SECURITY NOW!

Transcript of Episode #1018

THE QUANTUM THREAT

Description: The dangers of doing things you don't understand. Espressif responds to the claims of an ESP32 backdoor. A widely leveraged mistake Microsoft stubbornly refuses to correct. A disturbingly simple remote takeover of Apache Tomcat servers. A 10/10 vulnerability affecting some ASUS, ASRock and HPE motherboards. Google snapped up another cloud security firm but paid a price! RCS messaging to soon get full end-to-end encryption (done right!). How did an AI Crypto Chatbot lose $105,000, and what is an AI Crypto Chatbot? Looks like Oracle may take stewardship of TikTok to keep it in-country. Whoops! 23andMe is sinking don't let them take your genetics with them! The White House says "The cyber guys should stay!" AI project failure rates are on the rise. Anyone surprised? We then have some relevant listener feedback, and a very interesting update on just how looming is the threat from quantum computing?

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-1018.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-1018-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. He'll talk about a bug Microsoft has known about for years, refuses to correct, and is now being used by 11, count 'em, 11 hacker organizations. A very disturbing remote takeover of Apache Tomcat servers, something you're going to want to patch right away. He's going to talk about the Signal breach, the Department of Defense's use of Signal, and why that's an unsafe thing to do. And then finally, if you weren't worried about the future already, stay tuned because Steve's going to be talking about the threat that post-quantum cryptography poses to everything you know. It's all coming up next, a big one, on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 1018, recorded Tuesday, March 25th, 2025: The Quantum Threat.

It's time for Security Now!, the show where we cover the latest security news, privacy information, with a little dollop of sci-fi and stuff like that thrown in, with this guy right here, Mr. Steve Gibson, the man of the hour. Hi, Steve.

Steve Gibson: And hopefully some fun. One of the things that I often hear from our listeners in feedback is that they find this entertaining.

Leo: It is entertaining.

Steve: So it's a strange crowd we have.

Leo: If you're a nerd. If you're into this stuff, it's the best thing ever; right? It's better than sliced bread. I mean, you know, this is the good stuff. I know people, many people consider this the best show on the network and wait all week long for Steve to show up on Tuesday. So we're glad you're here.

Steve: Well, we're back again for Episode 1018. Whenever I tell my neighbors, my neighbors sort of had this vague sense that I do something with a podcast. And so when Lorrie and I encounter them out walking, they go, "Still doing that podcast?" I say, "Yup, I just did number 1017." They go, 1017?

Leo: What?

Steve: That's right.

Leo: You're a madman, Steve. Congratulations.

Steve: Well, we've got a neat episode this week. I titled this one "The Quantum Threat." I ran across a really nice piece of sort of "where the industry is" update from Hewlett-Packard's security people, which just perfectly contextualizes the status now. And I found that after I had absorbed it, I thought, okay, there's so much good stuff here. This needs to get shared. So that's going to be where we wrap things this week.

But first we're going to talk about the dangers of doing things you don't understand. Espressif's, you know, the Chinese producer of the ESP32, the most popular IoT processor, they've responded to those claims of that backdoor.

Leo: Ah, the Bluetooth backdoor.

Steve: Yeah, that Bluetooth backdoor which we decided wasn't. We've got a widely leveraged mistake which we talked about last summer, but Microsoft stubbornly refuses to correct, even though, like, I can't remember now, 14 different threat groups are all using it now? It's like, come on, Microsoft. A disturbingly simple remote takeover of Apache Tomcat servers, like all Apache Tomcat servers. There is also a 10 out of 10 vulnerability affecting some ASUS ASRock, and HPE motherboards. Google has snapped up another...

Leo: Do they call that, by the way, "ass-rock"? No.

Steve: Well, "as-rock"?

Leo: Or "A-S rock," maybe?

Steve: You're right. There are not two S's. So I guess it ought to be "as-rock."

Leo: It's not a great name if that's what they...

Steve: Although I did rename those other routers the "Microtic" routers.

Leo: Oh, the MikroTiks, yes.

Steve: The Microtic, yeah, that sounds really bad. It's like, oh, I think that's microtic, you'd better have that removed. So we also, oh, I was saying that Google snapped up another cloud security firm, but they did pay a price for doing so. We have RCS messaging soon to be getting full end-to-end encryption, and it was done right. We're going to talk about that. Also, how did an AI crypto chatbot lose $105,000, and what is an AI crypto chatbot?

Leo: Yeah.

Steve: It's like, what?

Leo: Huh?

Steve: We're going to note that it looks like Oracle may be taking over stewardship of TikTok in order to keep it in-country. And, whoops, 23andMe is sinking. You may not want to let them take your genetic data with them on their way out.

Leo: Or your spit, yeah, yeah.

Steve: Also the White House says that the cyber guys should stay. We'll touch on that. Also AI project failure rates are on the rise. Is anyone surprised? We've got some really, I think, relevant and interesting listener feedback to share. And then, as I said, we're going to wrap up by looking at just where do we stand with quantum computing, and what's the threat? We've got a Picture of the Week. And because the news broke after I put all of this together, which was actually early yesterday afternoon, we need to talk about the only cyber thing that anybody is talking about at the moment, which is this mistake that the White House, I guess Cabinet members made of using Signal to discuss very privacy-sensitive, national security-sensitive war plans. So that's not in the show notes, but we should open with that after we look at our Picture of the Week.

Leo: Yeah, yeah. Steve?

Steve: Well, I will say that a lot of our listeners have said that the podcast has made a huge difference to their lives and their careers.

Leo: Nice. Nice. I would agree with that.

Steve: And so I...

Leo: It's made a big difference to my life and career, actually, to be frank.

Steve: I appreciate the feedback. Okay. So I gave this one the caption "Once seen, never forgotten."

Leo: All right, I'm going to scroll up.

Steve: Because this is just - I love human cleverness.

Leo: Wow. That's clever.

Steve: And I don't know who could look at 3.14 - this was of course on the radar because we just had March 14th a couple weeks ago. And who could look at 3.14 and realize that, if it were in the mirror, and you tweaked the shape of the numerals a little bit, the mirror image is PI.E. That's just brilliant.

Leo: That's cute. It's very cute.

Steve: Again, once seen, never forgotten. I actually had a really, really good Picture of the Week, and I thought, oh, I just, okay...

Leo: This one's timely. You have to do this one.

Steve: Yes, exactly. Because it's going to be April Fool's Day next time we're doing a podcast. And you never know what could happen there.

Leo: That'll be fun.

Steve: Okay. So I've said many times that, like when someone screws up, an employee makes a mistake, I know that some people's reaction is to say "You're out of here. You're fired." To coin a phrase. I've always thought, I guess I've taken a more tempered approach and thought, okay, well, if a lesson has been learned, if the employee who made a mistake, an honest mistake, who didn't intend to do what they did, learned from it, then you've got a better employee after that than you had before.

Leo: That's fair, yeah.

Steve: So are you going to, you know, can a better employee? You know, some other employer is going to get him, and he will have learned the lesson at your expense, and the other employer gets the benefit. So for that reason I'm glad that what happened yesterday, I guess it was, happened. And I'm not glad because there's, you know, it's egg on the Trump administration and Cabinet's face. That doesn't do anybody any good. I'm glad because this was a crucially important lesson for this new group of Cabinet officials and people who are in charge of the nation's security to learn.

We on this podcast more than anywhere else know that our phones are not secure. It doesn't matter that Signal is secure. We know it is. In fact, I'll be talking about it a little bit later, and the Ratchet protocol, which we talked about a long time ago when it was called TextSecure. We know Signal is state-of-the-art security. We also know that Pegasus and many other types of malware arrange to get themselves installed in people's smartphones specifically so that, if they do something like this, foreign intelligence agencies will obtain that information.

