The COVID Effect

Description: This week, as an interesting case study, we continue tracking the latest actions being taken by Zoom, and share another unfortunate consequence of their overnight success. We have two pieces of Chrome browser news. Our security news includes what happened with last Tuesday's Windows patches, rollbacks in authentication plans, Signal's reaction to the planned EARN IT act, trouble at the Tor Project, and an interesting CAPTCHA change at Cloudflare. I also want to share my recent change in preferred VM platforms and two bits of listeners' closing-the-loop feedback. We end with a SpinRite update, since stuff's beginning to happen!

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-763.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-763-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here, and there's lots to talk about, including all the things Zoom is doing right to protect security. Our favorite polar bear hacker has a new job. Congratulations! And then we're going to talk a little bit about 113 patched flaws - yes, our Patch Tuesday report - coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 763, recorded Tuesday, April 21st, 2020: The COVID Effect.

It's time for Security Now!, the show where we, boy, more than ever protect you against all sorts of little beasties out there on the Internet. This is the guy with the shield, the sword, the face shield, the mask, everything. Steve Gibson of GRC.com. Hi, Steve.

Steve Gibson: Hey, Leo. Great to be with you again. You're talking about - I was thinking about my moustache because I have...

Leo: Well, that, too, yeah. It's a filtration device.

Steve: I have two high school buddies who are both MDs, and so they're both feeling the effects professionally of this coronavirus and the COVID disease. And one of them shaved, had had a goatee, like, forever.

Leo: Yeah, yeah.

Steve: And shaved it off because they just...

Leo: Facial hair's not good.

Steve: Yes, they wanted less places for the virus to perch. And speaking of COVID, this is Security Now! Episode 763. And COVID and its effects on our society, as we've already been seeing, we've been talking about it, is having an impact everywhere. And I realized that the thing that glued all of these various security stories together this week was aspects of COVID.

Leo: Yeah.

Steve: So I just titled this "The COVID Effect." Not because it's about anything in particular, but it's affecting everything. So there is no big single topic. We're going to talk about, whoa, boy, we have the best Picture of the Week. Our listeners are not going to believe what happened. We also have, really as an interesting case study, we're going to continue tracking the latest actions being taken by Zoom. I bet you it'll end up being a business school study of how a company should react to what has happened to them. We also have an unfortunate consequence of their overnight success. We've already seen a few. Here's another one.

We've got two pieces of Chrome browser news, and security news including what happened with last Tuesday's Windows patches; rollbacks in authentication plans; Signal's reaction, the Signal company's reaction to the planned EARN IT act that we've touched on once before; trouble at the Tor Project; and an interesting CAPTCHA change at Cloudflare. I also want to share my recent change in preferred virtual machine platforms. I've fallen in love with one that surprises me. We've got two bits of listeners' closing-the-loop feedback, and I've got a SpinRite update since stuff's beginning to happen.

Leo: Ooh.

Steve: So I think our listeners will be interested in all of that stuff.

Leo: That's the best tease of all. Love hearing that. That's great. Well, we have a great show for you planned, as always, thanks to Steve Gibson. Steve?

Steve: So our Picture of the Week. I missed this, and it was from a comment that I saw somewhere in the security machinations online, talking about the probable reason that we had been seeing so many more-serious-than-usual bugs being fixed by Microsoft. The news is that SandboxEscaper, who we have covered extensively in the past, remember she has that really cool - she likes, well, she calls herself a polar bear. She likes solo camping in, like, Antarctica or crazy snow places; has this cool little single-person tent thing.

Anyway, she also, from her prior tweets, I mean, sort of seemed like a malcontent, maybe struggling with depression or, you know, I don't know what. But an incredibly gifted developer, hacker. We know that because of all of the grief that she was putting Microsoft through last year, finding problem after problem after problem in the Windows

kernel. Anyway, she tweeted: "Goals for 2020: Become the best programmer at Microsoft so people don't regret hiring me."

Leo: Awesome. Awesome.

Steve: "Meet other bears. Have more CVEs than the haters. Run to work every day, do lots of exercise, and defeat depression forever."

Leo: Good, good.

Steve: And then a little bear emoji.

Leo: Aww, that's great.

Steve: So they had the wisdom to track her down and say, hey, you know, we'd like to have you work on our side. Because, you know, she was just letting these things go. I mean, she was publishing zero-days. And it was like, ooh, ooh, ooh, ooh, ooh. So now she's fixing them rather than them being zero-days. And so, yes, last Tuesday we had 113 things that needed to get patched in Windows. But we'll get to talking about that in a second. So but anyway, I just wanted everyone to know that our friend of the podcast, SandboxEscaper, got hired, which is just a win for everybody concerned, certainly we users and both, I'm sure, she and Microsoft. So neat. Congrats.

As I said at the top, I think it's quite instructive from a security viewpoint to watch how Zoom deals with all of the various consequences of the overnight explosion in the popularity of their platform, even though it had been around since 2011. If their response had been lame, it wouldn't be interesting. But so far they've been anything but lame. Their response has been very impressive. And the past week brings us some even more impressive news. Last week they announced that they had hired Luta Security, which was founded by Katie Moussouris, a well-known cybersecurity veteran. Katie created some of the most important vulnerability programs still running today. She started Microsoft's Vulnerability Research and Symantec's Vulnerability Research.

Leo: She's really good. I'm so thrilled to hear this. This is great.

Steve: Yes. And the bug bounty programs for Microsoft and the Pentagon. She has been given a free hand to rebuild Zoom's existing security program, which had previously been based on HackerOne. So she's now taking input from across the entire cybersecurity community, seeking any ways, all suggestions welcome, to improve Zoom's vulnerability disclosure process. In her own posting about this new assignment, last week she wrote: "No company can bug bounty their way to being secure, and we at Luta Security emphasize building strong internal engineering to reduce the number and severity of vulnerabilities before software is released, as well as being..."

Leo: What a concept.

Steve: What an idea. Who woulda ever thunk about that?

Leo: Who'd have thought?

Steve: Yeah. And she said: "...as well as being capable of fixing bugs efficiently when they do slip through security development practices. When the pandemic hit, we were already wrapping up a full internal vulnerability coordination and management maturity assessment against ISO 30111 with Zoom." Which is interesting. I didn't realize. I mean, Zoom was already, before this was happening, saying we want to be proactive about this. So they were already there.

