The SMBGhost Fiasco

Description: This week we take a deep dive into the many repercussions preceding and following last week's Patch Tuesday. Wouldn't it be nice to have a quiet one for a change? But first, we look at a nice list of free services being maintained by BleepingComputer's Lawrence Abrams. We look at a recent report into the state of open source software vulnerabilities, and at new and truly despicable legislation aimed at forcing social media companies to provide "lawful access" to their customers' encrypted content.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-758.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-758-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here, but he's here by the hair on his chinny chin chin. He almost fell prey to, he thinks, COVID-19. Steve's coughing. He's feeling better. But he is here, and there's lots to talk about, including the latest Windows Update fiasco. We'll also talk a little bit about some of the best COVID resources and information you can get. And then why is open source software buggier than closed source software? It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 758, recorded Tuesday, March 17th, 2020: The SMBGhost Fiasco.

It's time for Security Now!, the show where we cover everything having to do with your security, including I think this week maybe a little bit of COVID-19. There he is, the man, the myth, the legend: Steve Gibson, who we hope lives long and prospers.

Steve Gibson: That's my plan. I surprised Leo.

Leo: I was a little worried when you told me the news, yeah. What happened?

Steve: Yeah, I've been very sick this past week. And that's unusual for me. The last time I was sick that I'm aware of was March 12th of 2015.

Leo: That's how rare it is. He knows the day.

Steve: It was determined by someone, I think I must have mentioned it in the transcript.

Leo: You did. I remember that.

Steve: And so they went back and found it. And of course we also know that I've never missed a podcast.

Leo: Never.

Steve: Because I've never been on my butt for one.

Leo: And I remember March 5th, 2014 you said I almost missed this podcast. I remember that.

Steve: Wow, okay.

Leo: Yeah. That's how little you get sick.

Steve: Exactly. So the first question you asked is have I been tested. Unfortunately, you know, that's the natural question to ask, and I would be first in line. Everyone knows. At one point I was having so many blood tests during my Vitamin D, natural Vitamin D production, that the phlebotomist who I rode up the elevator with at LabCorp every morning finally turned to me and said, "What the hell's wrong with you?" The point being that I'm all pro testing. But the truth is you can't get tested. I mean, and I'm not really sure except for that it would be interesting to know about the spread of this because this is what's really interesting is what does our next few weeks look like. For example, if I'm positive, I'm not on anyone's map or anyone's chart. I have verified that we have community spread in my neighborhood.

Leo: Oh, wow.

Steve: So it exists here. So for me, the fact that I'm so rarely sick, and the fact that I happened to get sick last week. So, okay, it could just be pure coincidence. But the second thing is that this has a different trajectory for me than anything I'm used to. I mentioned before we began recording...

Leo: Have you ever had the seasonal flu? Do you know what that feels like?

Steve: I don't know. I don't get seasonal flu.

Leo: I think it's rare. People often get gastroenteritis, the intestinal bug, which is a norovirus, not the seasonal flu, and they call it the flu, or the stomach flu. But if you had the flu, you would know. And the only reason - and I've never had it, either. The only reason I mention that is because I think that that would give you some benchmark for what it would feel like to have this flu.

Steve: Yeah. So I've done a lot of reading and research, wondering what this was.

Leo: Because there's still plenty of regular flu going around, you know.

Steve: Right. And in fact I was interested to see that, when people are wanting to get the test, what they are first tested for is everything else that we already have lots of tests for, in order to eliminate it being something other than COVID-19. Only if they're then negative for everything that we know about, then that qualifies them to see if they're positive for COVID-19.

Leo: That makes sense, yeah.

Steve: So there's an elimination screen first, which is exactly what you would want to do, and then you get the real test. There was some company opened two mobile testing stations, and their locations were kept secret. But of course nothing is secret.

Leo: And immediately jammed, yeah.

Steve: But in social media someone posted their location, and they were instantly swamped.

Leo: Which doesn't work because in order to give you the test, which is a laryngeal probe, goes way down...

Steve: It's not fun.

Leo: You cough. They have to wear all that protective gear, and they have to change it in between each test. So the only time you're going to get tested in a drive-through testing is if you have an appointment. They are not equipped to handle people just driving up, saying "Test me." I understand that. It's a safety issue.

Steve: If there's a laryngeal test, then there are two because the one I'm aware of they stick this Q-tip, like, further up your nose than you knew your...

Leo: It goes back down into your throat. Yeah, yeah, yeah, that's right.

Steve: Okay, yes, yeah. So anyway, I don't know. Someday I will know because the second there's an antibody test - what they're doing right now, they're testing for fragments of the virus's DNA, which they have located. So they grab that. They strip it apart. They amplify it. They turn the RNA into DNA so that it's able to replicate. They then make it copy itself several million times so there's enough of it for them to see, and then that they test.

Leo: Wow, that's quite a process. No wonder [crosstalk].

Steve: It is, yeah, oh, my god. And the problem is, it's that the test that we have now, that process requires a whole bunch of intermediate step reagents. And it's the reagents that we just don't have a stock of. Nobody was ready for this to happen. So anyway...

Leo: Are the reagents specific to COVID-19? Or are they just generally the same for all tests?

Steve: I don't know enough about the spread of tests. But what I have heard is that that's the shortage, that it's just there isn't...

Leo: Well, the CDC sent out a nonfunctional reagent at first. That was part of the problem.

Steve: Yeah, exactly. So the antibody has been identified. There's a group of 10 scientists, I don't remember where they are, who have demonstrated the antibody deactivating the virus, so they're jumping up and down. It was published in New Scientist a couple days ago. So there's lots of progress being made. The second I can get a test for the antibody, just it won't matter then except to satisfy my own curiosity, I will do so to see whether I did have it.

There were some reports of people getting reinfected, and the medical community thinks that's extremely unlikely. They were in China. They said they got better, then they got reinfected. They're thinking flawed tests in various stages. But apparently, once you get this, your body responds with its immune response, generates antibodies to deal with it, and then you're better.

And so that's what, to me, that's what feels different about this, is that I'm, like, I mean, I'm still having fitful sleep, and my right eye became incredibly infected late last week. This began with a tickle in my throat Monday night, a week ago, when I was working on the podcast. And I thought, hmm. Now, I still have my tonsils, so they're like hair trigger. And they're the first indication that some foreigner is trying to get in. And so it was worse Tuesday morning. I coughed a couple times during the podcast. I was self-conscious of it because I was aware I was probably getting sick.

Leo: Didn't even notice. I cough all the time, so I didn't even notice.

Steve: And of course I mentioned this to Lorrie, and she immediately disinfected the entire house. She went through medical school, so she understands a lot of this and has been a big help. We immediately put ourselves into separate bedrooms. And normally we're, as you know having been around us, we're very touchy-feely.

Leo: Yeah, it's very cute.

Steve: So now we miss each other.

Leo: I bet you do. I bet you do. That would be very hard for me and Lisa, yeah, yeah.

Steve: Yeah. So it'll be interesting to see another data point. I mean, I desperately don't want her to get sick. So who knows whether that'll happen or not. So I don't know. So the coincidence of, I mean, like almost never getting sick except now. Oh, what I was going to say was that the trajectory of this feels different. Normally, if I'm hit by a virus, it's a two- or three-day deal, and I dispatch with it. You know, thank you, immune system.

Leo: You're very healthy, yeah.

Steve: I'm never sick. Even back before Vitamin D in the GRC days where I had 23 people, something would wash through, unfortunately to quote Trump, would wash through the company, and I'd be the lone man standing. Everyone at one point or another would just be nuked by this thing, and it just wouldn't get me. Or maybe I'd feel a little something, and then it would go. So I have a history of...

Leo: Yeah, me, too. Are you Type O?

Steve: I don't know. I should know my blood type. It's weird that I don't.

Leo: Somewhere I read, probably specious, that people with Type O are less likely to get it than Type A blood.

Steve: Huh.

Leo: But anyway, I don't know if that's...

Steve: So anyway, so Lorrie and I are on self-imposed quarantine, like not only from the world, but from each other. I'm at probably Day 8 of symptom. I'm sounding much better right now. I'm really happy with this. I mean, I've got Kleenex around me, and I've got tea instead of milk-based drink because that's better for phlegm. Anyway, so I wasn't sure that I was going to be able to do this. A couple days ago it seemed unlikely. I took Sunday off, which I never do, just because I just didn't have any steam. And again, for me, that's sort of the indicator that I'm not over this yet, and that my body is at war with something that's taking it three times its normal length of time so far to deal with. Normally it just dispatches something very quickly. This time is different. So, you know...

Leo: I'm willing to accept there's a high likelihood that you got it. And I'm glad you survived it.

Steve: It's in the area. I happened to get sick at this instant in time, which is like, what? They're very coincidental. And also it has a different feel. It feels like this is something my body's never encountered before, so it's taking longer to work up its antibody population and deal with it. But anyway, so I just thought our listeners might find it interesting. Not that I'm representative of the population. I mean, this is...

Leo: But you're almost 65. You're going to be 65 when? Soon; right?

Steve: Next Thursday, yeah.

Leo: Happy Birthday.

Steve: Thank you.

Leo: Yeah. I'm glad you made it.

Steve: And so now I'm just, I mean, it seems so unlikely, if this is COVID, that I didn't already infect Lorrie before I became symptomatic, before we even knew, although we did instantly implement lockdown for ourselves, living together, when we became suspicious of that. But so that'll be interesting to see. She just got a pneumonia shot a few weeks before. So she was thinking maybe that gave her just a little opportunistic boost at a time when it might need, you know. We don't know.

