Listener Feedback #234

Description: Leo and I catch up with a busy week of security happenings, including a surprising end to the TeslaCrypt file encrypting malware, Google's increasing squeeze on Flash, 117 million old LinkedIn account email and hashed passwords for sale, the encryption technology Google is using in their new Allo messaging app, Cory Doctorow keeps fighting for our rights, some fun miscellany, and questions and comments from our terrific listeners.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-561.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-561-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. We've got all the security news including, oh, man, more problems than you could shake a stick at, a complete indictment, frankly, of Microsoft and their Windows 10 upgrade process. Plus 10 of your questions and 10 of Steve's answers. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 561, recorded Tuesday, May 24th, 2016: Your questions, Steve's answers, #234.

It's time for Security Now!, the show where we protect you and your loved ones, your privacy, your security online, thanks to this man right here, a hero for our times. Ladies and gentlemen, I give you Steve Gibson. Hi, Steve.

Steve Gibson: You know, every Tuesday evening, after your group pulls this together and gets the audio posted, I download it in order to recompress it for Elaine. And I listen to the beginning of this, and I think, you have achieved such consistency through the years. It's the same sort of rev up and go.

Leo: Some would call it consistency. Some would call it a kind of a boring sameness.

Steve: Well, and also on The Tech Guy on the weekends, it's, "Well, hey, hey, hey."

Leo: Right. That I do on purpose. But, you know, that was because I couldn't say

"Good morning" or "Good evening" because The Tech Guy is heard across the country. So I needed a greeting that was agnostic, time agnostic.

Steve: Yeah, so sort of a Yogi Bear kind of thing.

Leo: We even have some stations tape-delaying it. I can't - yeah. [Crosstalk] Hey, hey, hey, Boo-Boo. It's time for tech talk. So it's a Q&A day today.

Steve: Yeah. We've got lots of fun stuff in the mailbag, since we had skipped several Q&As, although we did do a double Q&A three weeks ago because, remember, there was so much to talk about we only got, like, four done out of the 10 that we had scheduled. So I had 352, I think it was, pieces of unread mail when I dumped the mailbox, and so found some great things. And also, oh, you know, just a crazy week. Not a ton of news, but interesting stuff.

There was a surprising end to the TeslaCrypt encrypting malware episode. Google has announced their plans to continue putting the squeeze on Flash, and we'll talk about the details of that. Of course, appeared on the Internet for $2,200 was the sale of an additional 117 million old LinkedIn email addresses and passwords from 2012. So we're going to cover the details of that. We have an interesting little tidbit I just sort of liked about the underlying technology of Google's announced-last-week Allo messaging system.

Leo: Oh, I can't wait.

Steve: Cory Doctorow has been, it turns out, doing a series of posts. And I didn't pick up on it until the most recent one, but it's really significant, about, again, the entertainment industry struggling to close content on the Internet. And so I want to talk about, I want to share what he wrote because it's not very long, and actually I think it's really important that we understand at the technical level what he's talking about. And then we've got some fun miscellany and feedback from our listeners. So I think another great couple hours for our listeners.

Leo: And I see behind you that you have received something new and exciting.

Steve: Well, yes. When you mentioned the Ring Pro, or I did, someone did last week, because it was on - I'd seen it on Amazon, or I think I'd seen it on their site, and I didn't know what it was. And then I thought, hey, I don't think it's been four weeks yet. And sure enough, it had only been three since I ordered it from Amazon. So I was able to return it. And then I went to Ring.com/securitynow and saved myself shipping and got the Pro.

Leo: Smart man, yeah. Actually, I don't know, did you save shipping? Because I thought that they said that free shipping only applies to the original Ring. So, good. Good on you.

Steve: Yeah, yeah. So, and what I like about it is that it is - they solved the problem of the bezel coloration. So you get all - you get three different bezel colors.

Leo: Oh, they just snap on bezels, yeah.

Steve: Yeah, a silver...

Leo: Otherwise you have to order the one you want, yeah.

Steve: Right, a silver, a brown, and a black. And then the unit itself - or I guess a white, a brown, and a black. And it has the silver one snapped on it already. And as you said last week, basically there's not a lot of difference, but it is 1080p rather than 720p. So I figured, oh, since I hadn't drilled any holes yet, I might as well take the time and upgrade to the highest resolution one.

Leo: Yeah. Steve Gibson, Leo Laporte. Let's get to the security news.

Steve: So this was really odd. And there are a couple things that strike me as strange about this. We've talked often about the so-called TeslaCrypt, which was one of the early and - I hesitate to use the word "successful" in the case of file-encrypting malware, but it was very successful, meaning that it generated a lot of income for the cretins who created it. And as all of our listeners know, this is something that people would get their machines infected with inadvertently. And it would identify basically all of their content files, stuff that was the irreplaceable, unreinstallable portion of their world - their DOC files, their MP3s, their spreadsheet files, whatever - and encrypt it with a key.

And the confounding thing about this was that the technology was well designed. Before it did any encryption, it would contact a master server. And from the server, which would generate a key pair, it would use public key crypto to encrypt the files such that only the key which could decrypt them, that is, the matching asymmetric key, was available on the server. It was never on the victim's computer. So that made the decryption irrevocably one-way. There was no way to reverse this after it was done. And believe me, lots of security researchers looked at it carefully.

Now, we have talked about some "me, too" clones of this that were less well done, where they did leave the key inadvertently around so it could be found, and other versions or other complete, separate builds - not builds, well, just separate malware was doing the same kind of thing. So what was covered in the last week was that TeslaCrypt was shutting down. And so in what was a surprising end to this reign and run of TeslaCrypt, an analyst at ESET, noting that they were sort of winding operations down...

Leo: It's just so weird.

Steve: It is.

Leo: What, did they make enough money to buy the Tesla, so now they're quitting? What's the deal?

Steve: Well, and I don't get - because in some of the coverage they talked about TeslaCrypt had been slowly closing its doors while their previous distributors had been switching over to distributing the CryptXXX ransomware.

Leo: Huh.

Steve: So there was another whole family of ransomware. But the notion of having distributors for file encryption malware just boggles me.

Leo: It's a business now, yeah.

Steve: Yeah, exactly, boggles my mind. So this ESET researcher posts on TeslaCrypt's support chat, asking if, since they were apparently shutting things down, would they consider releasing the master decryption key? And they did.

Leo: What?

Steve: Now, first of all, I didn't know there was a master decryption key. And in trying to go back and find some early reference to there being one, unfortunately the only thing Google would show me was like all of the news, the recent news about there being a master decryption key, and I didn't spend a lot of time trying to dig into the past. But I don't remember at any point in our coverage there being an idea that there was a galactic master key. Somehow...

Leo: That's what they gave the NSA. That was the backdoor key.

Steve: Right. So now this ESET researcher, just he knew or he assumed there was one. So he...

Leo: Wow. He probably went, you know, he went through the code, obviously; right?

Steve: Yeah, and he said, hey, would you guys let that loose? And they said yeah, sure. So they posted it.

Leo: Sure, we're not using it. Wow.

Steve: So as a consequence, two things now exist. Over on the BleepingComputer.com

site - which we have been referring to since the beginning of this whole drama with file-encrypting malware because they've been really right on the leading edge of news and coverage. They've got some good forums and lots of good tools and feedback. Someone there, one of their contributors has created TeslaDecoder v1.0. And the way the coverage read, apparently earlier, pre-1.0 versions existed, but it wasn't done.

So when this master key was released, TeslaDecoder went to v1.0, and it is now available. I'm not sure how it's valuable because of course it would require somebody who had maybe never succumbed to the blackmail, decided they could live without their files. So, you know, maybe there are hard drives around that were TeslaCrypted and, for whatever reason, ransom wasn't paid; decryption didn't work; they waited too long. Remember there was the whole timeout. You had, like, what, 72 hours, and then after that it was over, they weren't going to help you any longer. So maybe there are drives around that have encryption still in place, in which case this is one of two tools that would be able to decrypt those files.

The other is that ESET has their own. ESET's site is WeLiveSecurity.com. And they've released a nice-looking command line. So you fire up a DOS command shell window, and theirs runs in a command-line environment; whereas TeslaDecoder has a GUI with drop-in fields and buttons and all kinds of bells and whistles. So anyway, I thought it was just - who knew that there was a master decryption key, and that these guys would say, yeah, yeah, you know, we're done, so here you go.

Leo: So funny.

Steve: If there are any drives lingering out in the world that are still encrypted, obviously you're not going to pay us or you would have already, so here you go. Here's your master decryption key.

Leo: Amazing.

Steve: Weird.

Leo: Weird.

Steve: Yeah. And creepy that there's, like, the previous distributors of TeslaCrypt, oh, they've all switched over to CryptXXX. So for whatever reason. Maybe the TeslaCrypt people just got tired of doing this. I don't know.

Speaking of tired of doing things, Flash continues to get the squeeze. Google announced - and I presume this was at I/O last week because this is May 15th is the date of this coverage from VentureBeat, that picked up the story. Although then I followed the link to Google's - they had some kind of funky developer-looking slides. So, yeah, that must have been from I/O because they also said on the slides, you know, all of this terminology is subject to change once people with suits look at it.