So she said: "So that's where the real change has to happen - internally. One of the five capability areas Luta Security measures is organizational. This is the executive will to change company culture, which we are all fortunate enough to witness with Zoom in real time." She said: "It's putting effort into investing properly in security and privacy, not just with words, not just by bringing in big names in security or jacking up bug bounty prices in a frenzy to create the appearance of diligence."

She said: "That being said, increased transparency from the many experts who are working together with Zoom to bring the very best security help gives the folks watching this effort a chance to see changes unfold." She finishes: "In cases like Luta Security's work with Zoom, we now get to ask the public for feedback on Zoom's bug bounties."

And then I asked, who were these big names in security Katie was referring to? Her follow-on tweet last Thursday read: "I'm excited to highlight my colleagues who are adding their expertise in the next few weeks. In addition to welcoming my former colleague @alexstamos" - who we spoke of last week - "to the extended Zoom security family, I'd like to welcome" - and then we have a series of twitter handles: "@LeaKissner, @matthew_d_green, @bishopfox, @NCCGroupInfosec and @trailofbits." She tweeted that on the 16th.

So Lea Kissner was the former global lead of privacy technology for Google. We all know cryptographer and Johns Hopkins professor Matthew Green. He's now on the team. And then there are three well-known security auditing firms: Bishop Fox, the NCC Group, and Trail of Bits. So perhaps some auditing is in the works, as well, as I was saying last week I hoped would also be happening.

So to maintain a high degree of operating transparency, Zoom's CEO, Eric Yuan, has started hosting a weekly "Ask Eric Anything" webinar. During last week's webinar we learned a few more things. He shared during this a "past week" and "next week" timeline, basically everything we've covered in the past week -changing defaults, hiding the meeting ID, the security icon added to the toolbar, disabling or disabled renaming participants, cloud recording, Zoom chat, dashboard enhancements, and also password complexity, something we hadn't talked about before. And they're adding a few more things going forward.

Account owners and admins can now configure minimum meeting password requirements to include numbers, letters, special characters, allow only numeric passwords. In the past it was possible just to use a number. So now they've made passwords much stronger. And free basic account users will now also be able to use alphanumeric passwords by default, rather than numeric passwords.

Last Saturday account admins acquired the ability to choose to have their data routed through specific datacenter regions geographically, giving them control of their interactions with Zoom's global network. This feature is intended to help with fears that Zoom chats and encryption keys might be spending some time over in China. So admins can override that nonspecific behavior and specify where they want things to go. And

then on Sunday, two days ago, the system added the ability to report abusive users so that Zoom can shut down accounts engaging in Zoom bombing. And that's a very quick automated process where you can just tag somebody who is Zoom bombing, and Zoom will immediately be able to take some measures in order to thwart them.

And then, during the same webinar, Alex was present, Alex Stamos, and he announced that in a matter of weeks they'll be moving from Zoom's currently, it's probably fair to call it barely adequate call encryption, to a more widely tested and trusted solution. Specifically, Alex said that Zoom will be moving away from the current AES-256 ECB - remember that's the Electronic Code Book encryption - to a more secure AES-256 GCM encryption, which by the way is what SQRL uses to encrypt its identities. So that is a good choice for them to jump to. And Alex also noted, he said: "The long-term focus will involve a totally new cryptographic design that greatly reduces risk to Zoom's system."

So to me, Zoom's response looks like a business management school case study in the proper way to engage and manage the explosive growth of a highly used, highly targeted, and inherently abuse-prone online facility. So again, I say bravo to Zoom. I just think they're doing everything right.

But there is always a dark side. Meanwhile, more than 500,000 Zoom meeting IDs and passwords are currently for sale. Apparently someone's been sucking them up using automated bots on the 'Net. And as we know, there's also been - there was essentially a robo dialer that was able to look for Zoom meetings based on ID and was finding a handful every hour. The price is not very high for these meeting IDs and passwords, apparently about a tenth of a cent, a U.S. cent each. To no one's surprise, a black market for Zoom meeting IDs and passwords has quickly sprung into existence. And we can assume since the price is so low that even the seller knows there's not much value there. The credentials are gathered through credential stuffing attacks and just scraping social media for any mention of IDs and passwords.

Leo: Yeah. So almost certainly worthless. Every meeting we do is a new ID. So unless you had a standing meeting, and you never bothered changing the ID or something, it's worthless.

Steve: Yes. Unless that was completely static. But on the other end of the pay scale, Motherboard reports that people who trade in zero-day exploits are sure there are two Zoom zero-days, one for Windows and one for macOS, currently on the market at an asking price of half a million dollars. So, yes, IDs and passwords are worthless. These guys - although informed people believe that's still very overpriced.

So here's what we know. Hackers are selling two critical vulnerabilities for Zoom which would allow someone to hack users and eavesdrop on their calls. According to three independent Motherboard sources who are knowledgeable about the market for these kinds of hacks, one each reportedly exists for the Zoom client for Windows, and another for the Zoom macOS client. The sources had not seen the code for the vulnerabilities but have been contacted by brokers offering them for sale.

Motherboard had previously reported that there had been a sudden increase in interest in zero-days for Zoom after, as we know, hundreds of millions of people, including employees and executives at big companies around the world, had moved onto the platform and were conducting sensitive and in some cases confidential meetings. A guy named Adriel Desautels, the founder of Netragard, a company that used to sell and trade in zero-days, said from what I've heard, he said, there are two zero-day exploits in circulation for Zoom. One affects macOS; the other Windows. He added: "I don't expect

that these will have a particularly long shelf life because when a zero-day gets used, it gets discovered."

Two other independent sources who asked to remain anonymous so they could discuss the sensitive topic confirmed the existence of these two exploits on the market. One of the sources, a veteran of the cybersecurity industry, told Motherboard: "The Windows zero-day is nice, a clean remote code execution, perfect for industrial espionage." The zero-day for Zoom on Windows, however, would allow hackers to access the app, but would need to be coupled with another bug to access the whole machine. So it sounds like it would need to be joined with probably a privilege elevation bug in order to do more. The macOS flaw is not a remote code execution, according to two anonymous sources.

So as I noted at the start, the asking price for these is half a million dollars. According to one of the sources who deals in the procurement of exploits, but has decided not to purchase this one, that source said: "The exploit requires the hacker to be in a call with the target, making it much less valuable for a government spy agency that is hoping to be stealthy and doesn't want to get caught." To me, this guy sounds like a vulnerability reseller like Zerodium. He also told Motherboard that he estimated the exploit was worth about half the asking price in terms of what the market will bear. And the macOS, as I said, is not a remote code execution, making it less dangerous and harder to use in a real hack, according to two other anonymous sources.