Leo: It is the case, if you're older, you should have a pneumonia shot - I had one - and that it is a good thing in this case to have that, that it helps, a little help, little protective, extra protective.

Steve: Yeah. And in general, you know, of course, now we're a day into a much increased lockdown, which I think makes so much sense. You know, in theory, I was thinking about this, if it had an R naught of one, then nothing would happen. That is to say, if one person infected one other person, it would just sort of linearly and slowly move through the population. Measles has an R naught of about 18. If this had that, it would be an atomic bomb. I mean, it would just be over. If you think about the difference between one, nothing happens, and 18, I mean, it would just be an explosion of unbelievable magnitude. And it's been fun to watch all of the popular press trying to explain exponentiation to the general population. It's like, you don't understand yet.

Leo: Have you ever seen a hockey stick?

Steve: Well, and the other thing is that I keep reading in the press, I was reading about Orange County just this morning, they were saying there are 17 cases in Orange County. And I thought, did you actually just write that? No, there are not. You don't know about me. And the point is, unless you've tested everybody, you can't cite any number. There are 17 people who have been tested were positive. That you can say. But you can't say there are 17 cases in Orange County. Someone gave it to me. Who knows?

Leo: And you haven't been able to get tested, so you're not in that number.

Steve: Right.

Leo: Which is ridiculous. So you've tried to get tested. And what did your doctor say? Just we don't have any.

Steve: Yeah. He said no. He said, "First of all, Steve, we know you. Nothing knocks you down." He said, "You sound fine. You didn't ever..."

Leo: Oh, he didn't believe you.

Steve: Well, no, I mean, he also knows me long enough to know that I know my body, and I know what's going on. But the point is, and I don't really understand the logic of this, there are so few tests that they're rationing them. But I'm as valid a test subject because what they would always do is, as I said to you, what they're doing is they're giving all the tests for all the other things that cause seasonal stuff. And only if you're negative for all of them, that is, if they show that it's not any of the things we know about, then you get the special unavailable COVID-19 test. So I'd love to take all of those other things. Anyway, he just said, "I'm busy, go away."

And also I was already thinking, because normally I go in for my annual physical on my birthday. And I was thinking, I'm not sure I want to go into a doctor's office during a period of a global pandemic because there are going to be sick people there. Of course, that was before I became symptomatic. So I'm not sure how I feel right now. I think I'll wait until the summer, or at least till we get - see, the other thing is we don't yet - we haven't seen what China has seen. As a consequence purely of the draconian measures they implemented, they've seen, they've hit a peak, and they've reversed it.

We've seen so far no reversal. And you don't know anything about the future until you see a reversal. That's the indication. And of course you don't really know anything until you get tests. And it's looking like we're going to end up probably having many, many, many more sick people than we expect.

Leo: Yeah, that's obvious.

Steve: Because we just don't know how many people...

Leo: We just don't know, yeah.

Steve: ...are still "pre."

Leo: Yeah. I'm assuming everybody I come into contact with is sick. So I'm trying not to come in contact with them. But we, you know, and we should mention that we have instituted policies here. We're in one of the lockdown counties, or will be. Seven of the Bay Area counties are locked down. Sonoma County, our county is about to - oh, Steve, geez. You poor guy. Sonoma's about to join that. You're in Orange County, not locked down.

But I think that this lockdown will go nationwide at some point, which means even though we're considered essential, media companies are essential, radio is essential and media companies, most of our employees are home right now. Carson's home right now. We have a skeleton crew that comes in, and we need an engineer here to

set up the board. But they're in another room. I'm in my office. I'm doing the whole day and will continue to do all the shows from my office, which only I enter. Not even the cleaners come in here. I've locked it. And so if it's got germs, it's only my germs. It's only Leo germs. And then of course I'm staying inside at home.

Steve: Which your body already knows all about.

Leo: It knows. It's got the antibodies. And then Lisa and Michael and I are staying at home, and nobody's coming over. Actually this morning my trainer FaceTimed me. We have a little home gym, so I was able to work out at home because they closed the gym. But I was able to work out at home with my trainer on FaceTime. You know, I didn't see her, but she could see me. And that worked great. So we're doing everything we can to keep our family, our TWiT family safe, and I hope you are, too, wherever you are. And Steve, you're scaring me. We've got to get to 999, that's all I'm saying.

Steve: Well, I hope there's an antibody test before we run out of digits here.

Leo: Well, I'd be curious to know. It sure sounds like - the only data point is that you didn't get a fever at all; right?

Steve: Yes, although there are asymptomatic, there are completely asymptomatic carriers of the virus. We know that.

Leo: That's what's so weird about this; right?

Steve: We know that for sure now.

Leo: But you weren't asymptomatic. You just got a different set of symptoms.

Steve: Well, no. And so the point is there's a range from asymptomatic to oh, my god, get ye to the hospital. And, you know, I mean, I've been symptomatic of something.

Leo: That's clear.

Steve: And so tonsils...

Leo: But the fact that you didn't have a temperature, maybe you got something else. Maybe it was just a bad cold. I've been taking...

Steve: We'll know someday.

Leo: ...our temperatures. We have an instant-read thermometer. I've been taking Lisa, Michael, and my temperature every day.

Steve: Boy, and have you seen those are now $400 on Amazon?

Leo: I'm trying to find them because I want to get one for my daughter. She's not feeling well.

Steve: Yeah, no.

Leo: Yeah, because - but the good thing is it's one of the in-ear ones and goes beep-beep.

Steve: Yup, I have one of those.

Leo: And I take our temperature every day, hoping.

Steve: I have one, too. I got it due to those E. coli experiences from Souplantation before I wised up and said, okay, no more tainted salad, thank you.

Leo: Oh, my god. COVID is not the topic of the show. We talk about security. But really COVID is part of the security scene; right? I mean, it's not - I mean, for instance, the HHS got - hackers tried to break into it.

Steve: Oh, my god, I know. Several attacks on different health-related organizations in the last week, just because they've got to aim their bots at somebody, so let's get into the news by attacking a group that are trying to help the planet. So I just wanted to say...

Leo: Go ahead.

Steve: I just want to say that the sequestration is the key. If we could instantly separate everybody, this thing would burn out in 14 to 21 days. That is, immediately it would be over. And we're expecting to have more. It's interesting, too, that we sort of have to be convinced of this because it's enough of an inconvenience for most people. I have about a five-minute drive from where Lorrie and I are to where I go to work in my original Fortress of Solitude here every day. Yesterday morning, whoa. And I'm commuting, such as it is, my five-mile...

Leo: There's nobody out there, is there.

Steve: No. The traffic just disappeared. It was, you know, it did not look like 8:00 a.m. on a Monday the way it normally looks. So I guess this is enough of an inconvenience that people need to be convinced from the evidence that this is necessary. But the

problem is, due to this time delay and the nature of exponential growth, by the time you get convincing evidence, you're already way past a point that you could have been. So as what's his name...

Leo: Fauci. Dr. Fauci, yeah.

Steve: Fauci said, he said: "I'd far rather be accused of having overreacted than underreact and see the results of not having done so."

Leo: The analog of this is the Y2K bug, which everybody said, well, see, nothing happened, nothing wrong, nothing went wrong. Yeah, only because everybody worked their buns off...

Steve: Yes. Yes.

Leo: ...to make sure nothing went wrong.

Steve: Yes. That's a perfect example. The general public didn't see all the engineers checking for this months beforehand.

Leo: So let's hope. Let's hope that we are the guys coming in off the golf course to rewrite our COBOL programs. And if we do it right, everybody'll say, see, there was no problem.

Steve: Or the Chinese restaurant program that I was involved with, Leo, because it was only there that it went from 1999 to 19100.

Leo: This is probably a story you've told. I don't remember it. The Chinese restaurant project?

Steve: Yeah. There was a place, the Mandarin Gourmet.

Leo: 19100.

Steve: Isn't that perfect?

Leo: That's not the bug we were hoping for, or we were looking for. Actually, everything would probably work if it went to 19100. It was 2000 that confused people.

Steve: Yeah, they were just unhappy that the receipts said 19100. And so they knew I was sort of a computer guy.

Leo: Steve, Steve. Free soup. Just fix this.

Steve: It was the best hot-and-sour soup and Szechuan string beans anywhere. So they said, "Can you do anything about this?" And I said, "Well, we need to concern ourselves about when Leap Year happens because you'd like to have February 29 happen at the same time."

Leo: Oh, man. He's good. Yeah.

Steve: I said, but if we were to just move the date back to a similar, to a synchronized calendar, then you wouldn't have a five-digit date any longer. It wouldn't be the right date.

Leo: Wouldn't be the right year, but it'd be the right day.

Steve: And he's like, "Oh, perfect." I said, "No, but I could really do more." And he said, "No, no, no. That's fine."

Leo: That's good enough.

Steve: "That's fine. That's brilliant. Thank you." And I said, "Oh, okay." But then, a few months later...

Leo: That explains why on your receipt it says February 29th, 1904. If you were wondering why, now you know. Oh, my god.

Steve: That's right. And then it was a few months later they had a bigger problem. Gerald came to me, and he said, "Orange County's changing our tax rate." And I said, "Oh." And he said, "So now we're in real trouble," he said, "because all of the amounts are going to be wrong on all of our checks." And I sighed, and I said, "Okay. Let me take a look at this."

Leo: Let me fix this.

Steve: So I copied the software onto a zip drive.

