Halfway Through 2021

Description: This week we look at the story behind an important Edge update and revisit Google's now-delayed FloC liftoff. We consider the cost of Ireland's recovery from the Conti ransomware attack and ask who's responsible for the damage and data loss following the remote wiping of many Western Digital My Book NAS devices. We take a moment to observe the passing of an industry legend. Then we look at the mess surrounding questions of where Windows 11 will run. I share my favorite web browser keyboard shortcut, and also my favorite website cloning tool, which I just had the occasion to use. We have a worthwhile-looking cybersecurity Humble Bundle. Then we'll wrap up by responding to two pieces of closing-the-loop feedback from our terrific listeners, and that will bring us to the end of the first half of an event-filled 2021.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-825.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-825-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here with a little rant. Why is it so hard to figure out what machines Windows 11 will run on? It's just Windows 10; right? We'll also talk about the My Book Live hack. The true story is getting kind of interesting. And then why did it cost Ireland $600 million to fix that ransomware attack? It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 825, recorded Tuesday, June 29th, 2021: Halfway Through 2021.

It's time for the dweebcast. That's a good name. You've just renamed the show. I'm talking Security Now! with this guy right here, the king of the dweebs - that's a mean thing to say - Steve Gibson.

Steve Gibson: That's better than the myth. I think I like that better than the myth.

Leo: The man, the myth, the legend.

Steve: Yeah.

Leo: Oh, I never thought about that. There is no myth. It's all reality; right.

Steve: We are going to be talking about a legend of the computer industry who we lost last week. That was after the podcast finished. So anyway, we've got a lot to talk about for Episode 825. Actually we're closing in on the end of Year 16, Leo, so...

Leo: Hush your mouth. I don't want to get to 999 anytime soon.

Steve: No, that's going to be a dilemma. Anyway, we are, with the finish of this podcast, halfway through 2021, thus the name of today's podcast. We're going to look at the interesting story behind a very important Edge update and how some rent got paid. We're going to revisit Google's now-delayed, well, FLoC flop. We're going to consider the cost of Ireland's recovery from the Conti ransomware attack, which I think is very suspicious. It's, like, got to be the most expensive expectation we've seen. Also ask who's responsible for the damage and data loss following the remote wiping of so many Western Digital My Book NAS devices. We're going to take a moment to observe the passing of an industry legend. You know who that is.

And then we look at the mess surrounding questions of where Windows 11 will run. And I even heard Andy touching on that during MacBreak Weekly. I'm going to share, just because it occurred to me I was using it so much yesterday, my favorite web browser keyboard shortcut; and also, and I also used this yesterday earlier, my favorite website cloning tool. Maybe that was on Sunday. Anyway, I just had the occasion to use it again. I thought, I've got to make sure everybody knows about this because it really, it just works. And it turns out that's not an easy thing to find. We also have a worthwhile-looking cybersecurity Humble Bundle.

And then I want to wrap up by responding to two pieces of closing-the-loop feedback from our terrific listeners, which as I said will bring us to the end of the first half of an event-filled 2021. And of course we do have a great Picture of the Week, apropos of one of our topics.

Leo: I haven't glanced at it yet, just in case it's something surprising.

Steve: I think we're going to have fun. Don't be drinking any coffee while you look at it. You may spit it out.

Leo: Might spit it out? Uh-oh.

Steve: That's right.

Leo: You made me spit my milk through my nose again. That's why we should rename you, and this was a suggestion from the chat room, thanks to Logan5, "the man, the mirth, and the legend." How about that?

Steve: Oh, now, that I can go with.

Leo: Yes, yes.

Steve: I gave our Picture of the Week the caption, "Why place an arbitrary lower bound on Windows 11's minimal requirements?" And the picture is our beloved Windows 95 desktop. And this is a completely spoofed picture because the PC Health Check will not run. It won't even run on my Windows 7 machine, which I'm talking to you from right now. But anyway, this was just somebody took the time to mock this up, which I got a kick out of, apparently running the PC Health at a Glance showing a 32MB, not GB, of RAM, a 1GB hard drive, also showing 25 years old. And then apparently someone checked whether or not this machine would be able to run Windows 11. That is the Windows 95 machine. And lo and behold, no. It says "This processor isn't supported" - it's probably an 8386 - "for Windows 11." So oh, darn. Anyway, we'll be coming back to that as a consequence of much activity in the last week on the topic.

Leo: Oh, it's been crazy, yeah.

Steve: Oh my lord, yes. Okay. So here's a true interesting story. On June 3rd, so the beginning of the month, what's that, like a little over four weeks ago, a little over three weeks ago, a team of non-Russian-speaking hackers who call themselves "Cyber Xplore" were searching for vulnerabilities on the Russian site Mail.ru. And probably not hard to find. Mail.ru is, wisely, one of HackerOne's many Bug Bounty program clients, and these enterprising hackers were hoping to pay the rent. Their tool of choice for web application security testing is something known as Burp Suite, which they run on their browser of choice, which is Firefox.

The trouble was the web subdomain of Mail.ru that they were needing to poke at, and it was shown as redacted in the stories where I was trying to pull this information together, the mail subdomain was all in Russian, which none of them spoke. They knew that Chrome would do translation for them, but they didn't want to use Chrome. So they went looking for Firefox extensions to perform the Russian language translation. But they soon discovered, when looking for a translation extension, that a great many of them had been removed due to critical security vulnerabilities. And in thinking about this further, they realized that any page translator would need to have direct and deep access to the web page's DOM, you know, the document object model. In other words, due to the fact that all these had been removed because of security problems, they realized that it's very difficult to make a translator fully secure; and, conversely, very easy not to.

So one of the members of the team had previously found multiple vulnerabilities in other Microsoft products, so they had some experience in dealing with Microsoft. And what captured their attention was that Microsoft's Edge browser now had built-in translation. That was something that had been added a while ago. And since Edge also has a bounty program, they figured they might be able to get their rent paid. So they decided to switch to Edge.

Leo: This is such a funny story.

Steve: It's great.

Leo: This guy, it's got to be like a 12-year-old script kiddie; right? I mean...

Steve: Yeah, yeah. It's like, let's see if we can make some money.

Leo: Okay. Let's see now.

Steve: So they switch to Edge. They go back to the Russian site, and they use Edge's built-in translator.

Leo: Yes.

Steve: They were immediately swamped with cross-site scripting error pop-ups. They didn't quite believe it, so they did the same thing with Chrome, using its built-in Russian translator. No pop-ups. So Chrome's translation system appeared to be secure, whereas Edge's was looking like a total meltdown.

So they began digging into Edge, and they quickly discovered that Edge's translator was failing to properly sanitize HTML image tags. This allowed them to provide their own malicious JavaScript, which would run in the context of the origin domain. In other words, you could take over any site that you visited, like with Edge and a little bit of tweaking. So as web browser security bugs go, it doesn't get much worse. In fact, it's so bad that they realized that they had found a class of cross-site scripting problems known as UXSS for Universal Cross-Site - too bad it's not "G" for Gourmet. Anyway, it's Universal Cross-Site Scripting.

They then verified that anyone accepting a friend request on Facebook could be compromised; that web-based applications, for example Instagram, published on the Windows Store would also be vulnerable because the Windows Store operates under the same Microsoft Edge Translator that was responsible for triggering this universal cross-site scripting attack. And as regards to paying the rent, their story had a happy ending. Edge is now significantly more secure. And Microsoft replied: "Thank you for taking the time to share your report. Based on the assessment of our engineering team, we have determined that your case #65633 is eligible for a U.S. $20,000 bounty award under the Edge on Chromium Bounty Program. Congratulations." So they published...

Leo: Nice. Very nice.

Steve: Isn't that great? They published their timeline on the 3rd of June.

Leo: See, it's good not to know Russian.