So to recap, last September, so September of 2015, what, eight months ago, Chrome 45, Google's Chrome browser v45, began pausing any Flash content that was not - and I remember we had fun talking about this at the time because Google's terminology was

not central to the web page. And it's like, what? So Google's now deciding what Flash content is important. I mean, that's good. We'd rather that they just paused everything. But in this case there are, like, sites that rely on Flash. They didn't want to disturb those. But things like ads. If you had a Flash ad where things were bouncing up and down and flashing in your face and just really being an annoyance, Google said, eh, no. We're just - that's an ad. That's not central to the page's content. We're just going to pause it. And you could wake it up if you wanted to, but we were all happy that they had put those things to sleep.

So now, essentially one year later, meaning in Q4 of 2016, which would put us back to September again, Google intends to further squeeze this. Again, well, but this time also applying these rules to the central content, as they define it, such as Flash-based games and videos. So they call this new initiative, which will happen, well, we're still a ways away, but presumably like a year from when they did the last one, so Q4 of 2016, they're calling it "HTML5 by Default." And again, I don't know if that'll be the final term. That was the name of this in the developer slides.

So Flash Player will continue to be bundled with Chrome, so it'll still be there. However, its presence will not be advertised by default. Now, what that means is that, when you've got script running on a page, there is an array called navigator.plugins, and another one, navigator.mimeTypes. And so script is able to enumerate through the entries in the array to determine all the plugins that the browser has and all the mime types. Mime is like .html, .mp3, you know, it's basically the type of file that the extension represents. And so by not advertising those, what that means is that Flash will be there, but script that checks the browser to find and launch Flash won't find it.

So what Google says is, as a consequence, sites that offer both Flash and HTML5, but bias themselves to the past, essentially, to Flash, they will no longer do that. They'll then, feeling that Flash is apparently not available, will fall back to - or actually fall forward because HTML is where we're going - to HTML5 for rendering what they would have otherwise rendered with Flash. So that becomes, as Google puts it, HTML5 experience becomes the default.

Then, when a user encounters a site that needs Flash Player, a prompt will appear at the top of the page, giving the user the option of allowing it for a site. So now we're getting to the "do you want to run Flash" on this domain, or on this website, behavior. So again, sort of just putting up an additional barrier. You can click through it. If you do, Chrome will remember your choice so you're not forced to do that every time. So it'll honor whatever decision the user made, pro or con, on subsequent visits.

Then there is a concern that, on the very most popular sites, which are still dependent upon Flash, that this would create what Google is calling "overprompting." So they will separately maintain a whitelist in Chrome of the then Top 100 sites based on aggregate usage. And that whitelist will prevent that extra prompting question from coming up and just allow Flash to run. So sort of a heuristic tradeoff. And that whitelist apparently will be groomed and evolve over time as sites get their acts together, finally say, okay, I guess it's time for us to stop using Flash and do that. Google will bring in some other site and presumably remove the one that got things fixed.

Now, this is where it gets a little kludge-y because basically all of this behavior is a kludge. This is not the way anyone intended the Internet to work, where the browser pretends not to have services to offer, and it says, oh, well, unless you're really important, then we'll let you have them. Or if you're not, then we're going to make the user go through extra hoops and all that. Okay? So as a consequence, sites like Pandora.com will direct the user to download Flash Player when it determines that the

browser doesn't support Flash, which is now the faade that Chrome in September, starting in September, will be presenting.

So Google doesn't want that to happen because you actually do have Flash. So somehow they're, like, special-casing that behavior. And if Chrome sees some sites like Pandora, and I guess it's on a site-by-site basis that they're checking for this, they - it just sounds horrible. They intercept the request to download Flash Player. Or maybe that's what they're doing, so they're able to get all sites because you get an intercept page from Pandora saying, oh, you need Flash Player to proceed, you know, click here to download Flash Player. So when you do, you click a link, get.adobe.com/flashplayer. Google Chrome will see that, will intercept and cancel the navigation, and instead present the Allow Flash Player "infobar," as they call it.

So as I said, just a nightmare. But I don't - obviously this is all aimed at increasing our stability of the web, using Chrome's power to put pressure on websites to move away from Flash. And we know that, if pressure wasn't applied, all of the experience that we have of these technologies on the 'Net, which have so much inertia, is that Flash would never die otherwise. And we all understand it's time for it to die. It's only inertia today which is keeping it going. Anyone starting from scratch now would just use HTML5. So there will be a policy setting available to enterprises which gives them the ability, enterprise-wide, to override all this nonsense with "Always run Flash content."

Now, maybe that's only - it wasn't clear whether that was browser-wide or just for their site, so that their own users wouldn't be harassed if they wanted to run Flash on their own corporate site. But under user-accessible, that is, for all of us, content settings, there will be the option of specifying how we want this handled. So we'll be able to, on an instance of Chrome basis, to select always run Flash, allow sites to ask to run Flash, ask the user to always be prompted about running Flash, or never run Flash. So very much the way like cookies are handled, like keep them forever, never accept them, or keep them only for this session. Similarly, we have four different settings for how the user wants Flash handled.

So I think this is - it's unfortunate that this is what's required. I can't think of a better solution. We do want Flash to get phased out. We've got good alternative replacement technology now. And so Google is saying, okay, we're taking a stand.

Leo: People are asking why is TWiT still using Flash. We don't use Flash; but some of our providers, not all, but some of our providers do. And so it depends on what stream you're getting and so forth. But obviously we don't require Flash because you can visit our websites on iOS and Android and watch live video. So some of this is a signaling issue with your browser and our site and so forth. But Ustream, for instance, if it sees that you're not supporting Flash, will give you an HTML5 stream or an HLS stream. BitGravity I think is Flash only. I don't know if Twitch offers the alternative. Probably does. Amazon owns Twitch now.

Steve: Yeah, I don't think we're ever really going to get rid of it. These things just never completely go away.

Leo: We don't provide our own - we stream to these providers, and then they choose what to send you. So we don't really have that much control over it. We pay, because we wanted to be on iOS, we do pay a company called Flosoft for an HLS

stream that works on iOS, and that's what you'll get on the iOS apps. But it costs us money. I don't know. I mean, you know...

Steve: Yeah. I had, you know, I've got a bunch of videos on GRC. I've got the PDP-8 videos, and then the SpinRite, what it does and how it works videos. And the SpinRite stuff I took the time, and I'm not - I don't remember now if I did that yet with the PDP-8 videos. But I wanted it also to be able to run on mobile devices, non-Flash-based devices. And so I have three different codecs, the WebM, the Ogg, and MP4. And it's really funky because in the HTML5 they have to be offered in a specific order. And one of them is, like, oddly out of order, specifically because of the way iOS works. But this stuff is now available. And it's a little bit of a pain. But it's sort of where we are at this point.

Leo: Right.

Steve: And actually we're going to talk about Cory Doctorow's posting at the EFF a little bit later about what, unfortunately, movement we're seeing in terms of closing this down.

Leo: Good. Good, good, good.

Steve: So we talked back in 2012, four years ago, when 6.5 million email addresses and - I'm doing air quotes, no one can see it, but trust me, around the word "encrypted" - passwords leaked onto a Russian hacker forum. And the air quotes are around "encrypted passwords" because, at the time, and this was in 2012, still well downstream of when this was not correct behavior, LinkedIn had unsalted SHA-1 passwords.

Leo: Eww.

Steve: So, I mean, they weren't MD5. That would be worse. But still, SHA-1, the GPU code for screamingly fast hash-cracking of unsalted passwords was already mature. And what we found was - we had some fun at the time at the expense of that 6.5 million users because "monkey" was number 12, and many passwords were 12345, and then the next most likely was 123456, and so forth. And so it's like, oh, come on. So anyway, the news this week, and that's odd because I don't get this, now an additional 117 million passwords, actually it's 167 million, but about 50 million are missing some of the information. So there's 117 million complete email address and password pairs still, I mean, from the original breach with unsalted SHA-1.

So what's so weird about this is that this is time-sensitive value. And at the time, LinkedIn informed everyone who was affected, that is, the 6.5 million people whose email addresses were part of this public posting, that they forced a password reset. So, sorry, you can't log in again. You've got to use password recovery. We'll send you a recovery link in email because we and everybody else has your email address now, and then you'll be able to update your password. They also advised all of the rest of the non-affected subscribers at the time that they should probably change their password, too. Well, yeah, because apparently there's 167 million, or at least 117, with full account compromise information.

But again, what's strange to me is that that information, that additional 117 million, was far more valuable as part, you know, like four years ago in 2012 as part of the original offering. I'd love to know the back story behind, like, what has been happening for the last four years. Now a hacker who goes by the moniker Peace, P-E-A-C-E, is offering to sell this next batch, or old batch, of 117 million for $2,200 USD, payable in bitcoin. So, what, like five bitcoin. And again, the database has been looked at; 90% of the passwords were cracked within three days, within 72 hours, because again...

Leo: Rainbow tables they're using, or...

Steve: In 2016, we can just cut through SHA-1 unsalted hash like butter. It just doesn't pose any kind of a barrier any longer. And so this is interesting, too, because it's a little bit of a lesson. One of the things that our listeners have watched over the coming up on 11 years of this podcast is how the whole crypto and security industry is routinely retiring technologies and rolling forward into new ones. And of course we've just been talking about SHA-1 and the problem with signing using SHA-1. It's very different than a password. Remember that the reason we can crack a password is that a GPU can easily guess short alphanumeric phrases and 123456 and things, and go, oh, look, you know. And in fact there's all sorts of ways also to dramatically accelerate that kind of brute-forcing. Basically we're sort of reversing the hash. So, and of course TheRegister.co.uk snarkily reports that LinkedIn users haven't learned any lessons about proper passwords. And I observe, well, yeah, except that those are all from four years ago. So this was part of the original breach, apparently.