So I'm sure that everyone must know that a mistake was found because a journalist was inadvertently included in a multiway Signal conversation where the details of war planning by the U.S. was being shared using Signal and people's smartphones. And that's just not secure. And, you know, I'm watching the press coverage and people saying, well, Signal is secure. It's like, yes. But we know that you get the data after it's decrypted and displayed on the screen. And while it's being typed in, before it is encrypted...

Leo: It's unencrypted on your device, is the point; right?

Steve: Yes. And that's the key. And these smartphones we absolutely know cannot be trusted. And, you know, and there's been lots of dialogue. That's why there are SCIFs. That's why people have to leave their smartphones at the door and come in without them and on and on and on. So anyway, so my take is that this mistake will not get made again, and that there was without question a cavalier, too casual, but probably due to just a lack of understanding, lack of appreciation. You know, these are people who are not in the administration, haven't been historically. In fact, that's why they're here; right? Because the U.S. voted for the return of Donald Trump, and he was going to bring his own people that he felt comfortable with, who were not part of the so-called "deep state."

So this is what you get is you need to learn some lessons. This was an important lesson. And I'm sure everybody involved has learned it. I'm sure we're not going to have more, you know, national security conferences being held on random smartphones any longer. So, and better that it happened now, like soon, and that now for the rest of this administration I'm sure this won't happen again. So, you know, again, I don't tend to fire employees when they make mistakes, if they've learned a lesson, and it was an honest mistake, and it wasn't malicious. It certainly wasn't. It was just casual. And that can't happen. So I'm sure that message has been received, you know, across the administration. So lesson learned. That's the way these things happen.

Okay. Our first piece of news that I had, I said: "Don't try this at home, or anywhere else, for that matter." And I've touched on this before. But it's worth repeating. Again, I don't think it's something that would affect our listeners. But over 100 auto dealerships were being abused in a supply chain attack from a compromised shared video service which was unique to dealerships. It's something that dealerships were using as an outsourced managed service provider that was providing these video services to them, who knows what for. But when active, the attack would present visitors to this dealership-hosted website with a webpage containing infected JavaScript.

So when they visited this, at any of over 100 dealerships, there was a chance that a specific - this malware JavaScript would load, containing malicious code. If it did, it would redirect the user to a page on a compromised host that prompted the user with something everybody is now seeing; right? It would show a dialog box with a big headline, "Robot or human?" And then it would say, "Check the box to confirm that you're human. Thank you." And then the thing we've all seen, just a checkbox that says, you know, that alleges "I'm not a robot," and the little reCAPTCHA logo. And, you know, who would not click it? We're having to do that now increasingly. In this case, however, of course, this is malicious. So this is not actually the reCAPTCHA single-click dialog. This is malicious JavaScript running.

So the next thing that would happen is unusual. It would drop down, like that little "I'm not a robot" dialog would drop down, expanding, with three additional verification steps. And here's where I said we've encountered this before because we've talked about this before. The first verification step, Press Windows button, Windows+R. Second step, Press CTRL+V. Third step, Press Enter. Well, okay. Listeners of this podcast understand that Windows+R opens the Run dialog down at the lower left of your screen and gives it focus. Pressing then CTRL+V will paste whatever the malicious script had placed onto the Windows clipboard, and it was able to do so when you clicked the "I'm not a robot" button. That wasn't actually "I'm not a robot." That was yes, here's permission to paste onto my Windows clipboard.

So now the string has been pasted into the Run field of the Run dialog, which will be executed when you follow Step 3 and press Enter. So if the user performed these steps, a Powershell script was executed on the user's machine that would download further payloads and ultimately install the remote access trojan SectopRAT, a remote access trojan, RAT. And again, I've mentioned this before. I'm deliberately revisiting this because it's so diabolically clever, and because - I mean diabolic. And I believe that it perfectly captures a significant and fundamental problem that doesn't have any simple solution, and that's the human factor.

I know that listeners of this podcast would not blindly follow these instructions. But we would all pause to consider what's going on here, which suggests we're like, wait, what? And then we're looking at it and go, oh, I'm not doing that. But the important point here is that tech-savvy PC users are in the clear minority. We as the techies in our social groups, our families, our, you know, the people that others come to, we hear their questions. We understand that many people, when presented with this, would go, oh, okay, I get, you know, and like follow one, two, three, follow the instructions. The vast majority of PC users have no idea what's going on at all. And as a consequence, "instruction following" has always been their way of life within the PC world.

Leo, you had a radio show for decades, and you were Mr. Instruction Giver so that, you know, because people needed to follow instructions in order to solve their problems. You know, the person could be a brain surgeon by training and education and experience, but that would still not prepare them for all of the many clever ways a PC user can be tricked into doing something self-destructive.

The great annoyance for me is that I cannot see a future where this is resolved. I don't know how we get out of this mess. The only thing I can see that might resolve this - and I'm actually not kidding - would be an entirely different user interface experience with our PCs, meaning there isn't a Run dialog, there isn't like a copying from the clipboard and pasting into it and pressing Enter. Those things go away. Imagine an entirely different user experience for our personal computing environment where active AI agents interface the user to their personal computation and communications devices. You know, it might sound far-fetched, but I was watching Leo before MacBreak Weekly talking to an AI, having a conversation with it, back and forth, and it was very...

Leo: Yeah, it was great.

Steve: Yeah. I think, it was like you could - and here was Alex talking about how he's using, was it Vibe, in order to...

Leo: They call it "vibe coding," but it's - I don't know what he was using. There's a variety of tools.

Steve: Oh, so "vibe" is a generic term.

Leo: It's a style.

Steve: For, like, not - it's sort of the way you read books, Leo, without actually doing any reading. I get it.

Leo: Audio counts.

Steve: I get it.

Leo: Audio counts.

Steve: Uh-huh.

Leo: Yeah. You're not typing code because you don't know how to code. You're telling the chatbot to code. You're giving it the vibe of the app, not the actual code.

Steve: I see.

Leo: Yeah. I don't know how good that is.

Steve: We want something sort of like this.

Leo: Yeah, yeah. Make me an app that looks like this.

Steve: A little more green in there on the corners.

Leo: Yeah, yeah.

Steve: So as we know, the reason, I mean, the reason I think I'm kind of serious is once upon a time - let's go back in time. All interaction with computers was via - I mean all - a teletype which had a clunky, clankety keyboard, and it typed text onto a wide roll, a continuous roll of paper. A big jump was to the textual video display screen, which was faster and a lot quieter. And then for a long time that's all we had. That's all there was. And then the next big change was to a graphical display which we interfaced to not only with that same keyboard, which was now quieter, but also the game-changing mouse and onscreen pointer. You know, that was...

So my point is there have been in the past several real upheavals, several real arguable breakthroughs in the way humans interface, interact with computers. I think we're on the cusp of another one. And so I can see where one way of taking the human out of the execution loop, which hurts them as much as it helps them, is for there to be an AI agent, a Dave saying, "I'm afraid I can't do that." I guess it was Hal, Hal saying to Dave.

Leo: I mean, this attack would not have worked on an iPad or a Chromebook. It works on Windows, and it could probably work on Macintosh. I think we need both, Steve. I don't want to give up my capability to run arbitrary code on my computer. That's my computer. But there are a lot of people who shouldn't have that capability. They should probably be using a Chromebook or an iPad. And I think that's the theory of this; right?

Steve: Yes. I completely agree. And again I'm, you know, Windows 10, where I plant my stake...

Leo: Lets you do anything.

Steve: I'm planting my stake here, baby. There's no Copilot anything here. So I'm safe.

Leo: Yeah.

Steve: But this would be a great benefit for many people who just want, I mean, this whole notion of agency coming, that's overall a good thing. We've got a lot of, you know, sharp edges and corners and things to polish off.