Leo: Oh, my god.

Steve: And brought it home.

Leo: You had to disassemble it; right? It was...

Steve: I did. I had to hack it. I went in. What I did was I knew what the current tax rate was. And so I converted that into floating point to see what the floating point representation was of the current tax rate. Then I searched the code for that string of bites which would represent the current tax rate. And I found it. There was exactly one hit on it. And so then I computed the floating point representation for the new tax rate and just patched it in. I held my breath, crossed my fingers, and it worked.

Leo: Amazing.

Steve: So I was able to just do a binary hack of their existing software. Didn't have to reverse assemble it or do anything. I just went in and went "gink" and fixed the tax code where it was in floating point representation.

Leo: Back in the day, that's how we would take copy protection out of disks.

Steve: That's the way we solved these problems.

Leo: Hex editor, little bit of editing, make sure it's not bigger than the original, and you're good. Just change the jump.

Steve: So this week we're actually going to talk about other things. We take a deep dive into the many repercussions preceding and following last week's Patch Tuesday. And, oh, my god, Leo, this is a drama. Wouldn't it be nice to...

Leo: I am never, I mean, I have taken Windows off of everything. That is, it's just unacceptable.

Steve: I know. Wouldn't it be nice to have a quiet Patch Tuesday for a change.

Leo: Every month. Every month.

Steve: Every month. But also we're going to look at a nice listing of free services being maintained by BleepingComputer's Lawrence Abrams. We're going to look at a recent report into the state of open source software vulnerabilities, what's going on over there. And, oh, Leo, at a new and truly despicable - and I have never used that word before, just never occurred to me, but wait till you hear about this - despicable legislation aimed at forcing social media companies to provide lawful access to their customers' encrypted content. And of course we have a fabulous Picture of the Week.

Leo: I love that. And I agree with it.

Steve: Yes, our Picture of the Week. My best buddy iMessaged this to me, and I grabbed it and thought it was perfect. So we have the headline: "Coronavirus Lockdown Rules: Do not travel. Do not socialize. Remain inside." And then the effect of those rules on two groups of people. Normal people in the first frame, looks like somebody who's just had

his beloved break up with him or something, and he's very distraught, like over the top. And then the second group, gamers. Yeah.

Leo: Yeah, baby.

Steve: This is like, okay. Do not travel? No problem. Do not socialize? That's how I role. And remain inside? Where would I go? So, yeah. And does this look like Tom Cruise to you?

Leo: It is Tom Cruise. That's the crazy Tom Cruise. I think it's when he was on "Oprah," and he was talking about his new relationship.

Steve: Oh, when he jumped around on the couch.

Leo: Jumped around on the chairs, yeah. I think that that's from that moment.

Steve: Was that Oprah, or was that Ellen whose chair he jumped off of?

Leo: It actually looks like Ellen, but I think it was Oprah. But anyway, does it matter, Steve? I'm surprised you even know who Ellen and Oprah are.

Steve: I am, too, Leo, frankly. You are the pop king, and I'm - what's pop?

Leo: I might be a little bit ahead of you, but not much. You know, this isn't just gamers. All of us, that's the funny thing, all of us are going, yeah, great, I'll have more time to code. Okay. I can finally read that book.

Steve: Well, and as we know, for me, my life is already like that.

Leo: It's no different.

Steve: Exactly. Except I'm no longer getting my coffee from Starbucks in the morning because thank you anyway. I'm back to making it myself.

Leo: Would you like some COVID-19 with that, sir? A shot of COVID-19?

Steve: Yeah, well, think about it. If somebody, if a barista did not have clean hands, they're snapping that plastic lid on every single paper cup that goes out. And then you're putting your mouth on it.

Leo: Yeah, exactly. It's been an opportunity for Lisa and I to do more cooking. We don't go out to eat. We cook. I cooked up a big batch of spaghetti sauce and

vegetarian black bean chili last night. I just, I mean, it's fun. Actually, I'm having a great time. I took my sourdough out of the starter. I'm going to make some bread. It's good. It's good times.

Steve: It's the sad times at the Houlihan's Bar, however.

Leo: Yeah. On St. Patrick's Day, too.

Steve: St. Patrick's Day, nothing's happening. Okay. So Patch Tuesday redux. We're actually going to do this in two parts. I forgot to mention that the title of Episode 758 is the SMBGhost Fiasco, which is one of the things that arose from Microsoft's - the interesting nature of their rollout and pullback and then delivery of a patch for an important vulnerability. So looking first at just Patch Tuesday, every single Patch Tuesday so far - well, okay, there have only been three of them this year, but still - it's resulted in, as we know, in a flurry of after-effect scrambling of one sort or another.

Last week's Patch Tuesday did not break the pattern. And it seems that increasingly, as Microsoft works to fix one problem, another one springs up. And as I was thinking about this yesterday, I was immediately put in mind of one of the most famous Three Stooges episodes titled "A Plumbing We Will Go." Which I have a link to a snippet from it. It's a minute and 40 seconds from a 17-minute episode. But Curly...

Leo: Curly has a pipe. It gets worse.

Steve: Oh, god. It's just so brilliant. Curly, of course, has very short hair. He attempts to solve the problem of the shower leaking by screwing a pipe into it. And then he's all happy until he turns around and realizes that there's a T-junction on the end of the pipe, and now there's two fountains of water coming out. So of course the point is that, rather than thinking that maybe he needs to rethink his strategy, he thinks like Microsoft that the strategy is good, I just need more of the same. So of course he continues adding pipes to this contraption until he ends up, we'll see here toward the end, he's basically jailed himself in a containment. It really is a funny episode. It's no longer politically correct, but it is quite funny.

Leo: None of these are - yeah, he's - oh.

Steve: And here he is.

Leo: Oh, there he is. Oh. That's Microsoft in a nutshell, right there. That's Windows, right there. That's exactly what the code of Windows looks like.

Steve: This is the analogy for Windows Patch Tuesday is you just keep adding pipes to the leaks, and it solves the leak where it was; but, oops, it springs out at the end of the pipe. So we have a whopping 117 vulnerabilities.

Leo: Oh, geez.

Steve: I didn't count them myself, and I saw 115, 116, 117. So you get the sense of scale, depending upon who you ask. But in any event, 25 of them are rated critical. All of them, all of the critical ones enable remote code execution and in some cases privilege elevation. In addition, that 25 are fleshed out by 91 rated as important, and then a single one at moderate. The top 20 of the 25 critical vulnerabilities are the most interesting. And believe it or not, Leo, I can't believe that it's 2020. Windows is still having problems with .LNK files, with dot L-N-K files.

Leo: Oh, my god.

Steve: Remember Windows 95, anyone? Unbelievable. We have CVE-2020...

Leo: I swear to god, this is why I've switched to Linux. I just - it doesn't happen. It doesn't happen.

Steve: CVE-2020-0884 describes, get this, a remote code execution vulnerability in Windows, occurring when a user opens a specially crafted and malicious .LNK file, which is just supposed to be a pointer to something else. So this file could be, this .LNK file could be presented to the victim on a removable drive or a remote share, and when opened would execute a malicious binary embedded in the .LNK file. So it's a sort of self-contained buffer overflow in a Windows .LNK file. And what's significant about this is that since .LNK files are non-executable, they are often passed over by any channel-monitoring AV system in the interest of it saving time.

These AB systems are desperate not to slow things down because they're already criticized for the fact that they do in fact impede the flow because they've got to open everything up and see if anything looks bad. So when they see a .LNK file, like, ah, that's just a .LNK file, we're fine, and lets it by. Except now. So that allows them to bypass AV system protections, which makes this worse. So one of the 25 was a remote code execution provided in a Windows .LNK file.

Then we had four memory corruption vulnerabilities in Microsoft's Media Foundation. Any four of those could allow an attacker to gain the ability to install programs; view, change, or delete data; or create new user accounts on the victim's machine. None of that's good. And worse, a user might have run afoul of this merely by accessing a malicious file or a web page, so it's easy to encounter. Attackers are most likely to try and exploit this vulnerability via spam email with malicious links and attachments. And I didn't dig any further in. But it sounds like we have four still surviving buffer overflows somewhere in the media content interpretation. We've often seen how difficult it is to get everything right in interpreters. But Microsoft still hasn't managed to.

And you know, Leo, doesn't it feel like with Curly and bathtub, we're not making progress on this problem? I mean, it's just like, when is this going to end? 117 things to patch now? Anyway, next up, and I had to count them, I counted 10. So half of the top 20 of the important vulnerabilities were all found in the way Microsoft's ChakraCore scripting engine, which of course is the engine Microsoft wrote from scratch for the first attempt at its illustrious brand new Edge web browser, which of course it later abandoned, and Edge of course replaced the creaky old Internet Explorer. In every one of these 10 different instances, an attacker could successfully corrupt - I've been suppressing a cough for a while - could corrupt the victim machine's memory in a way that would allow them to execute arbitrary code in the context of the current user.

Given that our web browsers are now the way we reach out onto the Internet and expose ourselves, I'm sure everyone is happy with Microsoft's decision to simply put their own window dressing around the open source, community developed and maintained Chromium web browser. But until you switch to that, 10 problems have been found, serious remote code execution problems in the original ChakraCore engine for Edge.

Then we had two additional critical remote code execution vulnerabilities fixed in the VBScript engine. That's not the JScript.dll, which is the old one that earlier versions of IE used, but IE11 doesn't use, but still would get invoked. This is JScript.dll, which is what IE11 now uses. So an attacker could exploit those two bugs by tricking the user into visiting a specially crafted website in IE11, or by marking an ActiveX control "safe for initialization" in an application or Microsoft Office document that hosts the IE11 rendering engine, as many of them do.