Leo: Oh, interesting.

Steve: It's strange to me that something that's no longer nearly of as much value has taken this length of time to get back out onto the market. But what the heck. So I guess, if you want to take something away in terms of an action item, if you have an account on LinkedIn, if it predates the 2012 breach that we talked about four years ago, and if you have a simple password, and you ignored LinkedIn's advice at the time, even though you weren't one of those initial 6.5 million people, and you did not change your password, probably...

Leo: Now's the time.

Steve: Too late.

Leo: We all know it. It's not so much LinkedIn. It's really that, if you used monkey123 for LinkedIn, you probably used it for everything else.

Steve: Correct. Exactly. And in fact we know there was some reporting that indicated there were people who still had an unchanged password because there had been breaches of LinkedIn accounts following the release of this database. So it's like, okay. Again, some people just won't change their password.

Allo. One of the things we learned at Google I/O last week is that Google is jumping into

the messaging chat, sort of feature-crazed messaging app business. And they have something called Allo, A-L-L-O, which is the name of their messaging client. I have to say, Leo, before I forget, I thought that the idea of showing the incoming video before you answer it is brilliant.

Leo: Knock-knock, yeah.

Steve: Just like the kind of thing, it's like, why didn't anyone think of that before?

Leo: Right.

Steve: So hats off to them for that. But what we learned was that Allo would not have encryption enabled by default; that it would support encryption, but it would be turned off. And a whole bunch of people throughout the industry have weighed in on this on both sides. And what we understand is that a lot of the features that Allo offers, like - and in fact I was listening to you guys talking about it during the announcement. As I understand it, Allo is able to, in a dialogue with somebody, suggest responses.

Leo: Yeah.

Steve: And so you just choose, oh, yeah, I like that response; and you just click, you know, click the suggestion.

Leo: Yeah, exactly.

Steve: Well, clearly, for Google to do that it has to see into the conversation.

Leo: Of course, yeah.

Steve: Yeah. So Allo offers users a choice. And, boy, talk about some social experimentation. I'm interested to see how this comes down. So Allo will offer users a choice. Do you want to enable encryption, thus having privacy and security; or opt not to have end-to-end encryption, which then enables the entertainment and interactivity side. And TechCrunch, in their coverage of this, suggested that, most likely, consumers will likely choose the latter.

Leo: Well, they'll choose...

Steve: They will go for entertainment and interactivity. They want that feature over privacy and security. And I agree.

Leo: They won't choose anything. They'll choose the default. This was the only argument is what should the default be.

Steve: Right, right.

Leo: I mean, Google clearly needs to see into your stuff to do all the magic that it does. It does that with inbox on email, too, to suggest responses. And they're very good. They're uncanny because they're reading what I'm saying, and they put it in my voice. They're very, very good. And I don't have a problem with that. But of course if you - see, what I think Google should have done, I don't think crypto should have been by default. I think there's a middle ground where you could turn it on, and it would stay on. Because right now you choose incognito per conversation.

Steve: Ah, okay.

Leo: In other words, it's not a setting.

Steve: Not globally.

Leo: You say, I'm going to do an incognito conversation now. What you should have is a checkbox that says I want all my conversations to be incognito. And they can put up a big thing that says, well, you understand we're not going to be able to do anything we want to do.

Steve: Right.

Leo: But they decided not to do that. I don't have a big problem with that because use Signal or WhatsApp if you...

Steve: That's precisely what I was going to say, was use two different messaging systems. Use the fun one that has all of the Google enhancements where you're just talking about where you're going to have a meeting and so forth. And if you have something you need to have private, use a high-security messaging app that only operates that way. The good news is where they got their encryption.

Leo: Right.

Steve: If you do turn it on, it's from Moxie and company, Open Whisper Systems Signal Protocol that I talked about several weeks back and was just knocked over by from a technology standpoint. Those guys, in terms of the design of the crypto, for an asynchronous secure messaging system, Signal is it. And of course that's what WhatsApp adopted. And we have a question in our Q&A later about what, of all these different alternatives, what would we recommend. So we'll talk about that when we get to it. But

anyway, I thought that was interesting. And I think you're right. I think, as we know, as I call it, "the tyranny of the default," people will just leave it the way it is. They will like all of that stuff. And they may notice, if they do bring up security, that suddenly all of that extra stuff isn't there, and think, oh, well, I want that.

Leo: Yeah. I mean, it's there if they want it. And it's kind of nice to have it as an ad hoc option. You don't have to install another messenger. And if you're going to...

Steve: Yeah, if you kind of want to whisper to each other.

Leo: You know that the tech blogs are calling it the "sexting mode."

Steve: Okay.

Leo: That's where they're going. I'm excited. I think this, you know, I actually bought a book now on machine learning because I'm very interested in what the limits are, what the capabilities are, how hard this is to do, how it works. I think Google is smart to say we're going to reinvent search and start using this knowledge. And it depends on them gathering information about you. And so if people understand that, and that this is what they get in return, I think that's fine.

Steve: Yeah. Jeff Hawkins, hierarchical temporal memory (HTM) is the work that he's doing. You had him on Triangulation quite a while ago.

Leo: He was amazing. Graffiti guy, yeah.

Steve: And, yeah, I mean, he gave us the Palm Pilot and Graffiti. And I loved his notion of compromising, where the user could learn how to form letters that were still the letters, so it was easy to remember, but they were also - it disambiguated them from all the other letters of the alphabet. Just really a brilliant solution.

And he turns out to know a lot about brain science, too, and he's one of the major technology - I remember seeing the demonstration of his vision system where you were - and it sounds like the kind of stuff that Google has now. Doesn't seem like such a big deal as it was at the time. But you could show this software a whole bunch of different boat pictures, and then show it some pictures of completely different-looking boats and non-boats, and it would find the boats. Like somehow it's like, wow, you know? I mean, it, like, understood boatness somehow. So very, very impressive. So, yeah, Leo, it's - that's cool stuff.

Leo: I'm excited, yeah.

Steve: So Cory Doctorow. You had him on Triangulation.

Leo: Oh, he's been on TWiT many times. He's a friend of the network.

Steve: Many times, right.

Leo: We love Cory.

Steve: Neat, you know, "for the people" guy. So it turns out he's really got a burr in his bun over something that's happening over at W3C. And I didn't realize it until I saw this most recent posting and then saw that it ties into some previous ones. And there's enough interesting specifics here for Security Now! that I want to share this. So this one is titled, and this is posted over at EFF, "Save Firefox." And with a little bit of an introduction here, he says:

"Once upon a time, there were two major browsers that virtually everyone used: Netscape and Internet Explorer, locked in a death battle for the future of the web. They went to enormous lengths to tempt web publishers to optimize their sites to work best inside their windows, and hoped that users would follow. Then, a game-changer: the open, nonprofit Mozilla browser spun out of Netscape, with the mission of putting users, not publishers, in charge. Mozilla defaulted to blocking pop-up ads, the scourge of the early web. It was a step none of the major browsers could afford to take because publishers were convinced they would go broke without them, and any company whose browser blocked pop-ups by default would alienate the publishers, who'd throw their lot in with the competition.

"A little over a decade later," writes Cory, "and the world of browsers is unrecognizable: Mozilla turned into Firefox, Internet Explorer turned into Edge, Apple launched Safari, and Google launched Chrome. Every one of them blocks pop-ups by default. Literally none of the dominant browsers from a decade ago are in widespread use today. Which is not to say that there isn't competition. There is, and it's fierce as ever. It's a strategic fight to please both publishers and users, whose interests are not always the same. Publishers want to gather more information on users; users want to keep their information private. Publishers want to control users' browsing and viewing experience; users want to sit in the driver's seat.

"We need competition. We also need diversity. We need the possibility that young, game-changing market entrants might come along. We need that idea to be kept alive, to make sure that all the browsers don't shift from keeping users happy to just keeping a few giant corporations that dominate the web happy because there's always pressure to do that. And if all the browsers end up playing the same old game, the users will always lose." So, he says: "We need more Firefoxes," meaning an ecosystem that encourages upstarts.

He says: "We need more browsers that treat their users, rather than publishers, as their customers. It's the natural cycle of concentration-disruption-renewal that has kept the web vibrant for nearly 20 years." And he says: "We may never get another one, though. The World Wide Web Consortium, once the force for open standards that kept browsers from locking publishers to their proprietary capabilities, has changed its mission. Since 2013, the organization has provided a forum where today's dominant browser companies and the dominant entertainment companies can collaborate on a system to let our browsers control our behavior, rather than the other way around.

"This system, 'Encrypted Media Extensions' (EME), uses standards-defined code to funnel video into a proprietary container called a 'Content Decryption Module.' For a new browser to support this new video streaming standard, which major studios and cable operators are pushing for, it would have to convince those entertainment companies or one of their partners to let them have a CDM (Content Decryption Module), or this part of the 'open' web would not display in that new browser.

