Here Comes 2019!

Description: This week we look at the NSA's announced forthcoming release of an internal powerful reverse engineering tool for examining and understanding other people's code; emergency out-of-cycle patches from both Adobe and Microsoft; and, yes, we do need to mention PewDiePie again. We also need to mention our prolific zero-day dropper SandboxEscaper, a new effort by the U.S. government to educate industry about the risks of cyberattacks, some welcome news on the ransomware front, some VERY welcome news of a new Windows 10 feature, and a note about a just-published side-channel attack on OS page caches. Then we'll wrap with an update on my work on SQRL and my discovery of a VERY impressive and free large file transmission and sharing facility.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-696.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-696-lq.mp3

SHOW TEASE: It's time for Security Now!. We've been off for a few weeks. Oh, my goodness. That means there's lots to talk about, including new Microsoft zero-day exploits. Aye-aye-aye. Steve has discovered a great file transfer utility. An update on SQRL: It has an API. And GHIDRA - or is it GHIDRA, or is it GHIDRA - the NSA's latest tool. All the deets coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 696, recorded Tuesday, January 8th, 2019: Here Comes 2019!

Happy New Year! Time for Security Now!. Yes, there's still a need for security in 2019. Thank goodness Steve Gibson's here.

Steve Gibson: Yes?

Leo: What would we do without Mr. G, Steve Gibson of GRC.com, the Gibson Research Corporation - our amanuensis, our maitre d', our chief cook and bottle washer. You enjoyed three weeks off, huh?

Steve: Yes, well, I'm apparently a little fuzzy because I got the episode number wrong and the year number wrong.

Leo: In your show notes.

Steve: But I did get my facts straight, so I think that's really what...

Leo: That's all that matters, Steve.

Steve: ...matters more than anything else. There was no major theme that came through. I mean, I did have three weeks' worth of news to catch up on because we skipped two episodes; I did. There was no news for a total of three weeks spanning the weeks on either side of the two that we missed. So I just labeled this one "Here Comes 2019."

Leo: Don't hackers take the holidays off?

Steve: Actually, it did seem to be a little slow. I think maybe everyone just said, "Eh, we'll hack things later. We'll get around to it. All those routers, those routers aren't going anywhere. There are more of them every day." We're going to take a look at the NSA's announced forthcoming release. The upcoming RSA conference is in March. They have announced they're going to release their own internal powerful reverse engineering tool for examining and understanding other people's code. So we'll talk about that.

Leo: Huh.

Steve: We've got emergency out-of-band, out-of-cycle patches, both from Adobe and Microsoft, that now have occurred, but I just want to touch on those. And, yes, starting off 2019 with a bang, we do need to mention PewDiePie once again.

Leo: Oh, dear.

Steve: It does not go away. We also need to mention our prolific zero-day dropper, SandboxEscaper. And Leo, you are going to love her travel photos. Oh, my goodness.

Leo: Oh, no.

Steve: Apparently she's a hiker, and she's got the coolest little tent. It's like a little personal shelter tent kind of thing. Anyway, I'm sure you'll be scrolling through them when we get down to that.

Leo: I will.

Steve: But anyway, so actually there were two things that she did, and we didn't tell our listeners yet, but I killed another processor this morning, and that threw off my game a little bit. The good news is I got a lot done last night and some this morning before I decided, oh, I really should reboot the system, and it didn't come back from the reboot.

Leo: Oh, boy.

Steve: Anyway, I've scrambled around a bit. But there are actually two new zero-days that SandboxEscaper dropped. And I meant to get to the fourth one...

Leo: Wow.

Steve: Yeah, I know, she's busy. And somebody, I noticed somebody tweeting who saw the show notes already, who said, "Steve, you really shouldn't refer to her as a" - well, her as a she, or this person as a female. Except I didn't know when - now I have her locked in here as a woman. I didn't know the first time who this was, and somebody said, like, "We know this is a female." So I adjusted myself for all the subsequent zero-day drops that she has dropped. So until I actually learn definitively otherwise, now as a consequence, well, we'll get to this. But her Twitter account and her GitHub account have both been suspended or canceled or deleted.

Leo: Oh, wow. Oh, wow.

Steve: Yeah, she's finally really upset people.

Leo: It's fine if we don't - whether we know or not, the default doesn't have to be "he." It could be "she." That's fine. Or "they." I mean, who knows?

Steve: I do see people reading, I mean, I read people who write "she" for some reason when there's no reason to think either way. And I think, whoa. But I don't know, I guess I think of "he" as being more generic. But anyway.

There's a new effort by the U.S. government to educate the industry about the risks of cyberattacks. We have some welcome news on the ransomware front, some very cool announcement from BleepingComputer I'm going to talk about. And some very welcome news about a new Windows 10 feature. And also a note about, just as I was getting ready to wrap things up, the news of a new side-channel attack on OS page caches was announced, which I had no chance to look at. It didn't look - I scanned it quickly. It didn't look like it was going to be a big deal. It was, like, really out on the fringe. But I'll have more about that next week.

And then I want to wrap up with a brief update about my just-finished next and actually final phase of work on SQRL; and, as a consequence of something about that, my discovery of a very impressive and free large file transmission and sharing facility, which I needed in order to move a 6GB VM to a developer in Denmark. And you probably know about it already, but I was very impressed with it, so I just wanted to give them a shout-out. So something for everybody.

Leo: Nice. Now, I have delved into SandboxEscaper's blog.

Steve: Ah, okay.

Leo: Where I found, I'm going to say "her," profile page. She's transgender. And it looks from the picture of it that she's chosen to be a woman. But she doesn't state

what pronoun she prefers. So I think it's appropriate to say "she" unless she states otherwise.

Steve: Okay.

Leo: Based on her picture.

Steve: And did you scroll down through her hike history?

Leo: Yes, yes. The blog is called "The Blog About Polar Bears."

Steve: Yeah, we don't know why.

Leo: I don't see any polar bears. But she says: "I currently do not own any social media accounts after losing @Evil_Polar_Bear. People have tried to impersonate me in the past after having account banned. So whatever, you're warned. I'm a retired vulnerability researcher. I make a living writing travel blogs now. Besides that, I'm also transgender. Hobbies include fencing and hiking long distance trails." So what she doesn't do is say which pronoun she prefers, and certainly we would use whichever she prefers. But given that it looks like she's decided she's a woman, so we're going to call her "her."

Steve: Well, and relative to polar bears, she did tweet a picture of what she decided was an angry polar bear. And I looked at it, and I thought, it looks very comfortable to me. It doesn't look like it's in any way upset with seals or dolphins or anything else in its, you know, penguins or anything.

Leo: Maybe it's an ironic polar bear, probably.

Steve: Anyway.

Leo: All right.

Steve: Never a dull moment on the Security Now! Podcast.

Leo: Yeah. Anyway, that's the deal from here, the view from here.

Steve: Thank you. And in the meantime, I want a readout from you, Leo, on this tent that she is using. It's very cool. It's a little personal thing. Anyway, see what you think. Meanwhile, so speaking of passwords.

Leo: Yes.