So these bugs, fortunately, well, there's only two of them, specifically require some user interaction and would rely on some form of social engineering on the attacker's part. Although they're both rated critical, and they're remote code execution, you have to, like, first go there and then load a document and then get it executed. So it requires more jumping through hoops, but that's not that high a bar these days.

So we wrap up the top 20 with two final ones, 2020-0881 and 0883, also remote code execution vulnerabilities, this time in GDI+. They're trickier because it's much more necessary for an attacker to get the user to jump through some hoops. But given that that could be done, they were rated critical, and Microsoft has patched them now. So I'm going to stop talking about last Tuesday because something way more bizarre that had the whole industry scratching its head happened last week, which I decided needed its own treatment, and it's the title of the podcast, the SMBGhost Fiasco, where I don't hold Microsoft to blame, at fault. I mean, it's bad that they had the problem. But it's a weird set of coincidences that caused them to really create a mess. So we will wrap up by talking about that.

I did want to note that last week we mentioned four companies - Microsoft, Google, Cisco, and LogMeIn - who are all making their various telecommuting resources available for, in the case of Google, Cisco, and LogMeIn 90 days; in the case of Microsoft 180 days, to help with, minimize the impact of lifestyle changes being driven by the need for isolation. Of course that's more important today than it was a week ago. So that's even more significant. I stumbled upon this. BleepingComputer's Lawrence Abrams is now created and has expanded upon this and is actively maintaining a page. I've got a link to it in the show notes. I imagine if you were to google "list of free software and services during coronavirus outbreak," that's in the tail of his URL, you would probably find it.

He wrote on that page: "In response to the Coronavirus (COVID-19) outbreak, many organizations are asking their employees to work remotely. This, though, brings new challenges to the workplace as users adapt to video meetings, screen sharing, and the use of remote collaboration tools. To assist a new wave of remote works and get some publicity at the same time, many software developers and service providers have started to offer free licenses or enhanced versions of their software and services." He says: "Below is a roundup of the free upgrades to services and software licenses being offered during the coronavirus outbreak."

Leo: This is very handy. I've been looking for something like this. This is really good, yeah.

Steve: Yeah. And he said: "If you are a software developer or technology service provider and would like to add any free offers to the list, please contact us and let us know."

So if I have helped to spread the word, I'm delightful. I'm delighted.

Leo: And delightful, yes.

Steve: Yeah, well, okay. Hopefully. When I'm not in everyone's ear. So rather than go through - he provides a detailed list of all of the vendors...

Leo: This is great.

Steve: ...with descriptions of what they are doing. It would take two more...

Leo: Most of these are time limited, usually for three months or thereabout, which is the presumptive time we'll be stuck inside.

Steve: Right. It would take about two more podcasts to go through in detail what they're each doing. So here are the vendors: Adobe, AT&T, Avid - which I thought was interesting - Cisco, Cloudflare, Discord, Drastic Technologies Ltd., Google, Instant Housecall, LinkedIn, LogMeIn, Loom, Microsoft, OneClick, Splashtop, TechSmith, Zoho, and Zoom. So if you know any of those companies, you like their stuff, you might check with BleepingComputer's list to see what is being offered and whether that's of use to you.

Leo: A number of people tried Teams because Microsoft has offered that for free. And it crashed, so many people tried it. It was down.

Steve: Well, yeah, that's the other really interesting thing. Our buddy at Cloudflare posted a blog about the observed change in traffic that they are seeing as a consequence of more people beginning to move to home work.

Leo: A lot of people are home. Get ready, because it's going to be a landslide over the next seven days.

Steve: Yeah, it is. Oh, and there was one other item. I noted that Lawrence did not include Pornhub, Leo, on his list of special services being offered...

Leo: Is it free now?

Steve: ...during this stay-at-home response to the global pandemic.

Leo: You and I have girlfriends. We don't really...

Steve: Yeah.

Leo: But if you're all alone, you know.

Steve: Well, I got a surprise. It was in the news. So I went looking for the details in order to put it into the show notes. And I figured I'd go to the horse's mouth. A Google search returned the headline "Coronavirus-free Video for Quarantined Italians" at Pornhub. What I was confronted with was definitely not the horse's mouth.

Leo: Now I know why you're coughing.

Steve: Yeah, do not go there, by the way, anybody. I've never gone; and, whoa, it takes no prisoners.

Leo: No.

Steve: Anyway, I found a banner: "Pornhub is donating its March proceeds..."

Leo: Oh, that's nice.

Steve: "...from Modelhub to support Italy during this unfortunate time. Model earnings will remain untouched. This is coming straight from Pornhub's share. To help keep you company during these next weeks at home, Italy will also have free access to Pornhub Premium through the month." So it's looking better, being stuck indoors if you're in Italy. Yes, never a dull moment for our listeners. That's interesting. I wonder what'll happen with April 15th deadline.

Leo: I think they already said you have 90 days to pay.

Steve: Think they're going to extend the filing deadline?

Leo: Normally you can file and do an extension, but you still have to pay. You can now do an extension, and you can defer payment, as well, I think, for up to 90 days. That's what Lisa...

Steve: That's a nice bit of cash relief.

Leo: They have to do stuff like this. Many states are making it so that you can't get evicted, that you can't get your power turned off. I mean, there's a lot of people who are going home without a job, in so many cases without a severance check. They're just on the streets, and this is tough for all of us.

Steve: Well, and I wish there were some way to say don't send me a thousand dollars because I'd much rather give it to, like have it spread around people who really need it.

Leo: Good point.

Steve: I'm not impacted by this. But there's no way to do that. But I guess I could donate it to a charity or something. But, yeah.

Leo: Anyway.

Steve: So the state of open source vulnerabilities. This was cool. I had to be very careful in the reporting on this because this company WhiteSource looks like they're sort of competing with the systems in place for dealing with open source vulnerabilities. So there was a little bit of a nanni-na kind of thing, which I had to filter out. But at least they did the work of surveying 650 developers that nobody else did.

So they collected some data. And it actually wasn't surprising, which in itself is interesting. They collected data from 650 developers, from the national vulnerabilities database, from security advisories, peer-reviewed vulnerability databases, issue trackers, and other sources. That allowed them to formulate a snapshot of the state of software vulnerabilities among open source projects. I have a link to their page that makes you put in an email address in order to get the PDF. It's like, okay, fine. But I have it.

So Sophos was a little bit brutal in their summary of the report. They wrote: "Open source bugs have skyrocketed in the last year," they said, "according to a report from open source license management and security software vendor WhiteSource." Thus the bit of a competitive challenge. "The number of open source bugs sat steady at just over 4,000 in 2017 and 2018, the report said, having more than doubled the number of bugs from pre-2017." In fact, we can see that in the chart below, where it was much lower. Then there was a big jump at 2017 and 2018, which were about the same. And then another nearly 50% increase last year.

So something's going on. And the question is, what? The CWE, that's the Common Weaknesses Enumeration system, which broadly classifies bug types, in the report states that by far the most common CWE encountered in the open source world is cross-site scripting problems. So that's not a surprise. That's been an ongoing problem. That accounted for nearly a quarter of all bugs. And it was the top for all languages except C. Cross-site scripting was followed by improper input validation, then by buffer errors...

Leo: Let me guess where the C was.

Steve: ...out-of-bound reads, and information disclosure. You're probably right. It's probably the buffer-handling things that C is, like, makes so easy to get wrong.

Leo: There's no range checking, and it's easy to go outside the buffer accidentally, yeah.

Steve: Yeah. Well, yeah, I mean, absolutely no checking whatsoever. You get a pointer to RAM.

Leo: Right, anywhere you want.

Steve: And you're supposed to not go below it. I mean, and many C techniques, like to scan the buffer...

Leo: Oh, yeah.

Steve: ...you increment the pointer.

Leo: Ninety percent of what you learn in C is pointers, and pointers to pointers, referencing and dereferencing, and tricks thereon. That's mostly what people do.

Steve: Yeah, it's a lot of fun, and you can get yourself in a lot of trouble.

Leo: We used to have, in the old BASIC days, PEEK and POKE. It's kind of like that, you know, you can look anywhere in memory. You can put anything anywhere you want.

Steve: Yeah. Now it turns out that Pornhub has PEEK and POKE, Leo.

Leo: PEEK and POKE as well, yes, it's another - yeah.

Steve: That's right. So there's also...

Leo: These numbers bother me because I think the difference is with open source it's open. And so you have these CVEs and the CWEs. And there's a lot of them. They issued them, I feel like it's FUD against open source. You just don't have as many in closed source because it's not open.

Steve: Correct.

Leo: So people don't know about the bugs.

Steve: Yes. Okay, shall we say Microsoft Windows?

Leo: Yeah, yeah.

Steve: We're not lacking for bugs in Windows, yeah.

Leo: And the other thing is of course they get fixed, and I think they get fixed right, not by Curly, most of the time.

Steve: Yeah, yeah. So then there are use-after-free problems where your language allocated some dynamic memory to hold something. You got a handle to it, which is often a pointer. And then the system garbage-collected it, or you released the memory, returning it to the system, but you still have the handle. So if the language you're using doesn't invalidate the handle to prevent its use, you're able to access memory that could be - or rather an attacker - access memory that could be pointing to anything at that point. So that distribution of the bugs is no surprise. That's the common bell curve of distribution. So there's been no explosion over the years in any one particular class of bug.