"This is the opposite," writes Cory, "of every W3C standard to date. Once, all you needed to do to render content by a server was follow the standard, not get permission. If browsers had needed permission to render a page at the launch of Mozilla, the publishers would have frozen out this new, pop-up-blocking upstart. Kiss Firefox goodbye, in other words.

"The W3C did not have to do this. No copyright law says that making a video gives you the right to tell people who legally watch it how they must configure their equipment. But because of the design of EME (Encrypted Media Extensions), copyright holders will be able to use the law to shut down any new browser that tries to render the video without their permission. That's because EME is designed to trigger liability under Section 1201 of the Digital Millennium Copyright Act" - our good old friend the DMCA - "which says that removing a digital lock that controls access to a copyrighted work without permission is an offense, even if the person removing the lock has the right to the content it restricts.

"In other words, once a video is sent with EME, a new company that unlocks it for its users can be sued, even if the users do nothing illegal with that video. We proposed that the W3C could protect new browsers by making their members promise not to use the DMCA to attack new entrants in the market, an idea supported by a diverse group of W3C members; but the W3C executive overruled us, saying the work would go forward with no safeguards for future competition."

And he wraps up, saying: "It's even worse than at first glance. The DMCA isn't limited to the USA. The U.S. Trade Representative has spread DMCA-like rules to virtually every country that does business with America. Worse still, the DMCA is also routinely used by companies to threaten and silence security researchers" - as we talk about often - "who reveal embarrassing defects in their products. The W3C also declined to require its members to protect security researchers who discover flaws in EME, leaving every web user vulnerable to vulnerabilities whose disclosure can only safely take place if the affected company decides to permit it."

And he finally says: "The W3C needs credibility with people who care about the open web and innovation in order to be viable. They are sensitive to this kind of criticism. We empathize. There are lots of good people working there, people who genuinely, passionately want the web to stay open to everyone, and to be safe for users. But the organization made a terrible decision when it opted to provide a home for EME, and an even worse one when it overruled its own members and declined protection for security research and new competitors. It needs to hear from you now. Please share this post and spread the word. Help the W3C be the organization it is meant to be."

And this was one of a series of similar postings where Cory goes back and looks in similar fashion to looking back at the circumstances under which Firefox was born. And he notes that we would not have Netflix today if this were the environment that a Netflix were trying to be created under. And people who've been around, you'll certainly, Leo, remember that Netflix was under attack by Hollywood because the original model was mail you movies, which you would watch and then return. And the entertainment industry hated that and tried to sue them into nonexistence. And as we know, historically, the same thing happened when home video recording tried to happen. Again,

that was, you know, the entertainment industry tried to absolutely prevent that from happening.

And so Cory notes, not only Netflix, but even iTunes, iTunes was fighting in the beginning an uphill battle. I mean, so this whole - the model that we have and the history that we keep seeing being repeated is that the copyright holders are - it's in their nature to want the most comprehensive sweeping blanket protection that they can get. We have to remember what's in the interest of the people because that's the intent behind copyright is to maximize the value for the population, giving creators of content real, but limited, you know, curtailed rights. And it's kind of creepy to imagine that we're moving towards a technology where we're going to have essentially DRM pushed into browsers, and only browsers that are permitted to display that DRM will be able to display that kind of protected content.

Leo: Yeah, I agree.

Steve: So bravo to Cory for carrying the torch and...

Leo: Carry that torch.

Steve: ...helping us.

Leo: Back we go to Steve Gibson and more security news, yes, yes.

Steve: So, yeah, a couple bits of miscellany. I wanted to note that, as a consequence of Microsoft's latest Get Windows 10 shenanigans, which has everybody really upset, Graham Cluley, who's been writing in the industry forever, he wrote a piece this morning with the headline, "Microsoft has a dirty little Windows 10 upgrade trick up its sleeve. Clicking 'X' won't stop your PC upgrading to Windows 10."

Leo: Oh, no. Yeah, we were showing that window.

Steve: Yeah.

Leo: You can't just close the window?

Steve: No. No. And in fact I'm going to read something from someone we all know, and I'm not going to tell anybody who it is first. So the title was "Upgradegate: Microsoft's Upgrade Deceptions Are Undermining Windows 10." This author says: "For months now, I've complained about the software giant's heavy-handed tactics in trying to trick customers into upgrading to Windows 10. But a recent change to the Get Windows 10 advertisement that is forced on Windows 7 and 8.1 users takes things entirely too far. This is indefensible. Frankly, this entire episode has been indefensible, with Microsoft introducing a non-stoppable, non-hideable advertisement on several hundred million PCs from around the world, and then upgrading that advertisement to thwart those who do

seek to remove or hide it. It has changed the language of the ad, made no clear cancel choice available, and jammed it into the recommended updates that auto-install via Windows Update. If you read this site," writes this author, "listen to Windows Weekly or What the Tech, you know how bad things are. It's been a constant refrain."

And this author writes, "Well, I've had it. Last week Microsoft silently changed Get Windows 10 yet again, and this time it has gone beyond the social engineering scheme that has been fooling people into inadvertently upgrading to Windows 10 for months. This time, it actually changed the behavior of the window that appears so that, if you click the close window box, you are actually agreeing..."

Leo: No. You're kidding me.

Steve: No. "You are actually agreeing to the upgrade, without you knowing what just happened."

Leo: Oh, my god.

Steve: "Previously, closing this window would correctly signal that you do not want the upgrade. So Microsoft did not change the wording in the window. It didn't make an Upgrade Now button bigger, or a nonexistent Don't Ever Upgrade button smaller. It pulled a switcheroonie. It's like going out to your car in the morning and discovering that the gas pedal now applies the brakes, while the brake pedal washes the windshield. What a fun commute. The violation of trust here is almost indescribable. It's bad enough that Microsoft has been training Windows 7 and 8.1 users, i.e., most Windows users, to not trust Windows 10 because of this horrible unstoppable advertisement, but now they will not trust their own sanity because all they'll remember is that they dismissed the advertisement by clicking the Close Windows box. "Why on earth did Windows 10 just install on my PC?" Why on earth, indeed.

"Coupled with the growth of clean personal computing platforms like Chromebooks and Macs, and the fact that Microsoft cannot convince its own PC maker partners to not ruin the Windows experience with crapware, one has to wonder: Is this all part of some plan to destroy Windows from within? I mean, seriously. You couldn't write a dumber story about how to ruin something that is otherwise as wonderful as Windows 10. My god, Microsoft, just stop.

"And for you Windows 7 and 8.1 holdouts out there, please feel free to utilize a third-party utility like Steve Gibson's Never10 to hide the Get Windows 10 advertisement from appearing and prevent Windows 10 from silently downloading to and upgrading your PC. You shouldn't be treated like this, but at least you can stand up for yourselves." And that piece was written this morning by our friend Paul Thurrott.

Leo: No, I could tell. And of course we'll talk about it tomorrow. So just to be clear, this window is not new. It's a terrible window to begin with because it says Windows 10 is a recommended update, and you have two choices: the OK button, which will start the installation, and where you would normally see a Cancel button, Upgrade Now button. So that's the same thing.

Steve: Well, now, and remember that there was a previous version that had two buttons. One was Upgrade Now, and the other was Upgrade Later.

Leo: Well, that's what OK does because OK will do it later tonight.

Steve: Correct.

Leo: Now, here's the button you need to click. It's not the "X" button. It's the Click Here to Change Upgrade Schedule or Cancel Scheduled Upgrade. And it's not obvious that you want to click that link, that blue link underneath the date and time.

Steve: And it's not even underlined.

Leo: No. I mean, if you hit Return, it would be okay. The thing that's upsetting Paul is upsetting, which is in every other case hitting the "X" would indicate cancel. They're not even letting you do that. You have to - the only way out at this point is to Click Here and then say no. And then does Never10 stop this particular thing?

Steve: Oh, yeah.

Leo: Yeah, you don't see this.

Steve: Yeah, it just all goes away.

Leo: Yeah.

Steve: Yeah. So what's interesting is there has been a skyrocketing explosion of downloads.

Leo: Oh, it's terrible.

Steve: We're at, when I looked this morning, a total of 535,000 downloads, and we're tracking at more than 25,000 copies of Never10 per day.

Leo: Microsoft's become the Borg.

Steve: Wow.

Leo: Resistance is futile.

Steve: And again, I'm Steve "I Love Windows" Gibson. This is not anti-Windows. This is anti-Microsoft. This is like, as Paul wrote - and we know Paul's not anti-Windows. In fact, he did a piece over the weekend, he installed a brand new Windows 7 and was tweeting through the experience. Actually it was pretty much all day Friday, like I can't believe it's this slow. I can't believe I still have - he says, I'm going to go out and have some more kids and come back, and I'm still going to - this thing won't be updated.

Leo: So we're going to make this the TWiT Bit for the show. Patrick Delahanty's saying this in the chatroom, and I agree, Patrick. This will be our TWiT Bit. And we will put this on our YouTube TWiT Bits channel, which is YouTube.com/twit. So you can link to it. It'll just be a couple of minutes of Steve talking about this, us showing the dialogue box, where to click, and the warning. And I think Patrick wants to share it with friends and family, and I think others may well, as well. So this is, right here, the little snippet from Security Now! we're going to put up.

Steve: Well, and what's sad is, oh, my god, there were 232 responses, an hour after Paul posted this. And the first three of them were people telling stories, like from this morning, getting tech support calls from people saying, "Nothing works. I got up this morning, and my computer is broken," and so forth.