Steve: Yes, it comes in handy.

Leo: Comes in handy.

Steve: On the 3rd of June they sent the report to Microsoft. On the 7th, four days later, a reply from Microsoft saying that they were reviewing their June 3rd report. The next day, additional impact information was sent. On the 15th, report was triaged. The 17th was the notification that they had been awarded a $20,000 bounty. Two days later, on the 19th, a pre-release patch was issued. And then on the 24th, last Thursday, a patch update was pushed. A CVE was assigned. So that's not too bad. Microsoft was first

notified on the third, and the bug was patched and pushed out exactly three weeks later, as I said, last Thursday on the 24th.

So that's not the three days which appears typical, or at least possible, for the Chromium team. But it sure beats the catastrophic three months during which Microsoft apparently twiddled its thumbs before publishing a patch for the Exchange Server ProxyLogon flaw which, you know, gave us all of our excitement toward the beginning of this year. So a happy ending. These guys got their rent paid. It paid off to poke around. And I'll just remind our listeners that some of these problems are not hard to find. You just have to kind of try stuff and, you know, use something that does web application security checking. There are a bunch of free tools and open source tools available for that. And just do things. And when stuff happens, then pursue it, and maybe you'll be able to pay your rent, too.

Leo: Really, that is really - a lot of exploit discovery is just trying things; right?

Steve: Yes, yes. The automated version of that we call fuzzing; right?

Leo: Right.

Steve: And the human - but you can also fuzz as a human. You can just do things that the fuzzers won't do because they haven't been aimed at it. And it's things like this. It's like trying combinations that haven't been tried before. It's sad, but that's pretty much all it takes to find something that crashes or something that pops up and, wait a minute, this looks like a cross-site scripting vulnerability. Look, explore this further. Because it's unfortunate that the security industry, or the security of the industry is currently at this state where, yeah, just do something. And you might discover a vulnerability and make tens of thousands of dollars.

Leo: Yeah. That's hysterical.

Steve: Okay. So we're not yet FLoCed. Of course, I had to title this that.

Leo: Mm-hmm.

Steve: The future of user profiling remains uncertain. Now, as our listeners will recall, back near the start of COVID, the very clever Bluetooth-based, privacy-enforcing, exposure notification device proximity tracking technology, which was jointly designed and developed by Apple and Google, was met with skepticism. No one understood it. So in the immortal words of the Monty Python troupe, "Run away." And Amazon's recent rollout of their beautifully designed, triple-encrypted, multilayered tunneling, low-bandwidth Sidewalk technology was greeted with hysteria by the popular press, claiming that it allows your neighbors to use your WiFi. Gasp. A well-meaning non-technical friend of mine phoned, warning me to disable Sidewalk immediately. And of course those of us who share this podcast know that's not at all what it is.

Meanwhile - reality check - hundreds of millions of people are blithely plugging all manner of inexpensive IoT devices into their home networks, joining them to their internal LAN WiFi, whereupon those devices immediately connect back to servers in

politically hostile foreign lands over which there is absolutely zero oversight or security. But trust in Apple, Amazon, and Google, who are all carefully designing super-secure solutions, oh, no. Run away.

In a similar vein, I was, and I continue to be, enamored of Google's FLoC technology. Yes, warts and all. If we must have user browser history profiling, it seems to me that being tagged with an amorphous and periodically changing interest-based cohort identifier beats the hell out of having everyone carrying unique third-party cookies around which uniquely and statically identify them individually, rather than as merely a faceless member of an amorphous cohort.

I would far prefer that legislators simply outlawed all forms of online profiling. We know that the EFF will be satisfied with nothing less. But that doesn't appear to be close to happening. And just like the $5 IoT devices which connect to cloud servers located in hostile countries, many people are missing the forest for the trees because let's not forget that these days most of us are already being identified by a highly static 32-bit identifier known as an IP address. Some identity blurring occurs thanks to multiple machines located behind NAT routers having a single public IP address. But if IPv6 ever succeeds in giving each and every endpoint its own IP, which is its goal, that blurring will also disappear.

So I wanted to briefly revisit FLoC today because, as with those other well-conceived and explicitly well-designed solutions, Google's FLoC has landed with a hard thud. Not one other browser has agreed to adopt FLoC, including those that are based on Chromium's own open-source codebase - Brave, Edge, Opera, and Vivaldi. And Firefox, not based on Chromium, is also a definite no, thank you. A recent analysis by Digiday discovered that Amazon - Amazon - is already preemptively blocking Google's cookie-free solution across its various web properties, including Whole Foods, Zappos, Shopbop, and Goodreads.

So as a result of all of the FLoC pushback, the reason we're talking about it today, is that Google recently updated their rollout timeline, which is putting it politely, announcing that they would be delaying FLoC's wider rollout from its originally planned usage starting early next year to now late year after next, meaning somewhere toward the end of 2023. And I don't know how they arrived at that.

Leo: Sounds like the 12th of never, I think, yeah.

Steve: Yes. I think that's the case. And perhaps not coincidentally, Google has been hit with some new regulatory setbacks in the EU, after the European Commission opened a wide-ranging investigation into Google's digital advertising business to examine its "plans to prohibit the placement of third-party 'cookies' on Chrome and replace them with the 'Privacy Sandbox' set of tools," meaning FLoC, and assess its "effects on online display advertising and online display advertising intermediation markets." So it sure sounds to me as though there's some moneyed political lobbying going on behind the scenes there. And in a similar move earlier this month the UK's Competition and Markets Authority, their CMA, announced that it's taking up a "role in the design and development of Google's Privacy Sandbox proposals to ensure they do not distort competition." So again, there are clearly some powerful forces behind this legislative saber-rattling.

Of everything that is happening, the third-party cookie stovepiping that was introduced in Firefox 86's "Strict" privacy mode is the best solution until something better comes along. By breaking the browser's traditional single shared cookie store into individual "stovepiped" per domain cookie stores, third-party cookies will continue to be honored in Firefox in exactly the way they were originally designed to be. But when a user who received a third-party cookie in one domain then visits a different domain, that third-

party cookie from the same third party will not be returned. Rather it will be given a different cookie for that stovepiped first-party domain. So this may be the solution.

And of course the problem is that we have fingerprinting and other sorts of persistent storage that those that want to track us are using. And of course the fact that, even with Firefox's solution, the fact that all of those various queries will still be coming from the same IP means that all of that fancy dancing we're doing in the browser, whether with cookies or fingerprinting or FLoCs, amounts to very little. While we run around in circles, the tracking companies are probably chuckling because they're thinking, hey, you know, we got the guy's IP, and that's not changing very often. So we know what they're doing, even when they try to bob and weave.

Okay. This headline brought me up short. And I thought, what? The headline was "Irish Ransomware Attack Recovery Cost Estimate: $600 Million."

Leo: What?

Steve: I know.

Leo: That's crazy.

Steve: $600 million. It's like, how expensive were those servers, and did they melt? It's like, what? So back in the middle of last month, Leo, you'll remember it was about six weeks ago, we covered the news that Ireland's national health system, known as the HSE, that stood for the Health Service Executive, was hit by the Conti ransomware gang.

Leo: I remember, yeah.

Steve: Yup. And this forced them to take their entire national healthcare IT infrastructure offline. Also recall, not only was the Conti gang demanding - it was an odd amount. It was $1,000 shy of $20 million in ransom. And, what, is that like there's some limit that gets triggered, or some transaction limit? Who knows why?

Leo: You get a little discount. You get, yeah, a little bit off.

