center, which is one of those icons that's installed down in the tray, that's all part of the value-add that Lenovo provides, it creates a process called the LSC, for Lenovo Solution Center, Task Service. And that task service runs with full admin rights. It opens port 55555, five fives, and listens for incoming connections on that port over an HTTP protocol. So it can be instructed via GET and POST HTTP requests to, get this, execute code in a directory that a local user can access.

It can also - it executes with full privileges and can execute programs found in an arbitrary location on disk, which the user can write to so that any malware placed there

will be executed with admin rights, and it can be induced to perform remote transfers. And finally, any visited web pages are able to pass commands to that local LSC web server to execute with full privileges because we now have in JavaScript the ability to access whatever ports we want to on localhost. That is blocked in Edge - no, no. It was going to be disabled by default. But at the last minute, Microsoft left it enabled. It is a setting where you can block localhost servers.

So essentially what we have is another big problem with Lenovo where, very similar to Dell, they are opening a port and listening for connections. And behind it is a powerful abusable server which, I mean, again, echoes the mistakes that Microsoft was making for years. Now the OEMs are making similar mistakes. Wow. And we have search engines like Shodan that's out there enumerating them, listing them. So it makes them easy to find.

Leo: So sad about Lenovo because...

Steve: Yeah, boy, yeah. Okay. So AOL Desktop. I don't know, actually I do know at least several people who are non-techie friends that still have AOL email accounts, and they still use the AOL Desktop. I look at their computer, and they think it is the Internet. It's like, well, this is my Internet. Okay. So we have to turn the clock back to understand this because the AOL Desktop dates from 1993, so way back when no one had high-speed Internet connections, when AOL was operating over a dialup modem.

In order to provide a rich environment, this AOL Desktop environment, they designed their own scripting language, which is called FDO. FDO stands for Form Definition Operator. And in AOL's FAQ they said: "AOL communicates using this programming language. For example, after clicking any icon or button in AOL, FDO code is sent by the AOL system and interpreted by your AOL to create a window. So the FDO language is the language used to describe forms on the AOL client, that is, the AOL Desktop client. This site has focus on learning how to program in FDO" - they actually documented this back in the day - and they said, "and provides a surfeit of examples and tutorials" - there's a word you don't hear often - "for those who want to learn."

So essentially AOL created a homemade protocol which was designed to minimize its bandwidth utilization. It is a compiled-into-bytecode language. So what you see going over the line is bytecode, basically hex binary blobs which represent verbs and then have arguments following them, which the AOL Desktop interprets. What has just come to light is that there is no authentication on the protocol. It runs, not over SSL, but over a plaintext connection. And anyone who is able to interfere with the connection, a man in the middle, is able to alter and inject, because there's no authentication of encryption, any scripting of this FDO language that they wish. They're able to cause the desktop to go fetch files and run files.

So it completely opens AOL Desktop users to a massive breach of their security. There are tokens, they're the fm_* series of tokens, "fm" for file management, which allows the script to cause the client to read and write files on the Internet. And there's a token 0d19, which is the async_exec_app opcode, which tells it to go run an app, a file, on your system. So essentially, ever since - and this has been in place since 1993. It's still in use today and exposing anyone using AOL Desktop to this kind of power.

So once again, well, this is sort of a different sort of mistake. This is a system that was never secure, back in a time when really we weren't nearly as focused on security as we are now. So it's legacy insecurity and way too much power in today's Internet, where we

have lots of people who could easily make an AOL Desktop, an FDO script sniffer, see when somebody has traffic using AOL Desktop, and then use it in order to get a wedge into their system. Oh, and under "mitigation advice," it was "uninstall AOL Desktop." Meaning you don't need it anymore.

Leo: I get a lot of calls about it.

Steve: Do you, do you.

Leo: Well, yeah, you know, the radio show. Understand we get a lot of older people who probably, I mean, there's still people who use NetZero and all sorts of weird, you know, WebTV. And it's hard. You always want to say, when somebody says, well, I'm having trouble with my AOL, you always want to say, please, please. The answer is get rid of it. But, now, the Desktop, that's really old. That one I think you could safely say just use the web version.

Steve: Have you seen it? Looks like Romper Room.

Leo: Oh, yeah.

Steve: It's just, I look at it, and I go, oh, wow.

Leo: Even AOL replaced that essentially with AOL.com long ago.

Steve: So that you go to their website instead of using the Desktop.

Leo: It has the same functionality. I don't know if it's AOL.com anymore. But for a while the web portal had the same functionality as the Desktop. Even to their "You've Got Mail" and all that stupid stuff. Hey, by the way, I don't know, it's not on your rundown, but Wired magazine thinks they found Satoshi Nakamoto.

Steve: Wow. Again?

Leo: Yeah, again. But this one, remember, it was Newsweek who famously fingered some poor old Japanese fellow who really didn't know what was going on. This one's a little more credible. It's an Australian fellow, Craig Steven Wright, and there's a...

Steve: We should remind people who that is, if they don't recognize the name.

Leo: Oh, inventor of Bitcoin.

Steve: Yes.

Leo: Guy who published a paper in 2009, anonymously, under the name Satoshi Nakamoto, that effectively created Bitcoin, did the math and all of that stuff. And, boy, the evidence, I'm just looking at all the evidence they have, including his use of a PGP key that is tied to Nakamoto. So he said, if you want to get in touch with me - this is back in 2008 - use this PGP public key. And that's the same public key used by Nakamoto on his Vistomail address. So it's pretty hard, you know, either he is Satoshi Nakamoto or is trying, and has been trying since before the paper came out, to convince people he's Satoshi Nakamoto, and has built a paper trail. It's really interesting.

Steve: Wow. And, well, it'll be fun to see how this develops because I would like to understand why he's hiding. I mean, like, why does he want to stay under wraps?

Leo: Kind of hiding in plain sight. He even says that. They lead off with his appearance at a Las Vegas Bitcoin Investors Conference in which the moderator says, why are you on this panel? And he said, well, I have a couple of masters, a couple of PhDs. And then...

Steve: I invented Bitcoin.

Leo: Well, and then the article goes on, one of the panelists said, well, how did you first learn about Bitcoin, as if trying to determine Wright's significance. Wright paused for three full seconds. "Um, I've been involved with all this for a long time," he stuttered. "I try and - I keep my head down." He seemed to suppress a smile. The panel's moderator moved on. But basically the suggestion Wired makes is he really just wanted to say "I am Satoshi Nakamoto."

Steve: This is just good.

Leo: But there's his post, his blog post the morning before the Bitcoin paper came out, saying it was going to come out, a post which has since been taken down, but caches exist. I mean, there's a lot of evidence. So I'll let you review it. But the article just came out today, like an hour ago. And pretty interesting.

Steve: Wow.

Leo: It's just a fun game. It doesn't really matter.

Steve: Yeah, it is, it is. So Let's Encrypt public beta has gone live. So it is now officially live.

Leo: Fantastic.