Steve: That is apropos of the Picture of the Week. We have a picture of a little beagle sort of forlornly looking up at the person taking the picture, and the caption says: "Someone figured out my password. Now I have to rename my dog." So sort of - is that cart before the horse or something? Anyway, I do use LastPass, Leo, and I don't know any of my passwords anymore because we're not supposed to.

Leo: No.

Steve: They're impossible to know. And the only real downside is when I try to, you know, LastPass, I think my default is 20 characters of upper, lower, and special case and everything. And something says, oh, you can only use 15.

Leo: I hate it when that happens. I hate that. But then I'll use, like, 12 or 13 because I don't want to use 15. You don't want any hints.

Steve: Ah, that's true.

Leo: Does that make sense?

Steve: You've been paying attention, my friend.

Leo: I have.

Steve: That's very true. I didn't want to give away my secret, but you did.

Leo: Never mind what we just said.

Steve: So on Podcast Tuesday of March 5th, so that's, what...

Leo: Three months.

Steve: I'm really off my game. February, March. Two months from now, Robert Joyce, a senior advisor with the U.S. National Security Agency, will be offering his talk titled - this is at the RSA conference - "Come Get Your Free NSA Reverse Engineering Tool."

Leo: Oh, geez.

Steve: Yeah. Robert's talk abstract reads: "NSA has developed a software reverse engineering framework known as GHIDRA." And I did some googling, thinking, okay, I mean, it's got IDA in it, so that was a clue because that's Interactive Disassembler, IDA. And so they kind of crammed - and Ghidra is something from Final Fantasy V, "an enemy fought at Ronka Ruins alone and can also be fought in the battle with an Alchymia. It is a dangerous foe, and it has auto-reflect and battles using poison breath and lightning."

Leo: Well, it was also a many-headed serpent in Greek mythology. I mean, it was...

Steve: Well, that was just a hydra; right?

Leo: Yeah, H-Y-D-R-A.

Steve: Yeah.

Leo: So this is more letters.

Steve: G-H-I-D-R-A. Yeah, we've got more letters in there.

Leo: Oh, G-H-I-D-R-A.

Steve: Anyway, so whatever they have, it will be demonstrated...

Leo: This sounds like GHIDRA, maybe GHIDRA.

Steve: Okay.

Leo: I don't know. We'll find out.

Steve: I don't know. I'm sure there's got to be some Final Fantasy people around listening. Sorry about that.

Leo: So it's a Final Fantasy character.

Steve: Yeah. So it's going to be demonstrated for the first time at the RSA Conference 2019. He says: "An interactive GUI capability enables reverse engineers to leverage an integrated set of features that run on a variety of platforms, including Windows, Mac, and LINUX" - and it's written in Java - "and supports a variety of processor instruction sets." The whatever we call it, GHIDRA platform includes all the features expected in - this is the NSA bragging - "in high-end commercial tools, with new and expanded functionality NSA uniquely developed, and will be released for free public use at RSA."

Leo: It was also in Vault 7.

Steve: Yes. We first learned of it in the Vault 7 WikiLeaks.

Leo: So we've had it for a while.

Steve: Well, we've known of it, but apparently it's been evolving. So the WikiLeaks quoted version was 7.0.2. We know that it requires Java 1.7. So according to the Vault 7 documents, GHIDRA, for lack of a better pronunciation, was initially developed by the NSA in the early 2000s; and a Reddit user named "hash_define" who claimed to have had access to GHIDRA said that the tool had been shared with several other U.S. government agencies, mentioning the CIA.

Leo: That's why it's in Vault 7.

Steve: Right, over the past few years. So while there's no explicit announcement yet that the NSA plans to open source GHIDRA as opposed to just make it available, some believe the agency will also publish GHIDRA source code on the NSA's GitHub code repository, which we've mentioned a couple times. It's an amazing trove over there. Currently there are 32 released projects, NSA projects over on their GitHub port. So the open source community may have access to this and be able to maintain it for free.

So for what it's worth, the buzz about this within the reverse engineering community is the promise of a good solid user interface, which apparently is what's missing, even from the IDA Pro, which is sort of the standard, although it's pricey. And the belief is that it has a strong typing feature set. I'll explain what that's about in a second. But they're suggesting that this would fill an important gap that's currently lacking in the current reverse engineering tools. IDA Pro that I've mentioned, where IDA stands for Interactive Disassembler, is the current favored tool. And I'm sure it's pirated like crazy because consider its audience. But if you license it, it's $1,866.99.

Leo: What?

Steve: Yeah.

Leo: How did they come up with that?

Steve: That was my thought, too: $1,866.99. That's like, okay. That's what they want.

Leo: I'm sure it means something.

Steve: So the company that produces IDA Pro is Hex-Rays, which is kind of cute. And I'm sure that everybody but them is delighted at the idea of the NSA releasing something that apparently blows it away. Okay. So think about this. For those of our listeners who don't know - so we're all familiar with the term IDE, Integrated Development Environment. An IDA is sort of the reverse. Its challenge, the IDA's challenge, the Interactive Disassembler's challenge is that the act of compiling source code discards so much of the programmer's originally supplied information that what you end up with, of course, is the famous pile of ones and zeroes.

So there have been mistakes made in the past where the debugging information has been almost certainly mistakenly left in the code. That can happen, in which case basically you get the names of all of the things. You get the names of the so-called "symbol table," which is the mapping between what the programmer called a variable

and where the variable is located, what the programmer called a subroutine or a jump point and where that is. But normally - and that's big. That is, leaving the debugging information in the object code makes for a much larger result. So it's almost always the case that that is stripped out. So what you're left with is just ones and zeroes. And so you're just looking at it, and it's just an opaque blob.

So the automated portion of the disassembler can analyze the program's flow. It can essentially step through the code. It's not actually doing what the code says. It's not executing the code. But it can step through it to find the branches and see where the branches branch to, and then essentially build a tree of all of the bytes in the executable that could be executed if every branch was followed and not followed, and every jump was taken, and every subroutine was called. So it's able to do - that's typically called a "static analysis." It doesn't run the code. It analyzes it like crazy. Essentially what that does is it creates a flow of the code, but it also shows what areas cannot be executed. And so it assumes those are data. And in some cases then it can go further.

Once it's sort of done that, then it can look and see, oh, look, we're moving something with an instruction that moves something to memory, and it knows the address of that. So it's able to provisionally label that as a variable of some sort. It doesn't know what to call it yet. So it just gives it sort of a temporary name. So the idea is that the automated portion is able to go through and, without understanding what the program does, without ever executing a single line, it's able to sort of unfold it, sort of unwrap it into pieces. And it's able to say, you know, this is data. These are instructions.

And we've showed snippets of this, of a disassembler output, many times in the past in some of our coverage. It's able to then graphically create, like, blocks, where typically there's an arrow coming in, and then a block of code, and then maybe one or two arrows going out to places that block jumps to, that goes to other blocks. So it can sort of allow you to move around graphically.

But the other thing that can happen now that we have operating systems with known APIs is that a good disassembler will see, oh, look, the OS is being called to read the registry here, because that's a known operating system call, and the parameters that that operating system call requires are known. So that allows it to further reverse engineer and go, well, this has to be the handle to the key which has already been opened, so we can label that a registry key handle. This has to be the name of the key that's being opened underneath the handle so we can label that now.