Leo: I think it's just going to introduce more exploits. It's not going to get rid of them is my personal feeling.

Steve: Change them, yes.

Leo: Yeah. It's just going to be different, yeah.

Steve: I think...

Leo: Then they'll take advantage of Dave; right?

Steve: I would have a hard time arguing that, Leo. I think you're probably right.

Leo: Yeah, yeah, yeah.

Steve: I think that is the case. Okay. Shanghai, China. Recently, Espressif just responded to the Spanish researchers' backdoor discovery. They wrote: "Recently, some media have reported on a press release initially calling out ESP32 chips for having a 'backdoor.'" And they used air quotes. "Espressif would like to take this opportunity to clarify this matter for our users and partners. Recently, some media have reported on a press release initially calling out ESP32 chips for having a 'backdoor.' Of note is that the original press release by the Tarlogic research team was factually corrected to remove the 'backdoor' designation. However, not all media coverage has been amended to reflect this change."

So they said: "What was found: The functionality found are debug commands included for testing purposes." And that's entirely feasible, by the way. I didn't suggest that when we talked about this; but, yes, that makes absolute sense that you would want to verify that the host controller interface, for example, is able to read and write to main memory as it must for DMA, Direct Memory Access, to function. So the way to do that, have some undocumented commands that cause it to do so, and then check to see whether main memory has been altered as those commands requested in order to verify. So it fits perfectly.

They said: "These debug commands are part of Espressif's implementation of the HCI (Host Controller Interface) protocol used in Bluetooth technology. This protocol is used internally in a product to communicate between Bluetooth layers. Please read our technical blog to learn more." But they said they had five key clarification points. "First, Internal Debug Commands: These commands are meant for use by developers and are not accessible remotely," which is the main point we made when we talked about this. They said: "Having such private commands is not an uncommon practice. Two, No Remote Access: They cannot be triggered by Bluetooth, radio signals, or over the Internet, meaning they do not pose a risk of remote compromise of ESP32 devices. Third, Security Impact: While these debug commands exist, they cannot by themselves pose a security risk to ESP32 chips. Espressif will still provide a software fix to remove these undocumented commands." Which that's news.

Okay. "Fourth, Scope: If ESP32 is used in a standalone application and not connected to a host chip that runs a BLE (Bluetooth Low Energy) host, the aforementioned HCI commands are not exposed, and there is no security threat." And finally, "Five, Affected Chipsets: These commands are present in the ESP32 chips only and are not present in any of the ESP32-C, ESP32-S, and ESP32-H series of chips." So they finished with their commitment, stating - just, like, to put everyone's mind at rest: "Espressif has always prioritized security and is actively working on continuous product security improvements. We have a standard Product Security Incident Response Process with underlying bug bounty program that is active since 2017." Meaning they're state of the art, and like saying we want to know if we make any mistakes.

They said: "This program offers a bug bounty, encouraging researchers to collaborate with us to discover and fix potential issues, enhancing the security of the entire ecosystem." Now, we should note that the guys, the Spaniards at the conference, said that they had contacted Espressif, who had not responded. We don't know the back story there. So okay. Espressif said: "Espressif also extends its gratitude to the security research community for promptly clarifying that the disclosure does not constitute a backdoor. Their responsible disclosures and continued support have been invaluable in helping users accurately assess the security implications and maintain the integrity of their connected devices." And understand this was initially, right, like a big black mark, and oh, China, you know. So it's good that a lot of the community said, uh, wait a minute.

"At the same time," they finish, "we recommend that users rely on official firmware and regularly update it to ensure their products receive the latest security patches. Should you have any questions, please do feel free to contact Espressif's official support channels." So as we know, this is exactly what we concluded from an examination of the location and nature of these so-called "backdoor" commands. The key is that they were never externally accessible. They were simply commands for the internal native Bluetooth HCI controller. And boy, does the idea that they would be for debugging the hardware, like during initial QA, you want to make sure that the controller's working that's able to do these things.

So totally makes sense. And also for doing things like setting the MAC address. Could you use it for spoofing? Ooh, yes. But you can always change the MAC address of this stuff. So, fine, not a big problem. And besides, you can't do it remotely. You have to deliberately do it on the chip using those commands. So that wasn't a problem.

Here's something that is: Eleven Advanced Persistent Threat groups are known to be abusing a Windows zero-day.

Leo: Oh, man. Eleven?

Steve: Eleven. We know them by name. But because what they're doing is not technically leveraging a flaw in Windows, so far, although this was reported to Microsoft by Trend Micro's ZDI, their Zero-Day Initiative, six months ago, last September, Microsoft has declined to address the issue. They're like, let's not. It's like it's what it's supposed to do. It's like, but Microsoft, it's bad. We talked about this at the time because it was, you know, it just a head shaker that in 2024, let alone still today in 2025, Leo, Windows LNK link files are still being exploited. And what's more, despite the fact that the exploitation of this single zero-day vulnerability goes back eight years, Microsoft says "no fixie."

The 11 APT groups operate out of North Korea, Iran, Russia, and China - so, you know, the good guys - none who have recently been behaving as friends of the West. They've all used this zero-day to hide their malicious instructions in LNK files sent to targets, and Trend Micro has discovered nearly 1,000 malicious LNK files which are abusing the technique. Microsoft's response is that it's all working just the way they want it to.

As I said, we covered this before. Recall that there was (and unfortunately still is) a way to format the Fields of the LNK file to essentially "white space pad" the actual content of the LNK field, the target field, so far off to the right that none of it shows up where the user goes to examine the LNK file's properties. So if you right-click and do Properties to look at the LNK file, you don't see anything in the target field. The user won't see that they're going to run EvilMalwareDownloader [.]exe when they click the link. I have a link to Trend Micro's fully detailed report in the show notes for anyone who's interested.

The high-priority takeaway for our listeners is to NEVER click any link that has an apparently empty Target field because the Target field cannot be empty. That field must be non-empty for the link to have any effect. That's the field that tells it what to do. So it makes no sense for the target to ever be blank. Never make the mistake of assuming that a blank field means the entire link is benign just because there's nothing obviously nefarious about it. You know, it's just heavily space-padded in order to move the bad news out where you can't see it. And in fact I think I recall that there was also an exploit where what you would see looked deliberately benign because that was just the left-hand portion of a much longer thing which had a bazillion spaces in it, and then the actual bad news.

So it's even possible to spoof what is in, I mean, Microsoft, as we've seen from time to time, there are some design corners that you can get yourself painted into which just don't have good solutions. And so here's Microsoft basically committed to supporting, you know, LNK files. They can't take them out now. It would break all kinds of stuff in

Windows. So they're stuck with it. But it was a bad idea, back when it was added to Windows 1.0, and it's not gotten any better since. But Leo, half an hour in.

Leo: Yes?

Steve: I think we should talk about what has gotten better since.

Leo: Oh, okay. I think we could do that.

Steve: Then we're going to look at the trouble that Apache Tomcat servers are in.

Leo: Oh, please. Oh, that's bad news. There's got to be some reason for LNK files; right? I mean, people share LNKs or something; right?

Steve: Oh, they're handy. My desktop is covered with them.

Leo: Well, there you go.

Steve: Yeah.

Leo: You can't get rid of them.

Steve: No.

Leo: Steve's desktop is covered with them.

Steve: Can't. Actually, I haven't clicked on any of them in about 12 years, so I'm not really sure what they do.

Leo: Probably shouldn't. I'm thinking at this point you might not want to. That's hysterical. Yeah, yeah, those are the aliases; right?

Steve: Yup.

Leo: Yup, I use them, too. Maybe they should change how they work. That might be a better solution to that than anything.