So as for Zoom, especially with their current very vigilant posture, you can imagine they're not taking this news lying down. When asked, they said: "Zoom takes user security extremely seriously. Since learning of these rumors, we've been working around the clock with a reputable, industry-leading security firm to investigate them." They said: "To date, we have not found any evidence substantiating these claims."

So of course that's what they're going to say. To me this sounds very credible, given the fact that it's multiple sourced and, if we believe the sources, they've had a chance to vet them and decide if they're worth, like how much they're worth, decided they were not worth a half a million dollars. So anyway, that's what's going to happen when there's something with this much overnight popularity. And Zoom is, as we know, scrambling to shore up its security. To that end, though, you'd have to say they are taking all the right measures. So tip of the hat to these guys. I really do think...

Leo: You're right, I mean, this is almost, this is a textbook example of how you solve this.

Steve: Yes. Yes.

Leo: I mean, it gives me huge confidence in them. Frankly, they're probably safer than almost anything else once this is complete.

Steve: I agree. They've got the best experts in the industry. It looks like they will soon be announcing a formal audit throughout their system and architecture. And with Matt Green in there, and Alex, they're probably going to have someone who they trust take a look at their code. I mean, that's already apparently happening on some level, at least at the API level, and say, okay, here's the things we need to fix. So I agree with them.

Leo: Super smart because here's their opportunity; right?

Steve: Yes.

Leo: Everybody's using them. And if you can give people confidence and say, look, we have stuff that no - we're more secure than anybody else, you know, I don't think any other conferencing system is undergoing audits, security audits right now. I don't know of anything like that.

Steve: No, no. And in fact, in the coverage of this, and I didn't add this to my discussion, but all of the articles say we still recommend it. That it is better to have something which is easy to use, and so the adoption friction is low, which is being fixed literally as we speak.

Leo: Yeah, yeah. You're not sharing state secrets. It's probably okay.

Steve: Yes, exactly, exactly. We've got two bits of news regarding Chrome. Google just updated all three desktop platforms - Windows, Mac, and Linux - to 81.0.4044.113 to squash a critical flaw that existed in earlier versions. Unfortunately, that's both the short and the long version of the story, since Google is saying nothing more. They wrote, as they do: "Access to bug details and links may be kept restricted until a majority of users are updated with a fix. We will also retain restrictions if the bug exists in a third-party library that other projects similarly depend upon, but have not yet fixed."

What little we do know is that Google was made aware of the problem by researchers at Qihoo 360's Alpha Lab, and that it addresses the Critical CVE-2020-6457, which is described as a use-after-free vulnerability that exists in Chrome's speech recognizer. So we don't know whether you need to be spending a lot of time talking to your browser for this to grab a hold of you, or whether a malicious website might have been able to leverage the flaw on any page that you visited. When I looked, that was the version of Chrome I was already using. And so I imagine that by now everybody already has it. Whether you're talking to yourself or talking to your browser, you're probably safe. I tend to talk to myself.

Leo: Yes, but your browser's listening, don't forget.

Steve: It might be busy translating it, yes. And something else turned out to be different than was planned in Chrome 81. Chrome has undeprecated FTP, of all things. We've talked about this a couple times already. For the past six years, since 2014, Google had been wanting to eliminate support for FTP in Chrome. I mean, really, who do you know? I mean, my super geeky friend Bob, who has unfortunately left this mortal coil some time ago, I remember seeing him putting ftp:// into a browser. And I said, "Really, Bob?" And he says, "Well, it's the best."

Leo: No, it's not. I actually own FTP clients; you know? I wouldn't use a browser for this. If you use FTP, why wouldn't you have a client?

Steve: That's exactly right. There are much more feature-complete useful FTP clients.

Leo: Yes.

Steve: Anyway, so they found that between 0.1 and 0.2% of the browser's users, and I should say slightly higher on the Unix platform...

Leo: Well, of course. It's because we're smart.

Steve: ...were using FTP. And again, there are way more feature-embellished FTP clients available. By the end of 2018, Google had moved FTP into the "won't fix" category in Chrome for iOS and began the march to slowly deprecate FTP support on their desktop browsers, as well. We talked about this at the time, with Google writing, and our listeners will probably recall that Google wrote: "FTP is a nonsecurable legacy protocol." They said: "We've 'won't fixed' FTP support on iOS, but its usage in Blink-based Chrome is high enough that it seems difficult to remove it all at once. This seems like a reasonable way of reducing its visibility as an attack surface as a stepping stone to more complete removal."

What they're referring to as "reducing its visibility" was their plan to continue displaying FTP directory listings, but no longer render files in the browser, only allow users to download them by clicking on a link in an FTP directory in your browser. Again, really? So with Chrome 80, which as we know was released a couple weeks ago, Google added an "Enable FTP" flag to control whether or not any FTP support would be present. It was still enabled by default, but Google used the flag to conduct a test where it was turned off for 1% of its user base to see whether anyone noticed or complained. The plan was to finally disable FTP support by default in Chrome 81, but still allow it to be enabled again using its #enable-ftp flag. But then COVID 19.

So on April 9th Google software engineer, let's see, it's Asanka Herath, posted to the "Remove built-in support for FTP from Chrome" Chromium bug topic that: "In light of the current crisis, we are going to 'undeprecate'" - and I had to force my spell checker to accept that - "FTP on the Chrome..."

Leo: "Undeprecate" is a rarely used word, I'm guessing.

Steve: Yes, "...undeprecate FTP on the Chrome stable channel. In other words, FTP will start working again. As with support for TLS 1.0 and 1.1, FTP support [fanfare sound] is being restored by default."

Leo: Undeprecated.

Steve: I know, to make sure there will be no problem with people accessing content on FTP sites during the pandemic. Turns out, for instance, many government agencies still utilize FTP sites, including the - wait for it - National Institutes of Health, the NIH. So Asanka Herath stated that this momentary reversal of FTP's deprecation, thus undeprecation, would endure until things were back to normal, and people were in a better position to deal with potential outages and mitigations and migrations and so forth. So yes, thus sticking with our theme, COVID.

Last Tuesday was our late-in-the-month Patch Tuesday. And it's a good thing that all Windows 10 users will have by now installed this month's Patch Tuesday updates and rebooted because everyone who did eliminated 113 notable...

Leo: You're kidding me.