Steve: Yes. And a bunch of sites are using it. There's even a - and I thought I had it in my notes. I know I captured it, but I'm not seeing it here. There was a government site, I think it might be - it had a funky URL because it was https://https again, dot I think it might be cert.org. I'm not sure that it was cert.org or .gov. I don't have it written down. And some people were confused because they didn't get the double https part. But they're issuing certificates, and I've seen a lot of feedback from our listeners who have been really, really pleased with it.

So what's happened is a really nice ecosystem is already beginning to form around it. The protocol is ACME, A-C-M-E, which is the way, the protocol you use for interacting with the Let's Encrypt service, where you ask it for a certificate for the domain. It sends you a challenge, which you answer by demonstrating you have control over the domain. You say, okay, I'm ready to have you verify my challenge. It does that. Then it gives you the certificate and so forth.

So basically we've automated the entire domain validation, that is, the lowest level of assertion of identity, just saying that this is a server that has control of this domain, which is exactly what we want. It's not the OV, the Organization Validation, or the EV, the Extended Validation, where much more background checking is done, that really does need some human aspect to verify, like people call your phone number and verify that you're a corporation operating at the phone number that's available in your WHOIS, or Dunn & Bradstreet records and so forth. So this is just saying, I'm a server that is on this DNS name. I want a certificate so that I can offer, now and forever, TLS, HTTPS connections. This now makes that for the first time automated and free.

Now, what's cool is this ACME protocol is in the process of being IETF standardized. So it's going to be a standard protocol of the Internet. And we're seeing an ecosystem already sprouting up around it. There is a way to issue certificates using Let's Encrypt for Windows, which was not initially supported. It was Linux and Nginx were the two out of the gate. But now both IIS and Apache, when Apache's hosted on Windows, have add-ons that allow them to use the Let's Encrypt system. There's even a command line free certificate generator.

So there's a project called Let's Encrypt No Sudo, you know, no S-U-D-O. And the guy writes on GitHub: "The Let's Encrypt initiative is a fantastic program that offers free HTTPS certificates. However, the one catch is that you need to use their command program to get a free certificate. The default instructions all assume that you will run it on your server as root, and that it will edit your Apache/Nginx config files." He writes: "I love the Let's Encrypt devs dearly, but there's no way I'm going to trust their script to run on my server as root, be able to edit my server configs, and have access to my private keys. I'd just like the free SSL certificate, please. So," he writes, "I made a script that does that."

So lots happening. There is also on GitHub, it's GitHub.com/kuba/simp_le. And that's a Simple Let's Encrypt client. So I expect we're going to see a bunch of this happening now. And the days of having to pay every couple years anything for just a DV certificate are over. And the curmudgeonly grumbling about, well, I don't want to offer security because I don't want to support the whole public key infrastructure system and sort of the Richard Stallman belief system, there's really no justification for that anymore. So this does what I think we've been hoping for, and that is, it removes any additional barriers from someone being able to say, yeah, I want to be able to have my server

secured. It's free and automated, and that's going to be a good thing. I think a year from now the terrain is going to look very different than it does today.

And speaking of that, I listened to President Obama at 5:00 p.m. Pacific time, 8:00 Eastern on Sunday. And I paused and backed up and listened to a few times one sort of chilling line. I don't know what it means. I just wanted to put it into the record. We'll be waiting to see what it means. But quoting him, he said, and I'm just jumping right in the middle here, said: "And we constantly examine our strategy to determine when additional steps are needed to get the job done ... and that's why I will urge high-tech and law enforcement leaders to make it harder for terrorists to use technology to escape from justice." Of course this is in the wake of the San Bernardino attacks here in Southern California and the most significant terrorist-inspired attack since 9/11.

So anyway, we were celebrating not long ago that the administration had come down in favor of the overwhelming majority of academic and industry technologists and crypto people, saying, look, backdoors don't work. This is a bad idea. And now we have the President saying high-tech and law enforcement leaders need to make it harder for terrorists to use technology to escape from justice. So as I have said before, we live in interesting times.

Meanwhile, France is considering blocking Tor and public WiFi after the Paris attacks. Now, this is just-proposed legislation. And like the legislation we've talked about that's sort of being ruminated over in England, this isn't law yet. But, oh, and I should mention that, when I was looking at this, this was a story on The Verge, there was something over on the side panel that caught my attention, which was news of - it was a little animation, and because it was moving it caught my eye, of a flamethrower mounted on a quadcopter. And that led to the question of drone-mounted firearms. And I thought, what? But this is something that never got on my radar. Apparently this was back in July. Anyway, we're deferring this to the miscellany at the end of this podcast. But it leads to some interesting concerns.

So what The Verge wrote was that French security forces have drafted proposals that would ban public WiFi and access to the Tor network. And actually this was reported in the French newspaper Le Monde. And I went there, and it was all French to me. So I had to take The Verge's translation, which cites internal documents from the Ministry of the Interior. And there are two different proposals. I'll make clear what they are and how they work in a second. The antiterror proposals come three weeks after Islamic extremists killed 130 people and injured more than 300 in a series of attacks across Paris, which of course we all know about.

"According to Le Monde, the documents outline two legislative proposals that French police and security forces would like to implement in the wake of last month's attacks." [Yabba dabba do in background] And I forgot to silence one of my devices.

Leo: All right, everybody. Everybody run and buy a copy of SpinRite, and we'll hear a lot more Fred Flintstone.

Steve: Sorry about that. I run around before the podcast and turn everything off so that we're not being interrupted.

Leo: It's great. I actually love it.

Steve: It is fun. It drives my brother-in-law out of his mind. Whenever I go up for the holidays, he'll, like, pick me and Jenny up at the airport for this little shuttle ride over to San Mateo. And if Fred ever does a "yabba dabba do," he just says, "That really bugs me." You know, since it's his house, it's his rules, so I silence my phone for the duration.

Leo: A buzz is all you need. You don't need the sound.

Steve: So anyway, so The Verge continues, saying one of these pertains, one of these legislative proposals pertains to the country's current state of emergency protocol - actually, I think I wrote this after figuring out what the difference was. The other concerns France's counterterrorism laws. Both could be formally presented as early as January, next month, the newspaper reports, adding that the ministry has yet to decide on the measures they outline. So again, nothing except a proposal. So on the Tor side, this would be non-emergency counterterrorism, meaning that it would be permanent. The emergency measure is just for now and has been extended for an additional three months.

But the point is those provisions, under the emergency measures, would ultimately expire. So but this Tor, this potential Tor ban they're proposing would not be that. It would be part of the permanent counterterrorism measures, which would forbid and block communications over the Tor network within the country. And it also includes a measure that would oblige VoIP services to hand over - and of course VoIP, that's phone. That's smartphones. They're all VoIP. Well, I guess they're not, technically. They're still cellular, aren't they. Anyway, so I'm not sure how far this extends - would oblige VoIP services to hand over encryption keys at the request of the government. And the Tor project, which runs of course the Tor network, did not immediately respond to a request for comment. For what it's worth, China has been blocking Tor since 2012, and both Iran and Russia have been targeting Tor, as well. But all three of those countries are very different than France.

Leo: Understand, though, this is the equivalent of our Director Comey at the FBI saying, "You know, we really ought to ban encryption." It's just the law enforcement people saying we would like this. So far there's been no move to make this the law.