Steve: Well, one wonders why Microsoft is just saying no, we're not. We're not. We're not - we don't care that you've got, literally, I saw some examples in this Trend Micro link, there are some that are 32K of spaces. How do you defend that, Microsoft?

Leo: What do you need that for? Yeah.

Steve: Yes, how do you defend having something that obviously makes no sense?

Leo: Malicious, yeah.

Steve: Okay. So the API security firm Wallarm (W-A-L-L-A-R-M) posted an announcement last week titled "One PUT Request to Own Tomcat." And they said: "CVE-2025-24813 RCE is in the Wild." They wrote: "A devastating new remote code execution vulnerability, 2025-24813, is now actively exploited in the wild. Attackers need just one PUT API request to take over" - oh, Leo, it's so bad.

Leo: One.

Steve: "...to take over vulnerable Apache Tomcat servers. The exploit, originally published by a Chinese forum user iSee857, is already available online." Okay. So here's what we know: This newly disclosed attack leverages Tomcat's default session persistence mechanism, along with its support for partial PUT requests. Tomcat is Apache's Java web application server that provides a "pure Java" HTTP web server environment in which Java code can run. This new exploit works within this environment and requires just two simple steps. One of the reasons this is so bad is it is so easy to do.

"First, the attacker starts by sending a PUT request to upload" - I should explain. HTTP has a number of, sort of at its base original definition, a number of verbs. There's GET, which is the most commonly used verb ever, which just gets content, gets HTML content from the server. So the client says GET and then provides the path to what page should be gotten and then receives it. POST is another common one where the client is sending some data back. That's what typical forms use. They use POSTs in order to send data back to the server. Another one is HEAD, which says just give me the headers of the page so I can see if it's changed recently, how big it's going to be, you know, I don't want the whole page, I just want the headers. And then, similarly, a final verb, although there's a bunch of others, is PUT, which says here is a file that I want you, HTTP server, to accept from me.

So the attacker starts by sending a PUT request to upload a malicious session file to the server. The payload of that PUT request is a Base64-encoded ysoserial gadget chain that's designed to trigger remote code execution when it's deserialized. You know, like, and we've talked about serialization and deserialization, deserialization being the interpretation phase. This initial PUT request writes a file inside Tomcat's session storage directory, where it stores session state. Because Tomcat automatically saves session data in files, the malicious payload is now stored on disk, just like any other valid session would be, waiting to be deserialized. So the first step essentially causes the Apache Tomcat server to upload and store the attacker's Java attack file. In toto. In whole.

Then, with the session file uploaded, the attacker simply triggers deserialization, that is, the resumption of what Tomcat believes is a stored and saved session, which it has every reason to trust because it thinks, well, I create the session files; right? I'm the one who made these. So now I'm going to reconstitute this previously stored session. The attacker triggers the deserialization of that file by sending a simple GET request providing a JSESSIONID cookie which points to the malicious session. So literally two commands, two simple, well-documented, well-understood, out in the public domain now with proofs of concept floating around. And it happens. Seeing that Session ID, Tomcat dutifully retrieves the stored file, deserializes it, and executes the embedded Java code, which typically grants full remote access to the attacker.

So this is about as horrible as a remote attack can get because it's dead simple to execute, requires no authentication, and very little imagination even. No technical expertise. Lots of proofs of concept are out there. The only technical requirement is that the Tomcat server is using file-based session storage, which is common in many deployments. Also, the use of Base64 encoding allows the exploit to bypass traditional security filters, making detection somewhat more challenging. And of course before you can detect it, you need to know to look for it in the first place.

Wallarm detected the first attack in the early afternoon of March 12th, Central Standard Time, originating from Poland a few days before the first public exploit was released on GitHub. And for anyone who's curious and interested, I've got the GitHub posting from this person who tweeted it, iSee857, with the proof of concept ready to run. The Wallarm folks caution about the future, writing: "While this exploit abuses session storage, the bigger issue is partial PUT handling in Tomcat, which allows uploading practically any file anywhere."

Leo: No.

Steve: Yeah. Just, like, what year are we? We're still doing this? "Attackers will soon start shifting their tactics, uploading malicious JSP files, modifying configurations, and planting backdoors outside of session storage." They said: "This is just the first wave. The reality is that reactive security - waiting for CVEs, adding Web Application Firewall rules, and hoping logs will catch threats - will always be a losing game. CVE-2025-24813 went from disclosure to public exploit in just 30 hours." So a day plus six hours and bang. Now it's happening.

It's not the first time that this has happened. And I'll just note that 30 hours is not time enough for Apache's Tomcat team to get up to speed and patch, let alone test and deploy, what is a critical update, to say nothing of having those updates deployed and actually get servers patched. I mean, this is just too quick to turn around. And of course that's what we're seeing now; right? We've talked about this before. There's a race for exploitation to occur before patches can be deployed.

Leo: It feels like it may be that the disclosure was either too complete, like it gave people too much information, or maybe they should have done it in private first.

Steve: Well, it wasn't - it was certainly not a responsible disclosure. This was posted on a Chinese forum.

Leo: Yeah. Oh, okay. Yeah, that's right, okay.

Steve: And so this, yeah, this was...

Leo: This wasn't a security firm, this was some kid.

Steve: No way was this responsible. And we can't always count on that; right?

Leo: Right.

Steve: It'd be nice if we could, but not everybody says, hey, I need brownie points here, please. You know, this was some, you know, Chinese person, or at least a person posting over on a Chinese forum, saying look what I found. Everybody give this a shot. See if it works. And lo and behold.

Leo: They did.

Steve: Ouch.

Leo: Wow.

Steve: Yeah. NIST's National Vulnerability Database concurs about the severity of this CVE, assigning it the maximum common CVSS severity rating of 9.8 and formally labeling it "CRITICAL." Now, there's a little bit of good news here. The global inventory of these Apache Tomcat servers appears to be somewhere just short of about 19,000 installations. So it's not 19 million. That's good. You know, it's not a huge amount of global exposure. But on the other hand, they are likely to be running within enterprises that would qualify as prime targets. For an enterprise to be running, you know, a Java application server, probably a more substantial organization.

So our takeaway here is the refrain that, yes, security is difficult, and features will almost always come back to bite you in the butt. No matter how you pronounce the ASRock server or the ASRock motherboard.

Leo: I think we've decided it's ASRock now.

Steve: ASRock, yes.

Leo: Yes.

Steve: Good.

Leo: Not ass rock, okay?

Steve: Not ass rock.

Leo: Just be clear.

Steve: Before we leave the topic of really bad remotely exploitable vulnerabilities, I should mention that the firmware security company Eclypsium discovered a remotely exploitable vulnerability in AMI MegaRAC, R-A-C, MegaRAC baseboard management controllers, you know, BMCs. Those are sort of like the pre-boot firmware which allows remote management of servers over the Internet by connecting, typically, you have a reserved NIC, a Network Interface, you know, an Ethernet connection to allow you to manage that server remotely. Well, they found a problem. The vulnerability, which is being tracked as CVE-2024-54085 received a 10/10 severity score. The reason for the maximum score is that the vulnerability allows attackers to bypass authentication and access the baseboard management controller's remote management capabilities.

In other words, you're certainly going to protect this. You sure don't want this thing exposed to the Internet. But over 1,000 devices with these MegaRAC interfaces are currently exposed on the Internet with ASUS, ASRockRack, and HP Enterprise being the major vendors that supplied the machines. So unfortunately over a thousand of these buggy, now known to be vulnerable, baseboard management controllers are publicly accessible, meaning that bad guys are going to say, hey, let's have some fun and bypass authentication. And then you're in, I mean, you can upload firmware, you can change the passwords, you can reboot the systems, you can get up to all kinds of mischief using the BMC port. And not something you ever want to have publicly exposed.