So as a consequence of the fact that we know everything about the functions that the program calls in the operating system, that again further really gives us a foothold on what's going on. But there's a limit, of course, to how much can be done with automation. It can't understand anything, but it can really go a long way toward setting things up and getting it ready to be understood, which is where the interactive portion comes in. Then a human, a hacker, somebody at the NSA or somebody, basically, anyone who wants to reverse engineer and understand somebody else's compiled code, I mean, certainly all of the people that are taking malware apart in order to understand what it's doing and how it works, and we're talking about this all the time, they're using this sort of tool.

So then they'll take a look at one of these blocks and see what registry, for example, to continue the example I was drawing, see what registry functions are being used, look at the actual name of the key that's being read or written, and then think, aha. And that tells them what's actually happening.

And so what you can do is you can, with all of the help that the automation portion was able to provide, you sit there, and you start filling in the blanks. You say, well, if this registry key is reading this into here, then this here must be named that. And so you

start giving things names. And as you do, the disassembler will propagate all the other instances of that throughout the code and, basically, although it's not completely automated, working interactively with one, it's very possible to make a really good stab at reverse compiling, essentially reversing the process of all of the information that was lost when the compiler discarded all of the labels that the programmer had put on things in order to make their own code intelligible to themselves, which the computer doesn't need.

So anyway, I'm sure we're going to be talking about this on the 12th, which is the podcast after March 5th where this will be announced and made available. And I have a feeling it's going to be very popular. I mean, if they've done, you know, they're touting this as commercial-grade GUI; and arguably it is that aspect of it, it's the ease of use GUI side which most of these reverse assembly tools don't really finish out. So this is very exciting. I think it's going to probably - and it's interesting that they're choosing to do this. Maybe, Leo, as you noted, it's because, well, the cat was already out of the bag a little bit with the CIA WikiLeaks Vault 7 stuff. So they thought, well, what the heck, let's formally announce it at RSA. But very cool.

Leo: Yeah.

Steve: And kind of fun to play with, if you're interested in understanding how stuff works.

Last Thursday, January 3rd, Adobe released a pair of emergency out-of-cycle patches for their Acrobat and Reader PDF system. The good news is that, while the bugs are rated critical and do allow for remote code execution and privilege elevation, Trend Micro, who found and reported the problems to Adobe, was unaware of any ongoing exploitation in the wild. However, an attack leveraging these flaws only requires the victim to open a specially crafted PDF and remote code execution on your system with privilege elevation. So really not good.

So this makes these high value targeted for phishing attacks, so they would be unlikely to be used widely. They would be too valuable to just spray out in an email blast or something. So if they were in use, it would be unlikely in this day and age that they would have been spotted by Trend Micro. Which is to say we don't know that, because they haven't been seen, they aren't in fact in use. So for what it's worth, if you haven't already, this was last Thursday, just check for updates in whatever version of Adobe Reader or Acrobat you may be using, and make sure you're up to date. Again, unlikely that this would bite you unless you would be a target of a phishing attack. But still, it's better to be safe.

And believe it or not, Leo, on this first 'cast of the new year, we're going to talk about, yes, PewDiePie.

Leo: Oh, PewDiePie.

Steve: This time Chromecast users have had PewDiePie-pushing video content interrupting their viewing.

Leo: Whoa.

Steve: If you can believe it or not.

Leo: Wow.

Steve: Yes. On Reddit, someone posted: "TV randomly switching to some PewDiePie video." He posted: "Every 20 minutes or so, my TV switches to some crappy YouTube video about PewDiePie with [and he said] rap music and a #ChromeCastHack hashtag."

Leo: That's not annoying at all.

Steve: "Anyone know how to stop this? It's driving me bonkers." Now, Google's response to this from GraceFromGoogle, the Google Community Manager, Grace wrote: "Hi everybody. We know how frightening this is. The good news is your Chromecast hasn't actually been 'hacked,'" in quotes. "Rather, somebody was able to cast to your Chromecast due to an opening in your home network." Oh, yeah. That's a great comfort. "This is the result of your router making some smart devices, including Chromecast, publicly reachable." No, actually it's a consequence of Chromecast telling your router that has Universal Plug and Play enabled that it would like some ports mapped to it, pretty please.

Okay, so it is both. It is Universal Plug and Play. How many times must we say? I will say that the instant it appeared, on this podcast we said turn it off. This is really bad. Turn it off. And we know that Xbox people, that was a hardship for them because arguably this was created so that Xbox would be able to have ports mapped into it. So anyway, what we have is the return of @HackerGiraffe. Remember that twice now, Leo, once while you were gone, then the second time, for you the first mention on this podcast of PewDiePie, was his second hack of a greater number of printers which are exposed on the Internet, all sending out the - there was like, the No. 2 YouTuber was some Israeli or...

Leo: Yeah, it's an Indian channel, Teapot or something, yeah, was starting to beat PewDiePie.

Steve: Right, right, right. Okay, so...

Leo: It worked, by the way. I think PewDiePie has - T-Series has ceded its lead to PewDiePie.

Steve: That's what it was. It was T-Series. So anyway, on the FAQ for TheHackerGiraffe.com, they ask themselves: "What's going on? If you came here because you're a victim of CastHack, then know that your Chromecast/Smart TV/Google Home is exposed to the public Internet and is leaking sensitive information related to your device and home. What information is leaked? What WiFi your Chromecast/Google Home is connected to, the Bluetooth devices it has paired to, how long it's been on, what WiFi networks your device remembers, what alarms you have set, and much more. What can hackers do with this? Remotely play media on your device, rename your device, factory reset or reboot the device, force it to forget all WiFi networks, force it to pair to a new Bluetooth speaker or WiFi point, and so on.

"What can't hackers do?" He says: "Assuming the Chromecast/Google Home is the only problem you have, hackers cannot access other devices on the network or sniff information besides WiFi points and Bluetooth devices. They also don't have access to your personal Google account, nor the Google Home's microphone. They do have access to the noise level in the room," however, which is interesting.

Then the FAQ that they wrote for themselves asks themselves, "Who are you? Your friendly neighborhood @HackerGiraffe. We just want to have a bit of fun [uh-huh] while educating and protecting people" - of course, this is breaking the law, but what the heck - "and protecting people from open devices on the Internet. We were also behind the #PrinterHack and #PrinterHack2. Why are you doing this? We want to help you, and also our favorite YouTubers, mostly PewDiePie. We're only trying to protect you and inform you of this before someone takes real advantage of it. Imagine the consequences of having access to the information above. What do you want? Well, fix your device. And also subscribe to PewDiePie on YouTube. Also Pyrocynical, Dolan Dark, and Grandayy." I'm not going to spell it.

Leo: This is why you're never going to succeed on YouTube. You've got to be able to read these.

Steve: Wow. "Don't forget good old Keemstar."

Leo: Keemstar, whoo.