Steve: Yeah. Oh, talk about fixing it after you've shipped it. How old is this? Oh, my lord. Nineteen of them were rated critical, existing in Windows and related software. And that crop of 113 problems included three critical zero-day flaws that Microsoft was aware of being actively exploited in the wild. The uncomfortable news for those of us who have chosen for whatever reason to continue using Windows 7, is that these three zero-days, and many other problems that are also present in our beloved Windows 7, unless you've got Extended Security Updates, will remain unpatched forever.

Leo: Oh, that's - see, it took a while for this to happen with XP, but it's happened right away with Windows 7.

Steve: It has happened right away, yes.

Leo: That's interesting.

Steve: Because Microsoft just cannot keep their hands off of their operating systems.

Leo: Well, that's probably a good thing.

Steve: Yeah.

Leo: I mean, they seem to need some hands-on, a little TLC.

Steve: Boy.

Leo: Geez.

Steve: Yeah. Two of the zero-days found being exploited in the wild were in Adobe's Type Library. We've already talked about one of those before, where we suggested temporarily disabling, renaming, or deleting, if you can, the offending Windows DLL. The problem with those rather heavy-handed moves was that some other somewhat important pieces of Windows like Media Player were dependent upon the offending DLL. An alternative for Windows 7 users was to consider subscribing to the micropatch service, that 0patch.com service, which would have these fixes deployed on the fly. So that's still a possibility. I'm going to trust Defender, which happily is still being updated on my Windows 7 machine. And unfortunately switching to 10 is not a simple thing. It requires - I guess I could make an image and then try upgrading to 10 and just hold my breath that, like, everything would still work.

Leo: If your hardware isn't superannuated, it should probably work.

Steve: Yeah, and it isn't.

Leo: Really, the only issue is drivers.

Steve: Right, right.

Leo: And the nice thing is, after you do that, you can always roll back because they do give the rollback.

Steve: Yeah. I might consider that.

Leo: I think you might have to at this point.

Steve: And I'd have an image so I could always just say, oh, boy, if the rollback failed.

Leo: Right. No, I would certainly do that, yeah.

Steve: Yeah, yeah, yeah. The third zero-day was a Windows kernel elevation privilege vulnerability that, being a zero-day, was found by Google's Project Zero being used in the wild. This one only rates as important, presumably because it doesn't allow for remote code execution. But as we know, privilege elevation vulnerabilities can be combined with other flaws to create a much more powerful attack, so it ought not be ignored.

There's also been some question in the security community about whether there might actually have been a fourth zero-day vulnerability fixed this month. But it appears that the advisory for the critical IE flaw, which was CVE-2020-0968 - which is interesting because that's a low number, so they've known about that for a while - was revised to indicate that Microsoft was not yet receiving reports and had no knowledge of it being exploited in the wild. Nevertheless, the advisory says this IE bug is likely to be exploited soon, and that would not be good since it's a scripting engine memory corruption vulnerability existing in IE.

Microsoft explains that a remote code execution vulnerability such as this exists in the way the scripting engine handles objects in memory. The vulnerability could corrupt memory in such a way that an attacker could execute arbitrary code in the context of the current user. On the other hand, IE. So, yeah, I mean, the danger is that there are things, as we know, that manage to invoke IE sort of behind the scenes. And that's the way the Adobe type flaw was still being used was in IE.

So anyway, it's good to get these things fixed. Also of note was another low numbered 2020-CVE-0796. If that number rings a bell, it's because that's the CVE for that Windows SMBv3 client-server remote code execution vulnerability, which prompted me in the middle of March to comment that Microsoft has just never been able to create a secure Internet-facing server, not only remote desktop protocol, but Windows file and printer sharing. This was the one that really had Microsoft freaked out and worried. They called it a "wormable" pre-auth remote code execution vulnerability.

And Microsoft released an emergency out-of-cycle patch in the middle of last month because they were unable to wait until this month's very late in the month Patch Tuesday, after a handful of public proof-of-concept exploits appeared. And although none of those has successfully performed the dreaded remote code execution, yesterday, April 20th, researchers at Ricerca Security demonstrated exactly that. So it's a good thing it had been fixed the week before and that all Windows 10 users were now immune to it.

And in more "we changed our minds because of COVID-19" news, known as Basic Authentication and originally specified in an RFC 2617, which was published back in June of 1999, so 21 years ago, Basic Authentication is a dead simple method of providing HTTP authentication for an online web app or a web browser page by simply adding the HTTP query header "Authorization:" followed by the one-word token "Basic" and a Base64-encoded username and password where the username and password are concatenated by a colon. The Base64 encoding wasn't meant to obscure it because it barely does. I mean, it's easy to Base64 decode. It was just so that the username and password could contain anything that they wanted to, and that wouldn't confuse the server receiving this query with other HTTP-ish things.

So anyway, the point is that this was simple and convenient because rather than any sort of back-and-forth handshaking or sticky state created by cookies, this simple query contained and asserted the application's credentials for making the query. In a single query it just says "This is who I am, and this is what I want." And once upon a time, without HTTPS, doing this would have been horribly insecure since there's no cryptographic challenge and response, nor even any encryption of the credentials, just a static assertion of the requester's identity, basically in plaintext.

So today, 21 years later, there are myriad ways of accomplishing the same goal with far more security, with OAuth 2.0 currently being the industry's favorite. So the use of this seriously old Basic Authentication has been falling by the wayside for a long time. Given TLS authentication and encryption, it's better. But no, nobody should be using it now.

Way back in, well, two years, way back in July of 2018, Microsoft announced it would be switching off support for Basic Authentication in its Exchange Web Services (EWS), that's the API for Office 365, and it planned to turn off support for the entire feature on October 13th, 2021. So about a year and a half from now. Google also committed to turning off Basic Authentication in December 2019, so five months ago. Google warned that it would deny what it called "less secure apps" access to its backend services, favoring OAuth 2.0 instead. That was meant to happen two months from now on June 15th of 2020.

But COVID-19 happened, and now both companies have reconsidered and changed their plans in the interest of giving their online users more leeway as they cope with the COVID-19 chaos. Earlier this month, on April 3rd, Microsoft said it would postpone the deprecation of Basic Authentication for Exchange Online for those tenants using it, keeping it available until at least the second half of 2021. And Google also announced at the end of March that it will defer its Basic Authentication switch-off until further notice. But as I said, anyone still using Basic Authentication really should be reading the handwriting on the wall and move to a much more secure authentication. And there's a lot of support now for OAuth 2.0, which is what both companies are now recommending as their preferred authentication flows.