Google purchased Wiz Cloud Security. And we've recently covered some news involving the good work of the cloud security startup "Wiz." And due to the sound of its name I felt the need to spell it, it's W-I-Z, as in Wizard. In case we talk about them in the future, and I imagine that we will be, I wanted to note for the record that they were just acquired by Google in what must have made their venture capital investors very happy since, as I said, this was a startup, and the acquisition was the largest cybersecurity-related acquisition ever. So the size of Google doesn't appear to be shrinking.

Google first attempted to purchase Wiz last year for the measly sum of $23 billion. But that deal fell through, and I imagine there was plenty of disappointment to go around. But Google came back again, this time closing the deal for 32 billion in cash. The deal will need to pass regulatory review, and that might not be such smooth sailing at this point. But I have no real idea. Since I expect we'll be encountering them in the future, just as we do Mandiant, another one of Google's security acquisitions recently, I wanted to mention that. So they are now part of the Google juggernaut.

Leo: Are they like Mandiant? Are they a security research firm? What is it that they do?

Steve: They're a cloud security group. You know, they find things and report things and offer security services, yeah.

Leo: Yeah.

Steve: GSMA is the GSM Association, where GSM stands for the Global System for Mobile, as in communications; right? They made some news Friday, actually it was Friday before last, with their announcement's headline "RCS Encryption: A Leap Towards Secure and Interoperable Messaging." So here's what Tom Van Pelt, the technical director of GSMA, posted. He said: "In my last post [which was] 'RCS Now in iOS,'" he said, "'A New Chapter for Mobile Messaging,'" he said, "I celebrated the integration of Rich Communication Services (RCS) with Apple's iOS 18, a culmination of years of collaboration across mobile operators, device manufacturers, and technology providers." He wrote: "Today I am pleased to announce the next milestone, the availability of new GSMA specifications for RCS that include end-to-end encryption..."

Leo: Hallelujah.

Steve: Yes, "...based on the Messaging Layer Security (MLS) protocol, Messaging Layer Security." He said: "Most notably, the new specifications define how to apply MLS within the context of RCS. These procedures ensure that messages and other content such as files remain confidential and secure as they travel between clients. That means that RCS will be the first large-scale messaging service to support interoperable end-to-end encryption between client implementations from different providers. Together with other unique security features such as SIM-based authentication, end-to-end encryption will provide RCS users with the highest level of privacy and security for stronger protection from scams, fraud and other security and privacy threats.

"These enhancements to support end-to-end encryption are the cornerstone of the new RCS Universal Profile release. In addition to end-to-end encryption, RCS Universal Profile 3 makes it easier for users to engage with businesses over RCS messaging through a richer deep link format and includes additional smaller enhancements such as improved codecs for audio messaging and easier management of subscriptions with business messaging senders. In addition, RCS continues to support a range of interoperable messaging functions between iOS and Android users, such as group messaging, the ability to share high-resolution media, and see read receipts and typing indicators."

He finishes: "I would like to thank all of the contributors for their support in developing and finalizing these new specifications. They represent significant progress in enabling even more of a thriving RCS ecosystem built on the foundation of secure and private messaging for the benefit of end-users worldwide."

Okay, now, I took a brief look at the 90-page specification, and it looks like the right people have been involved. Among other things, I noted that the word "ratchet" appears 20 times in the document. We've discussed the use of ratchets for group messaging key distribution in the past, having first encountered the term when we discussed Moxie Marlinspike's Axolotl Ratchet - actually it was a double ratchet - which he developed along with Trevor Perrin as part of the TextSecure project, which was later rebranded and expanded into what we now know today as the Signal protocol. I guess I would take issue with Tom's characterization of the RCS's MLS as more secure and better and blah blah blah. It's not. It's at parity. But that means it's really, really, really secure. You know?

Leo: It's good. Yeah, yeah.

Steve: It's all you need. It's, you know, it's good as it gets. It's state of the art.

Leo: Good enough for the Department of Defense, it's good enough for me.

Steve: That's right, it's good enough to discuss war planning. So the bottom line is that it appears that the cross-platform RCS multimedia secure messaging protocol, that even Apple now supports as of iOS 18, will be obtaining strong, state-of-the-art, end-to-end, double-ratcheting, Signal-style encryption, and it will be done correctly. So one has to wonder what the UK and the EU will have to say about that.

Leo: A little bit of history, when RCS, the RCS spec came out from the GSM Association, it had no encryption. Google decided encryption had to happen. So their implementation had a Google end-to-end encryption. But because that came from Google, Apple did not implement it. Apple said until there is a standard, we're not going to implement encryption in, you know, Apple Messages has encryption, but not RCS. So that was a problem because Apple users using RCS might have thought, oh, it's encrypted, because it is, if it's Google to Google, but not if it's Apple to Android. So this is a big, a very important improvement, and I do hope Apple moves quickly to implement it because then, I mean, that's the problem right now with SMS, it's not secure.

Steve: Yes. Yes.

Leo: Then we will have on both Android and iOS end-to-end encrypted secure messaging technologies. And that's a big, big improvement. You're right. The EU and the UK are going to hate it, but...

Steve: Yes, they are. I mean, they're going to have a fit.

Leo: Yeah. Because all your text messages will be suddenly encrypted.

Steve: Yeah, I mean, like well-encrypted, where it's been - it's encryption done right, you know, a la Signal and Messenger and everything.

Leo: Although, again, and this is an important lesson that I do hope Pete Hegseth has learned...

Steve: The fact that it's encrypted in flight does not mean that it's encrypted on your phone.

Leo: Not on your phone. And of course I don't know what it'll be like with RCS. But when you use iCloud to back up your Signal messages, they're backed up in the clear. So, you know, that's something you might want to consider, as well; you know? I don't know what they're going to - I will read up on this. I'll be very curious what happens to [crosstalk].

Steve: Well, and I know I have not ever really paid attention to what equipment our presidents receive. But I think they have special phones; don't they? I remember Obama was bitching and moaning about...

Leo: That's right. He had a Blackberry, and he really loved his Blackberry. But he got elected President, and the first thing the Secret Service did is hand him a greatly modified Windows CE phone that Obama hated. He hated it. And he came on, it was on The Tonight Show, bitching about it. But that was a long time ago. When Trump was elected 2016, when he took office in 2017, very famously refused to hand over his iPhone. So it's my guess that they don't give him a Windows CE phone anymore. But that really does raise issues because, you know, if you're using it to communicate super-secret stuff, it's not super secret. Especially with Pegasus out there and, you know, all these other ways the Chinese hackers who are sitting in our phone systems specifically listening to governmental interactions. This is - you should be in a SCIF.

Steve: Well, and again, Leo, there's no way this lesson has not been learned. I mean, they will be...

Leo: Well, they only got caught; remember? They got caught. That's the problem. They've probably been doing this all along. It is a violation of...

Steve: That's why I'm glad. That's why I'm glad they got caught because this...

Leo: But it is a violation. You know, there are going to be hearings because it's a violation of DOD regulations. I'd be really curious, you know, DOD has its own secure messaging technology that they use. And they of course have SCIFs. I'd be very curious. We probably won't be able to learn any details about it.

Steve: I just think it was very convenient, and they just - they didn't understand that they have to have these kinds of communications under really controlled circumstances. Now they understand.

Leo: I'm sure they were told that.

Steve: Probably part of the...

Leo: Part of the briefing.

Steve: Part of the instruction manual that you receive.

Leo: Maybe they slept through that part. I don't know.

Steve: Let's take a break.

Leo: Yes.

Steve: And then we're going to ask - we're going to answer the question, what world are we living in today?

Leo: What timeline are we living in today?

Steve: I don't recognize some parts of this world, Leo.