Leo: And one last piece to the TWiT Bit: GRC.com, is it /never10?

Steve: Yeah, that'll get you there.

Leo: Slash N-E-V-E-R-1-0. The thing I want to really emphasize is Steve writes this in assembly language. It's a few hundred bytes. You download it. A few hundred kilobytes. Right? It's under - it's a megabyte.

Steve: 81.

Leo: 81 kilobytes?

Steve: Yup.

Leo: You download it. You run it. It is using Microsoft's approved method, the method that they prescribe to enterprises so that, you know, enterprises don't want to see this in their business.

Steve: Right.

Leo: That makes the edits that group policy editor would make; right?

Steve: Correct.

Leo: The registry changes. So unless Microsoft really gets crazy, which they could, this will work forever. And you can then delete the program. You don't have to keep the program. It's made those edits in your registry, and you're done.

Steve: Correct.

Leo: It will also, if you check the box, uninstall, you see this "Remove Win10 Files"? What a lot of people don't realize is, even before this comes up, Microsoft has been in the background secretly downloading the Windows 10 installer.

Steve: About 6.5GB of Windows 10, ready to land on your drive.

Leo: Once it's expanded, it's giant. And so that's sitting on your hard drive right now. So there's a button on here that says Remove Windows 10 Files. Do that before you delete the program. And as far as we know, this is not going to ever happen again.

Steve: Correct.

Leo: Once you run this Never10.

Steve: Correct. With all of the instances out there, there's been no report of anyone who's run it ever being harassed again. And for what it's worth...

Leo: And that makes sense because Microsoft's not going to cheese off their big enterprise customers. That's...

Steve: They can't, no. It's like on their site. It's that page. And I'm actually, the way this has turned out, I'm happy for. It's not, again, I don't have anything against people upgrading to Windows 10 if they want to. The whole point is, for whatever reason, people don't. And they should have the right to be able to control that, not to. And essentially Microsoft is overriding their will. What I'm pleased about is that, when the Microsoft documentation first appeared, we talked about it on this podcast. And it was like, you know, your eyes crossed over, like, trying to navigate through the registry and...

Leo: Oh, yeah. And no normal user should be asked to edit their registry. That's just a recipe for disaster. That's terrible.

Steve: Right. And so I stole a week from the work on SQRL because I just thought, you know, this needs to be simpler. There was that GWX control panel, but it was hundreds of somethings, I mean, it was big, and it was covered with buttons. And I looked at it and was confused by, it's like, well, okay, all I want to do is not have this pop up. And so I thought, okay, I've just got to fix this.

What I'm really pleased about is that this Never10 launched sometime, I think it was like early in March. And so it had enough time to be around and to get some traction so that now, in this last week, when it's really become a problem, everyone knows that it exists. And so people are, I mean, I'm seeing tweets about it constantly. And as I said, 25,000 copies a day now. So it's...

Leo: Yeah, and I'm going to say I like Windows 10. I mean, it's not that we're - you might not like Windows 10 for the privacy reasons. But it's not so much that it's - and I know Paul loves Windows 10. It's not so much that we're saying, oh, you don't want Windows 10. You should have the right to choose. And no company should ever trick you, trick you into installing an upgrade like that. It's a massive upgrade. It does break some systems. It does break some software. It should not be forced on you.

Steve: But mostly it's for grandmothers who, like, have figured out how to use 7.

Leo: Makes me cry. Yeah, makes me cry.

Steve: It's not like an iOS update, 9.3.2 goes to 9.3.3, where nothing changes, essentially. The move from 7 to 10 is like, what happened? I mean, it's just like, wow. And Paul used a term - he posted over the weekend before this morning's posting, where he used just exactly the right term. He talked about "Windows enthusiasts." And I thought, yeah, I like that because that's not me. I am a user.

Leo: Yeah.

Steve: I'm, you know, for me it's a tool. But I get it. I mean, that someone could just want to play with the latest and greatest, a Windows enthusiast. And so of course you're going to want Windows 10. And you wanted 8, and 8.1, and you're going to follow the train. And for me, it's like, I want stability. I just want it to run my programs and for me to use it as a tool. An enthusiast here I'm not. So, but I liked the differentiation that he made over the weekend. I thought that was really good because, you know, he is one. And a lot of people who are using Windows 10, it's like, yeah, I want the latest Windows. Cool.

Leo: Right, yeah. But they should get to choose.

Steve: Yeah. I'll just also say that I've listened to you guys, I think it was last week, wondering whether the upgrade would end. That is, are they going to terminate it? And I have to think...

Leo: They say they're going to make people pay starting July 29th.

Steve: Yeah. And I have to think that, with this much backlash, with this, I mean,

Microsoft can't be deaf to everything that's being written. Brad, it looks like Chacos, C-H-A-C-O-S, who's the senior editor of PC World, he wrote that it is a nasty trick. He said: "So after more than half a year of teaching people that the only way to say 'no thanks' to Windows 10 is to exit the GWX application, and refusing to allow users to disable the pop-up in any obvious manner, so that they had to press "X" over and over again during those six months to the point that most people probably just click it without reading now..."

Leo: Oh, they trained you, yeah. Wow.

Steve: "...Microsoft just made it so that very behavior accepts the Windows 10 upgrade instead, rather than canceling it."

Leo: Yeah. Isn't that interesting.

Steve: Ugh.

Leo: That's a good point. That's a nasty trick.

Steve: So anyway, I have to think Microsoft is aware of this, and they're going to go, okay, fine, message received, we gave everybody a year, no excuse. If you didn't want it for free, fine. We're going to stop pushing it on you. So I have to think they'll take it away.

Leo: I don't know if there's a lot of evidence for that. People have been screaming about this for months.

Steve: So I did want to mention many, many, many people have been experimenting with the Healthy Sleep Formula. And I had previously mentioned that one of the key ingredients, Seriphos, apparently as a consequence of the Healthy Sleep Formula and the timing of the manufacturer choosing to drain the channel in order to replace it with a reformulated version, no one has been able to get it since, like, for a couple months.

Well, just this last weekend it reappeared. And the bad news is they ruined it. It is not the same. It is at best 44.4% the dosage of the original at currently about twice the price. So it was already one of the most expensive, I think it was the most expensive single ingredient with the reformulated Source Naturals L-theanine in number two.

There is something called Enerphos, E-N-E-R-P-H-O-S, but I'm a little worried about that, too. It's from a company called T.E. Neesby. And they were once in Fresno, but I think they're gone. So I think we're in the same position of there being, in this case, a stock, an existing inventory of this Enerphos, which to me looks the same as the original Seriphos. But unfortunately, if all of us Healthy Sleep Formula people go buy it, we're going to buy it out of stock again.

Anyway, I have a bottle of Enerphos. It literally came today because I purchase it the moment I realized that it might be the same. And of course I also have a bottle of the

reformulated and ruined Seriphos, which I've already seen some anecdotal reports from people saying, yeah - they're not Healthy Sleep Formula people. I immediately, over on Amazon, I put up a warning that this Seriphos bore no resemblance to the eight-year historical Seriphos that all of the - there's like 233 glowing reviews of it for adrenal fatigue and lowering cortisol. And unfortunately, unless this was brought to people's attention, they'd be buying this new one thinking it was, you know, trading on the reputation of the previous one. And it no longer deserves that at all. So I wanted to give people a heads-up.

I don't have a Healthy Sleep Formula response yet. I will play with this Enerphos and post on the page my results to see whether it could be an interim replacement. But again, it looks to me like we're just draining Internet stock that may exist. This company appears to be gone. So I will let people know. And I'm just gratified by the amount of help this has been for people. I have no scientific study to demonstrate what the efficacy has been. I don't know whether people are sending me more positive responses than negative. I know that there are some people for whom it has been ineffective. But when I hear that 35 years of insomnia has been completely cured, the people are, like, sleeping, as they put it, like a six-month-old baby through, I guess - do six-month-olds sleep through the night? Anyway, I think of it as like sleeping like a teenager because I think of teenagers...

Leo: [Crosstalk] kids.

Steve: Like logs.

Leo: Yeah, like sleeping like a teenager, yeah.

Steve: Anyway, so it's worked for, I don't know, maybe 90% of the people who've played with it. And the change to the Source Naturals L-theanine was a big help, too. So I'm just happy that it's been of use to so many people. And I will tweak it when I have some more information.

Leo: Our lawyers have asked us to say that Steve is not a doctor, and you should consult your physician before taking any supplements.

Steve: Oh, and I should mention, many people have also written saying they did go to their doctor, and their doctor has been very impressed.

Leo: But ask YOUR doctor.

Steve: Yes.

Leo: I'm just saying. Because you may be on medications they're not on, et cetera, et cetera.

Steve: Absolutely.

Leo: So before taking any supplements, always consult your physician.

Steve: So I'm a little embarrassed about what this person writes. But it's kind of true, so I decided, well, okay, even though it embarrasses me, I'll share it. This is Curt M. in Southern California somewhere. The subject line - this was written on the 20th of May, so, what, four days ago. He said, "My personal experience with an old friend, SpinRite." And he says: "Dear Steve, in the '70s you would call the TV repairman to replace the tubes in your TV. They were expensive and went out often. In the 1980s, computers were much the same. Hard drives, though more reliable than floppy discs, for anyone who still remembers, that's not saying much.