Steve: Right.

Leo: But you're right, I mean, we have to keep an eye on these things.

Steve: Keep an eye on it. Now, what's really interesting is the second part because I just - I have always come at this stuff from a technology standpoint. And that's this public WiFi blocking. The measure to block free and shared WiFi connections falls under the proposed state-of-emergency changes, which would mean that it's temporary while the state of emergency exists. "The documents obtained by Le Monde argue that public WiFi networks should be blocked because it's difficult for security forces to identify users connected to them." Yeah.

"Police also proposed changes that would allow them to search vehicles and luggage without consent and to conduct identity checks without providing justification." And it goes on, but that's the gist of it. So again, it's like, wait a minute. You, like, loudly

proclaim that everyone offering free and shared WiFi needs to discontinue that? I mean, I guess. You just make sure everyone...

Leo: Just in case of emergency.

Steve: Yeah. But, like, exactly. Under the current state of emergency. So it wouldn't be permanent. That measure would expire if it were ever even to pass once the state of emergency had been - was no longer in place.

Leo: Well, you know, Donald Trump said we've got to call Bill Gates and turn off the Internet. So...

Steve: Has he said that? That one I hadn't heard.

Leo: Oh, this is yesterday.

Steve: Oh, I heard a lot yesterday, but I didn't hear...

Leo: I'll find and play the clip for you.

Steve: Oh, he actually said "Call Bill Gates"?

Leo: Yeah.

Steve: Oh, lord.

Leo: It doesn't - I hope it doesn't matter.

Steve: It's just entertainment.

Leo: It's just entertainment at this point. God, I hope it doesn't matter.

Steve: Wow. Now, here is another little interesting tidbit. The Republic of Kazakhstan - Kazakhstan? How am I...

Leo: Kazakhstan. That's where Borat comes from, yeah.

Steve: Kazakhstan is considering requiring all Internet users to install new communications certificate. We know what that...

Leo: Oh, who issues that?

Steve: Yes, and we know what that means. We've been talking about this. On the smallest scale, your corporation requires you to install a communications certificate so that they can decrypt encrypted traffic at the corporate Intranet border to do deep packet inspection, which is otherwise impossible, unless they're able to decrypt your connection. And that requires that they be able to proxy the connection to a remote secure server and have your browser be happy with that.

The next stage of concern is where, and we've discussed this, and I'm not looking forward to the day that I read this blurb of news into this podcast, where an ISP has decided that they're going to require all of their subscribers to install a certificate in their machines. But I hope that day is not coming. Now we have the larger sphere, where a government requires that all of its citizens install the government communications certificate in any device which they wish to use for communication outside the country. That's what this is.

This was posted on November 30th. Now, it's significant that it has since been taken down. We don't know now the - I grabbed the link. I grabbed the text the moment it got posted, and it's gone now. So I don't know what's happening behind the scenes. But so this reads, and the English translation is rough, but this is what it is:

"Kazakhtelecom JSC notifies on introduction of national security certificate from 1 January 2016," meaning, and this was meant to be a one-month notice, a 30-day notice. "From 1 January 2016, pursuant to the Law of the Republic of Kazakhstan Committee on Communication, Informatization and Information" - well, it says information and information - "Ministry for investments and development of the Republic of Kazakhstan introduces the national security certificate for Internet users.

"According to the law, telecom operators are obliged to perform traffic pass with using protocols that support coding using security certificate, except traffic, coded by means of cryptographic information protection on the territory of the Republic of Kazakhstan. The national security certificate will secure protection of Kazakhstan users when using coded access protocols to foreign Internet resources.

"By words of Nurlan Meirmanov, managing director on innovations of Kazakhtelecom JSC, Internet users shall install national security certificate, which will be available through Kazakhtelecom JSC Internet resources. User shall enter the site telecom.kz and install this certificate following step by step installation instructions," underlined Nurlan Meirmanov. "Kazakhtelecom JSC pays special attention that installation of security certificate can be performed from each device of a subscriber from which Internet access will be performed - mobile telephones and tabs on base" - that one got me - "of iOS/Android, PC and notebooks on base of Windows" - oh, so base is operating system - "PC and notebooks on base of Windows and Mac OS. Detailed instructions for installation of security certificate will be placed in December 2015 on site telecom.kz." Signed the PR Department of Kazakhtelecom JSC.

So it's not clear whether this was put up. They're saying that it's pursuant to a law. What backlash this may have generated, whether it's still in place and moving forward. But it's clear that what this said was that they're going to, that Kazakhstan is going to be installing decrypting proxies of exactly the sort we've been talking about being installed on corporate Intranets at all of the Internet connections to the country and so that only communications encrypted under their certificate, which all users inside the country who

wish secured egress from the country will be required to use, only their certificate will be allowed to pass through that international border. So if anyone doesn't have their certificate, and just tries to connect to some remote secure service, it'll be blocked at the border. You'll need to get their certificate in order to access the secure Internet outside of Kazakhstan. And so, again, I hope we are not seeing the beginning of wider spread of this. But this is the way it would look.

Leo: Here's what candidate Trump proposes. See if I can get this to play for you. It's just a 20-second clip.

Steve: Yeah.

Leo: It's not playing. I guess it's something to do with Flash, no doubt. Oh, well. I'll have to...

Steve: Keep working on that, and I've got...

Leo: If he starts talking, just shut up. That'll be the new requirement, incidentally.

Steve: So, okay. Oh, boy. So now ISIS, the infamous Islamic State, has released its own smartphone app.

Leo: How do we know this is really from ISIS?

Steve: I'm sorry?

Leo: How do we know it's really from ISIS?

Steve: Well, Telegraph.co.uk reports that "The Islamic State has released its own app for Android smartphones, which it uses to spread propaganda, including videos of beheadings and messages about terrorist attacks in various parts of the world."

Leo: I guess it is.

Steve: "The existence of the app was uncovered by the Ghost Security Group, which is a vigilante collective which has been aiming to and has been disrupting ISIL's online operations. Rather than using the Google Play Store, which of course would allow Google to take such an app down, ISIS is distributing installation links through encrypted Telegram App messages. Although thousands of Twitter accounts have been taken down, and Telegram has banned dozens of ISIL channels already, the use of its own app" - that is, Telegram - "would allow ISIL to avoid" - or, I'm sorry, use of its own app, that is, this app that ISIS has developed would allow it "to avoid such attempts to police and block its communications."

So you're right, I don't know how, I don't know what evidence there is that this is ISIS. But it certainly makes sense, unfortunately, that they would say - so essentially what this means is that they now, rather than using Twitter and other outlets to post their propaganda, which are then quickly responded to and taken down, they're using those outlets to post links to an app that then allows them to establish their own channel.

So unfortunately, what we've seen is that this group is taking advantage. In the U.S., at least, we're constantly talking about how they have much better social media than our own government does. And they leverage social media with a great deal of skill. And so it's hardly surprising that they're going to develop an app that allows them to establish a persistent connection. Hopefully there'll be a way to respond to it and block it and thwart it. But, again, it's the technology being used.