Steve: That's right. So it was $1,000 shy of 20 million that they wanted, figuring that they'd hooked a big fish. And then, remember, Ireland's Prime Minister himself declared that no ransom would paid. And not only that, in something that was a little curious, the High Court of Ireland then issued an injunction against the Conti ransomware gang, whom they couldn't find, demanding that the 700GB of stolen HSE data be returned and neither sold nor published. And, further, that once having done that, the members of the gang identify themselves by revealing their full and true names, their email addresses, and their physical addresses, then come to Ireland to turn themselves in to Irish law enforcement immediately.

Leo: You must turn yourself in immediately.

Steve: This is the High Court of Ireland. We shall not be denied. Right. Well, today we have an update on the situation in Ireland. First off, it will surprise no one to learn that the Conti gang members, doubtless based in Russia, were somehow able to resist the urge, the compulsion, to comply with the Irish High Court order; and that all gang members, as far as we know, remain unidentified and are still at large. What has surprised many, however, is that Paul Reid, the HSE's director general, has estimated the recovery costs to total $600 million. 600 million.

Leo: Wow. Maybe they should have paid; you know? Geez.

Steve: Well, actually this is not even for the key. It was given to them.

Leo: Oh.

Steve: Yes. So upon closer examination, the great majority of that appears to be more than just recovery. During the hearing, which was last week, Reid noted that the immediate cost of recovery would total 120 million. Which, okay, is still far more than...

Leo: Still a lot, yeah.

Steve: ...the 20 million requested in ransom. Reid stated that further investments in replacing and upgrading the affected systems and other expenses, he said, which is a real question mark in my mind, would bring the total cost to an estimated $600 million. Now, I'd sure love to see an itemization of that. He predicted it would take months for HSE to fully recover from the attack. Among the many expenses was the cost of hiring technical experts. Okay. Maybe I'm for hire. I hadn't considered this before.

Leo: Yeah, you know, there's good money in there.

Steve: If he's got $600 million he needs to find a place for, you know, I might be able - no. Not until after SpinRite 6.1. Don't worry.

Leo: Okay, thank you.

Steve: But, you know, yeah. Apparently they're in no hurry to get this thing fixed. So anyway, Reid said: "We have also engaged international expertise." Okay. They didn't phone me. "There are costs we will incur in the future, and we need to put in place a security operation center" - apparently it's going to have lots of big screens, Leo, very impressive - "to monitor our network on a more comprehensive basis." Yeah. Maybe that would be a good idea. So it does sound more as if he's softening them up for his forthcoming budget.

He also reported that, so far, HSE has decrypted 75% of the affected servers. Despite threats from the Conti group to leak the hacked stolen data, HSE stuck to the Prime Minister's refusal to pay and instead forwarding all the information they had about the attack to Ireland's National Cyber Security Center. And then, a week after the attack, the Conti gang provided a decryptor, which Irish officials began testing.

So, much as has happened in other major attacks where the gang suddenly realized, oh, crap, we stepped in a big one here, let's just try not to have Putin's goons come after us. We're going to try to be a little socially responsible after the fact. What's interesting is that a week after the attack, they provided them with a decryptor. The decryptor's been used to decrypt three out of four of the affected servers. Yet they're saying that, oh, this really hurt, and we're going to need $0.6 billion, right, $0.6 billion to recover from this. So I guess they're going to get some really pretty shiny new servers, Leo, and maybe a big network operations center with those screens where you've got little blinky lights all over the map showing connections and things. It's got to be like what they have on TV for that much money.

Leo: That's crazy.

Steve: Yeah, it's nuts.

Leo: Crazy. Maybe they're just throwing everything out and starting over.

Steve: It may be that their stuff is really old, and they're able to make a case for, like, look, we can't fix it. We've got to replace it.

Leo: Yeah.

Steve: Maybe, Leo, they had a bunch of Western Digital My Book NAS devices.

Leo: Oh, lord. Oh, lord. Geez.

Steve: So I titled this next one "Dude, where's my data?" Last Friday, Western Digital posted the following. They said: "Western Digital has determined that some" - I love that. Turns out maybe 55,000, but we'll get there in a second - "that some My Book Live and My Book Live Duo devices are being compromised through exploitation of a remote command execution vulnerability. In some cases, the attackers have triggered a factory reset that appears to erase all data on the device. We are reviewing log files which we have received from affected customers to further characterize the attack and the mechanism of access. The log files we've reviewed show that the attackers directly connected to the affected My Book Live devices from a variety of IP addresses in different countries. This indicates that the affected devices were directly accessible from the Internet" - which of course they were designed to be - "either through direct connection or through port forwarding that was enabled either manually or automatically via UPnP." Which, again, they were designed to do.

"Additionally, the log files show that on some devices the attackers installed a trojan with a file named .nttpd,1-ppc-be-t1-z, which is a Linux ELF binary compiled for the PowerPC architecture which is used by the My Book Live and Live Duo. A sample of this trojan has been captured for further analysis and has been uploaded to VirusTotal." And it lights up like a Christmas tree. They said: "Our investigation of this incident has not uncovered any evidence that Western Digital cloud services, firmware update servers, or customer credentials were compromised." Well, okay, no evidence, but we'll see that it's completely possible. They said: "As the My Book Live devices can be directly exposed to

the Internet through port forwarding, the attackers may be able to discover vulnerable devices through port scanning." Uh-huh, yeah. That did happen.

Then they finish: "We understand that our customers' data is very important." Okay. We sold them something to store it, after all. They said: "We do not yet understand why the attacker triggered the factory reset." Okay, well, there's lots of speculation on the Internet. "However, we have obtained a sample of an affected device and are investigating further. Additionally, some customers have reported that data recovery tools may be able to recover data from affected devices, and we are currently investigating the effectiveness of these tools." Huh. "The My Book Live series was introduced to the market in 2010, and these devices received their final firmware update in 2015."

Okay. End of posting, so they had a five-year maintenance life after they were introduced to the market in 2010. So what we have here is an unfortunate situation. We have an instance of long-abandoned IoT NAS devices continuing to be used for six years past their end of support life. You can't really blame Western Digital for retiring support after five years. It's their right to do so. Much as we've said it's Microsoft's right to decide, okay, we're not going to keep supporting Windows 7. Sorry about that. Well, maybe if you pay us we will; but most of you, no. Nor, with two important exceptions, can you really blame the users of those apparently perfectly well-functioning NAS devices for continuing to use them. They appeared to be working well the day after their support ended, and even a year after their support ended.

And this reminds me of an experience I had as a youngster, definitely at the end of my teen years. I was responsible for paying for my car insurance, and I received a notice that my insurance had lapsed. I was horrified. But I was also hungry, and I wanted to go...

Leo: This sounds familiar.

Steve: I wanted to go - yeah, doesn't it? And I wanted to go get some food.

Leo: Yeah.

Steve: So, Leo...

Leo: What did you do?

Steve: I got in my car; and, to my amazement, it still ran. Even without insurance.

Leo: No insurance, and it works.

Steve: I guess it didn't know. And neither did those Western Digital My Book Live NAS devices know that their support had ended. They just kept on running.

Leo: Yeah. Ended six years ago or something. I mean, a long time ago, yeah.

Steve: Yeah, exactly. It was six years ago. Now, the plot thickens a bit when three years after that end of support, in 2018, a serious remote command execution vulnerability was found and made public. The flaw was assigned a CVE of 2018-18472, which NIST, you know, the N-I-S-T, described as: "Western Digital WD My Book Live and WD My Book Live Duo (all versions) have a root Remote Command Execution bug via shell metacharacters in the /api/1.0/rest/language_configuration language parameter. It can be triggered by anyone who knows the IP address of the affected device." Okay, in 2018. Lay it out. There it is.

The problem was first identified by WizCase in a 2018 report titled: "Vulnerabilities found on Western Digital My Book, Netgear Stora, Seagate Home, and Medion Lifecloud NAS." WizCase's report begins: "NAS devices have become the storage device of choice for many small and medium businesses. They're inexpensive, easy to operate, and you can add additional storage if you're running low on space. But is it secure enough to protect your company's data? That was the question on our mind when we brought in two security researchers..."