Steve: Okay. "How do I fix my device?" He says: "Disable UPnP on your router. And if you're port forwarding ports 8008, 8443, 8009, then stop forwarding them."

Leo: Will your Chromecast stop working if you do that?

Steve: No.

Leo: Okay.

Steve: "Thank you. Any way to show support? Yes," he says, "I, HackerGiraffe, have other things to do."

Leo: Oh, good.

Steve: Please, yes. "Use my free time teaching people cybersecurity and ethical hacking." Okay. "If you want to support personally or enjoyed this hack" - oh, yeah, it was enjoyable - "consider becoming a patron on my Patreon page." And, by the way, I went, and it had been canceled or closed. So I don't think that worked. Okay. So if you go to the page that is listed in the show notes, casthack.thehackergiraffe.com, you get a status page. Total exposed devices, 72,341. Of those, 8,254 were renamed, and 65,283, that is, the balance, have been forced to play video. So more than 65,000 Chromecast or Smart TV devices received this annoying YouTube video. That same number of 72,341

breaks down as 1,542 were Google Home devices, and the remaining 67,049 were Smart TVs or Chromecast devices.

So anyway, Google did say that this was the fault of UPnP being enabled. This Grace from Google continued, after blaming it on UPnP, and I don't because this is Chromecast saying, "Open ports to me, please," she wrote: "To make your network more secure, you can disable UPnP to avoid any unwanted content being played on your devices." How convenient. "The instructions are different from router to router, so we suggest checking with the manufacturer of your particular device. However, this may affect other apps and devices that use UPnP to function." Meaning Chromecast doesn't really need it; but we thought, what the heck, let's open some ports because why not?

So what I would note, there's been coverage of this. As we have mentioned before, the port mapping done by the UPnP API typically is hidden from the user so as not to confuse them, like wait a minute, I didn't map these ports. So they don't appear in the UI. What I would recommend, first of all, remember that GRC - the first time this became apparent to me on the podcast, Leo, that Universal Plug and Play was being enabled externally, it was like, okay, wait a minute, let's check for that.

So although this doesn't require an external presence, but our ShieldsUP! service still has, from that day on, a quick test for external access. That's what the bad guys are using for proxying traffic and setting up bots and so forth, and now turning around and using it to look inside people's networks. So you absolutely want that disabled from external access. But this is internal use; and it is the case that, as Grace notes, that there may be some things you are doing on your network that will stop working if you disable it. Typically, however, it is possible to manually configure the ports to the devices that need it.

The problem with having Universal Plug and Play enabled is there's - and this was the first point we made about it when it first hit our radar was there is no authentication. There's no username, no password, nothing. It is wide open so that anything inside your network has access to it if it's enabled and can do anything it wants to with your router behind your back. I mean, it's unconscionably bad. It always was. And we keep seeing instances where it's biting people.

So the point is that, if you disable it, you should reboot your router. The Universal Plug and Play mappings are typically dynamically made. They are not statically stored in nonvolatile memory. So a reboot should flush them. But turning it off won't necessarily close these holes because it'll prevent new ones from being mapped, but probably leave the existing ones in place. And if you're going through all that, take the time to check the router's manufacturer's website with the version number.

Remember that we've seen already an instance where the router itself wasn't aware that there was a newer version. So even a router that is trying to check to see whether it should update itself may not have the latest information about what is available for its own firmware. So check the manufacturer. Always update to the latest. Shut down Universal Plug and Play if you believe you can, and then do a reboot in any event so that, if you're trying to close things down, you have a chance of doing so.

Leo: And don't forget to subscribe to Pyrocynical, Dolan Dark, and Grandayy.

Steve: That's right. Give props to PewDiePie.

Leo: And good old Keemstar.

Steve: So also...

Leo: Sorry I threw you. I apologize.

Steve: I did, I had one last...

Leo: By the way, PewDiePie is beating T-Series, but it's really close as of seconds ago.

Steve: Wow.

Leo: Yeah, PewDiePie has about 400,000 more subscribers. He's got 80 million subscribers, by the way. It's amazing, the number, although probably those aren't real people. Or maybe they are. I don't know how it works. Yeah, he's got, if you really care, he's got 80,224,368 subscribers; T-Series 79,486,103 subscribers. I know you're glad. Now, I was just doing that to give you time to find your place. Go ahead.

Steve: And I did. Thank you, Leo.

Leo: You're welcome. See? You see? I'm helpful. I'm helping.

Steve: What's annoying is that Google knows about this. They have known about this for years. There are a number of YouTube hacks dating from 2014 showing Chromecast being commandeered, like play something on your neighbor's Chromecast sort of thing.

Leo: You have to be in physical proximity? Or can you do it anywhere in the world?

Steve: Well, at least this way here, you can do it anywhere in the world because it's publicly open. And that's what this guy did. This HackerGiraffe, how many was it, 72,341 devices were found. Of those, more than 65,000 had been forced to play videos.

Leo: Geez. Do you use Shodan to find that? How would you find that?

Steve: Shodan may very well because we know that that's a tool he used to find the printer exploits before. So he may have just said, oh, what else can I do to push PewDiePie? Because, after all, it's neck and neck with T-shirt. It's actually T-Series, I know.

Leo: It's T-Series. Pewd versus T-shirt. Okay, Steve. Back to you.

Steve: So you know I've been using, as a consequence of having killed another processor this morning, I've been using a laptop that I have Windows 10 on that I don't use very much. And in the bit of browsing that I've been doing this morning, and even just now during this announcement, I was wondering, I wanted to get some better information on overclocking killing CPUs. Websites are unusable without uBlock Origin. I have no affiliation with them. We've talked about them a lot, you know, Gorhill and...

Leo: It's your adblocker that you love.

Steve: Oh, my lord. Because I don't have it installed on this other laptop that I'm actually using right now because I just haven't ever used it very much. But it's like, oh, this is what people tolerate on a normal basis? So, uh-huh, yeah, I'm just saying, you know, uBlock Origin.

Leo: It's true. It's true.

Steve: Or whatever. Boy. So Microsoft issued an emergency out-of-cycle patch for IE. It was a while ago now, so hopefully everybody has received and updated, although it's comprehensive. It was the day after our last podcast they issued an emergency out-of-cycle patch to close a zero-day vulnerability in IE that was under active attack and being used to attack Windows users. It was discovered by Google's Threat Analysis Group. It's a remote code execution flaw in IE's JavaScript engine. And we've often talked about how difficult it is to get these right. You know, JavaScript is interpreting code that the browser downloads from wherever you go. And all pages have it, are using it these days, so you're stuck with it.

Famously, back in the day, before uBlock Origin, it was NoScript, and it made things a lot saner, and I liked it. But of course we gave up using it because you have to have JavaScript these days. Everything is using code that your browser is running. So when this particular vulnerability is exploited, it allows hackers or attackers to execute arbitrary code in the context of the current user, which is not as bad as also being able to elevate privilege, but you don't want random code running even under your context because it can still get up to mischief. And if the current user were logged on with administrative rights, then the attacker who exploited the vulnerability could take control of the entire system - install programs, view/change/delete, create new accounts even for themselves.