I was glad to see this. Mozilla has cancelled its plans for browser-based advertising. We talked just last week about how well Mozilla was doing with its, what was it, $330 million, something like that, that it had generated in 2014, and that the numbers for 2015 weren't out yet, but we would see those early next year, and they were going to be even better. And this is after their contract with Google expired because they are doing web-browser associations in other countries with search engines, Yahoo! and Baidu and in some cases Google on a nonpaid basis. So I was really glad to see that Darren Herman, the VP of Content Services, did a blog posting, what, four days ago. And it's short, so I'll just share this in its entirety because it gives also a sense for where they are.

"One of the many benefits of the web is the ability to create unique, personalized experiences for individual users. We believe that this personalization needs to be done with respect for the user, with transparency, choice, and control. When the user is at the center of product experiences, everyone benefits. Over the past two years, we've ideated" - whatever the hell that means - "built, and scaled a content platform that respects users. We served tens of billions of pieces of content. We experimented with all content, including advertising. We proved that advertising can be done well while respecting users. We have learned a ton along the way.

"Our learnings show that users want content that is relevant, exciting and engaging. We want to deliver that type of content experience to our users, and we know that it will take focus and effort to do that right. We have therefore made the decision to stop advertising in Firefox through the Tiles experiment in order to focus on content discovery. We want to thank all the partners who have worked with us on Tiles. Naturally, we'll fulfill our current commitments as we wind down this experiment over the next few months.

"Advertising in Firefox could be a great business, but it isn't the right business for us at this time because we want to focus on core experiences for our users. We want to reimagine content experiences and content discovery in our products. We will do this work as a fully integrated part of the Firefox team. Finally, we believe the advertising ecosystem needs to do better. We believe that our work in our advertising experiments has shown that it can be done better. Mozilla will continue to explore ways to bring a better balance to the advertising ecosystem for everyone's benefit, and to build successful products that respect user privacy and deliver experiences based on transparency, choice, and control."

So, yay. I wouldn't have minded the advertising tiles if it kept my favorite browser alive. But clearly they've decided they don't want to do that. They want to sort of maintain at least some purity, I guess limited only to the paid default search engines in the browser, which I think that's a nice tradeoff. So I'm glad for that.

And also, just today, they released Focus, which is the Mozilla content blocker for iOS9, of all things. Now, I'm a little puzzled by it because, for example, many people tweeted to me over the last week that Firefox was now available in the U.S. iOS iTunes store. I did know that, and I tweeted the news last week sometime. So this thing doesn't work in their own browser. And apparently it's because their browser doesn't have, apparently doesn't have access to Apple's content blocker API.

Leo: Right, that's right, yeah.

Steve: Yes. Which only Safari has. So what Mozilla has essentially done, for reasons I don't really understand, is to create a kind of a weak "me, too." It's simple to use, so it's not feature replete the way our favorite, 1Blocker, is. They call it Focus. And they say it helps you improve the privacy and performance of your mobile browsing experience. You control what types of page content are allowed. It is free. It's based on Disconnect.me's open source block list. So it's based on that list, as are many of these, although of course 1Blocker is based on EasyList and a whole bunch of other things, and lots of user control, which is why it's the power user tool of choice.

So you have five just toggles: block ad trackers, block analytics trackers, block social trackers, block other trackers, and block web fonts. So you can choose to turn those on or off. In the screenshot sample that I saw, they were all on. I don't know whether they default to on or not. I imagine that they do. And of course the content blocking itself you need to manually turn on in order to get that added to Safari.

And by the way, Leo, I'm having all kinds of - I was listening to Andy complaining, or maybe it was, no, I think it was...

Leo: It was Jim Dalrymple.

Steve: Jim. And, you know...

Leo: He was angry.

Steve: I was glad to hear it because iOS is collapsing on me. I use it extensively, and it is just so full of bugs. In fact, the icons on - I just was updating, I was running around updating my pads to 9.2, which was just released a couple hours ago. And I turned one pad on, and it was in TweetDeck. And I went back to the home screen, and the icons were scrunched so that they were almost touching each other. And I thought, oh. Now, if I just could have that by default, I'd be really happy. But of course I...

Leo: But that was a bug, of course.

Steve: It was a bug. And it's got so many bugs now. Safari, I'm seeing Safari lock up. Pages come up blank. Sometimes I have to force close Safari, then reopen it, and then the page displays. It locks up. It's just doing all kinds of sad sort of crumbly-feeling things.

Leo: Well, there's an update out today.

Steve: Yes. We can hope that they know about those, and they fixed a bunch of them. But I just wanted to vent a little bit. I was so glad to hear Jim saying, you know, this is really annoying.

Leo: He's really bitter about Apple Music, yeah. It's just not been a good thing for him, yeah.

Steve: So in the world of malware, we've talked about the Angler Exploit Kit in the context of malvertising because it's the one that many high-profile sites that hosted ads were - it was the way people were getting themselves infected. We then talked about sort of the shift to infecting probably lower profile websites, only because their security is probably on average more tightly curated. You know, high-profile sites like Google and Amazon and eBay, they've got a big team responsible, I mean, understanding the importance of that web-facing service being secure. But there's a bazillion sites out there, servers, many of them in closets or on hosting providers or people that have created a site and then just walked away from it. They're relatively low traffic, but they may not be zero traffic. And they may well be using add-ons, third-party plugins, that are vulnerable. In fact we talked about shopping cart plugins and what a problem those are, just in the last couple weeks.

So what's happening is there's a shift in the attack to these kinds of sites, to infecting vulnerable websites, web servers, one way or another, with malware, which then attempts to, in turn, infect anyone who visits that site. So what's happened is there's this new campaign is multi-payload. And the reason this thing popped up on the news is that it first loads a well-known data thief tool called Pony, which systematically harvests all usable, accessible, usernames and passwords from the infected system. So it gets itself in a position of sufficient privilege, and then knows where all the apps in the system that it's aware of store usernames and passwords. And so from its admin privilege, from essentially root-level access, it harvests them all and sends them off to remote servers. It does that before it then loads the Angler Exploit Kit, which is dropped into the user's machine.

Angler, which we've talked about a couple times, scans for vulnerabilities in popular third-party software and in known insecure Microsoft Windows processes if the system hasn't been absolutely kept current. Once security holes are found, Angler exploits them and force feeds CryptoWall 4.0 into the victim's system. At the moment, AV detection is extremely low for this new campaign. And the FBI, I caught in the coverage of this that the FBI is estimating that CryptoWall is costing its victims somewhere in the neighborhood of $18 million annually.

Leo: Oh, I bet it's more than that. Oh, it's got to be more than that.

Steve: Yeah, I imagine it's, right, it's way more. And you're hearing from people on the weekend about this.

Leo: All the time. All the time.

Steve: Yeah.

Leo: And people pay because they don't have backups.

Steve: Yeah. And then you take them into a Carbonite sponsorship.

Leo: Then we do a Carbonite ad, and then we think about [laughter]. If only...

Steve: Well, in that vein I will take us into a SpinRite sponsorship.

Leo: Okay.