Leo: Is there an alarm going off?

Steve: Oh, what do you know, spam.

Leo: You have a spam alarm? If I had a spam alarm, it would never stop going off.

Steve: So they brought in two security researchers, they said, "to see whether they could exploit any vulnerabilities in the leading NAS devices." And remember there were those four. "We focused on discovering only critical vulnerabilities that can be exploited remotely without any user interaction. Meaning authentication bypasses weren't enough. We wanted to execute commands on the devices remotely, with the highest privileges. We were successful in every device." So at the time of this, Leo, all four of those NASes were remotely exploitable with root remote privileges.

They said: "All four NAS devices tested suffer from a zero-day, unauthenticated root remote command execution vulnerability. The vulnerabilities allow hackers, governments, or anyone with malicious intention to read files, add/remove users, add/modify existing data, or execute commands with highest privileges on all of the devices." They finished: "It's our belief that there are many other NAS devices that suffer from similar vulnerabilities. Both the vulnerabilities" - and they were dubbed 2018-18472 and 18471 - "remain unpatched at the time of this publication." Okay. And this was three years, in the case of the WD, three years after the device went out of support. They said: "There are nearly two million affected devices online." That was then, 2018.

So we don't know how many of those nearly two million online NAS devices were WD My Books at that time. That was 2018, and now we're three years later. What we do know is that finding such devices has never been easier. The public Internet can be scanned, and it has been. A very recent count revealed 55,348 Western Digital My Book Live devices located, identified, known to be connected, and publicly accessible across the Internet.

So following last week's destruction derby, we need to collectively ask ourselves where the blame falls. Those forensically reviewing the logs have suggested that the owners of the WD NAS devices may have been caught in the crossfire between two warring groups. Given the detection of a Linux trojan on the device, it was a PowerPC-based Linux trojan, it seems that most of those WD NAS devices that were still in use had been found and commandeered into the service of a botnet years ago.

Leo: So they had actually, probably since 2018 when that exploit was published...

Steve: Yes.

Leo: ...been co-opted, but sitting passively.

Steve: Exactly. The users had no idea. It behooved those running the botnet to have those things stay on the 'Net so that they could be used for DDoS attacks and scanning for other things on the 'Net and so forth. So it's believed that their subsequent destruction via a factory reset wiping may have been the consequence of a rival group wishing to shut down a rival botnet.

Leo: I love this. This is hysterical.

Steve: So all of this lost data occurred as a side effect, as I said, caught in the crossfire between two warring groups. So I did say before, with two important exceptions, can you really blame the users of those apparently perfectly well-functioning NAS devices for continuing to use them?

Leo: No.

Steve: Those two important exceptions are, first, is it safe to continue to use anything that's connected to the Internet after its ongoing maintenance support has ended? Okay, that's a good question. At the same time, is it really practical to expect users of an expensive piece of equipment that's apparently working perfectly well to stop using it just because support, which it apparently doesn't need, is no longer available?

Leo: By the way, I think Amazon's still selling them. I mean, believe it or not.

Steve: Oh, wow.

Leo: Yeah. I know. I can buy one for 373 bucks. Oh, if you want it delivered by Friday, 399. So these are just some old computer stores who had some stock, and they're still selling them, which is depressing as hell.

Steve: It is. Secondly, we know in this day and age that anyone who is not maintaining multiple, and this is what I heard you mention when you were talking about this on a previous podcast, anyone who's not maintaining multiple backups of their important data is inherently placing that data at risk. After last week's disaster, many people were posting that they were totally hosed by the loss of 2TB of irreplaceable data.

You know, many years ago I designed an advertisement which to my surprise won some acclaim at PC Magazine for being the most responded-to advertisement in the magazine's history to that point. That ad began with the simple headlines: "Hard Disks Die." Then it posed the question: "Ever Wonder Why?" The point being that all mass storage systems

are in a perpetual battle against the forces of entropy. And in the end, entropy will win. It always does. As we know, nature abhors a sharp edge.

So it would be nice to think that Western Digital might have sent their registered owners of those drives a notice in 2018 warning them to take those drives offline because a critical remote compromise problem had been identified and would not be repaired since the drives were now three years out of service, out of warranty, out of maintenance. I would be surprised if that had happened, but Western Digital had moved on by then, three years earlier, to newer devices. So I guess I'd conclude that the responsibility falls on the users of those systems. They were obtaining many years of continued service life from an out-of-maintenance device. And in the cases where they were screaming about losing valuable information, it was probably going to happen sooner or later anyway. So, oops. You know? Maybe lesson learned? But Leo, your point about these things still being available for sale...

Leo: That's really shocking, isn't it. I can't believe somebody's selling them.

Steve: It's horrifying.

Leo: Yeah.

Steve: It's horrifying.

Leo: Yeah. And Western Digital abandoned these, I mean, really abandoned them, hard abandoned, because they knew there was a critical exploit in 2018 and did nothing.

Steve: Yeah.

Leo: But I think, you know, I mean, yeah, you should make sure everything you have is being updated, preferably automatically over the air, and not use stuff that is out of date. But that's easy to say. The people who are buying these are buying them at big box stores, and it's a big hard drive, and they're using it for backup.

Steve: And it's got a brand name. I mean, Western Digital is a great name. So they're probably thinking, hey, Western Digital, that's great. Wow.

Leo: That's too bad.

Steve: How big? A couple of terabytes?

Leo: The one I can buy right now for that $383 is 3TB. So 3TB. And yeah, just because it's labeled backup, people go, see, it's backed up, and then erase the original.

Before you go into this next story about John McAfee, I do want to tell people what you're about to hear might be triggering if you're considering suicide. There is a National Suicide Prevention Lifeline in the United States. You can call right now for free and get free confidential support, if you're in distress. Great crisis resources for you or your loved ones. It's 1-800-273-TALK. 1-800-273-8255. And we just want to be responsible since we're going to talk about John McAfee next.

Steve: That's good. And we know that COVID has been an extra stressor for people.

Leo: Especially teenagers. I know of two teenagers who took the very poor choice, I think because of loneliness during COVID. So, yeah, we're all going through it, but you don't have to go through it alone. And if you're not in the United States, you can google "suicide prevention lifeline," and you'll be able to find one in your area.

Steve: Good.

Leo: We don't want to lose you. We want you to be around. Anyway.

Steve: Yeah, I was unhappy when I was younger. And, you know...

Leo: It's normal. And that's the problem with suicide. It's a permanent solution to a temporary problem. You know? Things do get better, I know. But sometimes we just can't take it. And don't do it. Don't do it.

Steve: So I wanted to note that last Wednesday John McAfee was found dead by hanging at the age of 75 in his jail cell in Barcelona, Spain. His extradition to the United States, where he would have been facing a number of legal charges of willful tax evasion, had finally been approved by a court in Spain. And despite his earlier statements that he would never take his own life, and he said that foul play would definitely be involved if he ever appeared to have done so, everyone assumes that he changed his mind, and that that must have been what happened. His attorney said that his nine months in prison had brought him to despair, and attempts to revive him had failed.

And as we all know, John was a character and a half, with a life full of antics. I think that the first time we talked about him on this podcast was when he was being sought in connection - of course he was famous, right, because of McAfee and McAfee Systems and McAfee AV. I didn't realize he had some connection to ZoneAlarm, which was a little horrifying for me.

Leo: He, yeah, well, but back in the day I think he was quite a bit more respectable. You know, he made 100 million selling McAfee to Intel.

Steve: Yeah.

Leo: So he did quite well. But he, as far as we know, he squandered almost all of it in kind of oddball things.

Steve: Well, and things went weird, too.

Leo: Yeah.