What we want to know is whether the increased numbers arise from there actually being more bugs per line of code, that is, the reduced quality of code? Or is it increased scrutiny of the same quality code which, as we know, will reveal more previously undiscovered bugs? Or is it that there's been a rise in the quantity of similar quality code, thus naturally resulting in a higher bug count? And we know that the open source community is way more active now than it was four years ago.

Leo: And to be fair, it's all three because anybody can contribute to an open source project. So it's not like there's any, you know, you have to pass a test to become an open source contributor. But I think the open source projects generally do very well. I don't know. I feel better running open source. And I have to say, when I'm using Linux, I'm just going, "Thank god I'm not using Windows."

Steve: Well, you know, I mean, and it's extremely handy. I needed for SpinRite - and by the way, the little video clip you played in MacBreak Weekly about, I don't know what it was.

Leo: Oh, yeah.

Steve: What's on the agenda for Tuesday? Well, MacBreak Weekly and endless discussions of SpinRite.

Leo: That hasn't been true. You haven't even mentioned SpinRite in a long time.

Steve: Not been true for a long time, in my defense. But also historically, once upon a time...

Leo: Back in the old days, yeah.

Steve: Well, and I have to say that it apparently was useful because in the selfie lines, many of our listeners are coming up to me with CDs to sign. They want autographs of their SpinRite memorabilia.

Leo: I got no problem with you plugging SpinRite. That's something everybody needs to know about.

Steve: And at this point our listeners would desperately love to have me plug SpinRite, that is, to have SpinRite to plug. So we're heading there.

Leo: He's working on it. He had to take a little time off, but he'll get better.

Steve: So their report states: "Given the continued increase of both open source usage and security research, the number of reported open source vulnerabilities will surely keep rising. In addition, we're starting to see the open source community looking for new initiatives in order to address the chaos in the open source security process."

Leo: And there's a little bit of that, too. That is fair.

Steve: Yeah. And they said: "One good example is the GitHub Security Lab, which aims to help researchers, open source project maintainers, and users to easily report suspected vulnerabilities in a secure manner without exposing a zero-day vulnerability to the world." And that's really a good point, that - excuse me.

Leo: Steve, you're making me feel bad.

Steve: I am so exhausted, Leo.

Leo: I bet you are.

Steve: But I'm going to get through this.

Leo: We'll wrap this soon, and you can go back to bed.

Steve: I never really focused on that before. It's easy to keep a critical zero-day secret in proprietary closed source software.

Leo: Exactly, exactly.

Steve: Since its discoverer only needs to privately contact the software's publisher. But in an inherently open world, where all regular business is conducted publicly and in full view of the world, we need some mechanism to be able to operate behind the scenes. So it's very cool that we have the GitHub Security Lab to step in with that role.

Leo: Yeah. And I think the telling statistic is that 85% of open source security vulnerabilities have already been fixed before disclosure. That's the good news. That's what you really want.

Steve: Yes.

Leo: That means only 15% are zero days or, you know. I mean, that's a big difference.

Steve: Did I skip that, or did you see that?

Leo: I saw it. I don't know if you said it.

Steve: Yeah, I think maybe I skipped it. But that was - oh, yeah. Oh, yeah. Under the category - I did skip it. Under the category of "good news," the report notes that over 85% of open source security vulnerabilities are fixed, are disclosed with a fix already available.

Leo: Yeah, [crosstalk].

Steve: And they said tech giants, yes, tech giants have invested heavily in better securing and managing open source projects over the past few years. And the community is working hard at security research to publish newly discovered open source security vulnerabilities along with a fix. They said the fix will usually be an updated version or a patch for the vulnerable code.

Oh, and one thing that's a little bit of a twist, just to finish covering this comprehensively, there's a growing number of vulnerability reports facing an insufficiency of developer resources which are required to examine, evaluate, and repair them. This suggests that we need a good triage system. We need them to be assigned useful priorities so that the ones that are really critical are handled first, given that you can't do everything. Turns out that some recent changes have made this a bit more tricky. The report explains it.

They said: "The rising number of reported vulnerabilities demands that development teams quickly prioritize their security alerts. The CVSS (Common Vulnerability Scoring System) is usually the go-to parameter for remediation prioritization, but should it be? CVSS was updated several times over the past few years (v2 to v3, and most recently v3.1), in the hopes of achieving a measurable, objective standard that helps support all organizations and industries. However, it has also changed the definition of what a high-severity vulnerability is."

They said: "We looked at over 10,000 vulnerabilities from 2016 through 2019 and checked their CVSS v2, v3, and v3.1 to compare the severity breakdown of vulnerabilities in each scoring version over the past four years The most noticeable change we saw in the update from v2 to v3 is that scores rose substantially, since a vulnerability that would have been rated at 7.6 under CVSS v2 would quickly find itself with a 9.8 under CVSS v3." And they said with CVSS v3 teams faced a higher number of, you know, running around with your hair on fire critical severity vulnerabilities.

So the sense we got was that we don't yet have the prioritization tools necessary. That would be something to focus on, for the community to focus on, is let's get real about creating a useful distribution so that not everybody is given a 9.8. If something doesn't absolutely really have to get fixed immediately, it could live down in the sixes and

sevens, and it'll be dealt with, not never, but once the really hair-on-fire deals are handled.

So anyway, a useful, I thought, a useful snapshot of where we are. No big change. A big absolute jump in the numbers, but only because there's so much more open source software activity today than there was four years ago. And I agree with you, Leo. Oh, I was going to mention that SpinRite - oh, it's what put me on the SpinRite topic that we branched off to is that I have a customized version of FreeDOS that I was able to create only thanks to the fact that it is open source. The problem is that SpinRite 6.1 will be encountering many non-FAT drives. And FreeDOS never expects to encounter a non-FAT drive.

Leo: It's so old, yeah.

Steve: So it goes out and attempts to literally log onto them in succession at boot time. And it runs across something it has - it's like, what? In some cases it just explodes.

Leo: Well, that's not good.

Steve: So I was able to go in. I added a new config.sys option, skipinit, which will be turned on in SpinRite's case. And it just says, don't worry about anything out there. We've got that. We'll be taking care of that here in the future. Just you go, you know, finish booting and then give us control.

Leo: Cool.

Steve: Okay, now, Leo.

Leo: I know you're peeved.

Steve: I'm not sure if you should take your blood pressure before or after this one.

Leo: Oh, I know all about this, and we've been talking about it for a while.

Steve: Oh, oh.

Leo: And what's sad is they're sneaking this through during this COVID crisis because they know that nobody will pay any attention to it. I even saw one of them, I think Dick Blumenthal, say...

Steve: I'm so disappointed.

Leo: I am, too. "We don't mention anything about encryption. What are you talking about?"

Steve: We're not talking about encryption.

Leo: Well, you'd better explain.

Steve: Okay. So it surely does appear that our government, embodied by crypto-naive politicians, maybe willfully so, is one way or another going to figure out how to break into the encryption protection assets of American citizens. The most recent effort, dubbed the "EARN IT" act is almost despicable. Okay, first of all, EARN IT is the most tortured abbreviation we've encountered in some time.

Leo: It's called a "retronym."

Steve: Oh, my god.

Leo: They come up with the name, and then they say what it stands for. They figure it out.

Steve: Never has that been more obvious than now. It stands for Eliminating Abusive and Rampant Neglect of Interactive Technologies.

Leo: Oh, we've been neglecting them.

Steve: I think Lindsey was so proud of himself. Okay. So get a load of this.

Leo: It's Lindsey Graham and Dick Blumenthal, the sponsors of this, yeah.

Steve: What is it that strong data encrypting companies would be earning? The legislation proposes to strip the protection provided by Section 230 of the Communications Decency Act from certain apps and companies, which would then hold them responsible for user-uploaded content unless they provide a means for "lawful access" to their encryption-protected content. In other words, they're holding ransom the hold harmless...

Leo: Yeah, because these are unrelated issues.

Steve: Yes. They're completely independent. They are ransoming this necessary section, this Section 230 of the Communications Decency Act, which social media companies have to have. And everything about this is slimy. So in other words, the legal protections that currently serve, they're in place, to hold all of our online social media companies harmless for whatever their users post, would now need to be earned by allowing law enforcement to have decryption access.

Sadly, EARN IT is a bipartisan effort, having been introduced by, no surprise, anti-encryption crusader Lindsey Graham, and also Richard Blumenthal and other legislators

who continually use the specter of online child exploitation to argue for the weakening of encryption. Remember that we discussed this back in December, end of last year.

While grilling Facebook and Apple, Lindsey threatened to regulate encryption unless the companies gave law enforcement access to encrypted user data while pointing to child abuse. He said: "You're going to find a way to do this, or we're going to do it for you."

Leo: [Crosstalk].

Steve: Yeah. "We're not going to live in a world" - oh, and did you hear about how our illustrious DOJ is in the loop here? Anyway: "We're not going to live in a world where a bunch of child abusers have a safe haven to practice their craft. Period," said Lindsey. "End of discussion."

So the EFF notes that one of the problems with the EARN IT bill, among many, is that the proposed legislation "offers no meaningful solution" to the problem of child exploitation. In other words, it's got nothing to do with it. The EFF wrote: "It doesn't help organizations that support victims. It doesn't equip law enforcement agencies with resources to investigate claims of child exploitation or training in how to use online platforms to catch perpetrators. Rather, the bill's authors have shrewdly used defending children as the pretense for an attack on our free speech and security online."