Steve: Because I have a fun one. Now, the title gives it away a little bit. But he's a great writer, and he tells a nice story. This is Jeff Barr. He's a listener of ours, but he didn't post it in my mailbag. He sent it to Sue, who forwarded it to me. The subject was "SpinRite Saves the Walking Dead." And so he says, "Thanks, Steve, for a wonderful product. Longtime Security Now! listener, yada yada. I've been using SpinRite for years, running it on all my hard drives every year or so, and nothing seems to be happening, just like it should."

He says, "But a couple weeks ago I finished DVR recording the latest season of 'The Walking Dead' on my Dish Network VIP 722K DVR, all eight episodes ready for a weekend of 'Dead' fun watching. The DVR got unplugged for some reason, probably the dog, but that's not important. When it powered back up, I was presented the error of 'Failed hard drive. Call for support.' Well, a call to support told me to return the unit for replacement, and there was nothing that could be done. Returning the DVR would lose all my shows with over 30 hours of fine-quality HDTV. Unacceptable."

He says, "I do not endorse opening a Dish DVR. They are a cranky company" - I love that, a cranky company - "but there were no 'warranty void' stickers on my box, so who will know? I opened it up and extracted the hard drive, a normal everyday-looking Seagate SATA hard drive. I plugged it into my SpinRite machine and fired it up."

Leo: Aha. Everyone should have a SpinRite machine.

Steve: Everyone should have a SpinRite machine, just some old bucket of bolts that's not useful for anything else.

Leo: Empty case, yeah, with all the SATA and IDE connections.

Steve: That's right. "SpinRite grudgingly reported no devices connected. I investigated.

The BIOS registered the drive, but every time I ran SpinRite there was no device. The Internet told me there are some tricks with Dish drives, using power from the DVR and SATA from the computer." I thought, when I read that, I thought, what? No. He says, "Several power-up sequences with swapping cables. None of these worked for me." So there was some bad information on the Internet, not surprisingly.

But he said, "Finally, with little hope left, I downloaded and created a Ubuntu boot USB stick, and fired up for one last try. Using the hdparm tool I unlocked the 'power-up in standby mode'..."

Leo: It's a TiVo, that's - yeah.

Steve: Yes, exactly, "...on the drive." And he gives the command hdparm -S 0 /dev/sda, which of course is UNIX terminology for the first drive.

Leo: Yeah. So Dish licenses TiVo for its DVR. That's...

Steve: Right.

Leo: And, yeah, TiVo - SpinRite should have no trouble with TiVo, but they do weird stuff to the drive, yeah.

Steve: Yeah, in fact, exactly. So, and in fact there is this thing...

Leo: You have to bless it.

Steve: ...this power-up in standby mode, where you then need to unlock it.

Leo: Right.

Steve: So he says, "After that, I poked around a little bit on the drive in Linux and found plenty of files and directories with all but cryptic names. My task complete, I booted my SpinRite CD yet again and hoped for the best. This time SpinRite found the drive and was happy to scan all four Dish partitions. After running for six hours on the 500GB drive, it marked four sectors as unrecoverable, but at least it ran and recovered everything else.

"I returned the drive to the DVR unit and waited for the eternal Dish power-up sequence. The unit booted, and all my TV shows are back. I then spent the weekend watching 'Walking Dead,' and I am now all caught up. I don't know if you mentioned Dish Network hard drives before" - we haven't - "and it took a bit of 'above and beyond' to get the drive visible. But hooray, SpinRite saved another drive. I am now transferring all important shows to portable hard drive and will send this unit back. Thanks again for bringing the 'Dead' back to life. Jeff in Tempe, Arizona."

Leo: Very nice. Very nice.

Steve: Jeff, thank you for the report.

Leo: Yeah, once you know it's a TiVo drive, then you can do the research. That's...

Steve: Exactly.

Leo: It was looking for "Dish" probably that made it hard to find. But, yeah.

Steve: Yeah.

Leo: I recognize hdparm. Ah, those were the days.

Steve: Those were the days. So now a potpourri of miscellany things. Okay, first of all, as I promised earlier, I was just, like, whoa. It never occurred to me to mount a firearm on a quadcopter.

Leo: Why not, Steve?

Steve: And unfortunately, it's going to occur to bad guys.

Leo: Yeah.

Steve: Think of that. Now, I have to say, being a physicist, the first thing that occurred to me also is, wait a minute. If you shoot a high-velocity projectile out the front...

Leo: Back goes the drone.

Steve: Exactly.

Leo: Also, most drones can't handle, can't carry anything really heavy, so...

Steve: Right, right. And apparently there is a history of this, but they have been largely spoofs. So there have been videos of this before.

Leo: Oh, yeah. There's a guy and his brother, they put Roman candles on the drone,

and he shoots at his brother. It's quite funny.

Steve: Oh, my goodness.

Leo: But putting an actual heavy metal weapon on there would require a fairly industrial drone. And you're right, you know, Newton's Law, what goes out one end...

Steve: For every action, there is an equal and opposite reaction. So quoting The Verge and this story from July 16th, they said: "This isn't the first video we've seen of a firearm attached to a consumer-grade drone, but this is the most convincing. The 14-second clip, uploaded to YouTube last Friday [of July] claims to show a 'homemade multirotor with a semiautomatic handgun mounted on it.' The drone fires four times, with the recoil from each shot pushing it backwards in the air. If the footage is real, then the craft is certainly illegal, at least from the perspective of the Federal Aviation Authority (USFAA), which regulates aircraft and drones."

And then The Verge notes there have been fakes before, but "While the FAA certainly doesn't want people mounting guns on quadcopters, there's no reason that people might try to claim" - I don't think I transcribed it right. But anyway, it says "that this activity is their right." The question is, "Does the Second Amendment apply to drones with guns? Legal scholars have already investigated similar claims covering robotic weapons, for example, with one law clerk, Dan Terzian, suggesting in a 2012 paper titled 'The Right to Bear (Robotic) Arms' that there is a 'very real possibility of robots being defined as arms under current Second Amendment doctrine.' Presumably the same interpretation might also cover drones."

So my concern, of course, is that this creates an incredibly devastating weapon because drones are ubiquitous. They have video cameras on them, so you can see what they're seeing. Or if you, I mean, I don't want to, you know, this is - I'm not giving anything away because this would be obvious to any horrible person who wanted to do this. But you add a laser sight, and then the camera on the drone can see the red spot that the gun is aiming at, even though you're not able to sight down through the gun's sights. And this thing you can fly wherever it can go, remotely. It's horrifying.

So anyway, I just thought I'd put that into the podcast because, yikes. Just unfortunately it's the kind of thing where what can happen, does happen. And this is horrifying. This had never occurred to me before. They were talking about a flamethrower, which I guess has been done. A pump was purchased from Amazon, and it works, apparently. And that's the video on The Verge that caught my eye. But then, when I followed that link, it talked about this, it's like, whoa. That's unsettling.