All right. Sad to go from a nice high note to this, but we need to talk about this because it may be affecting us all. I think I used the word "despicable" when we first introduced this horrific pending legislation to our audience.

Leo: Oh, EARN IT, ugh.

Steve: It's despicable because it's employing an underhanded backdoor means for attempting to force encryption companies to alter their technologies to make them subpoena compatible. Joshua Lund is a developer and spokesman for Signal whom we've quoted a couple times in the past. Signal, as we know, is arguably the best and most securely designed end-to-end encrypted messaging solution. And not surprisingly, it's not only Zoom that has recently experienced a massive pandemic-driven adoption rush. In this context, Josh has recently spoken out about this EARN IT act. And I wanted to share Signal's position on this.

He writes: "Over the past several weeks, Signal traffic has gone through the roof. New users are signing up at unprecedented rates, and we've expanded our server capacity faster than ever anticipated. It means a lot to us that so many people are relying on Signal during this difficult time. When users check in on their families, share moments of solace, smile with their friends, or discuss sensitive health issues with their doctors, Signal's end-to-end encryption and privacy-preserving technology helps keep this information secure.

"At a time when more people than ever are benefiting from these protections, the EARN IT bill proposed by the Senate Judiciary Committee threatens to put them at risk. COVID-19 has us sheltering in place, but we cannot quarantine our concerns. Broadly speaking, Section 230 of the Communications Decency Act protects online platforms in the United States from legal liability for the behavior of their users. In the absence of this protection, many of the apps and services that are crucial to the way the Internet functions today may have never been created in the first place, or they couldn't have been created in America.

"The EARN IT act turns Section 230 protection into a hypocritical bargaining chip. At a high level, what the bill proposes is a system where companies have to earn Section 230 protection by following a set of designed-by-committee 'best practices' [he has in quotes] that are extraordinarily unlikely to allow end-to-end encryption. Anyone who doesn't comply with these recommendations will lose their Section 230 protection.

"Some large tech behemoths could hypothetically shoulder the enormous financial burden of handling hundreds of new lawsuits if they suddenly became responsible for the random things their users say, but it would not be possible for a small nonprofit like Signal to continue to operate within the United States. Tech companies and organizations may be forced to relocate, and new startups may choose to begin in other countries instead.

"For a political body that devotes a lot of attention to national security, the implicit threat of revoking Section 230 protection from organizations that implement end-to-end encryption is both troubling and confusing. Signal is recommended by the United States military. It is routinely used by senators and their staff. American allies in the EU are Signal users, too. End-to-end encryption is fundamental to the safety, security, and privacy considerations worldwide. Proponents of this bill are quick to claim that end-to-end encryption isn't the target. These arguments are disingenuous both because of the way that the bill is structured and the people who are involved.

"Riana Pfefferkorn, Associate Director of Surveillance and Cybersecurity at the Stanford Center for Internet and Society, wrote a detailed breakdown of some of the myriad problems with this bill. She also astutely points out that the bill would give unprecedented power to Attorney General William Barr, a vocal critic of end-to-end encryption, who would become the arbiter of any recommendations from the 'best practices' commission that the EARN IT bill creates.

"It is as though," he writes, "the Big Bad Wolf, after years of unsuccessfully trying to blow the brick house down, has instead introduced a legal framework that allows him to hold the three little pigs criminally responsible for being delicious and destroy the house

anyway. When he is asked about this behavior, the Big Bad Wolf can credibly claim that nothing in the bill mentions huffing or puffing or the application of forceful breath to a brick-based domicile at all. But the end goal is still pretty clear to any outside observer."

And Josh concludes with an "It's not too late" message. He says: "As billions of conversations transition online over the coming weeks and months, the widespread adoption of end-to-end encryption has never been more vital to national security and the privacy of citizens in countries around the world. Bad people will always be motivated to go the extra mile to do bad things. If easy-to-use software like Signal somehow became inaccessible, the security of millions of Americans, including elected officials and members of the armed forces, would be negatively affected. Meanwhile, criminals would just continue to use widely available, but less convenient, software to jump through hoops and keep having encrypted conversations."

He finishes: "There is still time to make your voice heard. We encourage U.S. citizens to reach out to their elected officials and express their opposition to the EARN IT bill. You can find contact information for your representatives using the Electronic Frontier Foundation's Action Center." He finishes: "Stay safe. Stay inside. Stay encrypted."

I have a full link to the EFF site, but I created one of my shortcuts for this purpose, grc.sc/earnit. That just bounces you easily to that EFF page where you can use it to look up your representative and send them your feelings about the idea of this legislation going forward. Ultimately it is up to us to keep this from happening. It just really is an amazingly slimy end-around legislation. We have to prevent this from happening. With any luck, it won't happen this year, and maybe we'll have different administration next year.

Leo: Yeah, I mean, I really do think it's Barr. Although, boy, you know, you've got Diane Feinstein who's always hated encryption. Dick Blumenthal.

Steve: Yes, yes, you're right. It's not just Republicans. It's Democrats are, like...

Leo: Blumenthal, ironically...

Steve: Blumenthal's behind it, too. He's the co-sponsor of the bill.

Leo: I know. He claims it doesn't prevent encryption, which either is naive or disingenuous. I can't figure out which. Recently he said something about how he had to have strong encryption. And I thought, well, why are you sponsoring EARN IT, then?

Steve: Yup.

Leo: So I don't - he may just be confused. But, yeah. It's a real issue.

Steve: And I didn't mention it again, but they always talk about protecting the children.

Leo: Yeah, it's always about the children.

Steve: Okay, come on, yeah.

Leo: That's the straw man. It's either terrorists or children because they know that nobody is in favor of child abuse or terrorism. So they can paint any opponent as being, oh, you must like child abuse, or you must like terrorists, instead of really debating the merits of it. And they don't want to do that because they know they lose.

Steve: And as we know, Josh's argument that the bad guys will simply use something else is exactly correct.

Leo: Right, they know that.

Steve: I mean, that is absolutely what will happen.

Leo: Dumb guy, you know, I remember back when we were doing The Screensavers, for some reason the Secret Service thought that Patrick and I knew something about technology or whatever. They asked us to brief them. And I remember talking to them. And they said, look, you know, most criminals just hand over the password eventually. They don't, you know, most of them aren't that sophisticated. Or if they are, they confess. They give up. It's really rare that you get somebody who is just not going to, you know, is going to be able to - but those guys you're never going to get because the math is out there. Remember they finally released the child pornographer, the guy who had a ton of child pornography on his hard drive.