Leo: It's a straw man.

Steve: Uh-huh. If passed, the legislation will create a "National Commission on Online Child Sexual Exploitation Prevention" - okay, is that an acronym? Doesn't look like it - tasked with developing - oh, here it is - "best practices" for owners of Internet platforms to "prevent, reduce, and respond" to child exploitation online. But, as the EFF maintains, best practices would essentially translate into legal requirements. They said: "If a platform failed to adhere to them, it would lose essential legal protections for free speech." Meaning Section 230.

It turns out that the best practices approach arose from a pushback over the bill's predicted effects on privacy and free speech - they had to get extra slimy - pushback that caused its authors to roll out the new structure. The best practices would be subject to approval or veto by the Attorney General, currently William Barr, who has himself already issued a public call for backdoors; the Secretary of Homeland Security, who has made a similar call; the chair of the FTC, the Federal Trade Commission, ditto again. Everybody wants encryption bypass.

CNET talked to Lindsey Barrett, who's a staff attorney at Georgetown Law's Institute for Public Representation Communications and Technology, who said that the way that the bill is structured is a clear indication that it's meant to target encryption. He said: "When you're talking about a bill that is structured for the attorney general to give his opinion and have decisive influence over what the best practices are, it does not take a rocket scientist to concur," he said, "that this is designed to target encryption."

If the bill passes, the choice for tech companies comes down to either weakening their own encryption and endangering the privacy and security of all their users, or foregoing Section 230 protections and potentially facing a liability wave of lawsuits. A senior legal counsel for the ACLU said: "The removal of Section 230 liability essentially makes the best practices a requirement. The cost of doing business without those immunities is too high." So bravo, you slimy snakes.

Leo: The thing that makes it slimy is if they were to be forthright and propose a bill, look, we don't like the fact that bad guys, including predators, child predators, can hide behind encryption, let's make encryption illegal, if they were to propose that bill, which is really what they want, everybody, we'd all stand up and say no, no. So they're sneaking it in. They don't mention, as Blumenthal pointed out, it doesn't mention encryption. It just has the impact. It's actually clever.

Steve: Yeah.

Leo: But it points out that there isn't, I don't think, and they've run up against this before, the will in this country, people understand why breaking encryption's a bad thing. So they're not going to - they're going to sneak around us. So we all have to sit up and take notice. Section 230's been under assault for a long time. And that's another big problem.

Steve: Yes, yes, yes.

Leo: It gives these online companies the same kind of protection the phone company has. You cannot prosecute AT&T if a bad guy calls you up and says let's plan an attack on the United States. You can't say, oh, that's AT&T's fault. It's not AT&T's job to listen to every phone call and make sure nobody's planning sedition. And no one ever knows that.

Steve: And we don't want that.

Leo: No.

Steve: Yes. We don't want, yes, we don't want that in our society.

Leo: It's make the phone company untenable.

Steve: We wouldn't use it.

Leo: So, well, that's the other side of this is you can't stop encryption. It's done.

Steve: Right, right.

Leo: So this pushes it underground, eliminates protections for us, normal people, honest people, and makes it possible for bad guys to get into anything we do, as well. Such a bad idea. There is a petition you can sign. I mean, I would go out and do that, let them know that they didn't fool us.

Steve: Well, and the problem is by so cleverly cutting this pie the way they have, where they made the cut, one also wonders, I mean, clearly this will be challenged. It'll go through the courts. It may end up getting up to the Supreme Court. And again, it's like, oh, you know, would it get overturned or not? I mean [sighing].

Leo: What are you going to do?

Steve: Yeah. Okay. I'm going to do one more, and then take a break for our last spot and give one final burst of energy. I wanted to share with our listeners, and I created a grc.sc shortcut for it: grc.sc/covid, C-O-V-I-D. Ars Technica has assembled the best backgrounder that I've seen. They have a writer for them. Beth, I guess it's Mole, or maybe Mole, M-O-L-E. She's their health reporter.

Leo: This is great. This is so good.

Steve: Yes. "She's interested in everything from biomedical research" - this is from her bio - "biomedical research to infectious disease, health policy, and law. And she loves all things microbial. Beth has a bachelor's in Biology and World Music from the College of William and Mary, and a Ph.D. in Microbiology from the University of North Carolina at Chapel Hill."

I learned things there that I had seen nowhere else. For example, COVID-19. What happened to -16, -17, and -18? Well, no.

Leo: 2019; right?

Steve: It's from the year, 2019, exactly. So, and she talks about the related strings, the other things that the other two, you know, SARS, as we call it, and then there's the something that dealt with more the Middle East where dromedaries were the first intermediary animal?

Leo: That's MERS, yeah, Middle East Respiratory Syndrome, yeah.

Steve: That's right, MERS. So anyway, for anyone who wants just a no-BS, clear, clean, incredibly factual walkthrough, she's been maintaining it daily. The last it was updated that I saw was March 15th. I'm sure that they'll be refreshing it. So again, grc.sc/covid will just easily bounce you to it. And I can't recommend it highly enough. It was definitely worth reading during our present crazy times.

Something that's an impact that all this has had for Lorrie and me, we were very much looking forward to attending a presentation by W which was going to be early in April. We subscribe to...

Leo: You mean George W. Bush "W"?

Steve: Yes, yes.

Leo: Forty-five? Forty-three? What is he, 43?

Steve: Yeah, he was, yeah. And I'd just like to hug him and apologize for all the horrible things I said about him at the time.

Leo: He's looking mighty good now; isn't he. How do you like me now, huh? What did he say at the inauguration? Do you remember that? He had a...

Steve: No.

Leo: I can't say it. It's a little profane. Look it up. Just look up "what did W. say at the inauguration."

Steve: Oh, I do know. Now I know what you're talking about. When you said "profane" it's like, okay, yeah, that went into a different - it was categorized differently. This is some weird "s" word.

Leo: Anyway, sorry. Okay. On we go. That ought to get you through this long march, please. So I'm sorry you're going to miss that.

Steve: Yes. We are, too. It's the Distinguished Speakers series, and it was, I don't know, maybe eight different highly known speakers who came like every month and gave a presentation to our big...

Leo: I love that, yeah.

Steve: Yeah. Neat. And I would have...

Leo: It also has impacted - we are going to do a LastPass event with you, I'm very excited about that, in May, I think May 14th. But that's going to be virtual now. You were going to come up, I was looking forward to seeing you. But I think the wise thing to do would be to put that online.

Steve: Oh, well, you can't. Can you? I don't, I mean, it would be very lonely to be lonely. Lorrie, before you guys switched it to virtual, she said, "Honey, I'll drive."

Leo: Aww.

Steve: She said, "I'm not getting on a plane."

Leo: No.

Steve: And I said, "Well, okay, thank you, honey." But then [crosstalk].

Leo: Well, you're always welcome to drive up here. And I'll just stand six feet away and wave at you. It'll be great.

Steve: Yeah, well, I'm not going anywhere until this is...

Leo: No.

Steve: What I feel is just this profound fatigue. And that's what's so unusual eight days in. I just, I bounce back in three or four. So to me this says this is something new that my body is busy dealing with. And it's, you know, it's letting me be functional, largely. But I don't have nearly the energy that I typically do.

Leo: Well, please, we're going to be done in five minutes. When we're done, go to bed. And you don't have to do next week. If you're not 100%, let's take next week off. Honestly.

Steve: Well, Leo. That's going to be two weeks. I'll be with bells on. Okay. SMBGhost Fiasco. Okay. So this also happened last week. And this is crazy. And it had the whole industry, like, what the heck? Although Microsoft has not commented. What appears to have happened is that Microsoft had become aware of an extremely critical flaw residing in its implementation of the latest version, which is v3.1.1, of its SMB file and resource sharing protocol, you know, SMB v3.1.1. And it had prepared a fix for this problem. But for whatever reason, Microsoft apparently decided at the last minute to pull it, not to include it in this last Tuesday's March Madness patch fest. Perhaps they wanted to wait until April. Who knows? They're not saying, but we'll see why that was likely the right call at the time.

What we do know is that news of the apparently planned, but canned, vulnerability update became public knowledge last Tuesday, on Patch Tuesday. I have a screen capture snippet from MalwareHunterTeam that says "A wormable SMBv3 vulnerability. Great..." and then the crying tears emoji. And this reads, and then the screen capture from clearly one of the official reports: "CVE-2020-0796 is a remote code execution vulnerability." Okay. So we know there were 25. There were actually 26. But this one got, as we'll see, the evidence is it got pulled.

So 0796 is a remote code execution vulnerability in Microsoft Server Message Block 3.0. An attacker could exploit this bug by sending a specially crafted packet to the target SMBv3 server, which the victim needs to be connected to. Users are encouraged to disable SMBv3 compression and block TCP port 445 on firewalls and client computers, which is tantamount to saying stop using SMB. The exploitation of this vulnerability opens systems up to a wormable - and that's the thing that scares everybody - attack, which means it would be easy to move from victim to victim. So that appeared on Tuesday, March 10th.

So shades of WannaCry and NotPetya. Those were also SMB wormable flaws. The flaw in SMBv3 could not be more critical. Those two infamous SMB worms exploited the flaws in SMBv1. But this was a flaw in Microsoft's most recent release of SMB. In fact, so recent that it affected only 32- and 64-bit versions of Windows 10 and Server, with releases 1903 and 1909. So what's that, the last year, right, because I have 1909 on my most

recent things, and they last for six months. So for the last year. Because earlier versions don't support the SMBv3.1.1 protocol.