Many people, on the topic that we talked about last week - and Leo, you were correct that there had to be something strange going on with this guy's Wells Fargo password where it wasn't until he shortened it to eight that it worked. You were surmising maybe that the ninth character was illegal, and it wasn't actually the length, but it was an illegal character, which it wasn't reporting. Many people said that they are using 14-character Wells Fargo passwords. So who knows. Maybe it was the way he came into this, where like the reason for changing it, or maybe the script happened to download with an error, who knows. But I wanted to mention that everybody had said, yeah, that doesn't seem to be the case, for what it's worth.

I also ran across an update to libsodium that I wanted all of our coding listeners to know of. Libsodium is the library which I chose two years ago, which incorporates Dan Bernstein's fabulous Curve25519 beautiful elliptic curve cryptosystem that allows encryption and hashing and Diffie-Hellman style public key exchange. Basically it is an absolutely complete library. And Leo, if you click that link, they have a page showing the language bindings. This thing has language bindings you cannot believe. Any language anyone is using, you can use to link to libsodium. I was back using it at 0.0, or I think it was 0.7 was where I was. It's now at 1.0.6. And it is just a beautiful, complete, cryptographic toolkit that I wanted to just make note of. Look at all those languages. I mean, it's like the Who's Who. I don't know if there's anything that's missing from that.

Leo: Hey, it's got Common LISP and Clojure, so I'm happy.

Steve: Yup.

Leo: Look at that. Erlang, Go, Java, JavaScript. That's great. Yeah, you're right, this is a pretty good place...

Steve: PHP, Python, R.

Leo: Racket, I like Racket.

Steve: Ruby.

Leo: Swift, there's two implementations. So, yeah, there's no excuse not to use it.

Steve: No. And it is, as we've said, do not roll your own. Here it is. Really good people are running it and moving it forward. And in fact the thing that brought me up short was that they implement an authenticated encryption which they didn't have back in 0.7. I ended having to write my own. I did my own implementation of AES-256 GCM when Ralph, who was the early author of the Android client for SQRL, he didn't like the fact that I was using Phillip Rogaway's sort of proprietary but really nice authenticated encryption. Phillip and I had talked because I wanted to use that back with CryptoLink. And he said, oh, my god, of course, you're welcome to use it freely. And he just, you know, he said it was never my intention to profit. But - I'm blanking on his name. I just said it. The Android author.

Leo: I don't know his name.

Steve: Anyway - Ralph, Ralph.

Leo: Ralph.

Steve: Ralph I thought made a good point that GCM was a publicly available authenticated encryption technology. And I changed it. I dropped the use of Phillip's patented but available technology and switched to GCM, wrote an implementation. The good news is any - oh, and that's what SQRL uses to encrypt userIDs. There are two blocks in the identity. Each are encrypted with authenticated encryption to prevent anything from being changed. And also that's how we verify the user's password is after decrypting the password, we attempt to use the result of that decryption to decrypt the identity block, and then we check the authentication tag and see whether it works or not.

The point is that now that libsodium has it, nobody else will have a problem using the encryption that I chose for SQRL. It's now part of libsodium. And in fact all of the other algorithms I'm using, even scrypt, which is the basis for the mcrypt algorithm that I designed on top of scrypt to give us much longer and controllable decryption times, even that's there. So it's essentially the only package you need, that anyone needs, in order to implement all the functions that SQRL uses, but also any general purpose crypto needs. It's wonderful.

Oh, and in fact I remember now how I stumbled on it. Somebody tweeted me, asking a question about public key crypto. And I went to libsodium to update myself in order to give him the link, and then I discovered that there'd been a lot of progress recently. So, yay. And let's see. Oh, there was just a observation from a follower, and I don't know how to pronounce this. Moriturimax I think is how he would - or maybe Moriturimax.

Leo: Morituri, which means those who are about to die, Max.

Steve: Oh. Morituri - well, thank you. Is that Japanese?

Leo: No, the gladiators used to say it to Caesar before the battle.

Steve: Just before they...

Leo: Morituri te salutant. We who are about to die salute you.

Steve: They probably screamed it in that case; right?

Leo: Yeah. Well, it was a big Coliseum.

Steve: Anyway, so this was on giving law enforcement the wrong finger. And he notes, he says, "One thing about the podcast where a panic finger was mentioned regarding law enforcement. If they wanted to make sure you were using the correct finger, couldn't they lift your fingerprint from the Home button/sensor and compare them?" Of course, brilliant. "Overkill maybe, but they do that stuff for a living. Cheers, thanks again." So I appreciated his tweet. And I thought that was clever. Yes. That button is shiny, and it no doubt carries the fingerprint that you always use for properly unlocking your phone. And so they check that first, and then they look at your fingerprints, and they say, uh, we'll take this middle one on your left hand instead of your thumb. So I thought that was clever.

Now, I talked about how many primes there were last week. Turns out there are many, but nine is definitely not among them, which unfortunately I glibly cited as I went one, three, five, seven, nine, 11, 13, 17. And of course our astute listeners, many of our astute listeners said, uh...

Leo: Excuse me, Steven. As you know, nine is divisible by three as well as one.

Steve: You're not really going to try nine, are you? So the question is how many. And that's interesting. It turns out you can ask that question to WolframAlpha.

Leo: Oh, of course you can. They would know.

Steve: And you say, "number of primes under 2^1024." Right? So that's how many - so 2^1024 is the number of primes that would fit in a 1024-bit public key. The answer is two, approximately - and there's an equation that actually knows this, so it's, you know, I love mathematicians - 2.53274x10^305, okay, 2.53x10^305. So we know that 128-bit absolute security, symmetric security, or if you really want to go crazy, 196, or really crazy, 256, is crazy brute-forceable-proof security. So this is 10^305, meaning - and in fact I actually...

Leo: So I said 2^24. What is the number that you're looking for? Is it...

Steve: 2^1024.

Leo: 1024. You know what I find interesting in this plot? It's a linear number.

Steve: Yes.

Leo: The primes are evenly distributed, which I did not know.

Steve: Isn't that interesting? Yes.

Leo: I did not know that. Should have.

Steve: It's just very cool. Counterintuitive as heck.

Leo: Oh, look, it goes off the page.

Steve: Oh, my, oh, you asked for the exact count?

Leo: That's the number. That's the number. Holy cow. All right. That's the approximate number of primes.

Steve: But we won't tell anybody if you use the last 15 digits as a password, Leo.

Leo: Wow. That's awesome.

Steve: Yup. Plenty of primes. Plenty of primes in the sea.

Leo: Wow. I love it that it's a linear - and I wouldn't have seen that with 2^1024 because it's such a big number.

Steve: Correct.

Leo: Because when you do 2^24, you see a graph showing you how many primes there are as you go up. And it's a straight line.

Steve: Nice.

Leo: Isn't that interesting. So you don't run out of primes, in other words.

Steve: Yeah, we're not going to run out anytime soon. And speaking of aluminium, which we were talking about the other day?

Leo: Yes?

Steve: Someone tweeting as Infinity Hammer said, "Something came to mind when you and Leo were discussing the number of syllables in the word 'aluminium.'"

Leo: Uh-oh.

Steve: Or aluminum. "I noticed that you often say the word 'mischievious,'" which he actually notes as "mischievous," with four syllables, "as if there were an 'I' after the 'v.'"