"As a young man in the '80s, I spent many an hour working in computer repair. The problems were many, from Compaq, and Mac 128K power supplies, to 30MB Seagate RLL drives, which were really just 20MB drives with a different controller. Drives of that era were just not very reliable. Over the course of my lifetime, I have repaired hundreds, if not thousands, of hard drives. You know how many times, after all those years, SpinRite failed me?" He writes, "0, zero, nada" (numeric zero, then the word zero)." Wow.

"To me," he writes, "SpinRite is the Rock of Gibraltar. I've always felt that, if you know SpinRite, you know the man behind it. I believe it was a labor of love, and it shows in the end product. And if you love what you do, then you understand in intimate detail the principles of what makes it all tick. It's clear that you do. Thanks for giving the world a product they can truly trust. I can attest that, with SpinRite, you can trust it like an old friend. Respectfully, Curt M."

Leo: Isn't that nice.

Steve: So, Curt, very nice.

Leo: That's very nice. All right, Steve. Let me get the PDF up on my screen, and I'm going to get you some questions. You ready to answer some?

Steve: Yes. Coffee refilled.

Leo: Yes, coffee refilled. Mug to the brim. Starting with Joel Davis. He's coming to this question-and-answer session via the Twitter. He says, and I quote: Regarding Z-Wave and ZigBee security, while I fully agree that a fully secure home automation protocol would be ideal, looking at the current state, what would be easier for a thief, hacking the protocols with a software-defined radio or just kicking in the door? I'm not a fan - I don't disagree. I'm not a fan of letting the perfect be the enemy of the good enough.

Steve: Yup. And I liked that because it sort of brings us back to earth. We've been talking for the previous two weeks about some of the details of IoT security, looking first at Z-Wave and SmartThings, and then also ZigBee security. And it's worth remembering

that, yeah, you know, we're talking about in many cases a door lock or alarm or security systems. But in terms of gaining entry, we've all got glass windows. And if somebody really wants to get in, that could be done.

Leo: Yeah.

Steve: You know, so anyway, I don't think it's black and white. It's certainly different if you could walk up to the door and twist the handle and walk in. That's an unsuspicious action that anyone observing you from the street would lead them to believe you had rightful access to that facility; whereas kicking the door in or throwing a brick through the window makes it pretty obvious that you don't live there.

Leo: Yeah, yeah.

Steve: Or, if you do, you have a real problem forgetting your keys inside the house.

Leo: You have anger issues.

Steve: But again, I appreciated Joel's note because, yes, it's easy - and I think we often do this, for example, when we're talking about crypto. You raised the point, Leo, a very good one, a few weeks ago. It's like, yeah, you may have end-to-end encryption that is just bulletproof, and it's got ratcheting, and Moxie Marlinspike has given it everything he's got. Except if you've got a keystroke logger, game over, because it's logging the keystrokes you type before the encryption and everything. So, yeah, it's necessary for us to keep some perspective on all of this. And so I appreciated what Joel said.

Leo: Bryan in Carlsbad, California saw the return of the dreaded 3035583: Steve, you mentioned some folks saw the Windows Update KB3035583 coming back. So did I, on my Windows 7 machine, despite running April 18's version of Never10. I also noticed many other updates; and, no longer being able to trust what Microsoft says, I looked it up, and KB3150513 is also purportedly for Windows 10. So I unchecked that box, too. What's the deal, my friend?

Steve: So this, I liked this question because we've gotten a lot of questions - we've gotten. We've received. What's happened to my English?

Leo: We've gotten many questions from all of you people.

Steve: We've received many questions. People are confused because they assume that Never10 is going to prevent this 3035583, it's going to remove it and prevent it from coming back. Which is not the way it works. During the development of Never10, I looked long and hard at doing that. And Microsoft, for whatever reason, it's an area where normally Microsoft has very comprehensive, expansive APIs that give you incredible granularity and control into the operation of things. Yet, oddly, that's missing from Windows Update. As a developer, and I dug into it, there's no way to say to

Windows Update, I don't want this update. You can't even have something running in the background that, like, filters through them.

So it would have been a real kludge where it would have seen it already arrive and then had to, like, invoke some sort of removal tool in the background. There was just no good way to do it. And it wasn't necessary. It's easier just to let it come in and set the registry keys, which it checks, and it goes, oh, shoot, I can't do anything here. And then it just sort of sits there limp, not bothering you any further. And we presume, after the end of July, maybe Microsoft will take it away. They'll just remove it.

So I wanted to make it clear that Never10 doesn't prevent these things from coming in because I would if I could, but there just isn't a practical means of doing that. Instead, I just tell it don't do anything once you get here. And it's not very big. I think it's 30K.

Leo: And I've got to presume that, again, that they're going to honor...

Steve: I think they're going to clean it up. I think they'll remove all this junk from people's systems.

Leo: On the 29th, yeah.

Steve: Yeah.

Leo: And they're going to honor what they told enterprises. They're not...

Steve: Oh, they have to.

Leo: They may be downloading stuff, but they're not going to...

Steve: They have to.

Leo: Well, you know, it's a new day. I don't, you know, I don't recognize this Microsoft.

Steve: Boy, that would be a bridge too far, I think. We'll hope.

Leo: Herschel Day, Houston, Texas, wondering about the security of video baby monitors.

Steve: [Groaning]

Leo: Steve, maybe you've covered this before, and I can't find it, but there are a lot of articles posted about baby monitors being hacked. From what I can tell, this is mostly with WiFi-based devices versus the radio devices. I've only recently become a parent, the little one is five months old, and this is obviously a concern. What prompted this search was that I currently have a radio-based monitor. It was given to us as a gift. It seems to be interfering with the 2.4GHz band on my WiFi, which has my Ring Doorbell and a few other things on it. I then began to look for something that wouldn't interfere, and I found these issues. Should I just get a Nest Cam and forget all this, or am I safe, or what?

I should point out one of our fans earlier today said he bought a security camera on Amazon, didn't like it, returned it, but he'd already installed the software. And a couple of days later he started getting notifications from the camera, and he's looking into somebody else's bedroom.

Steve: Ohhhh.

Leo: They then - yikes. We are really a brave new world here, huh.

Steve: Oh. So we discussed old school video baby monitors way back in the early days of this podcast. And so I thought, that's interesting. I have not brought myself up to speed lately. And I was pulling this all together last evening, so I did some looking around. And what I found was so horrific that I thought, okay, we have to - I just can't wave my hands around and say, "Oh my god, oh my god," because the details that are available are just chilling, and they make such fabulous content for this podcast that we're going to talk about it next week. So, and those are WiFi Internet-enabled. The security firm Rapid7, whom we've talked about often in the past, analyzed the security of nine baby monitors. Eight of them got an "F," and one got a "D." But, again, the details are just so juicy. Very much like what you just said, Leo. That was a perfect lead-in for next week.

So way back before IoT, when not everybody even had WiFi, baby monitors were what Herschel Day has now. That is, they were 2.4GHz. They were analog, but also had some sort of encryption. And back at the time we were talking about how it wasn't great encryption. The problem was it didn't have enough entropy, so somebody who knew what you had could essentially explore all of the possible settings for the encryption key that links the transmitter to the receiver and find your video. But that pales in comparison to anyone on the planet being able to look at your bedroom antics.

So Herschel, I think you should stay with what you've got. And this Rapid7 report was just in September. This is just only a few months ago. So it's not like it's back when LinkedIn was losing its SHA-1 unsalted passwords. This is contemporary. So we're going to talk about the details next week because, oh ho ho, it's just - it demonstrates a complete unconcern with security, which is, as you said, Leo, the brave world that we're in at the moment. Now, the Nest Cam may be okay. I mean, those guys certainly understand...

Leo: It's WiFi, yeah.

Steve: I'm sorry?

Leo: It's WiFi, yeah.

Steve: Yes. It's WiFi. But, I mean, when you hear what is available on the market that people are buying unwittingly, and how easy it is to...

Leo: I have to say there's also radio receivers.

Steve: And that's what Herschel has.

Leo: I'm saying there's radio interception devices, as well, but they have to be proximate to your house.

Steve: Correct. So, exactly.

Leo: [Crosstalk] put it on the Internet.

Steve: Exactly. And today, if I had to choose, I would either use a WiFi-based camera whose security you really understood - now, I've got here the Ring Doorbell. And somebody wrote that it was necessary to open six ports or map six ports through their router in order for the Ring to work. I will be researching this when I get mine installed.

Leo: Yeah, I didn't have to do that, yeah.

Steve: I'm sorry?

Leo: I didn't have to do that.

Steve: Okay. He may have wanted, instead of using UPnP, maybe static port mapping. I don't know. But anyway, so I'm still, you know, mine's still in the box. I'll be talking a look...

Leo: Yeah, I'm curious what you think, yeah.

Steve: I'll be taking a look at it. So I would say, if you can take responsibility in some fashion for what a web-enabled camera, for the security of a web-enabled camera, then okay. But, boy, based on the study of baby cams that are, I mean, contemporary baby cams, it's just amazing how bad they are. I mean, it's like, you've got to be kidding me.

Leo: Yeah.

Steve: So Herschel, I'd stick with what you've got. Yeah, somebody, as Leo said, proximate to your house, who really wanted to, could - typically they're encrypted. There is a key, so there is some security. They all advertise security. It's not great security, not nearly as good as WiFi security. But, boy, it's not available anywhere on the planet. And the Shodan search engine is immediately finding you every baby bedroom on the planet, where you just have an analog camera.