Steve: I think the first time we talked about him was when he was being sought in connection with the murder of his neighbor, a guy by the name of Gregory Faull, F-A-U-L-L.

Leo: In Belize. In Belize.

Steve: Yes. He was his next-door neighbor in Belize. This neighbor had been found dead, shot in the back of his head with a 9mm. And prior to that, Gregory had previously confronted John after one of John's quite aggressive dogs had bitten someone in the area. The dogs were apparently known to get loose and run wild in packs, terrifying the community. So he was a source, McAfee was, of adventure and controversy.

Leo: Adventure is a good word for it.

Steve: In his earlier years he had worked at NASA, Xerox, and Lockheed Martin, before launching the world's first commercial antivirus software in '87. And in fact he and I interacted just once by phone.

Leo: Well, that's what I was curious, if you had met him, yeah.

Steve: It was before his launch of McAfee AV. After I had written a series of three columns in InfoWorld, which he was reading, which imagined with as much detail and accuracy as I could exactly how a theoretical software virus would behave.

Leo: Oh, interesting.

Steve: And I don't recall now how clear I made it that this was conjecture. But a quite animated John McAfee, who was unknown by the PC industry at the time, phoned my office, wanting to compare notes and virus samples. He was sure, and amazed to discover, that I had viruses, clearly, because I had exactly described the behavior of the viruses he had. And he was very disappointed to learn, and actually it took me some time to convince him and like talk him down, and I'm unsure that I ever really did. I think he just didn't really believe that my three-column series about software viruses was entirely written from my imagination as a software developer, not as a virus discoverer. Anyway, I said, "Sorry, John. I mean, like, really, really, really, I don't have any. If I was a virus, this is how I would behave." And he's, like, "Really? Oh, well, I thought we could, you know, I'd show you mine if you showed me yours." So anyway.

Leo: I saw some stories about him fairly aggressively calling people to get information or copies of viruses. He was working at Lockheed when he got a copy of Brain in the late '80s and started writing McAfee. But, you know, I think he wanted

to write an antivirus, but he needed to understand what it was he was blocking, what he was preventing.

Steve: Yeah. [Crosstalk].

Leo: [Crosstalk] worked; right?

Steve: It's funny you mention that, Leo, because I was thinking the same thing this morning, like okay, we know how they work now. So would it have been behavior based? It's hard to imagine it would have been signature based because, what...

Leo: There weren't any. There were four or something, yeah.

Steve: Right, exactly. Exactly. Yeah. So it's crazy.

Leo: He probably was trying to come up with heuristics so that you could watch for a certain kind of behavior. That's the ideal way to do it, signatures plus heuristics. But I don't know, yeah.

Steve: Yeah. And we didn't have an Internet back then.

Leo: Right.

Steve: So they had to live, they had to jump from floppy to floppy.

Leo: You had to send him a floppy, yeah. Hey, John, I got one. It's on a floppy, here.

Steve: We didn't have USB. We didn't have thumb drives. All we had, the only thing that was transportable was diskettes.

Leo: Right.

Steve: And so the viruses, such as they were, had to be very tiny. I think I remember that some of them lived in Track 0 because there was still - I think there was still cylinder alignment. So I think there was space on Track 0 after the boot sector. And so you'd have - there were, like, I remember boot sector viruses, I mean, they had to be...

Leo: That's right, that's right.

Steve: ...really, really small.

Leo: So what you'd do is you'd put it on the boot sector of a floppy. And if somebody booted that floppy, attempted to boot from that floppy, it would infect their system. This is pre-hard drive. Or did it have hard drives?

Steve: Oh, yeah, if they had a hard drive. Or it would go into RAM and then move onto any other diskettes that...

Leo: Any other floppy you used, yes.

Steve: ...that they then stuck in. And before you knew it, I mean, and I remember there were like red floppies that were infected that researchers were, like, using.

Leo: Yes. Don't touch. Don't touch. Yes.

Steve: Wow. Okay. So a fun topic, and one that is up in the air. Where exactly will Windows 11 run? And the subtitle is don't ask Microsoft because they have no clue.

Leo: They've actually changed the story several times already.

Steve: I know, Leo. What a mess. So, okay. The trouble is there's no difference between Windows 11 and Windows 10. And everyone knows it. It's the same operating system. So Windows 11 can run anywhere that Windows 10 runs, unless Microsoft chooses to place what you'd have to consider somewhat arbitrary limits on where they will allow Windows 11 to run. And there's just no way that's going to go down well.

On my own lovely Intel NUC that I was just talking about last week, which is a fast 4-core Intel i7-6700HQ Skylake processor with 32GB of RAM, a very large GUID partitioned NVMe mass store, and TPM v2.0, I received that screen on the show notes above, saying: "This PC can't run Windows 11." It says: "The processor isn't supported for Windows 11. While this PC doesn't meet the system requirements to run Windows 11, you'll keep getting Windows 10 updates." Okay. So, right. So for some reason this perfectly reasonable Intel NUC, i7-6700, perfect little machine, nope, won't run it. Now, it runs great in a VM. I am running it in a VM. So, okay. But apparently not natively.

So because there's no actual legitimate reason why Windows 11 cannot run everywhere and anywhere Windows 10 runs, Microsoft themselves hasn't yet decided where Windows 11 should be allowed to run. Their own most recent statement, as of yesterday, essentially admits this. They said, and I quote: "Today we're releasing the first preview build of Windows 11 to the Windows Insider community." Meaning that's not that earlier dev one we were talking about last week and the week before. This is it, Windows Insider community.

They said: "In support of the Windows 11 system requirements, we've set the bar" - okay, right, it's a bar. Where are we going to set it? We haven't decided yet. So, oh, wait, wait, if it's too high, you can't jump over it. If it's too low, then you don't have to jump very hard. So we've set the bar, and it's settable, for previewing in our Windows Insider Program to match the minimum system requirements for Windows 11. Okay? So we've decided how much RAM you should have, how big your hard drive should be, those things. You know, it's all variable; right? How many cores you should have. We think two's enough.

Okay. "With the exception," they wrote, "for TPM 2.0 and CPU family/model. By providing preview builds to the diverse systems in our Windows Insider Program" - meaning maybe other people, maybe Windows Insiders have NUCs just like I do. Wouldn't want to rule them out. Anyway: "We will learn," they wrote, "by providing preview builds to the diverse systems in our Windows Insider Program, we will learn how Windows 11 performs" - what a crock - "across CPU models more comprehensively, informing any adjustments" - informing any adjustments to the bar, apparently - "we should make to our minimum system requirements in the future." And I wrote here: "What a load." Anyway: "We look forward to the product feedback" - oh, they're going to get some. Oh, and Leo, "and learnings."

Leo: They love that word. I hate that.

Steve: They're looking forward to the learnings. Not one learning. We're going to have multiple learnings. Oh, baby, I guarantee you're going to have multiple learnings coming from this. "As it's an important step," they wrote - yeah, deciding where it should run - "to prepare Windows 11 for general availability" - or perhaps limited availability - "this year. Thank you to the Windows Insider community for your excitement" - uh-huh - "and feedback thus far!" Oh, yes, it's already very exciting. Given the mess and confusion this is creating, and I loved you guys last week, Leo, talking about how, I mean, Paul and Mary Jo were just shaking their heads. How could they have screwed this up any more? I mean, it's their own OS. Anyway, they're getting blowback. They're going to be getting blowback.