Steve: On his hard drive. And he wouldn't, yup...

Leo: Wouldn't give up the password. And the judge finally said you can't hold this guy. Sorry. So I don't know. I don't know. EARN IT is not, clearly has nothing to do with child abuse, has everything to do with encryption. Period.

Steve: Yeah. Just another mention, sort of a public service announcement or a Tor Project service announcement. The Tor Project, of course, used to be The Onion Router. We did a really cool podcast back in the day about how it works, all the technology of protecting your anonymity on the Internet. Very difficult to do. It's not possible to do it perfectly, but Tor does everything humanly possible. I mean, it's been a real academic research project for years, just academicians trying to, you know, scratching their head, how can we make this better? How can we actually protect someone's identity? It is 100% donation supported.

And understandably, with so many past supporters worried now about the shape of their own future, the flow of donations has dwindled since the start of the year. Consequently, their recent staff of 35 people has just been reduced to 22, after a 13-person layoff. They were sorry to lose anyone, they said, since those were valuable contributors to the project. But there was just no money available to pay them. The project states that, with their reduced overhead, they should be okay. But if any of our listeners have been a user of Tor and/or you want to help keep their lights on and their servers spun up, it might be

worthwhile to drop them a little bit of monetary support, if you're in a position to do so. So yet another casualty. I mean, not the whole service in general, but they had to cut a third of their staff, essentially, in order to just pay the bills.

This didn't make it onto last week's podcast, although it was in my list of things to talk about. So I didn't want to pass it up because I thought it was just sort of interesting. I'm cutting the center out of a much longer blog post by Matthew Prince, who as we know is the CEO of Cloudflare. It was just sort of surprising, and I thought our listeners would find it interesting.

So jumping into the middle of his longer whole blog post, and I have the link to the whole thing, he said - this is Matthew Prince speaking, CEO of Cloudflare: "Since Cloudflare's earliest days, we have used Google's reCAPTCHA service. ReCAPTCHA started as a research project out of Carnegie Mellon University in 2007. Google acquired the project in 2009, around the same time that Cloudflare was first getting started. Google provided reCAPTCHA for free in exchange for data from the service being used to train its visual identification systems. When we were looking for a CAPTCHA for Cloudflare, we chose reCAPTCHA because it was effective, could scale, and was offered for free which was important since so many of Cloudflare's customers use our free service.

"Since those early days, some customers have expressed concerns about using a Google service to serve CAPTCHAs. Google's business is targeting users with advertising. Cloudflare's is not. We have strict privacy commitments. We were able to get comfortable with the Privacy Policy around reCAPTCHA, but understood why some of our customers were concerned about feeding more data to Google. Also, we had issues in some regions, such as China, where Google's services are intermittently blocked. China alone accounts for 25 percent of all Internet users. Given that some subset of those could not access Cloudflare's customers if they triggered a CAPTCHA was always concerning to us.

"Over the years, the privacy and blocking concerns were enough to cause us to think about switching from reCAPTCHA. But like most technology companies, it was difficult to prioritize removing something that was largely working instead of brand new features and functionality for our customers. Earlier this year, Google informed us that they were going to begin charging for reCAPTCHA. That is entirely within their right. Cloudflare, given our volume, no doubt imposed significant costs on the reCAPTCHA service, even for Google. Again, this is entirely rational for Google. If the value of the image classification training did not exceed those costs, it makes perfect sense for Google to ask for payment for the service they provide. In our case, that would have added millions of dollars in annual costs just to continue to use reCAPTCHA for our free users. That was finally enough of an impetus for us to look for a better alternative.

"We evaluated a number of CAPTCHA vendors as well as building a system ourselves. In the end, hCaptcha emerged as the best alternative to reCAPTCHA. We liked a number of things about hCaptcha solutions: One, they don't sell personal data. They collect only minimum necessary personal data, they are transparent in describing the info they collect and how they use and/or disclose it, and they agreed to only use such data to provide the hCaptcha service to Cloudflare. Two, performance, both in speed and in solve rates, was as good or better than expected during our A/B comparison testing. Three, it has a robust solution for visually impaired and other users with accessibility challenges. Four, it supported Privacy Pass to reduce the frequency of CAPTCHAs use. Five, it worked in regions where Google was blocked. And, six, the hCaptcha team was nimble and responsive in a way that was refreshing.

"The standard hCaptcha business model was similar to how reCAPTCHA started. They planned to charge customers that needed image classification data and pay publishers to

install their CAPTCHA on their sites. Sounded great to us; but unfortunately, while that may work well for most publishers, it doesn't at Cloudflare's scale.

"We worked with hCaptcha in two ways. First, we are in the process of leveraging our Workers platform to bear much of the technical load of the CAPTCHAs and, in doing so, reduce their costs. And, second, we proposed that, rather than them paying us, we pay them. This ensured that they had resources to scale their service to meet our needs. While that has imposed some additional costs, those costs were a fraction of what reCAPTCHA would have. And, in exchange, we have a much more flexible CAPTCHA platform and a much more responsive team."

So anyway, there was a big preamble about what reCAPTCHA is and so forth, or what CAPTCHAs are, and more. That was just the meat in the middle. And I thought our listeners would find it interesting that Cloudflare, a company that we think is doing a great job on many fronts, and that many of our listeners are users of, and a number of people we know of directly, decided, you know, reCAPTCHA, not so much anymore. We're going to look around. And I wanted to let our listeners also know about hCaptcha, yeah.

Leo: Yeah. I haven't tried hCaptcha, but I'm really starting to hate reCAPTCHA.

Steve: Yeah, yeah. A bit of miscellany. I mentioned a change of my virtual machine platform. I have been stunned by VirtualBox. I'm coming from an owner of VMware. It was sort of the early player, the original platform. I own it. I have a number of VM machines. When my XP machine hardware went belly-up, remember, about, what, maybe a year ago, I mean, the box completely died, I was able to pull the image from the RAID and get it into a VMware VM, so I was able to sort of bring it back alive enough to get the things off of it that I needed. Anyway, with the work on SpinRite, I don't know what it was that led me to VirtualBox. It is a free offering from Oracle. The more I use it, the more amazed I am.