Leo: That's because you're an Okie.

Steve: And I thought, "mischievious," don't people say that?

Leo: No. You're an Okie.

Steve: And I always say "mischievious." So...

Leo: Yeah, I think Grandma used to say "mischievious."

Steve: Mischievous, yeah, "mischievious" seems more mischievious.

Leo: Yeah.

Steve: You know, it's a little more twist the knife, oh, you little mischievious rascal.

Leo: But it is just mischievous.

Steve: Mischievous. So...

Leo: It's hard to say "mischievous." That might be it.

Steve: Yes, you're right. Your mouth likes that extra little "i" in there, "mischievious."

Leo: Yeah.

Steve: Anyway, thank you for the correction. Now, important sci-fi news. Don't know how it's going to be, so don't blame me. But Arthur C. Clarke's famous 1953 - you heard that right, two years before I was born, 62-year-old novel "Childhood's End" has been made into a six-hour, three-part, three-successive-night miniseries.

Leo: But no spoilers because this has a massive twist in the last sentence of the book.

Steve: I'm not saying anything.

Leo: Right? Isn't this the one that has the massive twist?

Steve: Yes.

Leo: So six hours, five hours and 59 minutes in, your jaw will drop.

Steve: So it starts next Monday.

Leo: Oh, where, where?

Steve: On Syfy.

Leo: Oh, they do crap jobs.

Steve: I know, I know. So you get what you pay for.

Leo: It's going to be cheesy.

Steve: Yeah. So it's two hours Monday, two hours Tuesday, two hours Wednesday, three successive nights.

Leo: I'll TiVo it. Why not?

Steve: Oh, yeah. Well, yeah. I mean, well, yeah, of course.

Leo: But read the book. You know what, read the book.

Steve: I was going to say, it's been so long since I read it that - and the book is always better. And it's a classic...

Leo: In this case, absolutely.

Steve: ...classic sci-fi book.

Leo: It is one of my favorites. I read it probably as a teenager.

Steve: Yeah.

Leo: But I still vividly remember it. Yeah, you know what? This would be a good opportunity to reread it. It's not very long, I don't think.

Steve: And that Monday is also the official kickoff of "The Expanse" series. The preview has been out and floating around. That is, sort of the prerelease of Episode 1. But immediately following this first two hours of "Childhood's End" is a repeat of the first "Expanse." So if you already saw it, because, I mean, it's everywhere, it's on Play Store

and iTunes and Fire and everywhere, and I think Hulu and Vudu and so forth.

Anyway, they're starting that series. And that will be running for some time. And as I talked about a couple weeks ago, it's like, eh, I'm not sure. The very first scene was a mess, and it was kind of important, and no one watching it would have any idea what was going on, which is of course why I read the whole book series when I knew that Syfy was going to be creating it. But for what it's worth, next Monday, you've been warned, three nights in a row, two hours each, "Childhood's End." And...

Leo: By the way, "mischievious," I take it back. The nonstandard "mischievious" is not a new phenomenon. According to the OED...

Steve: Whoa.

Leo: ...this spelling has been in use as a variant since the 1500s. It was also common for the word to be pronounced with the stress on the second syllable, mis-chiev-ious, at least until 1700. It's now viewed as nonstandard and tends to be seen in regional, colloquial, or humorous use. But it is...

Steve: And on this podcast.

Leo: On this show. But it is a venerable and respected construction.

Steve: Well, thank you for that. I've had some people grumbling about not knowing, my not having a list anywhere of the sci-fi that I like. And I realized that's because it's been a while since I reminded people that I did, at our listeners' request, produce a PDF. It is bit.ly/sgscifi, spelled correctly, scifi.

Leo: None of this Syfy.

Steve: Yes, scifi, bit.ly/sgscifi. And that will bounce you to a PDF, which is I think it's three or four pages, where I just took the time a couple years ago to write it all down. And if it's there, I'm standing behind it. It's all the good stuff - Peter Hamilton, Michael McCollum and his great trilogies, just a bunch of wonderful stuff. Oh, all of the - it's been so long I've looked at it or thought about it. There's about six or seven book series, I can't remember the name now, of really good space warfare stuff. I want to say David Drake, but that's something else. Anyway, for anyone who's interested in my reading guide, bit.ly/sgscifi.

Also, my recommendation of Auralux was a huge smash. Many people wrote and said they loved it. And I got a kick out of having Andy note on MacBreak Weekly what I have here in the show notes, which I was going to make sure people know. I tweeted it the moment I found out about it late last week, and that is that Monument Valley, another fabulous, just a visual feast of beautifully rendered 3D graphics, is my style of you're not in a hurry, no one's pushing you, puzzle game software, is free only until midnight tonight. Unfortunately, listeners of this podcast who receive this after tonight who didn't also see my tweet last week or my tweet this morning, because I did it again, asking my

followers to verify that it was still free. The reason I did that was that it was free last week, and I received a tweet saying it was free today. And it's like, wait a minute, well, where's the boundary?

And so a listener, Barry Wallace, said, yes, Monument Valley is still free. There's generally a new free app every week, starting on Thursday evening Pacific time, he wrote, and it stays free until the next Thursday. Except that in this case, maybe he meant Tuesday because it is, we are told, in fact the publishers of Monument Valley tweeted in their own feed that, you know, get Monument Valley for free until midnight tonight. So again, anyone listening to this who likes my style of kind of relaxing but interesting, you know, there's no timer running, nothing's going to kill you, you just solve the puzzle. Monument Valley is another one way up at the top of my list. And I know, Leo, that you love it, too.

Leo: Yeah. Great game.

Steve: And, lastly, and you just tweeted something earlier this morning, Leo, about Outlook. One of the many things that bothers me about iOS, especially Mail, is that I sometimes receive mail that, when viewed in the iOS mail client, all there is "This message has no content." For some reason, email from a friend of mine in Canada, whom you've met, Leo, Bob, he often, when he's sending, he's using Eudora still, so maybe it's this email came from a client that's too old to be taken seriously, I don't know.

But anyway, the point is that I got so tired of seeing that, that I thought, okay, what else is around? Well, of course Outlook, Microsoft's alternative client is around, and it displays it perfectly. So just a little tip. If any other iOS users out there receive email from people whose clients don't generate, for whatever reason, email that the iOS mail client sees as valid, and thus says this message has no content, at least using Outlook, having Outlook, it's free to download, having it configured as a backup allows you to open your mail in Outlook and read the message correctly.

And we'll wrap up this two hours by maybe a tease for what I'm going to talk about next week. And because Phillip Rogaway, who I was just mentioning, he's the cryptographer at UC Davis. I mean, he's deep into crypto. Many crypto algorithms are to his credit, and patents, and academic work, and he's very involved. He just gave a talk last week, on December 2nd, in Auckland, in New Zealand, at the Asiacrypt Conference. He wrote a paper which is long, it's 42 pages, so I have not yet had a chance to digest it. But it raises an interesting issue, coming from a serious major cryptographer.