Okay. So here, Leo. I actually have a solution to this, believe it or not. I think that what should be done is obvious. There's a beautiful compromise available. Unlike Windows 10, Windows 11 should require that any available security technologies be enabled on any platform where it runs. But given that, it should run anywhere Windows 10 runs. In other words, both of the systems I routinely use have a TPM. One of them is v1.2. That's the one I'm sitting in front of. The other is v2.0, that Intel NUC. And there's nothing wrong with v1.2. It works just fine. It's secure. But neither of those TPMs are enabled or initialized on my hardware. Both systems also offer Secure Boot, but neither have it enabled. Microsoft claims that their telemetry shows that they have seen up to a 60% reduction in malware when TPM-enabled features, like Windows Hello and BitLocker encryption, are used on supported devices. Now, it's unclear why that should be true at all, unless it's correlation and not causation. Meaning people running with those security features enabled tend to also be more cautious and careful. But okay.

Leo: So that's an important point. TPM does not help you avoid malware.

Steve: No. No.

Leo: It's for things like BitLocker. It's a secure, basically hardware security chip; right?

Steve: It does, when it is - yes. It's like a Secure Enclave. So if you have Secure Boot enabled, it will prevent a rootkit virus, for example, from getting into your system.

Leo: Right.

Steve: So that's useful. So it creates a secure anchor, and it verifies the signature of each item in a chain, up to and including Windows is running. So that's what Secure Boot is securing, is like that whole process. They also said that devices using the new Windows driver model, meaning signed drivers, can achieve a 99.8% crash-free experience. And of course that's apparently so long as you don't run Windows Update, which as we all know has the tendency of spoiling everyone's crash-free experiences.

Okay. So if the price of allowing me to run Windows 11 on systems that can be run with greater security is simply turning on those features, which I haven't needed to or bothered to so far, that's a choice I will make. But tell me that I cannot run Windows 11 on hardware where I know it can run just fine, well, good luck with that. The machine I'm sitting in front of while we record this podcast is equipped with an older Haswell processor, specifically because remember Microsoft originally threatened not to support Windows 7 after Haswell. So that forced me to immediately go get a Haswell-based system because I wanted to run Windows 7. They were later forced to backpedal on that one when corporate America refused to make the move to Windows 10, which no one wanted at the time. And corporate America insisted upon being able to run Windows 7 on more current hardware, so Microsoft ended up saying, okay, fine. Because they could.

So anyway, just to be clear, it seems it will be really interesting to see how this plays out for the rest of the year. And we have six months, so there's time. To me, I would have no trouble if Windows 11 looked and said, hey, you've got a TPM. Turn it on. Your system will do Secure Boot. Turn it on. And make you do that in order to run Windows 11. That seems okay. And there's been discussion of this for the last couple weeks. The problem is TPM 1.2 is fine. And TPM, it first appeared on laptops. Many fewer desktops, older desktops, have it. And so I think the problem is there will be many desktops running Windows 10 where Windows 11 can run just fine. But if they stick to requiring TPM 2.0 and Secure Boot, those systems are not going to be able to run 11. For no reason. I mean, it's the same as Windows 10. It just has better-looking icons and rounded corners. And boy, did you see the list of things they took out, Leo? That's really nice. They got rid of a bunch of the crap that nobody wants. Of course Xbox is still there.

Leo: This is the thing that puzzles me because you famously wrote the program Never10 because you never were going to go to Windows 10. Now you're all upset because you can't go to Windows 11. But I'm a little confused. I actually thought the thing people would hate the most, until the Microsoft Event, was that they centered the Start Menu. And I thought, oh, we're going to hear so much about it. Microsoft said "Hold my beer" and came up with something to get people really incensed. You know, we'll wait and see. It may not be - they've already changed the specs a little bit. And by the way, they changed that compatibility checker, too, without telling anybody.

Steve: Yeah.

Leo: So I think they're going to be a little sensitive to the pushback. But it's funny, I mean, it is Windows 10; right? Just cosmetically different?

Steve: Yes.

Leo: Do you want it because they took things out? Is that why...

Steve: Leo, if you click down a couple layers, you can still find a dialog for Windows 95.

Leo: Oh, yeah. Oh, absolutely.

Steve: I mean, it's the same operating system.

Leo: No, that's absolutely the case. So, yeah, I figure - I guess you can live without it. The only issue will be how long will they give you security updates for Windows 10.

Steve: Yes.

Leo: They've already committed to 2025, but they can extend that, as well.

Steve: They can. And so I've gotten used to 10. I had to make sure that SQRL ran under 10. I run 7, and I run 10. New systems that I set up are all running Windows 10. All the laptops that Lorrie's using for her remote home neuro clients, they're all running Windows 10. You know, I've made peace with it. I have no problem with it. I just think we need to keep Microsoft honest. And the idea of saying, oh, yeah, we're not going to let you run 11 on systems where it can, and we're not sure why...

Leo: Microsoft's real problem is communication. They just for some reason...

Steve: Oh, boy, they really stepped on it this time.

Leo: Yeah, yeah.

Steve: Okay. So speaking of, the next headline here I've titled "Why Not WhyNotWin11?" There's a new piece of well-intended, but very poorly written, junk known as "WhyNotWin11." You can most easily find it by going to https://WhyNotWin11.org. But don't go to WhyNotWin11.com, which is a domain that was grabbed up by someone else, who then ignored the author's pleas to synchronize with him. And don't go to http://WhyNotWin11.org because that won't properly redirect you to GitHub.

Okay. So the whole thing is a mess. I'm sure its author means well. It might even eventually provide some useful information. But you'll need to push past Chrome's and Windows' malware alerts because the app's compiled script is changing minute by minute as its author keeps trying to get it right thus preventing the code from ever maturing and having the chance to earn a reputation and the executable is unsigned. Since the app initially seemed useful, and since I could verify the safety of its operation from its source, I briefly toyed with offering to sign it for the guy. But having watched its subsequent implosion and mismanagement, GRC will never have anything to do with it. Lawrence at BleepingComputer picked up on it and gave it a lot of attention last week, which brought a lot of attention to it.

Leo: We mentioned it on TWiT, as well. Daniel Rubino plugged it. So, yeah.

Steve: Yeah. And so Microsoft, as we said, has tripped over themselves, creating a vacuum for it. And it may settle down. My sense is that ultimately Microsoft's own PC Health Check tool will be what people should use. But I wanted to make sure everybody knew about it. However, the coolest thing about WhyNotWin11 is that it made me aware of a very slick and quite capable 100% free Windows scripting tool and environment called "AutoIt Script." And that's something that I wanted to put onto our listeners' radar. I've tweeted about it. I mentioned it in GRC's newsgroups. It got a bunch of people excited. AutoItScript.com, A-U-T-O-I-T-S-C-R-I-P-T dot com. It compiles quite capable scripts. The scripting language is Turing complete. It's a complete scripting environment. It compiles them into standalone and independent EXEs that do not require any .NET libraries. It runs under any edition of Windows.

The language is extensive. It allows for Windows UI to be implemented to create quick Windows automation apps. And it includes a wonderful and complete 6.8MB old-style compiled Windows Help .CHM file. The help file contains a clear description, tutorials, a language reference, a GUI reference. It's able to invoke COM objects in order to make that simple. It runs PowerShell. You can script run-as events, completely script your existing Windows apps. It might be just the ticket for enterprise IT admins who need to quickly get something automated and pushed out without resorting to VB.NET or something heavier. Anyway, I just wanted to make sure it was on everybody's radar: AutoIt Script.

I use one particular browser shortcut like crazy, and that's CTRL+L. Happily, it's universally supported. It takes you to and highlights your URL, and you can imagine while I'm putting the podcast together because I've got links to everything in the show notes, I'm often needing to grab the URL that I'm looking at. So I just wanted to make sure everybody knew about CTRL+L. It is just really, really handy.

Leo: It's good to remind people because I forget. And that is a very useful keystroke, really useful.

Steve: Yeah. It just jumps you like right off the page to the URL and highlights it so you can then do a CTRL+L.

Leo: You can copy it or replace it, yeah.