So, boy. We're just in a rough time right now. I'd stick with an analog device, unless - or the other possibility is, if you could find one that was functional without needing the Internet, that is, where the Internet wasn't part of its feature set. Unfortunately, they're all offering, oh, view your baby's crib anywhere, like while you're at work during the day. So that of course means the signal's leaving your house over the Internet. And, boy, they just haven't cared at all about protecting their customers.

Leo: Yeah. Erik in Sweden wonders, why is my proxy not breaking SSL? Steve and Leo, as usual, great show and all that. I started listening around Episode 390. I've also gone back and listened to episodes 1 through 300, so I - wow. I'm almost caught up. I've run into something that's puzzled me for a while. I set up a proxy in Germany to make it look like traffic from domains I choose come from that country. And the strange thing is it works perfectly; or, to be more precise, it works perfectly with SSL. I tried using Google.com with SSL through the proxy, and I searched for my IP, and Google showed the IP of the proxy and not my ISP's IP. By the way, that's the search, "My IP," and that works quite nicely on Google. But I was at the same time connected to Google.com using SSL, and everything was green in my browser. But wait a minute, wait a minute, wait a minute. Shouldn't a proxy break SSL? I guess he's using Squid because he asks does it have some built in magic that makes proxying SSL possible?

Steve: So, great question, because we often talk about how, for example, corporate proxies on the corporate Intranet border are having to play all these games in order to intercept HTTPS connections, in order to see into what traffic is coming into the network. Squid, as an example of a popular browser, like many proxies, has the ability to leave the session alone. There's a command called Connect on a Squid proxy that brings up a tunnel. And any protocol can simply tunnel through without needing the protocol to be broken. That is to say, the TCP packets which carry SSL, or TLS now, they will go to the proxy's IP. And it simply rewrites the IP header on the packet, changing the destination IP from its own to where Eric is in Sweden, and then drops that packet back on the 'Net. Now that same packet that went to the proxy now goes to Eric.

So essentially it's sort of bounced through the proxy, but it wasn't ever opened up. And so proxies can inspect traffic, which, for example, they would have to do if they were going to cache it. There are caching proxies that must then look at the traffic. But it's also possible for it simply to be an IP-level proxy that doesn't go into the higher level protocols. So all it does is it changes the source and destination IPs and puts it back on the Internet. And so it sort of just bounces the packet through it. That way anybody who is outside, like Google, saying what's this user's IP, they see the IP at the proxy, when in fact those packets are then being forwarded to where Erik really is. So, you know, that's how it works. Proxies don't necessarily inspect the traffic. They're able simply to forward it, and that's what's happening in this case.

Leo: Mike, Question 5, in Chicago, wonders which secure text messaging app to use on his Android phone: I'm trying to decide once and for all which secure text messaging app to use. Seems like Signal Private Messenger from Open Whisper Systems is the way to go, but Telegram? Oh, boy. What are you guys currently using on your iPhone and Android phones?

Steve: I thought this was an interesting question because I see these kinds of questions coming in all the time, which one should I use? And he's saying, I'm trying to decide once and for all. Well, it's such a moving target.

Leo: Yeah.

Steve: You know? Here Google has just introduced or announced Allo, which wasn't an option, and it has all these features and optional security on a per-conversation basis, as you told us, Leo. And remember also that a messenger is inherently part of an ecosystem. That is, whoever you're messaging has to have the same one because we don't really, at this point, we're not at a level, maybe we will eventually be, but currently we're not in a standards mode. You know, everyone is stovepiping and hoping to capture the market for their own private messaging protocol. Maybe, if something like Signal created interoperability, that is, Signal being a great protocol around which many people could agree, then maybe that could allow different messaging apps to interconnect. But at this point you can only talk to somebody who's got the same thing on the other end.

Leo: Right.

Steve: So the decision is not an easy one.

Leo: Android has one advantage, though, Steve, that you're not familiar with because you use iPhones.

Steve: Okay.

Leo: Which is that you can name another arbitrary messaging system as your SMS messenger, as your default messenger. Just as you could say, I want to use Chrome or Firefox as my default browser, you can tell Android, this is my messenger. Which means text messages will come through there. Now, you're not going to get the security unless the other person is using the same messenger. But at least it could become your default messenger, which is kind of, I think, a good choice. You can't do that with Apple. You have to use messages. So you're exactly right that, if I'm going to use Signal, for instance, and I make Signal my default messaging app, anybody I want to have a secure session with has to also be using Signal.

Steve: Right.

Leo: At least if it's...

Steve: Although I do have...

Leo: Go ahead.

Steve: On iOS I have green and blue balloons, and so I'm able to do messaging to non-Apple users.

Leo: But surely you're not proposing that you think Messages is as secure as, let's say, Signal.

Steve: Oh, no no no no.

Leo: No, no. So...

Steve: No, no, in fact I've been leading the charge that, unless people manage their own keys and authentication, you have encryption, but you really don't have provable security.

Leo: Right, right. So what do you say? What do you like?

Steve: The answer to Mike's question - yeah.

Leo: You know what, I'd love it if anything that used Open Whisper Systems was interoperable, that would be awesome.

Steve: Right, right.

Leo: But I don't think they are, are they?

Steve: No. As far as I know at this point, they're not because they all want to do their own thing. So, for example, in Allo, again, we're still at an early stage where the various messengers are all hoping to acquire, like, a market share, and maybe win in the long term. And so we have complete fragmentation. And the fragmentation is increasing, rather than decreasing. So anyway, to answer Mike's question, the optimal solution - first of all, I think it's too soon yet to arrive at something. But if you truly need secure messaging, then remember that the other end has to have the same thing that you do. And for me there's nothing other than Threema. I know that it's not open source. It is open protocol. Yet, and so we're trusting them. They seem trustworthy. But you are managing your own key.

The alternative would be a Signal-based solution because I love the Signal protocol that Open Whisper Systems has created, although there you do need to take the initiative to verify the identity of the other end out of band, that is, through some other means. And we talked about that a few weeks ago. And turn on that off-by-default notification if the user's identity ever changes because it's stored locally, and there's an option to alert you if something like a man-in-the-middle were starting to intercept your communication, which you wouldn't otherwise know. So, I mean, the fact that you wouldn't otherwise know it, that's kind of problematic for me.

So, again, it's all a bunch of tradeoffs. I just feel like it's still too soon. It's like, it's all, you know, up in the air. People want security, but they also want convenience. I think the Allo experiment is going to be very interesting to see how many people really care. It's like, no, I'd rather have Google giving me features and listening.

Leo: You know, Threema's got that big advantage of the matching up in three dots and all that stuff. But it's closed...

Steve: And across platform.

Leo: But it's closed source, which frankly to me is a nonstarter. I think, in my opinion, you have to use an open source solution. And that's why Signal's the way to go. It's a little weird because we don't know exactly how WhatsApp has implemented it. So we have to take their word and Moxie's word that they've implemented it.

Steve: Yeah. I also heard something disturbing about Signal, and that is that they're claiming license required in order to use it. So it's not open source, and you can't actually use it without their permission and without a license. So I'm afraid that Open Whisper Systems has gone a little commercial. And I don't blame them. It's their right because they've got beautiful IP. But still it's like, oh, that's unfortunate.

Leo: I just went over to check EFF's secure messaging scorecard. And they've actually taken it down because they're working on a new secure messaging guide because things have changed so much.

Steve: Oh, good.

Leo: You can look at version one of their scorecard, and all of these checkboxes will give you some idea of what you're looking for, including open source and whether it's been reviewed and if there's an audit and so forth. And there aren't that many that are 100% green checkboxes all the way. ChatSecure plus Orbot is one. Off-The-Record Messaging for Windows using the Pidgin app is another. Signal, RedPhone, Silent Phone, Silent Text, those are all from Whisper Systems. Telegram Secret Chats, they give all green to - you're not so fond of it. It's open source, but it's using a non-standard encryption suite, one of their own design.

Steve: Yeah. Matthew was...

Leo: Matthew Green?

Steve: He tweeted something about it a couple weeks ago, like, you know, like who would ever use this? It's like, yeah.

Leo: TextSecure, I like that one a lot. TextSecure is quite good.

Steve: Yup.

Leo: You see, Threema loses one check because it's not open to independent code review. So if you google EFF Secure Messaging Scorecard, you can see the old one. And I can't wait to see the new one, yeah.

Steve: Great resource, yeah.

Leo: Yeah, be interesting. Moving on. Question No. 6 comes to us from Xi'an, China, where the terracotta warriors are. Li writes to us: You mentioned in a recent podcast or two that Windows Update was getting very slow. FYI, it looks to me like they have moved the antimalware scan from after the installation to the start of the "Downloading..." part of the update. Oh, that's interesting. That's the Microsoft Spyware Removal Tool or Software Removal Tool. Hence there's initially a long period of 0% downloaded, no network activity, and nothing appears to be happening despite a busy CPU. That's interesting.

Steve: I thought this was a really interesting observation. I shared it with Paul this morning. We corresponded back and forth about it. And so I've not confirmed it, but I wanted to share it with our listeners because I know we have a ton of techie listeners, and everyone has been observing something really bad seems to have happened with Windows Update, where it just, like, takes forever now. And so it's worth looking at maybe digging down to see where the processor is busy, like what process it's in at the beginning of Windows Update.