So what makes this more worrisome is that our browsers, as I was just saying, run JavaScript code all the time. And in this instance, not only is it a specially designed web page, it could be HTML email, a mail attachment, an MS Office document, a PDF file, anything else that supports embedded IE scripting engine content, and lots of things do. And this exists in all instances of IE, from IE9 on Windows Server 2008, which would have been what version of Windows, 7 or maybe Vista, I think, IE10, IE11. So just across the board. So just make sure that, I mean, I would imagine a lot of us are using Firefox or Chrome and not IE. But still the point is that it's the underlying engine component, not the browser itself. It's the JScript.dll library, and other things will invoke that in your build of Windows, even if you're using another non-IE browser.

So here we are. We are the second Tuesday of the month. This is Patch Tuesday. I have not had a chance to check to see whether this thing, well, we know that it was an out of-cycle patch, so I would imagine - my point was that, since then, and certainly if not before, then today, everybody's machines are getting caught up and patched. And so definitely worth doing. This is the kind of thing that would be sprayed on, you know, an

advertisement on an unwitting web page could use this. So this explains why Microsoft jumped the gun and put this out immediately.

And the day after that, SandboxEscaper strikes again. And she's apparently not any happier, Leo, than we've seen her in the past.

Leo: She's very angry, yeah.

Steve: I had to blur the F-bomb in her tweet because, you know, I thought, okay, this is an adult podcast, and we all know what the other three letters are after "F." So it's like, okay, why, really. But still it seems appropriate.

Leo: No, no, no. We have youngsters who want to learn about security, too, and protect their little ears.

Steve: Yes. So she was at that time tweeting as @Evil_Polar_Bear. And Leo, you noted that that account had been closed.

Leo: Yeah.

Steve: So she tweeted sandboxescaper.blogspot.com, which is where her blog is now. She said: "New zero-day. My GitHub got taken down. And screw it, I'm not going to get anything for this bug anymore. So you can all go, you know, 'f' yourselves. Bye, happy holidays." Charming person. Tweeted on the 20th of December.

Leo: However, I have to say, pretty good at finding zero days.

Steve: Oh, Leo, that's what's so sad. And in fact, the first link on her blog is a list of all of the CVEs that she's responsible for. And so she's been active for, I think it was like three or four years, going back a ways, and has found a bunch of stuff. And as I have said before when we've covered the two previous ones, looking at them, they were really good work. I mean, it's very nice work. So, yeah, you've got them on the screen now. There's a nice chunk of work. So I don't know what the back story is. She's never happy when she tweets. So we know people like that.

Anyway, so just to recap quickly, back in late August was the first of these that came to mind. She exposed details and provided a proof-of-concept exploit for a local privilege escalation flaw in Windows Task Scheduler. We talked about it at the time. It was present due to errors in the handling of the Advanced Local Procedure Call service in Windows. And a few days after the release of that proof of concept, a zero-day vulnerability was found, based on her work, actively being exploited in the wild.

Microsoft addressed it the following month in the September 2018 security patch, but people were being actively hurt in the interim before their systems were caught up. Remember we offered - there was one of those little jiffy patches, whatever they were called, where there's a company that does the little quick patches in order just to fix it until Microsoft catches up. But of course nobody who's not listening to this podcast knows about those or that there was a problem.

Okay. Then, two months later, in October of last year, she released a proof of concept exploit for another privilege escalation vulnerability in Microsoft's data sharing that allowed a low-privileged user to delete critical system files from a targeted Windows system and then demonstrated how that could be leveraged into something damaging.

So anyway, here we are again. There was even another one that, as I mentioned, I had intended to get to, but everyone gets the idea. Unfortunately, she is not as well retired from this as we wish she were. And apparently she either has a very good connection to the Internet while she's in the middle of hiking with polar bears on some frozen tundra somewhere, or she comes home and then does more about finding zero-days.

So this particular one, this zero-day, which did result in her Twitter and GitHub accounts being taken down because - and frankly, at the time, I remember being surprised that a damaging proof of concept was being left on GitHub. I was kind of impressed that it was because, well, okay, I guess we're going to be fair. But not anymore. So this one is a zero-day in the MsiAdvertiseProduct. And I am tempted to say, well, Microsoft, maybe you deserve this one.

Leo: At least they're honest.

Steve: Yeah, right, they didn't name it something funky. MsiAdvertiseProduct function of Windows that's responsible for generating, quote, this is their explanation: "An advertise script or advertises a product to the computer and enables the installer to write to a script the registry and shortcut information used to assign or publish a product." So this is a little glitch in Microsoft's Windows as a service feature set, which she found and has disclosed. Due to improper validation, the affected function can be used to force the Windows installer service into making a copy of any file with system privileges and read its content, resulting in arbitrary file read vulnerability.

So anyway, another zero-day. Microsoft, if they didn't fix it today, because it's now been about three weeks, I'm sure they are. They're aware of it. It was removed from GitHub. Her Twitter account has been removed. Maybe this is the end of it. But she did have a run of four very nice zero-days over the last few months. And the sad thing is she's finding important vulnerabilities. Better for her to find them and just report them than turn them loose. So I don't know. It's unfortunate.

Okay. What is fortunate is that the U.S. National Counterintelligence and Security Center, the NCSC, has begun distributing materials ranging from brochures to videos to privately held companies around the U.S. These promote and encourage heightened awareness of the rising cybersecurity threats from nation-state actors. Certainly, again, everybody on this podcast is well aware. But your random companies in the U.S. are like, oh, well, you know, how's our security? And the IT guys says, "It's great, boss." And it's like, okay, fine. Next item on the bullet point. How about something that makes money for us?

NCSC Director William Evanina wrote: "Make no mistake, American companies are squarely in the cross-hairs of well-financed nation-state actors who are routinely breaching private sector networks, stealing proprietary data, and compromising supply chains. The attacks are persistent, aggressive, and cost our nation jobs, economic advantage, and hundreds of billions of dollars." So this campaign provides detailed information on the growing threat from foreign state hackers.

The NCSC is an Office of the DNI that we've talked about, the Director of National Intelligence, which is designed to provide counterintelligence and security expertise in several areas, ranging from insider threat and supply chain risk management to personnel security. So to push back against what they perceive as and we know is a

growing threat to our commercial enterprises, the NCSC decided to provide the U.S. private sector with information it needs to understand and defend against cyber intrusions initiated by foreign governments. In their tweet yesterday, Monday, January - what?

Leo: I'm just looking at the card. Go ahead.

Steve: Oh, I know, I know.

Leo: Go ahead.

Steve: I know. In their tweet yesterday, on January 7th they tweeted: "The National Counterintelligence and" - oh, and in fact, Leo, you should click the link because it's animated. The actual image is a GIF. They said: "The National Counterintelligence and Security Center is today disseminating a series of videos, tips, and other materials to help U.S. industry guard against growing counterintelligence and security threats from foreign nation states and other actors." And we have a link to the tweet, and the tweet has a pic at the bottom of it. I managed to capture it after it had fully populated because it's five bullet points, and they populate with some animated glee. First one: Strengthen your...

Leo: I can't get it to play, unfortunately. I think I have video blocked everywhere somewhere.