Steve: Exactly. CTRL+C or CTRL+V if you want to copy over it and then go somewhere else. Also, for years there was a program, it was called Teleport Pro, which was my go-to when I needed to clone a public website. Sometimes you need to do that. And I'm sure that old-timers among us have sometimes needed to end up going to the web archive, trying to find something, like a link is broken because a site that we just assumed would always be there disappeared. There are a few reference sites that I use like crazy. And a couple times one of them, there's one at I think it's Ctyme.com, it's got an instance of Ralf Brown's Interrupt List. I'm sure, Leo, you remember the Ralf Brown Interrupt List.

Leo: I don't. I wish I'd had that back in the day.

Steve: Oh, it's like the standard reference for, like, everything. And because I'm working with SpinRite, I'm down in IRQs and interrupts and INT 10 VGA BIOS calls and things. And so I'm constantly using it. And a couple times over the last year it's been offline for a while. And I've thought, oh, crap. Like, I mean, there are other sources of this. Ralf Brown is a professor at Carnegie Mellon. And back in the DOS days he created, he began compiling this, and it just became the galactic standard. In fact, if you Google Ralf Brown, R-A-L-F Brown, so it's not - yeah, Ralf, R-A-L-F B-R-O-W-N Interrupt List, you'll get a ton of hits on Google.

Anyway, a couple days ago I just thought, you know, I have to copy this site just in case it ever actually goes away forever. What I used is my favorite now go-to website copy tool that again, I just wanted to tell everybody about. I made it this week's GRC shortcut. So you can get to it with grc.sc/825, grc.sc/825. It's Cyotek WebCopy. It's complete free. I like this company. They seem to be good guys. It's donation ware. If you like it, give them some money. They've been maintaining it for a while. This is one of several things they offer.

Anyway, there's really not much more to say except to say it just works. It gets the job done. It does a good job of taking a public site. It's got all the bells and whistles you could want for, like, don't go offsite. Don't go down more than N number of levels. Don't bother pulling images. Don't blah blah blah. Or whatever you want. It's also able to create a localized copy on your hard drive so that you then end up with a running copy of the site that was offline so that you never have to worry about something that you depend upon disappearing. So grc.sc/825.

I have a page over in my forum. I have my own private forum where my blog is over at forums.grc.com. I have a page of my favorite things. And I'm trying to keep that current, and I added this to that page. So if you ever kind of remember that I had once mentioned something like what was that site for syncing, what was that Syncthing, what was that WebCopy thing, anyway, if you think of it, you can check that page. And I am keeping it current. And a Humble Bumble. Bundle.

Leo: You always call it a Humble Bumble. I think it's the funniest thing.

Steve: I do, a Humble Bumble.

Leo: Yeah.

Steve: And that's bad because I created another shortcut which is not Bumble, it's Bundle. So grc.sc/bundle. And I realized that from time to time, when bundles come up, I can simply change where that shortcut points.

Leo: That's a good idea, yeah.

Steve: So the most recent bundle, yeah, it'll always be grc.sc/bundle. This is a cybersecurity bundle, Cybersecurity 2021 bundle by Packt Books. And here's what it's got. Looks like a bargain to me. One dollar. One dollar gets you three books: "Mastering Azure Security," "Cybersecurity Attacks - Red Team Strategies," and "Metasploit 5.0 for Beginners." One dollar.

Okay. For $10, you add eight more to that. "CompTIA Security+"; "Cybersecurity Threats, Malware Trends, and Strategies"; "Cybersecurity - Attacks and Defense Strategies"; "Mastering Malware Analysis"; "Learn Kubernetes Security"; "Learn Wireshark"; "Mastering Python for Networking and Security"; and "Cyber Minds." I have no idea what that one is.

And then, for an additional $8, for a total of $18, you get 13 more, totaling 24 books: "Microsoft 365 Security Administration"; "AWS Certified Security - Specialty Exam Guide"; "Learn Kali Linux 2019"; "Mastering Windows Security and Hardening"; "Learn Computer Forensics"; "Practical Mobile Forensics / Third Edition"; "Practical Threat Intelligence and Data-Driven Threat Hunting"; "Digital Forensics and Incident Response"; "Mastering Linux Security and Hardening / Second Edition"; "Practical Hardware Pentesting"; "Ghidra" - is that how you pronounce it, Ghidra?

Leo: Yeah, that's that reverse engineering tool.

Steve: Yes, yes. And it is not simple. So believe me, "Ghidra Software Reverse Engineering for Beginners," we're all a beginner. I looked at that thing, and it's like, whoa.

Leo: Yeah, it's amazing.

Steve: "AWS Penetration Testing"; and "CISA - Certified Information Systems Auditor Study Guide." All of that for $18, and it's a charitable contribution. Has it all been going to charity? I think it's all going to charity.

Leo: No, a percentage goes to charity.

Steve: Oh, a percentage, a percentage to charity. So anyway, grc.sc/bundle, B-U-N-D-L-E. And, I mean, even if some of those are not good, wow, you know, $18. There's got to be some good stuff in there.

Leo: They're all eBooks.

Steve: Yes, yes.

Leo: You have to be okay with that. But that makes it easier to search them, so that's a benefit.

Steve: Yeah. And PDFs, you're able to search a PDF pretty quickly.

Leo: Yeah.

Steve: Okay. Two pieces of closing-the-loop feedback. A frequent and very useful Twitter DMer sent this. He said: "Re: SN-824," which of course was last week. He said: "Surely

'the role of commercial providers'" - and first of all, to remind people, you and I, Leo, were scratching our heads. That was something that - was it a Google person? Somebody was talking about the rate at which vulnerabilities were occurring, and he referred to the role of commercial providers, and we were thinking, what in the world is he talking about? Didn't make any sense.

He said: "Surely it must be the commercial exploit vendors getting their hands on these, rather than Google and the Chromium project."

Leo: Right, right, right.

Steve: He says: "I guess they have reason to believe at least some of these zero-days" - oh, that's right, it was in the context of six zero-days so far this year. In fact, there had been six, and that was number seven, were being sold on the open market before exploitation started in the wild. So anyway, I wanted to thank him for that. I'm sure that's what the Chrome guy was referring to.

And finally, Mementh tweeted: "Serious question, Steve. Windows 11 might require TPM. How TNO is it? Can I trust it to keep the secrets the NSA wants from me from getting out? Would you put info behind it that would cost you your life if it got broken? I can't recall what your opinion on it was, and I recall the drive you fixed was locked by it." I thought that was a great question to wrap this up. The answer is no. I did some digging during that week that I was trying to come up with some way to unlock the contents of that BitLockered and TPM key-protected drive to bypass it. What could I do?

Turns out it's actually not difficult. The TPM chip which exists in chip form when it's not bound into the Intel firmware, and I suspect it may be a different story when it is in the Intel chipset, but I'm not sure. If it's part of a chipset and in an external chip in the family, then it may still be possible. The point is the TPM chip, when it's a standalone chip, is on the motherboard, and it can have a digital signal analyzer hooked up to its pins, and its communication can be and has been decoded.

So certainly the NSA knows how to do that. There's cool pictures, if you go to "Decrypt TPM" in YouTube, you'll find some YouTube videos of people doing that. You use a digital trace, a digital signal capture device, and out comes all these cool-looking little square wave signals. And that could be decoded. And the key will be moving across one of the pins, digitally encoded, and you can capture it and crack the encryption in the case of the TPM. So the secrets are being kept there. But unfortunately they move over the wire which is exposed. So not something that you could trust your life with. But a great question. Thanks for asking.

Leo: And I had to laugh because - and I thought of you during the Windows 11 announcement when they said "This is the most secure version of Windows we've ever made." And I thought, when have they not said that? But you mocked that I remember when Steve Ballmer said that back with Vista or XP or one of the older ones.

Steve: And because we know, we know the story.

Leo: Right.