If this observation is correct, then it would explain that it's like, especially on an older, bigger system, where there's just a lot to rummage through, if they're doing a pre-update like MSRT scan or a Windows Defender scan, like a full system scan, that takes a long time. And I've watched it sitting here, like with no network activity, like what is it doing? It's like, it's just - and I was assuming, as I wrote to Paul, that it was building a big dependency tree.

Leo: [Crosstalk] more accurate.

Steve: Because, boy, I would not like the job of having to engineer Windows Update and manage all of the different overlapping updates that replace this or that file and, like, filter through that and somehow figure out what set of updates this system needs. That's just, over the course of time and with so many files being updated and replaced, that's

just a horrific task. And so the way to do that is by building some sort of a data structure of what updates are available and which have been applied and then, granularly, which ones are replacing which files to figure out what you should do. Not an easy task. I've just been assuming that's sort of what it's doing. But it sure has slowed down, like, recently. And they may have changed the logic. So I just wanted to share this so that our listeners could explore that on their own.

Leo: Yeah, good theory. Interesting theory. Paul Konigsburg in Great Falls, Virginia wants safe browsing, or wants to know about safe browsing in a VM: Steve, I'm a medium-term follower of Security Now! for the last three years. On several of your recent shows you have mentioned that safe web browsing should be done in a virtual machine. I was wondering if you could give more guidance as you did with the Three Dumb Routers show [SN-545]. I'm currently using the flying turd, Windows 10.

Steve: He wrote that. I appreciated his humor.

Leo: Do you have a recommendation for a good VM for Windows? Or should I look, as Leo would suggest, to go to some flavor of Linux? If yes, which flavor and which hypervisor? In either case, how would you get data, mostly files, from the web browsing VM to my machine that I care about, the one that does my banking and hobbies? I'd appreciate any guidance. Paul Konigsburg.

Steve: So I pulled this, not because I have an answer, but because I will promise to have an answer. I think this will end up being as interesting and potentially as important as Steve's Dream Machine was back in the early days of the InfoWorld column, when I worked out all of the details of, like, choose this motherboard, these drives, this controller, blah blah blah, and gave a clear explanation of why I had made those decisions. I can't do it yet because that waits for me to move over to Windows 7, where I have enough memory and it's feasible to run a VM at the same time as my main system. But I still think that's the ultimate solution is we have to have true high-level containment of the web browser as the major element that contacts the Internet, and it's the conduit through which so much of these problems flow.

So it is on the burner as something that I want to work out for myself, and I will absolutely share it with everyone and provide all of the bases for my decision. You know, it's going to want to be lean, easy to bring up, a small footprint so it doesn't gobble up lots of memory, so that in the VM will be some sort of very small operating system, enough to give you networking and run the browser of your choice, and then also be able to provisionally communicate across the VM boundary. As Paul notes, there are times when you do want to be able to move a file out of that container into your main system and vice versa. So it remains to be resolved. But it's, like, it's something we need.

Leo: I'll be very interested to see what you come up with. Of course, you know, VMware is probably the king of virtual machines. And they offer free player-only solutions. There's a free one from Oracle they got when they got Sun, VirtualBox.

Steve: Yup, VirtualBox.

Leo: Yeah. And then a number of people are suggesting, and this would work, and this is what I'd do would be - I'm not that nervous. But if I wanted to be really secure, I'd carry around a read-only USB key, or you could put it on a DVD, and you could either put your choice of Linux distros on it - I use Tails, which is an intentionally secure version of Linux. You put it on a USB key, and you pretty much have a secure environment there that's pretty hard to...

Steve: Well, yeah, but you've got to shut down your whole world in order to...

Leo: You reboot, yeah.

Steve: Yeah. It's like, that's not happening. I typically...

Leo: Nowadays, machines boot pretty fast.

Steve: Yeah. Well, I have like a mature environment of Windows up. I've got logs that are running on a 24-hour basis and all kinds of stuff. So for me it's like, well, and I've got two big Firefox windows with the 290 tabs open right now.

Leo: You don't want to touch those, huh. I like to reboot once in a while. It's just me, though. Karl, Westfield, Indiana. He says, "I already have a real router." Steve, a week or two ago you were talking about a device that senses when your Internet goes out and reboots things. Your response was "get a real router." Just wanted you to know I have a nice Netgear cable modem, but every several days my Comcast Internet goes out. I could wait for an hour for it to come back or reboot my cable modem. I can't explain it, I just know it works.

Steve: So many people responded that they have this problem. And I thought about it, and so he has a real router, but he says, "I have a nice Netgear cable modem." And that when he restarts his cable modem, his Internet comes back. So it's like, okay, Karl, there's a problem with your Netgear cable modem. I mean, it's not that the cable is out, it's that the Netgear cable modem stopped being a cable modem, and it locked up, who knows why? But if rebooting it brings your cable connection back, then that's the problem. That doesn't happen for most people.

But I will say it was surprising, in response to this, how many people responded that they have DSL, or they've got cable or satellite or whatever, but their stuff is dying, and they're having to give it a swift kick every so often to get back on the Internet, which is unfortunate. My stuff just sits here and runs for months. I mean, like forever. It never has a problem. So I do think that equipment can be a little bit marginal. And also it can be power line, for example. There is flaky power in various areas of the country. Now, I don't know about Westfield, Indiana, where Karl is. But if you've got some big industrial motor starting next door that pulls the power down briefly, gives you a bit of a brownout, that can be all it takes to cause some of this equipment to hang. And so it may just be that the device itself is okay, but through the power supply it's getting glitched and causing it to hang. And that could also be a cause.

So I guess my point is you could put up with this kind of behavior, but you should recognize that a lot of the world isn't, and that you can probably diagnose it, if you care. Or you can just get one of the power reboot plugs and have it restart things whenever the Internet dies.

Leo: You know, that's two states of mind. And a lot of users just kind of grind along with marginal systems, put up with it. And then there's people like you who don't put up with things and say, I want to figure this out, even if it takes them days, and you pull all your hair out. They don't want to grind along with a suboptimal situation; right? You've got it just so.

Steve: Yeah.

Leo: Yeah.

Steve: And I think we're done. We've got two questions, but they were both SQRL, and we'll talk about them next week.

Leo: How's SQRL going? Going well?

Steve: It's going well, yeah.

Leo: Okay. Baby monitors next week?

Steve: Yes. Yes, we have to talk about some of these details. They're just - our listeners will love them. And it's a great cautionary tale.

Leo: Yeah, yeah.

Steve: And I'm sure we can come up with a great title for that one.

Leo: I'll leave it to you. You'll find Steve at GRC.com. That's where he hangs his hat. That's his website. That's where you can find, of course, this podcast, 64Kb audio, transcripts, and more. You'll also find SpinRite, the world's finest hard drive maintenance and recovery utility. Steve's sleep formula is there, all sorts of stuff. GRC.com. There's only one thing you have to pay for. That's SpinRite. Everything else is free. That's your ticket to entry. Oh, well, there is no ticket. Nobody's taking the tickets, anyway.

GRC.com. If you have a question for Steve, you can leave him a question there at GRC.com/feedback. Or on Twitter he's @SGgrc, and his DMs are open, so you can DM him. Or if you want to just ask in public and get a public answer, @SGgrc is his Twitter handle. We put the show up on our website, TWiT.tv/sn, as quick as we can

after the show is done. We are going to put a TWiT Bit up with all of that information about the Windows 10 and Never10.

Steve: Wow.

Leo: Wow is right. You'll find that at TWiT.tv/specials. We of course put this show on YouTube. There's audio and video at TWiT.tv/sn, or subscribe. That way you'll get it every week. There are podcatchers on every platform, and all of them have Security Now!.

You might have noted that we were not nominated in the Podcast Awards this year. There's some dispute over what happened. I maintain I received a letter from the organizers saying you are no longer eligible because you've won so often, so you're now a legacy podcast. They say, oh, that was just TWiT. You could have entered anybody else. But since you didn't, you didn't get nominated. I have nothing but a disdain for the Podcast Awards. I think they're exactly what's wrong with podcasting. We've been stripped of awards in the past because they didn't want to give us an award. Now they've decided we're not eligible. They sent us an ambiguously worded email two months ago. Now they're saying it's our fault. This is exactly what's wrong with podcasting, ladies and gentlemen, is it's small time. So I don't - in the past we've said we're not going to bother with it because we've won enough. We don't need anymore.

Steve: Yeah. And that's how I feel.

Leo: But for them to say, oh, you can't win is like...

Steve: And our listeners know what content we're offering.

Leo: They know, yeah.

Steve: And it couldn't be any more solid. We're close, in this case, the case of this podcast, closing in on year 11. So there's been no evidence of - there's no podfade happening.

Leo: Right.

Steve: We're here for a reason.

Leo: Yeah. So just because - and I know last year you wanted to win, and I just wanted to let you know that's why your name doesn't show up.

Steve: Yeah, and in fact, I saw that it was happening, and I just shrugged. It's like, eh,

you know. We have our followers.

Leo: Yeah. That's about it. Thank you, Steve. We'll see you next week. We do the show every Tuesday about 1:30 Pacific, 4:30 Eastern, 20:30 UTC. Tune in live. We'd love to have you.

Steve: Thanks, Leo.