So for whatever reason, actually it's because Microsoft's added compression, the earlier versions of v3 didn't have this problem. Microsoft made a mistake. And of course any time you hear compression, you just - our audience just nods wisely and says, "Ah, interpreters, yes." No technical details have been published, but short and official summaries describing the bug were posted on the websites of two cybersecurity firms. This is what's weird is that it wasn't in the set. But they posted them, Cisco Talos and Fortinet. Cisco's entry for it was quickly taken down, once it became clear that this maximally critical vulnerability was absent from the Patch Tuesday rollout. It was expected, but missing.

Fortinet's entry was definitive, and I have a link here in the show notes to their entry about this. Fortinet wrote: "The vulnerability is due to an error when the vulnerable software handles a maliciously crafted compressed data packet. A remote, unauthenticated attacker can exploit this to execute arbitrary code within the context of the application." They didn't add "within the context of the server" because both ends of an SMBv3.1.1 connection turn out to be vulnerable. And anytime we hear "compression," we know that an interpreter is underlying the problem.

Okay. Next, the guys over at the cybersecurity firm Kryptos Logic performed an Internet-wide scan for all public systems or networks exposing the default port 445 to the public Internet. And rather than just scanning for 443 - and boy, stand back, unfortunately - they checked the version of SMB answering at each discovered port and determined that approximately 48,000 Windows 10 hosts, whether servers or clients, or actually servers because they were accepting connections, 48,000 Windows 10 servers are, or were, vulnerable to attacks targeting this SMBv3.1.1 vulnerability.

And anyone who's curious, it turns out, can do the same. There are several vulnerability scanners designed to detect Windows devices exposed to attacks hosted over on GitHub, including one created by Danish security researcher Ollypwn, who we've spoken of many times in the past. It's designed to determine whether SMBv3 is enabled on the device, and whether the compression capability that triggers the bug is enabled. So yes, anybody who's interested can grab a copy of that and run it on I guess the public Internet and find out how bad the problem still is.

Okay. So this leaves us with the question of how the information leaked, and there are two theories currently circulating. The first one looks at the Common Vulnerability Reporting Framework, CVRF, and Microsoft's Active Protections Program, that's MAPP. These systems provide Microsoft with a mechanism for sharing details about upcoming patches with trusted industry partners - certainly those two are. I was going to say "or were," but I'm sure they still are - such as antivirus makers and hardware vendors. The theory here is that Microsoft may have shared a list of upcoming vulnerabilities slated for March. And after all, remember that they are staging the previous month's, I forget what they call it. It's not something anyone ever wants...

Leo: Hot fixes?

Steve: It's the cumulative updates, but it's in Optional because it's for the upcoming month. So they sort of have them there.

Leo: Oh, their, like, insiders preview.

Steve: Getting them ready, yeah. So it's like a preview of coming disasters. Anyway - I mean attractions. Patches. So the theory is they may have shared the list of upcoming vulnerabilities, but then removed the bug, that is, the patch, from the list with little time for some vendors, namely Cisco Talos and Fortinet, to update their own security advisory pages in time. Someone with the handle @regnil tweeted: "Microsoft releases early versions of their CVRF to MAPP, and then pulls CVEs at the last minute without telling anyone. When they then fail to publish the public CVRF in a timely manner, it's understandable that mistakes like this will happen." Which suggests that the CVE was where that description came from, and that they grabbed the CVE, registered it with that, but said keep it private and so forth.

So the second theory is that the info about CVE-2020-0796 was accidentally shared via the Microsoft API, which some AV vendors, sysadmins, and reporters scrape for information about Patch Tuesday patches, as soon as they come out. So there's an API which essentially allows bots and other automated access in a uniform format, thus Application Program Interface, to this information. So the working theory there is that the bug may have been initially scheduled to be patched last week, but was later pulled without being removed from the API's backend database, thus eventually making its way into the Talos and Fortinet advisories.

Microsoft, for their part, has been mum about all of this, reportedly not returning anyone's request for comment. And at the time they would not even say when a patch for what we knew on Tuesday was a glaring disaster just waiting to happen, would be delivered. Knowing enough about the nature of the problem, which was a convenient side benefit of the inadvertent disclosure, many sites quickly posted their recommendations for immediate remediation. They all said users are encouraged to disable v3 compression, SMBv3 compression, and block TCP port 445 on firewalls and client computers.

Now, of course most individuals were never in any danger from this, just as they were not from WannaCry. As we know, our NAT routers are all behind a stateful, essentially a stateful firewall that simply drops anything inbound, like scanner probes, TCP SYN probes, to any port where it's not expected. So if it's not a reply returning from something we initially initiated outbound, it's got nowhere to go, and it's just ignored.

So what happened next? Two days later, Thursday, March 12th, Microsoft released a security advisory just as though this had been its plan all along. I have a link in the show notes to the advisory. In their advisory they write, kind of happily, with a cheery attitude: "A remote code execution vulnerability exists in the way that the Microsoft Server Message Block 3.1.1 (SMBv3) protocol handles certain requests. An attacker who successfully exploited the vulnerability could gain the ability to execute code on the target server or client. To exploit the vulnerability against a server, an unauthenticated attacker could send a specially crafted packet to a targeted server. To exploit the vulnerability against a client, an unauthenticated attacker would need to configure a malicious SMBv3 server and convince a user to connect to it."

Then they said: "The security update addresses the vulnerability by correcting how SMBv3 protocol handles these specially crafted requests." Then they said under mitigations, none. Under workarounds they had one. They said: "The following workaround may be helpful in your situation. In all cases, Microsoft strongly recommends that you install the updates for this vulnerability as soon as they become available, even if you plan to leave this workaround in place."

And then they have a means for issuing a PowerShell command, which you could also definitely do from just the regular command shell. Basically it's setting a parameter under CurrentControlSet\Services\LanmanServer\Parameters. They're setting DisableCompression to equal one, a DWORD value of one, and forcing the change. No

reboot is necessary. The workaround they said does not prevent exploitation of SMB clients. Please see item two in the FAQ to protect clients. They said SMB compression, get this, is not yet used by Windows or Windows Server, and disabling SMB compression has no negative impact on performance. Which kind of makes you wonder why it's enabled now, if they don't use it. But that's Microsoft. And then they give a means for turning it back on after the storm has passed.

Leo: So the thing to do is turn it off; right? I mean, there's no reason not to.

Steve: Exactly. Exactly. So an examination of all available evidence strongly suggests that this super-critical bug was at first going to be patched on Tuesday. Then for some reason Microsoft pulled it at the last minute, but not before their original intentions had been broadcast to their security partners. Reading the description of the problem makes clear that this would be really bad. So some Curious George went looking for Tuesday's patch and found it missing. That made news, you know, OMG. And then Microsoft was pretty much forced to release the patch two days later.

But wait, there's more. Then the other shoe dropped. Can you guess what? If you guessed "a multitude of botched installations and other problems," you get the brass ring. Having attempted to put this out into the world after the news of the problem had been mistakenly published, it now appears that Microsoft's original decision to hold this one back until it was fully ready was correct because at the moment it appears to be anything but ready.

The fix to this vulnerability is KB4551762. According to user reports, it's failing to install and worse. It's throwing - all of them begin with hex 800. So we have f081f, 04005, 73701, f0988, 71160, 240016 errors during the installation process. And there's stuff posted all over Microsoft Forums and Reddit and everywhere. One had the subject "Win 10 Updates Giving Me Grief."

He writes: "So I've had this issue since 7165, but the latest 1762 is also giving me the same problem. Basically, after it installs, it gets to 7% on the 'working on updates' part, then tells me that it failed, and it's undoing changes. Since 7165 had people complaining about bugginess and the like, I figured maybe that specific update was the issue, and used the tool that lets you hide updates. Sadly, the current update is giving me the same issue, and I've done all the things like DISM, deleting the software distribution folder, using the update troubleshooter, CHKDSK, et cetera. Everything is supposedly fine, even though there's clearly something wrong."

He said: "Kind of at my wits' end. I know I can just hide/pause updates, but it's not exactly a good idea to do for extended periods. What can I do?" And of course we also know that Windows 10 has taken effective control away from its users, so we can temporarily defer updates, but in no instance for very long.

Someone else said: "Stuck when update." He said: "My laptop current in version 1909, KB4532693," meaning the current rollup. "But when I update to KB4551762 [the new one], my device show we couldn't complete the updates. Undoing changes. Don't turn off your computer, and stuck there. Thank you."

So users are posting on Microsoft's official Feedback Hub. By the way, I tried to go there, and I learned I had to install an application in order to look at the Feedback Hub.

Leo: Oh, that's crazy. Geez.

Steve: So it's like, oh, really? No, thank you. On the Microsoft Community website and on Reddit, they're all saying, these are people who hang out in these places, none of the usual workarounds for the many various errors helped. We also had f0988 and f0900 installation errors spotted and reported by Gunter Born one day after the release. So that would have been last Friday.

One user reported through Microsoft's Feedback Hub: "Manual Windows Update on the local client works once. It finds the patch, then does nothing. One can attempt to download and install from that page, but it doesn't work. Next, go to the catalog. Select correct configuration. Download the patch. Attempt to install. Doesn't."

Another user said: "When downloading this update, my PC started becoming slow and sluggish. The update got stuck at 100%. I restarted the PC, then Windows Updates broke and started looping for a while when checking updates. It's now back to normal, but now I have a failed cumulative update." Someone on Reddit wrote: "So I've had this issue since KB4497165." And this is a repeat pretty much of what the earlier guy said.