Steve: Security is only something that you can see that did happen in retrospect when nothing bad happened.

Leo: Right. You don't know until you put it out in the world, basically.

Steve: Right. Basically you cannot prove a negative. And all you have is no evidence in the beginning of whether it is secure or not.

Leo: We did our best. You could say, "We did our best. We tried really hard."

Steve: Yeah. And we really thought that if we would only allow it to work on processors that you couldn't use till next year, that nobody would have a problem this year.

Leo: I suspect it really comes down to selling more PCs, frankly. That's what we've speculated.

Steve: Yeah, yeah. Isn't that sad?

Leo: That is sad, yeah, yeah. But really, traditionally in the Windows environment, that's when you got a new version of Windows was when you bought a new computer. I think most normal people don't upgrade. Windows 10 broke that mold by offering a free upgrade to everybody. But that's why they had to give it away for so long.

Steve: You know, my older Apple devices still work. But they are slower than the newer Apple devices.

Leo: Yeah. That's right.

Steve: Right here is an iPhone 6 that I use because it's got this wonderful little hole.

Leo: It's got the headphone jack.

Steve: I love that hole. Oh, my god.

Leo: Miss that, yeah.

Steve: Oh. Now, and it's plugged in. The battery's still 100% good because I don't think it's ever been unplugged. Actually it was in my pocket for a while. But I never let it discharge much because we know that lithium-ion batteries don't like it. Oh, and by the way, Leo, I heard you talking about your exploded Pixel 4.

Leo: Oh, so depressing, yeah.

Steve: Yeah. I just had the battery in my iPhone 10, the iPhone X...

Leo: Swell up.

Steve: It was replaced last Friday because it was still working perfectly. It was funny, too, because I went to the genius at the Apple Store, and he said, "Oh, this is never going to pass the diagnostic." I said, "Yes, it will." He says no. I mean, you could see all of the silver clips had, like, they were - it was like the screen had popped out of the backing.

Leo: Yeah, yeah.

Steve: Yeah. And he ran their diagnostic, and he says, "I'll be darned. Works perfectly." I said, "I know."

Leo: But you need to replace it because it's going to explode if you don't.

Steve: Well, yes, I was worried that if I ever had to travel, the TSA would look at this and go, uh, we're not letting you on the plane.

Leo: What causes lithium-ion batteries to swell? Because they don't all.

Steve: It's overcharging and outgassing. So if you overcharge the cell, it produces gas. And the gas then...

Leo: Expands, yeah.

Steve: ...causes the battery to expand and pushes everything else out.

Leo: Interesting. And it seems to happen with age sometimes.

Steve: Yes, because what happens is you end up with some little tiny - can't remember now what the metal is. I don't think they're nichrome.

Leo: Oh, interesting.

Steve: But there's some little microfilaments.

Leo: Microfractures. Oh.

Steve: Which start to bridge. And that causes the chemistry to get a little freaked out, and then it begins to outgas.

Leo: Okay. So it's, I mean, the Pixel 4 XL is not that old. It's a couple years old. And it's swollen enough that it pushed the back off. And I guess I probably shouldn't continue to charge it; right? That means it's time to either replace the battery or get a new phone.

Steve: Yeah, whatever. I mean, I actually have somebody who had...

Leo: You don't think it will explode?

Steve: No, it won't explode.

Leo: Okay.

Steve: No.

Leo: So if you tried to jam it back together again, you might puncture it and then cause a fire. But if you just let it expand and let it expand naturally...

Steve: Well, and it's got nasty goo in it. You don't want to, like, have this goo...

Leo: I know. It's toxic. No, I know.

Steve: You don't want that goo coming out.

Leo: Yeah.

Steve: So I would just let it be a rocking horse for a while.

Leo: Not try - yeah, exactly, not try to reattach the back, but just let it...

Steve: And if it's a good phone, for example, my iPhone X is going to a buddy of mine. Actually it's the [crosstalk].

Leo: And I'm sure Apple replaced it; right? They replaced the battery.

Steve: Yeah. Yes. They replaced the battery. Cost $69 to do an out-of-warranty replacement.

Leo: It's well worth it.

Steve: And it's as good as new. It's no scratches. It's gorgeous. And it still runs just fine. But in the interim I did get a 12 Pro, and oh, it's so nice. It just - and this was my point is it does run faster. And so I would have no problem if you chose to get new hardware because Windows 10 was no longer fast enough on old hardware. But it ought to agree to run if it really does run.

Leo: You'd think.

Steve: I mean, if the technology hasn't been obsoleted.

Leo: Yes, you'd think. But we brought this up, we've talked about this before because Microsoft some years ago said we're not going to support these pre-Haswell chips, as you mentioned. And that makes sense because they're doing, I think, a lot of coding and patching to the chip, and they don't want to support older chips; right? I understand that.

Steve: Right. And that absolutely makes sense. It was, yes, and in fact installing Windows 7 on a Skylake does - because Skylake chipset doesn't support the same USB drivers. And Skylake was only USB3. If you had an older motherboard, you needed to, like, you needed to get the USB3 drivers for the motherboard and install them into the DISM image in order to get the thing to install because as soon as - it would boot up. It would start the install. And then it would die when it tried to switch to its own drivers, which didn't work on your hardware. So you had to jump through some hoops. But I'm running it. It's like, it works just fine. I've installed it on a number of machines like that. But yes. It certainly makes sense not to ask them to keep supporting older chipsets at some point.

Leo: Yeah, at some point. Two years later?

Steve: It's like, sorry, it's the same, yeah, it's the same as 10. I mean, it's running on all...

Leo: Yeah, it is 10.

Steve: It is 10.

Leo: It is 10. I think it's time to replace, by the way, this iPhone I got 14 years ago.

Steve: Happy Birthday to iPhone.

Leo: Maybe it's time to replace this one. This one, ironically, the battery has never swollen on. So 14 years later, the original iPhone. Steve Gibson, we're done.

Steve: We are.

Leo: We're done. Great show.

Steve: [Crosstalk] podcast.

Leo: Everybody should run out and buy SpinRite quick so you get the free upgrade to 6.1. He's working on it hard. By getting 6.0 you'll also participate in the development of 6.1, so that's nice. You'll find SpinRite at GRC.com, the world's best hard drive maintenance, mass storage maintenance and recovery utility. We also invite you to go there for some unique versions of this show. Steve maintains a 16Kb audio version, if you ever want it to sound like the original Thomas Edison gramophone.

Steve: Once upon a time Elaine had a very slow satellite connection.

Leo: Right.

Steve: That's right. And that's what started this was that it was burdensome. Oh, and she had a tight bandwidth cap. And so it was like...

Leo: That's really who it's for. Anybody who has a bandwidth cap doesn't want to spend extra bits and doesn't mind that it's a little scratchier. But it's a lot smaller.

Steve: I don't know, Leo, [intentionally obscured audio].

Leo: Now, the transcripts are even smaller, and those are great. Elaine writes those, does a great job listening to our words and turning them into English prose. You'll find that and the 16Kb version and the 64Kb audio version at Steve's site: GRC.com. While you're there, leave a question, a comment, a suggestion, just praise at GRC.com/feedback. You can also tweet him. He's @SGgrc on Twitter, and his DMs are open.

We live at TWiT.tv, and that's where you'll find this show and all the shows we do, both audio and video. I think that's about it. We'll see you next Tuesday about 1:30 Pacific, 4:30 Eastern, 20:30 UTC. You can watch the live stream as we do this show and all of our shows at TWiT.tv/live. Thank you, Steve. Have a great week.

Steve: As we begin the second half of 2021.

Leo: Hard to believe.

Steve: Oh, I know. I mean...

Leo: I still feel like we're in 2020 in some ways.

Steve: Okay, buddy. Bye.

Leo: Take care.