I posted to the grc.spinrite.dev newsgroup a post, which I'll read. The subject was "STUNNED [in all caps] by VirtualBox." I said: "The more I use this incredible free tool, the more amazed I am. For my work on SpinRite, I had built and fine-tuned an optimal FreeDOS-based DOS system with Windows file sharing so that the DOS machine could see the SpinRite development directory on my workstation. It also had a font replacement for improved 50-line text fonts, my favorite non-protected mode debugger and various other utilities, and a boot menu so that I could boot into different DOS configurations. This perfect DOS machine was operating in a VirtualBox VM. So now I wanted to create an image of the drive so that I could clone it into several physical systems for additional testing on real hardware.

"To do that I wanted to use my favorite bootable imaging tool, which is Terabyte's Drive Image. So I plugged a Drive Image bootable USB thumb drive into the Win7 host machine. I opened Windows Disk Manager and looked up the physical drive number that had been assigned to the USB drive. In this case it was number five. I then opened a command prompt and switched to the 'VirtualBox' directory" - that is, the install directory where VirtualBox is - "so that I could conveniently use the 'VBoxManage' command line utility."

And then I show the invocation, the command that I used, VBoxManage internalcommands createrawvmdk -filename, then my "%USERPROFILE%"\.VirtualBox\usb.vmdk -rawdisk \\.\PhysicalDrive5. "That created a mountable usb.vmdk virtual virtual disk from the physical USB drive plugged into the Windows box. It didn't copy it. It just, on the fly, created a virtual virtual drive. I added that VMDK to the virtual machine that I wanted to image and moved it to the primary

master position so that it would have boot precedence. I also added another virtual disk to receive the image that Drive Image would create.

"I then rebooted the VM, and the Drive Image main menu popped up, and it all worked perfectly. I was able to create a drive image of the working DOS VM drive which was stored onto another virtual disk. I then removed the temporary drives and dismounted everything. I copied the newly created drive image onto the USB to create a self-contained bootable 'set up a DOS machine' thumb drive and, using that, I cloned my working, I call it 'SpinDEV image,' to multiple laptops."

And this is after using this thing for a couple months. Anything I have imagined that I've wanted to do with VirtualBox has been possible. The UI is just sort of the frosting. It's the standard things you want to do. It makes mounting and dismounting, creating and doing easy things simple. The key, though, is this VBoxManage command line utility. Oh, my god. I mean, just anything you can imagine you want to do. And it's compatible with all of the formats of everybody's virtual disk format. And that may have been the thing that brought me to it.

Anyway, upon seeing that, that I posted, a long-time contributor in the forums, Greg Bell, replied: "Fifteen years ago, then again 10 years ago, I tried all the various VM technologies and settled on VMware Workstation as being head and shoulders above the rest for pretty much everything. And I've used it all this time. Recently I had a need to revisit VirtualBox so I could collaborate with someone else. And, man, have they come a long way."

He said: "Like *everything* [he has in asterisk brackets] *everything* is possible if you know the right VBoxManage spell. Things I have to wrestle VMware to the ground over, VBox is like 'Sure. Want a hundred other options, too?'" And he says, "Command lines for everyone." And then he said to me, "Wait till you start getting into USB device attaching," which I haven't had occasion to yet.

But anyway, so I just wanted to take a moment to share my utter amazement over this completely free VirtualBox solution from Oracle. If you haven't looked at it recently, I wasn't aware of it a long time ago. I was just happy with VMware Workstation, which I, like Greg, it was the best thing I had seen. But, boy, I'm a convert. It just - it does a beautiful job.

Two pieces of closing-the-loop feedback from our listeners. Geoff Clow tweeted @SGgrc: "Steve." And he said: "FF with TST." Took me a little bit to unscramble that. He said: "Do you disable the FF built-in horizontal tabs? If so, how?"

Okay. So FF is Firefox. TST is Tree Style Tabs, which is the add-on I use to put tabs down the left-hand side. So he's asking, if you add the Tree Style Tabs to Firefox, what about the tabs across the top? And so to Geoff and everybody else who's interested, yes, I disable them. He says: "If so, how?"

Firefox is based on an HTML - the actual Firefox UI is driven by an HTML style sheet. And so it is possible, down in your user profiles, there you can find a style sheet file which you are able to tweak in all kinds of interesting ways in order to change the way Firefox looks. One of the things you're able to do is to remove the margin from the top where the tabs are and squeeze them out of existence. I found it just by googling. There is a way to go into some settings and have it help you get to the path where the file is located. But if you just google "customize Firefox style sheet" or something like that, or "user customization" or that kind of thing, you'll find it. So that's what I did.

The second is Lee Hadassin. He tweeted @SGgrc: "Hey Steve. Listened to SN-762." So that was last week. He says: "I think I see Moxie's POV [point of view relative to

privacy]." He said: "Privacy is there," meaning for the secure tracing. "Privacy is there until you test positive. If this is a framework for third-party apps, and they get the diagnosis keys, what is stopping them from correlating the time/location to possibly identify who it was?"

Great question. And I guess I would say that's out of scope for the API. What we talked about, and all Apple and Google collaborated on, is creating the underlying foundation. You are needing to trust the apps. And I guess it's the case, depending upon the accessibility, the visibility they have into your keys, if a third-party app knew that it was posting its diagnosis keys, and if it had been tracking where you were all the time, well, the diagnosis key has a one-day granularity.

So anyway, you know, it would be difficult in order to reverse that. I won't say it's impossible. But, for example, it's why I'm glad both companies are moving this down into the OS and why they've both said they're going to produce their own app to reference this API. I feel much more comfortable using apps' interface to this facility on my iDevices than any governmental or other third-party app. I don't think we're going to have to wait long for it. Apple recognizes the need, and they did say they were going to produce their own app. So that's what I would use.

Again, I think I agree with you. I don't know if that's what Moxie was talking about. It is the case that we have a foundational technology that lets us be secure. But, yeah, we're relying on the upstream integrity, privacy-respecting integrity that uses it not to work to subvert it. Certainly I think it's possible that something could.

And lastly, a little SpinRite progress report. I'm pleased to report that SpinRite's technology for talking to drives through AHCI controllers is starting to work. I've successfully performed an "identify device" command on both a VirtualBox VM and on a physical Dell laptop. I chose a very simple 512-byte "identify device" query specifically because it required the least possible from the drive and because it was probably the easiest thing for me to get working. The logic here is that getting anything at all to work with an AHCI controller requires so much hardware to be exactly correctly set up that pretty much everything has to be working correctly for anything to work at all.