Leo: I know exactly what you mean. I can't wait to hear what you have to say about that. Steve and I are the old men shouting at the clouds, "Why, I oughta...." Let's talk about our sponsor for this segment.

Steve: Get off my WiFi.

Leo: Get off my WiFi. I'm using it. How dare you put a password on it? I was using your WiFi. Okay. Tell us about this brave new world we're living in, Steve.

Steve: Okay. Now, I want everyone to just listen to and contemplate this sentence, which for me at least begs the question, as I said, what world are we living in today? Here's the sentence that was published as a quick one-liner news blurb in a prestigious security newsletter. It read: "An attacker used malicious Twitter replies to hack an AI crypto chatbot and steal over $105,000 worth of Ether."

Leo: Wow.

Steve: Okay. "An attacker used malicious Twitter replies to hack an AI crypto chatbot and steal over $105,000 worth of Ether."

Leo: Okay. Okay. I have lots of questions.

Steve: I don't even know - I don't even know what that means.

Leo: Yeah, what does that mean?

Steve: First of all, you have to have some malicious Twitter replies, whatever those are. And those malicious replies need to be able to hack an AI crypto chatbot. What? Did those replies hurt the AI crypto chatbot's feelings?

Leo: Aww.

Steve: And what the hell is an AI crypto chatbot anyway?

Leo: It sounds like just a mushed together bunch of words.

Steve: And who in their right mind would give this thing reign over a big pile of Ethereum cryptocurrency?

Leo: You're right.

Steve: What is wrong with people?

Leo: What's going on?

Steve: So, you know, this podcast's listeners know that historically I am more or less bullish on cryptocurrency, at least upon the fundamentals of the technology, which I've understood from the start well enough to code it up myself, if I had to. But what this has all become, Leo, is utterly unrecognizable. It's just insane. Need any tulips, anybody? "An attacker used malicious Twitter replies to hack an AI crypto chatbot and steal" - you know, more credit to them. If you are able to use malicious Twitter replies...

Leo: Right, you're a better man than I am.

Steve: ...and hack an AI crypto chatbot, okay, you earned your money. Wow. You know, maybe I could try knitting. Is that still a thing?

Leo: Yes, it is.

Steve: I don't know. Anyway...

Leo: We still all need socks, Steve.

Steve: Oh, I forgot to mention that the Twitter account that perpetrated the heist or the hack or whatever the hell it was, the guy's Twitter account was "FungusMan."

Leo: Of course it was. Of course.

Steve: Which is just perfect. Just perfect. Okay. So the news on the TikTok U.S. takeover front is that Oracle is the frontrunner at the moment. Politico's reporting about this contained enough interesting techie bits to make it worth sharing here, particularly because there are still lots of technical questions left to be resolved about how it's possible to use TikTok safely, and because it looks like it's going to happen.

So here's what Politico reported. They said: "The software company Oracle is accelerating talks with the White House on a deal to run TikTok, although significant concerns remain about what role the app's Chinese founders will play in its ongoing U.S. operation, you know, like U.S. side operation, according to three people familiar with the discussions." So this was multiply sourced reporting, you know, done right.

"Vice President JD Vance and the national security adviser Mike Waltz, the two officials President Donald Trump has tasked with shepherding a deal to bring TikTok under U.S. ownership, are taking the lead in negotiations, while senators have voiced a desire to be read in on any talks, two people familiar said. A third person described the White House discussions as in advanced stages. The people who were granted anonymity were not authorized to discuss sensitive details of ongoing negotiations publicly.

"It comes amid ongoing warnings from congressional Republicans and other China hawks that any new ownership deal if it keeps TikTok's underlying technology in Chinese hands could be only a surface-level fix to the security concerns that led to last year's sweeping bipartisan ban of the app. Key lawmakers, including concerned Republicans, are bringing in Oracle this week to discuss the possible deal and rising national security concerns, according to four people familiar with the meetings.

"One of the three people familiar with the discussions with Oracle said the deal would essentially require the U.S. government to depend on Oracle to oversee the data of American users" - you know, Oracle obviously being big database people - "and ensure the Chinese government does not have a backdoor into it, a promise the person warned would be impossible to keep. The person told Politico: 'If the Oracle deal moves forward, you still have this algorithm controlled by the Chinese. That means all you're doing is saying trust Oracle to disseminate the data and guarantee there is no backdoor to the data.' If the algorithm isn't entirely rebuilt by its U.S. owner, or if TikTok's Beijing-based parent firm ByteDance retains a role in its operations, it could retain vulnerabilities that could be exploited by the Chinese government." In other words, you know, we need a cleanroom, and how are we going to get to cleanroom status here?

"The data security company HaystackID, which serves as independent security inspectors for TikTok U.S., said in February, last month, that it has found no indications of internal or external malicious activity, nor has it identified any protected U.S. user data that has been shared with China. Spokespeople for Oracle, TikTok, ByteDance, and the White House did not respond to requests for comment. The deal is still billed as a 'Project Texas 2.0,' in a nod to a previous agreement between TikTok and Oracle to relocate American users' data to servers based in Texas and block ByteDance employees in China from having any access to it, according to the first person. But that agreement, which also required Oracle to review TikTok's source code to determine its safety, failed to assuage congressional and Biden administration concerns that the app is being used by China as a spying and propaganda tool.

"The tech-focused outlet The Information reported Thursday that Oracle is a 'leading contender' to run TikTok, with ByteDance preferring it for the role. The details about the White House's approach and the seriousness with which White House officials are considering the proposal have not yet previously been reported. It comes as Trump stares down an April 5th deadline to secure a new owner for the Chinese video-sharing company after he signed an executive order in January delaying enforcement of Congress's ban on the app for 75 days. The app briefly went dark for about 12 hours in January after TikTok's parent company ByteDance failed to meet the deadline to sell its stake, and the Supreme Court upheld the congressional ban.

"JD Vance, during an interview with NBC News on Friday, said he was hopeful a TikTok deal would be reached by the early April deadline. Last week, Trump said that his administration was in talks with 'four different groups' about a deal. Trump told reporters in January that he was open to Oracle founder and executive chairman Larry Ellison buying TikTok. Ellison is a longtime Trump supporter, and he's part of the so-called Project Stargate, a 500 billion AI infrastructure initiative that also operates OpenAI, SoftBank, and MGX.

"While Trump during his first administration sought to ban TikTok over national security concerns, he embraced the app last year on the campaign trail. In December, he told throngs of young conservative supporters at a Turning Point rally in Phoenix that he has 'a warm spot in my heart for TikTok,' he said, because of the outpouring of support he received from younger voters in the 2024 election. It's unclear whether the deal the White House eventually reaches will satisfy China hawks on the Hill, though they may have little power to complain. Trump's executive order extending the initial deadline, in the face of concerns from GOP lawmakers and legal experts about the order's legality, showed his willingness to defy congressional will. And the decision on whether ByteDance sells TikTok or licenses its use by a U.S. company ultimately rests with the Chinese government.

"Beijing wants to protect TikTok's monopoly access to its user data and is hostile to any suggestion that Chinese firms bend to the will of suspicious foreign governments. Over the past year, authorities in Beijing and in the Chinese embassy in Washington have mostly dodged questions about the status of possible talks for the purchase of TikTok by a non-Chinese firm.

"What little Beijing has said about that possibility hasn't offered much hope that it's in favor of such an agreement. The Chinese government 'will firmly oppose,'" is their direct quote, "any forced sale of the company and require ByteDance 'to seek governmental approval in accordance with Chinese regulations' for any potential foreign ownership deal, a Chinese Commerce Ministry spokesman told reporters in March. That same month, a Chinese Foreign Ministry spokesperson accused Congress of 'resorting to hegemonic moves' to try to take control of the app. In January, the Chinese government deployed more conciliatory language about a possible TikTok sale, but offered no clues on whether it would approve such a deal. Any such transactions 'should be independently decided by companies in accordance with market principles,' a Chinese Foreign Ministry spokesperson said in January."