Steve: It's just a GIF, though, so it ought to - but it's good. I'm glad that it's not playing, Leo. That's good.

Leo: Yeah, it's good security.

Steve: Yes. So "Strengthen your Passwords." And they have a capital P-@-$-$-w-0...

Leo: In other words, use leet, and all will be well, yeah.

Steve: Exactly. That's right. No one's ever going to figure that out. "Lock down your social media accounts." Okay.

Leo: What do you mean, lock them down?

Steve: Exactly.

Leo: Like use a password? Okay.

Steve: Exactly, what does that mean? "Delete suspicious emails." Instead of what, like archive them? Click on them? Hold them? What? Yeah. This is cutting-edge security.

Leo: Oh, my god. This is security for fifth-graders. Oh, my god.

Steve: Yeah. Oh, and look at the title bar. "Know the Risk. Raise Your Shield." Doot-doo-doo. Oh, number four. "Don't expect privacy when you travel," especially from U.S. border agents. Yes. Especially when you're trying to come back in the U.S. Good luck to you. We covered this, what, last podcast? Yes, they are downloading your personal data, your private data from your phone, and not deleting it from their thumb drives. That's right. And then number five: "Know who you're talking to." What? Okay. Anyway, yes. More tips coming in the future. We'll have six through 10 in our next GIF slide.

Leo: I've got a tip I should pass along to the lawyers who put out the redacted Manafort filing.

Steve: Uh-oh.

Leo: Wait a minute, I've got to show you this one. This just broke. It's from @nycsouthpaw.

Steve: It is unredactable?

Leo: It's unredactable.

Steve: Oh, I hate when that happens.

Leo: Unredacted redaction. Basically, he or she says you can copy the black highlighted redactions in the Manafort team's filing, paste it somewhere else, and then see what it says.

Steve: Yeah.

Leo: Nice job with the redactions.

Steve: That's right. What you want to remember to do is to print the result of the redaction, and then that's what you use.

Leo: Or maybe just use a felt pen. I don't know. There's ways to do it. Holy cow, yeah.

Steve: Wow. So this announcement, this cutting-edge announcement from your NCSC government agency working to protect you and remind you to shield yourself from its

own border agents comes on the heels of a statement made before the U.S. Senate Judiciary Committee last month by Bill Priestap. He's the Assistant Director of the FBI's Counterintelligence Division. He said: "Many American businesses are just now starting to understand the new environment in which they are operating. The continued proliferation of cyber hacking tools and human intelligence capabilities means that this environment will only become more hostile and more treacherous for our companies. Our businesses face competitors in the form of foreign enterprises assisted or directed by extremely capable intelligence and security services." So anyway, everybody worry. Thank you very much.

Leo: Aye-aye-aye.

Steve: Thank you very much. Okay. So, Leo, there's another picture for you here. As we know, Apple no longer attends the industry's annual Consumer Electronics Show - that is, they don't set up a big booth and do that - which is normally held and has historically been held in Las Vegas every year because Apple is large enough now to create their own shows. But they couldn't resist this year plastering a huge graphic on - it's one of those, like, it's black and white, but it's one I guess where it's like a tint or perforated or something?

Leo: Yeah. You can see through the windows, yeah.

Steve: Yeah, because the people in the rooms of this hotel have to still be able to see out.

Leo: By the way, note the hotel.

Steve: I know, I know, I know, I know, I know. That's the little glitch here. So we'll ease into this. So this year, while still absent from CES, Apple decided to have some fun with the famous "What happens in Vegas, stays in Vegas" slogan, at the intended expense of their less privacy enforcing consumer electronics competitors, probably Amazon and Google, who as we know both last year suffered from some embarrassing privacy slips. So this huge, I mean, it is the entire side of the hotel, black and white, building-sized graphic facing the Las Vegas Convention Center, shows the distinctive outline of the iPhone with the slogan "What happens on your iPhone, stays on your iPhone." And then it has apple.com/privacy at the bottom.

However, as has been noted, Leo, by you and the industry, there's a tiny and somewhat ironic aspect to this which has been noted. The building-size graphic appears on the side of a Marriott Hotel, which as we know suffered its own embarrassing, years-long, or at least years-old, data breach which we learned of last year, as a consequence of them having purchased the Starwood Properties which had - what was it, 2014? I think Marriott bought it in 2016; but in 2014, two years before, they had suffered a breach. And I did see a little thing that didn't really make it into our bullet points for the podcast, but it was that the passport numbers, I want to say 518-some thousand passport numbers were leaked from that breach. So Marriott had reduced the size of the breach a little bit, but also said, yeah, we did, we have to confess, 518-some thousand passport numbers were divulged.

Okay. Now, the good news from our friends at BleepingComputer. We recently, it may have been the last podcast of 2018, ran through some of the many variations of

ransomware that had all been derived from a single poorly written starter which was on GitHub, and the fact that someone named Michael Gillespie was creating a series of decryptors for the ransomware descendants of that poorly written starter because, being poorly written, it was possible to decrypt the file contents without paying the ransom.

Since then, BleepingComputer, which as we know closely follows and reports on this ransomware universe, has been following and reporting on Michael's subsequent developments. On the second of January, Lawrence Abrams, the founder of BleepingComputer, posted: "How to Decrypt the FilesLocker Ransomware with FilesLockerDecrypter." Although Michael Gillespie did not produce a decryptor for this ransomware, well, not as a descendant, it turns out that on December 29th an unknown user released the master RSA decryption key for version 1 and 2 of FilesLocker, which allowed a decryptor to be produced, which has been done. Then, two days later, on the fourth of January, Larry again posted on BleepingComputer: "How to Decrypt the Aurora Ransomware with AuroraDecrypter," and provided a complete walkthrough of the use of Michael's decryptor for Aurora ransomware.

Anyway, so I was doing a bit more digging and catching up on everything that had happened since our last podcast, and I discovered an article that Lawrence had posted on Thursday the 20th, two days after our last podcast: "BleepingComputer.com is now a partner with No More Ransom." And Leo, you're going to want to click on NoMoreRansom.org. I've got the link on the next page in the show notes.

Larry wrote: "BleepingComputer is humbled and honored to announce that we have joined the No More Ransom project as an associate partner. We've been providing ransomware information, support, and the amazing decryptors from Michael Gillespie since the beginning, and this partnership will enable more victims to receive the help they need." And indeed it will. He says: "No More Ransom project is a joint project created by Europol, Politie, and McAfee to provide information and assistance to those affected by ransomware. Since its creation, numerous other law enforcement agencies, security companies, and supporters have joined the project, which now supports 35 different languages."

In fact, when you go to the home page, NoMoreRansom.org, you are asked to choose a language, which of 35. And so /en/ then takes you to - there is a decryption tools listing with a long list of tools that can be used for decrypting ransomware, if you are, and I guess I would say "lucky enough" to be encrypted with something that can be decrypted without paying the ransom. So I wanted to put this on everybody's radar, NoMoreRansom.org. If you or anyone you know or care about is hit by ransomware, there's a chance, I mean, first thing is you don't want that to happen. You want to be safe about it happening by somehow arranging to have really, really current backups.