So those were just the installation problems. And they may have been a saving grace for those users since, once the update is installed, all manner of things start going sideways. Although less numerous than the reports of installation failures, there are CPU usage spikes, high disk system usage spikes, system shutdowns, and freezes.

One user wrote: "These issues began yesterday, 3/13/20. The update 2020-03 Cumulative Update for Windows 10 Version 1909 for x64-based Systems (KB4551762) has failed every time I try to install it with the error code," and he's got a new one. It's 71160. I think that was new. "When the issue began, my disk drive also went to 100% with no change. I restarted my PC multiple times, but both issues persisted."

Or then we have: "After installing KB4551762 and KB4540673, my system has gone to trash. Extremely slow and takes ages...." Okay. I'm tired of reading these. Anyway...

Leo: I bet Microsoft is, too.

Steve: It's like, wow.

Leo: But the fact that not everybody has this problem, frequently Microsoft's bugs end up in interaction between that and something that people have installed, but not everybody's installed.

Steve: Yes, yes, yes.

Leo: This sounds like that.

Steve: Yes. And so on one hand we can say, okay, Microsoft, we're sorry that this system has become so fragile, making it necessary for you to test widely anything you do for these corner cases. But you've written a fragile system.

Leo: Right.

Steve: Clearly. I mean, we're talking about a patch to fix a problem in SMB compression, and that they're not using, and really for the last year. But it's there.

Leo: Is it possible something abused it or - I don't know.

Steve: I don't know.

Leo: It's weird, yeah.

Steve: In case any of our listeners are in or know of someone in this problem, there is a procedure which has worked. There's a video, a YouTube video produced by Microsoft Support, which I've linked to at the end of the show notes here. It's a final Hail Mary for when your system is seriously borked, and nothing else works. Basically it's a means for - it's called a "Windows 10 in-place upgrade" which preserves all your stuff, but basically it does an amalgamation of the past, binds it into an installation image, and then puts that back on your system so you are able to, you know. And so anyway, this video may be of use to somebody. Verify the criteria, and it may be the only solution for recovering from this in some cases.

Leo: Wow.

Steve: So it appears that Microsoft must have had, I mean, you know, they don't want this bug out there. They must have had some idea that this 4551762 might not be ready for primetime and therefore pulled it back at the last minute. And in retrospect this was probably the right decision. The problem is as critical as it gets. But on the other hand, we've seen that the total public exposure is around 48,000 systems, not 48 million. And it wasn't a zero-day. At the time it was completely unknown and not known to be exploited in the wild. So you could argue that someone probably did. You know, this is causing problems. Let's just wait until we see a zero-day report, and then we'll drop it instantly, and we'll be heroes. And so in the meantime let's see if we can make it work better because we have reports that it's not.

And it could have withstood. Had it remained a secret, it absolutely could have withstood, clearly, another month of development. It would have rolled out in April. Everyone would have said, oh, thank you for patching this problem that we didn't know we had that you created. But at least nobody got hurt by it. Now we've got this wacky patch that nobody is happy with. So just an unbelievable, here we are, third Patch Tuesday of the year.

Leo: Poor Microsoft.

Steve: Oh, yeah.

Leo: The thing is, if it's a third party doing something wrong, that's part of the issue with Microsoft, of course, a billion and a half installs.

Steve: That's a good point, too. You're right. Something has got its hooks in - if something has got its hooks into the OS.

Leo: Right. And maybe, you know, it's developers do all sorts of bad things. Maybe somebody found this compression routine and wrote a program and said, well, it's there, I could use it, and uses it. Or, you know, there are all sorts of things that could be causing this.

Steve: Okay. So there is a well-known term, "hooking the API."

Leo: Yeah.

Steve: That's bad.

Leo: Not okay.

Steve: Not okay. That's like the fact that hooking...

Leo: But it happens all the time on Windows.

Steve: Yes, yes, because Microsoft doesn't give people a non-hooked ability to do what they want to do. And so Microsoft imagines that they can just, like, no, we're not going to tell you about this stuff. And unfortunately, people who, I mean, Symantec and - I don't mean to pick on them. They just came to mind quickly because they're big. Avast and so forth.

Leo: All of these antivirus companies do this.

Steve: Yes. They're paying their engineers to solve the problem. So the engineer, who's happy to stay at home, especially now, rolls up his or her sleeve and says, "I'm going to find a way to hook this sucker so that I can get a brownie point at work." And so, yup. If you're allowed to be in the kernel with the rest of the kernel, if you're allowed to be in Ring 0, then that involves mutual trust because there are no rules down there.

Leo: Right.

Steve: And so all the AVs have to have a service component that runs in the kernel, and nothing prevents them from misbehaving. So I'm glad you brought that up because that really is probably the case, that it isn't sloppy coding. The fact that such a smattering of total users have the problem suggests that there's something those people have in common.

Leo: It's also why Microsoft's doing Windows 10X, which is going to come out this fall, which is a containerized version of Windows. And they want to do that, I suspect to isolate these issues into containers so, if it does cause a problem, it at least doesn't bork the whole thing. It only borks the individual containers. It'll protect the operating system against rogue programs, I think. I bet that that's the intent.

Steve, feel better. I am so glad that you have such a commitment to coming in. But seriously, dude, you're on death's door. Go to bed. We need you here next week and every week after that. If you don't feel better next week, call in.

Steve: I won't tell you.

Leo: Yeah, I know you won't. Here, just gargle some Purell and go to bed. No, don't. I shouldn't even say that in jest. Do not. That'll blind you.

Steve: And not bleach, either. Don't do that.

Leo: No, don't [crosstalk].

Steve: God, there is so much idiocy out there. Again, grc.sc/covid, C-O-V-I-D. Ars Technica's backgrounder is written by a Ph.D. microbiologist, is so compelling. For our listeners...

Leo: Ars knocks it out of the park with everything they do. Security, reviews, they are just - they have a standard that is just, I think, above and beyond. I'm always happy to consult them. If they say it, I believe it.

Steve Gibson, same thing. Man, that's why you've got to listen every Tuesday about 1:30 Pacific, 4:30 Eastern, 20:30 UTC. Steve's getting out of here. Go. Go, Steve. Go, Steve. You can catch him at his website.

Steve: Thank you, everybody. I'll see you next week.

Leo: Bye-bye. You can catch him at his website, GRC.com. That's where SpinRite lives, which is his bread and butter. But all sorts of other free stuff, discussions about SQRL. It's actually a really great resource. Look at this. Health resources for vitamin suggestions. I could just go on and on. And you will, too. It's a rabbit hole you'll want to go down, GRC.com.

If you want to message him, there is a feedback form there, GRC.com/feedback. But it might be better to do it on Twitter. He's always on Twitter, @SGgrc, and he accepts direct messages so you can DM him, @SGgrc.

When you go to get Security Now! on the site, you'll see there's a 16Kb version. There is a 64Kb version. Those are both audio. And there's a transcript. He pays to get a very nice transcript written by Elaine Farris - thank you, Elaine - who does a really stunning job. She's very good. And a lot of people, I think, because this show can be challenging, like to read along while they're listening to it. So get those all at GRC.com.

We have audio, but we also have video at our website, TWiT.tv/sn. You can go there, get a little bit of show notes, if you want. Most of the best show notes are at Steve's site. You can watch us do it live, as I said, on Tuesdays. That's TWiT.tv/live. Best thing you could do, if you ask me, subscribe. Then it's a no-brainer. You'll just have it. If you subscribe in your favorite podcast application, it'll download the minute it's

available, and you have it. You can go to YouTube, subscribe there, too. It's on YouTube.

It's also, and I always forget to mention this, but I'm going to mention it now. It's on Amazon Echo. It's on Google Home Assistant. Probably, for all I know, it's on Siri and Cortana, too. Just ask for it by name. Say "Voice Assistant, play Security Now! podcast." Sometimes adding "podcast" makes that work a little bit better. And it should play. The most recent version should play. The live stream is also available, if you say "Echo, play TWiT live." Most of the time that works. It doesn't always work. Don't know why. Most of the time that works, so you can listen to the live stream.

If you are listening live, go on into the chatroom, irc.twit.tv, a great place to get all of the background chatter. And a lot of smart people in there, too. It's a very good place to hang out. And this week, if you are sheltering in place, if you're self-isolating or quarantining, the chatroom is a great resource for you. They're there 24/7. There's somebody to talk to, some really nice people. Our mods are the best in the business. There's always a moderator in there. But there are also a lot of great people who are listening to the show: irc.twit.tv. If you need some friends in this tough time, we're here for you, and they're here for you.

I will be back tomorrow, Windows Weekly. We're going to interrupt right in the middle because Microsoft has a stream about their new Xbox One Sexy. And that'll be, I think, 11:40, right in the middle of Windows Weekly, so we'll stop. We'll start Windows Weekly. As part of it we'll show this Microsoft event. And then of course This Week in Google.

Stay tuned. In about an hour from now, All About Android. We're trying to be here as much as possible for you. Our hosts are working out of their houses in most cases. Our staff is, as well. There's only a skeleton crew here at the LastPass Studios because we want to all keep everybody healthy. I'm isolated, too. I'm in my own office. No one can come in here. So I feel like this is a safe place for me to do the show.

Thank you. Stay healthy. Take care of yourself. Take care of each other. And we'll see you next time on Security Now!.