So when I saw that I had captured the drive's identity information into RAM, I knew that now it was just a matter of refinement. Until now, until this time, SpinRite using the BIOS for its bulk data transfer has had the advantage of essentially hiding behind the BIOS. It was able to use the BIOS to provide a compatibility interface to whatever the motherboard's hardware happened to be. That's the big thing that's changing now, that SpinRite will be bypassing the BIOS for all mass storage access. So my plan is to refine this first utility, which I've been calling SpinTest, since it's intended to only be a development and proving ground for SpinRite's next-generation technologies. SpinTest will wind up being a complete robust mass storage device enumeration utility, talking directly to hardware. And as it develops, I will run it first on every piece of hardware that I own, and I own plenty since I never throw anything away. Then, once it's correctly working on everything I have, and I've tested as much as I'm able, I'll turn it loose into the guys over in the grc.spinrite.dev newsgroup for everyone there to test and to use on all their many pieces of both old and new hardware.

And I have no idea what will happen because I've seen reports of some very odd, finicky, and nonstandard hardware out in the field. Those may have been things that SpinRite had been isolated from, thanks to the BIOS. But wherever SpinTest initially fails, and I'm sure it will somewhere, I will get it working on everything that our testers are able to have it encounter. And this of course is a useful investment for me since this new technology will all be the basis for both the Beyond Recall product, which will follow SpinRite 6.x, and for SpinRite 7.

Back in 2013, before I put this SpinRite work on hold, I already had written drivers for the AHCI controller when it was in its legacy or compatibility mode, and also for older IDE motherboard controllers. That's how I was able back then to perform those benchmarks, which showed SpinRite reading 65,536 sectors at a time into a single 32MB buffer, and thus running at half a terabyte per hour. So I currently have all that code turned off to focus only upon AHCI. But once I've got native AHCI working completely with SATA drives, I'll turn that other code back on, and we'll have all system drives, both old and new, accessible to SpinTest without any BIOS involvement. So anyway, that's where I am, making great headway with this work on SpinRite, which I know a large number of our listeners are waiting for anxiously.

And I have news of next week. Unless something happens to derail my plan, I want to take our listeners on a deep dive into a very cool new service recently spun up by Cloudflare. It allows us to all test our own ISPs' BGP routing security in an effort to promote the adoption of an effective security framework known as RPKI, Resource Public Key Infrastructure. So stay tuned.

Leo: How exciting. I look forward to it.

Steve: Good stuff.

Leo: I've been - remember we talked some time ago, we were talking about, when we were talking about DOH, DNS-over-HTTPS, and we talked about Cloudflare. And then recently Firefox added NextDNS, and they had a quote on the front page from me which I didn't remember. Then I finally found the show in which I...

Steve: Right.

Leo: So I've revisited, and they have an interesting service. Cloudflare, you know, has added 1.1.1.2 and 1.1.1.3 for malware and ad blocking.

Steve: Yes.

Leo: And NextDNS does something very similar and very cool. So I'm just going to float that by your radar. I've started using it at home and on my mobile devices. And right now it's a free service, and it's really impressive. So just it's similar to - it's basically a pie hole that they're running for you, in effect. Malware protection, which I think is so important nowadays. If you want, ad blocking. But it does some fun things like it prevents typo squatting, so you don't accidentally go to T-V-V-I-T-T-E-R and enter your credentials and things like that. There's some very clever stuff. And I really love the logs because it gives you logging of all the devices using it. So really interesting. Just kind of run it over your radar at some point. I'm interested in this PGP protection because Cloudflare just announced that. That'll be very interesting.

Steve: Yeah, yeah, yeah.

Leo: As always, this is a must-listen-to show, every Tuesday. We're a little late today. We try to get it in at 1:30 Pacific for our live taping, if you want to watch us

do it live, anyway. That's 4:30 Eastern time, 20:30 UTC. The live streams, audio and video, are available at TWiT.tv/live. Also on YouTube Live, if you want to go there directly, although we link to that at TWiT.tv/live. If you're listening live, the chat room is live. Well, it's live 24/7. In fact, if you get lonely at all, any time of the day or night...

Steve: And it's got live people.

Leo: And there's actual people. And it's a really nice bunch. And so I know a lot of you are quarantining alone and maybe getting a little lonesome sometimes. This is a great place. I go in there sometimes in the middle of the night when I can't sleep, and there's always somebody fun in there. So irc.twit.tv. I want to give them a little plug. We also have a wonderful asynchronous community, kind of like your forums, Steve, in fact inspired by yours, running on the Discourse platform. That's www.twit.community, and there's even a Mastodon instance, twit.social. So we have lots of ways to interact. If you're a Steve Gibson type of fan, obviously, he's on Twitter at @SGgrc, and he takes DMs from anybody. So that's the best way to reach Steve, @SGgrc on the Twitter.

If you want copies of the show, he has some unique versions of it, a 16Kb audio version. It sounds a little like Thomas Edison singing "Mary Had a Little Lamb," but it's a very small file. So if you're bandwidth...

Steve: [Simulating poor audio]. This is Security Now!.

Leo: Mary had a little lamb. That's at GRC.com. So are 64Kb versions, if you want a little bit better audio. He even has transcriptions. It's the only place you can get transcriptions of the show that he commissions from Elaine Farris, and they are really good. So she gets every "um" and "uh" and everything. It's all in there. It's just like listening except you're reading. I think a lot of people read along while they listen, which sometimes aids with comprehension. There's a lot of material in these shows.

Steve's SpinRite is there, and the 6.0 is there, so you can get it right now, the world's best hard drive maintenance and recovery utility. When 6.1 comes out, you'll get early access to it if you buy it now. So if you don't have SpinRite, get it: GRC.com. That's the only paid thing on that whole site. That's his bread and butter. But he's got all sorts of other wonderful stuff there. Spend some time with Steve at the Gibson Research Corporation.

We have audio and video of the show at our website, TWiT.tv/sn. TWiT.tv/sn. You can also get it on YouTube. But the best way probably would be to subscribe. Find your favorite podcast application, search for Security Now!, and press the Subscribe button. That way you'll get it the minute it's available. And I know you don't want to miss an episode. This is one show where it's good to the last drop. You want to drink every drop of this fine, highly caffeinated beverage. So subscribe.

Steve, stay well, stay healthy, stay quarantined, and we'll see you next week on Security Now!.

Steve: Thanks, Leo.