And although I'm annoyed, for example, that I fried another processor this morning, I am not the least bit worried about any loss of data. My backups' backups have backups, and the images' images have images. And so I am, like, after having been caught by my XP machine dying last year, I'm not going to ever be in that position again. So I'm good. I even have drives that are not online, but briefly come online and then disappear so that, if anything did get me, it would have no way of knowing that there was a drive that technically was accessible that cannot otherwise be accessed.

So, I mean, I take this danger seriously. In my opinion, this is the biggest concern that exists now is the threat from software that encrypts, I mean, basically it's like potentially losing all, I mean, not just a drive crash. That we can recover from. We've got SpinRite. Or the motherboard dies. And that's fine. You still have your drives. But, you know, the idea of something trying to get into your system and to maliciously encrypt your data, no one wants that to happen. That's worse than a virus.

But remember, this only works on poorly implemented ransom crypto. If the crypto is done right - and the first ransomware, before this became a fad, the first ransomware, as we discussed at the time, was done right. A high-entropy symmetric key was obtained. It was used with AES-256 cipher with a varying initialization vector, which was stuck on the front of all of the encrypted files in order to do proper encryption of the byte stream that the file represents. And then that symmetric key was completely wiped and removed from the system. There was no trace of it left behind. You had to pay the ransom in order to get your data back.

So understand that this isn't universal decryption of ransomware. It's only if the ransomware that you happen to get bit by was not done properly, not done correctly, that you are able to back yourself out. But it's worth knowing, I mean, it's cool that we now have NoMoreRansom.org as an aggregation site for these tools. And props to BleepingComputer for joining up with them and helping them to do a better job by funneling Michael's work to them. Very cool.

Last August we covered the "mixed blessing" news that Microsoft was introducing something that I thought was really tasty. At the time they called it "InPrivate Desktop." And their description at the time read: "InPrivate Desktop (Preview) provides admins a way to launch a throwaway sandbox for secure one-time execution of untrusted software, basically an in-box speedy VM that is recycled when you close the app." And under prerequisites, and here's where I was disappointed, first bullet point under prerequisite, "Windows 10 Enterprise." And it ran on builds 17718 and beyond, any branch. It required hypervisor capabilities enabled in the BIOS, at least 4GB of RAM, 5GB of free space, and two CPU cores. So this was very cool, the idea of having an easy-to-use, readily accessible, throwaway VM for safely doing stuff. But of course it was also disappointing because who among us has Windows 10 Enterprise?

We're discussing this again because, shortly before Christmas, Santa Microsoft left news of a welcome present under our Windows 10 tree. I've got the link to the announcement in the show notes. Microsoft's Hari Pulapaka, I guess that's how I pronounce his name, he posted: "Windows Sandbox" - it's renamed. "Windows Sandbox is a new lightweight environment tailored for safely running applications in isolation." His posting says: "How many times have you downloaded an executable file, but were afraid to run it? Have you ever been in a situation which required a clean installation of Windows, but didn't want to set up a virtual machine?

"At Microsoft we encounter these situations regularly, so we developed Windows Sandbox - an isolated, temporary desktop environment where you can run untrusted software without the fear of lasting impact to your PC. Any software installed in Windows Sandbox stays only in the sandbox and cannot affect your host. Once Windows Sandbox is closed, all the software, with all its files and state, are permanently deleted."

And then five bullet points: "Windows Sandbox has the following properties: Part of Windows. Everything required for this feature ships with Windows 10" - and here it is - "Pro and Enterprise. No need to download a VHD. Pristine: Every time Windows Sandbox runs, it's as clean as a brand-new installation of Windows. Disposable: Nothing persists on the device. Everything is discarded after you close the application. Secure: Uses hardware-based virtualization for kernel isolation, which relies on the Microsoft's hypervisor to run a separate kernel which isolates Windows Sandbox from the host. And lastly, efficient: Uses integrated kernel scheduler, smart memory management, and virtual GPU."

And under prerequisites now, Windows 10 Pro or Enterprise Insider Build 18305 or later. Oh, actually they reduced the requirements, too. It does require a 64-bit architecture, virtualization capabilities enabled in the BIOS, at least 4GB of RAM (8 recommended), 1GB of free disk space - that's nice, that's down from five - and at least two cores. So

this is extremely good news, I would imagine, for all of us listening to this podcast, that Windows 10 Pro will soon have this feature. It's currently shipping in the Fast Ring of 18305, which is also known as 19H1. And it's hidden under that Programs and Features dialog.

So you go to Settings > Apps > Apps and Features, then Programs and Features, which gives you a dialog you could stretch out where there's a bunch of checkboxes, and look for - you want to Enable Windows Sandbox. Then you close it, it rummages around for a while, and then you'll have it. And very, very cool that we're going to have this built into Windows 10 Pro. So congrats to Microsoft for this not just being in Enterprise. I'll bet you that they took a look at this and thought, okay, this is definitely worth giving to everybody.

And as I mentioned before, there's a new page cache side-channel attack. From the looks of it, it doesn't look like a big deal. The page cache is something that, being a cache, that our OSes use in order to boost performance in a number of ways. I will dig into it, and I will have news either way, to either confirm that it's not a big deal or get a sense for what it means. The news just hit as I was putting the podcast together.

So I wanted to share a fun testimonial that I found from someone named Dunbar Pappy. He said: "Steve, we'd swapped emails a few years ago, but today I write with my profound thanks for your SpinRite creation."

Leo: Aww.

Steve: Yeah. Well, and get this. "Recently I'd been transferring all my patent work and other high-value documents and settings to an older Acer laptop with Ubuntu OS, which I use as a dedicated secure workstation. During this massive, multi-platform undertaking, an OS update came through; and, after restarting, the Linux system was completely locked up."

Leo: Oh, great.

Steve: Yeah. "Few files would even open, and no system operation would execute. It wouldn't even shut down. I envisioned hours of reconstructing files from other backups," he says, "(if even possible), a massive headache with profound monetary implications if unsuccessful. I decided to run my years-old copy of SpinRite 5 on it." And just so everybody knows, I mean, SpinRite 6 was released in '04, so...

Leo: Where did he get 5?

Steve: SpinRite 5, he's had it for more than 15 years. He says: "I decided to run my years-old copy of SpinRite 5 on it, just to reassure that the bits would be readable with my adapter transfer hardware during the laborious HDD swap-and-read attempts. Finished after 12 hours of plodding along, I decided to reboot the Acer just to see if anything would even function. Then lo and behold, it was all systems go, files recovered and system operations normal." He says: "The English language is inadequate to express my relief; and, further, in today's techno-centered disposable world, it is nearly impossible to find any product that actually does what it says it will, and at a fraction of the cost compared to the alternative. But SpinRite is one that delivers. My eternal thanks, Steve. Dunbar Pappy."

Leo: Yay. What a great story. Nice.

Steve: So the point is, you know, you write the software right, and it doesn't die, and it's still useful years later. And, yes, as soon as SQRL is behind me I will be back to updating SpinRite 6, since nobody doubts it's time for me to do that. But as we know, it's still helping a lot of people in the meantime.