So Leo, I guess the question is whether China would rather lose the U.S. market or compromise. You know? Bifurcate TikTok, if that's what it comes to.

Leo: It seems like, to be honest, this is the least of our worries. I mean, what are we worried about TikTok for? They have Chinese hackers in our phone system that we will never eradicate.

Steve: Because we're unwilling to upgrade our routers, our Juniper routers.

Leo: Yeah. We have hundreds of unregulated data brokers in this country who are selling your personal information to China completely legally. And we're not willing to do anything about it. China has disinformation...

Steve: And there's no evidence that TikTok ever misbehaved.

Leo: Right. But even if it does, they don't need it to. They already use Twitter and Facebook and every social network for disinformation. I mean, honestly, at this point, either way, I don't care what happens to TikTok.

Steve: And it might well be that a little bit of a dance is done here, that Oracle is, you know, is allowed to bless this, and we just could have let this all stay the way it is and not worry about it any further.

Leo: This is the problem with corruption is at some point you just throw up your hands and say, I give up. It's just more corruption. You know, Larry Ellison, you even said it, is a big donor to the President. The President saved TikTok after wanting to delete it, by the way, because Jeff Yass, who's another giant Republican donor, owns 30% of it. It's just crony capitalism of the worst kind. And I no longer can be bothered. They win. They win.

Steve: Well, we're about technology here.

Leo: We have other big problems to worry about.

Steve: Yeah, yeah.

Leo: And you have a few of them coming up.

Steve: And one is...

Leo: Yes.

Steve: Two days ago, day before yesterday, on Sunday, March 23rd, the original personal genomics company 23andMe filed for protection under Chapter 11 of the Bankruptcy Act. Their press release had the headline "23andMe Initiates Voluntary Chapter 11 Process to Maximize Stakeholder Value Through Court-Supervised Sale Process." Now, I'm mentioning this here from a personal privacy standpoint because now might be a good time for anyone worried about the future of any of their genetic data being held by 23andMe to delete it from 23andMe's databases and to close their account. As a founding member of 23andMe, I just did exactly that. I have a picture in the show notes of the little popup that I received saying "Your data is being deleted. We've received your confirmation to delete your data, and we're in the process of deleting your data. Your account will no longer be accessible and will be deleted per your request. For any further assistance, contact Customer Care."

Since it took me some poking around their website, I recorded the process to make it easier for anyone who might wish to do the same. You know, I spit in their test tube long ago, and I'm not in a panic about it. But given that they're going under, and someone I don't know will be purchasing their assets for pennies on the dollar, leaving my genetic data behind in their database seems unlikely to do me any good at this point.

So I logged in, selected "Settings" under that shadow head and shoulders icon in the upper right of the page. Once that page came up - which I thought it was interesting. It took a while. I've not used their site a lot, so I don't know if it's always been slow. Maybe there's just a lot of people doing this at the moment.

Leo: I suspect that's the case.

Steve: So I may have not been alone, yeah. So then scroll to the very bottom of the page, after you click on Settings under there, and that page finally comes up. Go to the very bottom, under the "23andMe Data" section. Then click the View button. Now, when I did that I noted that the View page has a clean- looking URL. There's no subscriber-specific gobbledygook in the URL. So it looks like it takes you directly to the page. It's you.23andme.com/user/edit/records. Alternatively, I wanted to make that easier for people. So after logging in, you could just use the GRC shortcut link I created to jump directly to the sayonara page. It's grc.sc/byebye.

Leo: Good.

Steve: B-Y-E-B-Y-E.

Leo: But you have to be logged in for that to do anything.

Steve: You've got to, yeah, log in first. And after you're logged in at 23andMe, grc.sc/byebye.

Leo: Did you download your genome before you deleted the data? Or do you care?

Steve: You know, I selected all those things to download everything.

Leo: Yeah. But what are you going to do with it?

Steve: Well, exactly. Well, exactly. Because I've got plenty of saliva for the future. So I'm generating it, you know, with great alacrity. So it's not a problem. It takes time for them to get the data to you. They said, okay, we've received, I mean, I checked all those things, and I queued myself up. And it said: "Once we get your data assembled, we'll send you a link in your registered email, and then you click on that in order to get it." And I just thought, screw it. I don't care. Get me out of here.

Leo: Yeah.

Steve: So, you know, I just deleted all my data and my account before I had a chance to receive any of that. So you can. They will send you all your reports. You're able to download your raw genetic data in its entirety, you know, your entire DNA readout. And so you could wait for that and then delete your data. But I just figured, you know, if I need to spit in a tube somewhere else, I'll do that.

Leo: Actually, I actually have done it elsewhere. One of the things, one of the issues with 23andMe is it doesn't actually do a full genome. It does a weird like statistical analysis of a small part of your genome. I had the father of modern genomics on Triangulation a couple years ago, George Church. And he has his own company, Nebula Genomics. It's more expensive than 23andMe, but it's the full genome. And you can download it, it's gigabytes of data, and then send it off to - there are many companies now springing up, saying oh, we'll analyze, if you have your genome, we can analyze it for, you know, certain diseases and so forth.

Steve: Yes. My sense is this is only going to get better with time.

Leo: Exactly, yeah.

Steve: And, you know, and I'm carrying my genome around with me.

Leo: You got it.

Steve: I'm not in any danger of...

Leo: Plenty of spit.

Steve: ...losing it.

Leo: Yeah.

Steve: So, you know.

Leo: I'm trying to remember if Nebula did - I think it did spit, as well. Some do a cheek swab, but this did spit, as well. And it took a while, but it was - it's a very - it was like a thousand bucks. It wasn't cheap. But it is the complete genome, which is, you know, still not that useful, but maybe someday. I don't know. I guess I'll delete my 23andMe stuff.

Steve: Well, and I know there are people that are big on it. I think that it tells you something about some various propensities that you might have.

Leo: Right.

Steve: But, you know, [crosstalk].

Leo: I found a number of long-lost third cousins, things like that.

Steve: Actually I had one of my high school buddies, who I mentioned I'm still in touch with, he knew that he was adopted, but it turns out that his birth parents were far more prolific than he ever knew. And he's found a huge extended family.

Leo: Oh, that's cool.

Steve: I mean, he's reconnected with them all, and he visits them, and, I mean, it's transformed his life.

Leo: Yes.

Steve: That he was able to find all of these other siblings that he never knew he had.

Leo: The same thing happened to Jennifer. And I think it was through 23andMe. She met a long-lost cousin, explained that they shared a grandparent, and they just had a family reunion for Thanksgiving where he and his family came out, because he was adopted, same story, and his long-lost family, and they all - I think that's wonderful; right?

Steve: Yup.

Leo: That's an amazing thing.

Steve: Yeah. Paul connected it through AncestryDNA.

Leo: Yeah.

Steve: And then that allowed him to link up with other people that he never knew he had.

Leo: So it does do something, yeah, yeah.

Steve: Yeah. Very cool. Okay. So finally in some good news for cybersecurity professionals, the White House administration has reportedly told federal agencies to please avoid firing any cyber guys.

Leo: We can't figure out if we need them or not, so...

Steve: Actually today they probably think they need them more than they did yesterday, so that's good.

Leo: Yeah.