So the abstract of his paper reads: "Cryptography rearranges power. It configures who can do what, from what. This makes cryptography an inherently ?political? tool, and it confers on the field an intrinsically ?moral dimension. The Snowden revelations motivate a reassessment of the political and moral positioning of cryptography. They lead one to ask if our inability to effectively address mass surveillance constitutes a failure of our field. I believe," writes Phillip, "that it does. I call for a community-wide effort to develop more effective means to resist mass surveillance. I plea for a reinvention of our disciplinary culture to attend, not only to puzzles and math, but also to the societal implications of our work."

So I'm, of course, these issues are something that fascinate me and that we've discussed often on this podcast. So I'm going to make time to read his paper. And if I think it is worthy of discussion, we'll take a look at it next week.

Leo: Great. Always looking for a subject to talk about. Maybe we'll talk about Satoshi Nakamoto.

Steve: Ooh, yes.

Leo: You've got to read that article.

Steve: If there's more revelation.

Leo: It's pretty compelling. Although he's not the kind of guy you really wish that, like, he's not, you know, I don't know. It's just some...

Steve: He's not like a superhero being unmasked?

Leo: Not a superhero. He's just a normal person.

Steve: He's just like the guy next door.

Leo: He does own a million bitcoins, however. One of the reasons they're pretty sure it's him is because there's one big cache of a million bitcoins that almost every agrees must be Satoshi's.

Steve: Oh, my lord.

Leo: Nobody's saying who owns it, but there's, well, read it. You'll see. There's evidence that he owns it.

Steve: You know that Mark Thompson's entire garage is wall-to-wall mining machines?

Leo: You were lucky. You got in early. You got 50 bitcoins.

Steve: I did.

Leo: And I think it's too late at this point. Well, Mark knows what he's doing. He probably has...

Steve: Mark is net positive $22,000 a month.

Leo: Oh. What?

Steve: Yes.

Leo: Is he including his power bill?

Steve: Yes.

Leo: Okay.

Steve: That's the key. Arizona Power is incredibly inexpensive.

Leo: Ah, yeah, Boulder Dam. Ah.

Steve: Yes. And I checked in with him when I saw that jump. Remember the prices went up from - they jumped like 450, and then back, they settled back down to around 350. But he's positive $22,000 a month.

Leo: A month.

Steve: Yes.

Leo: Good on him. That's a nice little side job.

Steve: He had a second 50-amp power added to his home.

Leo: See, you can't even do that here. I mean...

Steve: No. No, you can't do it. And our power is really expensive.

Leo: Yeah, yeah. And he's obviously got - does he buy those specialized bitcoin miners with, remember, the special ASICs and all that?

Steve: Oh, believe me, Leo. We both know him.

Leo: He's no fool.

Steve: He is so deep in...

Leo: If he's going to go after this, it's got to make sense, yeah.

Steve: He's actually turning the hardware over following the increase in power up the curve...

Leo: You have to.

Steve: ...paying for it from his earnings, in order to stay there. Oh, it's just a brilliant concept.

Leo: It's one of the brilliant little things Satoshi did was make it harder and harder to get bitcoin as the supply increased.

Steve: Exponential curve, yup.

Leo: Yeah. Computationally more difficult. So that's why you got in, you got in at a perfect time. You just had an old PC. You turned it on, and a day later, ka-ching.

Steve: Yeah, this thing was sitting here doing Skype. And I woke up in the morning, and there was 50 bitcoins. Like, oh.

Leo: That's pretty funny. Now, what is Mark's strategy for selling them, though? See, that's the trick; right? Because now it's a volatile market. You want to sell them now, you want to hold onto them...

Steve: Well, and actually he took profit. When it hit 450, he was smart. He said now's the time to pull profit out. And then, you know, he's putting it back into his system. But it's just sort of a fun thing for him to play with.

Leo: I'm willing to bet that the vast majority of bitcoins are now being mined in Arizona, only because of the power; right?

Steve: Yeah. Yeah, they're - actually, he knows where it is. There's somewhere in, I want to say Tunisia, under a hydroelectric dam.

Leo: Oh, yeah, that would be good, yeah.

Steve: Where power is so inexpensive that it's like the largest cluster of bitcoin mining farms.

Leo: And they're probably not Tunisians. They're probably foreign nationals who said...

Steve: Who are, like, leasing space.

Leo: ...where is the cheapest power in the world, yeah.

Steve: Yup.

Leo: Wow, fascinating.

Steve: Yup, interesting. Crazy times.

Leo: Yes. And we don't know where Mark lives, and so don't ask us. Or his bitcoin wallet number. Thank you, Steve Gibson. I know where Steve lives, GRC.com. That's his home on the Internet. You go there, and you might find some amazing things. Of course SpinRite, the world's finest hard drive maintenance and recovery utility. But you could also go there and find so many free things. The Vitamin D thing we were talking about, that's there. SQRL, that's there. Lots of freebies. And this show, amazingly enough, including transcripts, lovingly done by a human being. And lots of other stuff. Just go there, GRC.com. You can find audio and video of the show here, TWiT.tv/sn. Or subscribe, and you'll get it each and every week that way. Didn't we see somebody who just downloaded all the shows and started listening to them? Maybe that was...

Steve: Yeah, there was something in your Twitter feed this morning, I think, somebody saying that he'd grabbed them all.

Leo: Grabbed them all. All right. One more time...

Steve: There was somebody pulling 80Mb from GRC for about an hour not long ago.

Leo: Don't do that to Steve. If you're going to download them all, download them from me. You see everything like that because you monitor your traffic. Let me see one more time if I can get the Donald. I can't. I don't know why. This video will not play.

Steve: Anyway, so what you remember from it is that he's saying...

Leo: I'll read it to you: "We're losing a lot of people because of the Internet," says Donald Trump. "We have to see Bill Gates and a lot of different people that really

understand what's happening. We have to talk to them about maybe in certain areas closing that Internet up in some ways. Somebody will say, oh, freedom of speech, freedom of speech. These are foolish people." So as far as I can make out, it's not completely clear, he thinks that he can talk to Bill Gates to shut down the Internet.

Steve: Well, gosh, you know, that's who you want to talk to.

Leo: He's the guy, the boss of the Internet.

Steve: Probably give Ballmer a call first, see what Steve thinks about that.

Leo: Ballmer doesn't run Microsoft either anymore.

Steve: I know.

Leo: Yeah, all right.

Steve: He's busy with his basketball team.

Leo: He's got a nice basketball team for himself.

Steve: Yeah.

Leo: But I can bet one thing. Donald Trump will preserve the value of that bitcoin. Or maybe not. I don't know. I'll have to think about that. Ladies and gentlemen, thank you so much for being here. I wish I could have played this. You know what, whatever you think of him, he's fun to watch. He's very engaging.

Steve: Oh, this has been the most entertaining election pre-season that we've ever had.

Leo: Oh, my adblocker's preventing it. Let's try it without an adblocker, says John. You know, you forget that the adblocker does stuff.

Steve: Yeah, it's in there.

Leo: It's in there. No. Not yet. Just some mystery that we will never know. Thank you, Steve. Have a great day. We'll see you next time.

Steve: Okay, my friend, thanks.