What I wanted to mention about SQRL was that I have finished all of the work on a piece that I didn't expect to have to do. Having done it now, I'm glad. Which is, as I've mentioned before, I want to put up web-based forums for SQRL users who are wanting to understand it better, who want help with this or that SQRL client; for developers who want feedback on the work that they're doing. Basically, the equivalent of what we now do almost offline in our old-school, Usenet-style NNTP newsgroup. I wanted to create a website. The problem is that this thing is, well, it doesn't obviously natively support SQRL. And how could I have the SQRL web forums not allow you to use SQRL to log in?

So I mentioned this on the podcast. I had also posted a couple questions quite a while ago to the developers of this - I chose the XenForo forum software. I like it a lot. I don't regret the choice. This is like the third iteration of forum software they've written, and it shows. But it's written in PHP. And so what I was looking for was a couple questions because I assumed I would have to integrate SQRL into their forum software. I found a reply from an existing developer in Denmark who is a Security Now! Podcast listener. He's been listening, well, he's been coding since he was 15. He's now 29. And he's been listening for years.

He said: "Hey, I know XenForo. Do you need any help?" Well, it would be crazy to implement SQRL from scratch in PHP. Actually, it would be wonderful if someone eventually does it. But that didn't seem to be the shortest path. So what I decided to do was to create something that didn't exist yet, which was to create and define an API for an external SQRL authentication service that would allow any integration into a web server with virtually no knowledge of SQRL. That is, to basically move all of the work over to the SQRL API so that it would then be easy to make a couple calls to have all of the SQRL crypto done by this API.

So if anyone's curious - and Leo, you could bring it up right now if you were interested - there's a link in the show notes: GRC.com/sqrl/sspapi.htm. That's the SQRL Service Provider API. And so that page documents the API which now exists. And in fact we have a demo site, actually two demo sites, which are using the API, which I use in order to bring it up and verify it. And the reason this is a little bit interesting is that this developer is not a Windows user. He runs on Mac and has some Linux stuff around. But of course the API, my implementation of this API, it's my hope, for example, that the API will be implemented in Java and in other things because this creates a uniform interface to any web server that wants to avail itself of SQRL authentication, really minimizing the work that has to be done on the server side.

But the developer needed to use the API that I've written. Of course, I wrote it in assembly language for Windows. So it turns out that we could have used an unlicensed version of Windows, but Windows 10 allows you to install it without a license key. It asks you to eventually license it, but it runs forever, apparently. It disables some of the configuration stuff, you know, like the desktop background. And if you go to the control panel and try to do something, it says it's all disabled, and says you should license this copy of Windows. And it works just fine. And if you've been around Windows for a while, you know that you can pretty much do anything you want to with the registry and group policy. So needless to say, I have it running just the way I want. All of that incredible

videogame junk that's in Windows 10 when you install it now - Leo, have you seen a fresh install of Windows 10 recently?

Leo: I have a few here and there, yeah.

Steve: It's unbelievable. It's like, how do people tolerate this? I just cannot believe it. Anyway, mine is all stripped down. There's nothing in it except a Windows core. There's also something called IIS Express, which is a really cool IIS server which just runs as a desktop app. So I configured everything, put the API in it, bundled it up into a VM because he has VMware. I think he's using Fusion, and it works just fine there. So there was all that.

Then the problem was how to get it to him. I thought, okay. First of all, it was slow. I thought I'd stick it on my server, and then he could grab it. But it turned out that that was pretty slow. Then I thought, okay, I'll stick it up on Amazon. Well, it was 5.8GB for the super-minimized, compressed, optimized, dejunkified, like it was really stripped, 5.8GB. Amazon has a limit of 5GB for files on AWS. So I looked around. All of this by way of saying I found a very cool service, Leo. You probably know of it, but I wanted to make sure our listeners did. It's called Filemail.com. The guys are in Oslo, Norway. It is free forever for files up to 50GB. Fifty, 50GB.

And I'm always suspicious of something free. Why is it free? Well, they offer for commercial entities or people who want to keep files there longer or bigger than 50GB, I can't imagine who, but for $15 a month you get a bunch of additional features, like you can password protect the file. Of course I RARed this in order to - with a large dictionary and used a RAR password, since the file was going to be leaving my control, so that it would be protected.

But anyway, I wanted to make sure people knew. I was so impressed. I don't remember now the time of day it was. But I went to Filemail.com. I chose, rather than sending email, I wanted a link. I dragged and dropped this 5.8GB file on the browser, and it saturated my upstream cable modem at 33Gbps straight. I mean, it could not, I mean, I have a 30GB upstream bandwidth on my cable modem. It saturated it at 33. I was very impressed. And he got the same saturation performance at the other end when he downloaded it.

For free you're able to allow - you can select how long you want the files to stay there - a day, a week. I don't remember now, but I remember that it was either one day or one week. Maybe there were other choices. If you check that you want to password protect, it tells you that you need to be a licensed user, you know, you need to register and do the pay as you go. But, boy, I see no downside to using this for sharing large files, if you just want to send somebody a link with no privacy - the reason I didn't want to have their service do this by email is I didn't want to divulge even his email address. So I don't see any downside to this. This looks like a great service. So I wanted to make sure our listeners knew of that. And there's our podcast.

Leo: C'est fini. Thank you, Steve. A great beginning to 2019.

Steve: Yes. I will be beginning to - I'm not far away from being able to tell people where to go to get a copy of SQRL and play with it, I mean, to make it public and start having people get to know what it is I've been doing for the last five years on this crazy project.

Leo: Five years. Wow.

Steve: Yes, it is. And then get back to, yes, get back to SpinRite, everybody. I absolutely can't wait.

Leo: Steve's show, Security Now!, comes to you every Tuesday. We do it about 1:30 Pacific, 4:30 Eastern, 21:30 UTC. You can listen or watch as you choose, live at TWiT.tv/live. If you do that, join us in the chatroom, irc.twit.tv. You can also get on-demand audio from Steve's site, GRC.com. That's where you'll find, not only SpinRite, the world's finest hard drive recovery and maintenance utility...

Steve: Going strong after 35 years.

Leo: Yeah. Also everything you ever wanted to know about SQRL, Perfect Paper Passwords, Password Haystacks, ShieldsUP!, and on and on. Somebody called me the other day about, believe it or not, the Click of Death. They called the radio show about the Click of Death.

Steve: Wow. And you knew all about it.

Leo: I did, and I referred them to your Trouble in Paradise application.

Steve: Yup.

Leo: See, there are still people with ZIP drives out there. I don't know why.

Steve: I'm sorry.

Leo: GRC.com. He also has transcripts, which is always a good way to listen to the show is you can read along. We have audio and video at our site, TWiT.tv/sn for Security Now!. Or subscribe in your favorite podcast application. That way you'll get it the minute it's available. We're going to send this off to the editors now. It should be out in just an hour or two. So if you subscribe, you'll have it hot and fresh off the presses, ready for your commute tomorrow. Steve, have a great Tuesday, and I will see you next week on Security Now!.

Steve: Thank you, my friend. Till then.