Steve: And here's part of what Reuters wrote under their headline "White House instructs agencies to avoid firing cybersecurity staff." They wrote: "According to an email seen by Reuters, the White House is urging federal agencies to refrain from laying off their cybersecurity teams, as they scramble to comply with a Thursday deadline to submit mass layoff plans to slash their budgets. Greg Barbaccia, the United States Federal Chief Information Officer, sent the message Wednesday in response to questions about whether cybersecurity employees' work is national security-related, and therefore exempt from layoffs. He wrote an email to information technology employees across the federal government which has not been previously reported. He said: 'We believe cybersecurity is national security, and we encourage department-level Chief Information Officers to consider this when reviewing their organizations.'

"Describing 'skilled cyber security professionals' as playing 'a vital role in mission delivery and information assurance,' he said: 'We are confident federal agencies will be able to identify efficiencies across their non-cyber mission areas without negatively affecting their agencies' cyber posture.'" Which I guess means fire any of the non-cyber people you need to, but keep the cyber guys because we want to keep them.

So, you know, as part of the downsizing that Trump and Musk have controversially been engaged in recently, CISA had more than 130 positions cut. We've talked so much about CISA, more and more often for the past few years since they've objectively been doing an astonishingly good job, which is more than unusual for anything within the government bureaucracy. I certainly never expected CISA to amount to what it has. So I've been hoping that CISA would survive and remain as highly functional as they have been. And to that end there was some recent news that those jobs were being reinstated. So that's reassuring. We need CISA. They've really been implementing some terrific policies and creating needed requirements for the cybersecurity of federal agencies, and setting policies that the CIOs are able to use when having, you know, that difficult conversation with the CFO about, you know, the money that they're going to need to keep their enterprises secure. So, yay.

Oh, god, I love this one. The bit of news was "AI project failure rates are on the rise." It was an interesting piece that I saw in Cybersecurity Dive which caught my eye. It was a report that said that AI project failure rates were on the rise, which I thought was interesting. It suggests that just slapping a "Now even more better with AI!" label on anything and everything may not always produce a win. My guess, though, about the reason for failure rates rising is mostly the explosion in all of those labels having been hastily added. Still, it was interesting that, according to a report from S&P's Global Market Intelligence, based upon a survey of more than 1,000 responding enterprises across North America and Europe, the share of businesses scrapping most of their AI initiatives increased to 42% this year, up from 17% last year. Again, I'm sure largely this is because so many more were trying.

The average organization scrapped 46% of AI proofs of concept before they even reached production. 46%, so nearly half, were like, let's try this. It's like, okay, that didn't work. Just forget about it. The surveyed enterprises cited cost, data privacy, and security risks - yay - as the top obstacles. I wonder whether they heard any news about that AI crypto chatbot? Anyway, at this point AI adoption is predominantly being found within IT operations, followed by customer experience workflows, you know, like your little AI thing that comes in the lower right corner and says, "Need me to help you?" "Need any help?" And also marketing processes. So it appears that the initial "AI Everywhere" euphoria is quickly coming back down to earth and closer to reality. I'm sure not letting any of it get anywhere near SpinRite, that's for sure.

Speaking of which, in a piece of listener feedback, Ken wrote, saying: "Hi, Steve. Ken here, 65 years old, Canadian trucker for 40 years." He said: "I just wanted to say thank you for your dedication and enthusiasm in the tech world and the beautiful things you have contributed to tech. I just bought SpinRite recently, and it's a total game changer. I ran it on my current machine, and it tuned up my SSDs like crazy. Amazing software, thank you. I build computers and repair them, and recently a buddy of mine dropped off an old Windows 7 machine that was in a closet for seven years. He wanted the old pictures from it, of course. I managed to get it to boot and got all his old pics and transferred them to a new rig I had ready to go. I ran SpinRite, of course, and now that old beast runs like a champ."

So thank you for your report, Ken. The best thing about SpinRite, for me, is aside from it being the miracle that has largely provided for my life, I get to hear about how much its use helps people, and really nothing beats that.

Tom wrote: "Hi, Steve. Now that uBlock Origin is no longer supported in Chrome, I'm going to start using Firefox. I've exported my bookmarks from Chrome to Firefox, but I'll likely be using both browsers, at least for the time being. Do you know of any browser extension that mirrors favorites between Chrome and Firefox? If I make a change to any bookmarks while I'm using Chrome, I'd like for those changes to sync to my Chrome" - wait. While I'm using Chrome - to my Chrome - so he meant, you know, from Firefox to

Chrome, make a change in either browser, like to have them sync over to the other. "Thanks, Tom."

So that's a terrific question. I suppose for my part I've become so accustomed to only using a single browser platform at a time, and just assumed that each would have its own native and closed ecosystem, that I never considered wanting or needing cross-platform synchronization. But spurred by Tom's question, I poked around and found a very nice-looking third-party cross-platform extension for both Chrome and Firefox, as well as for Android. It's called "xBrowserSync," S-Y-N-C, and it's www.xbrowsersync.org. And, boy, these guys sure are saying all the right things.

Here's like a little snippet from their site that says: "xBrowserSync," as in cross-browser sync, "is a free and open-source" - so there it is, open source - "alternative to browser syncing tools offered by companies like Google, Firefox, Opera, and others. The project was born out of a concern for the over-reliance on services provided by big tech, who collect as much personal data as they can and have demonstrated that they do not respect their user's privacy. Now, with the proliferation of open-source code and projects, it's easier than ever to create tools and services that allow users to take back control of their data.

"xBrowserSync respects your privacy and gives you complete anonymity. No sign-up is required, and no personal data is ever collected. To start syncing, simply download xBrowserSync for your desktop browser or mobile platform, enter an encryption password, and click Create New Sync. You'll receive an anonymous sync ID which identifies your data and can be used to access your data on other browsers and devices. xBrowserSync does not only sync, but also enhances your productivity by enriching your native browser bookmarks with the addition of descriptions and tags, and an intuitive search interface enables you to find, modify, and share bookmarks quickly and easily. xBrowserSync even adds descriptions and tags to new bookmarks for you automatically. And you don't ever worry about losing your data thanks to the included backup and restore functionality.

"The xBrowserSync desktop browser web extension syncs your browser data between desktop browsers. It works with the browser's native bookmarking features so you can keep using the native tools whilst always staying in sync. If you like to organize your bookmarks into folders, don't worry. xBrowserSync respects your bookmark hierarchy and syncs it across your browsers." So, wow, that sure sounds like exactly what Tom is looking for, and it's from folks who clearly share the spirit and philosophy we'd like them to have. After reading Tom's note and running across that xBrowserSync extension, I sent this all back to Tom.

Not long after that he replied: "Thanks, Steve. I will look into this a bit more. But when I clicked to download for Chrome, I'm taken to the Chrome Web Store which shows: 'This extension is no longer available because it does not follow best practices for Chrome extensions.' Thanks, Tom," he said.

Okay. So that sure sounds like the Chrome folks don't like the whole idea of cross-platform browser synchronization. On the other hand, I tried it, and it worked for me. And as I said, I sent these notes out in the late afternoon yesterday, and I've already had feedback from a bunch of our listeners who are using it, and it is working for them. So I don't know what Tom hit. Maybe it was a temporary snag. I can't explain it. But for what it's worth, I've already had feedback from our listeners who have said this thing is great, and it works. So Tom, I hope you can get it working. Maybe just try again. Maybe there was something stored in a cache or who knows what that caused some trouble. Okay.

Leo: On we go.

Steve: Someone whose handle is BackGhost said: "I found your comments on the state of vendor support for old and outdated hardware intriguing, and wanted to add more insight into what is a very complex issue, as I work for a service provider that is also a manufacturer of networking gear, and often see both sides of the issue." So this is somebody, you know, on that side, on the industry side.

He wrote: "Hardware manufacturers deal with the same software and hardware End of Life/End of Support" - EOL/EOS he abbreviated - "issues as customers, just at a micro level. Every ASIC/CPU/IC has a lifetime, and its own software with a lifetime. When vendors have to support more products from a software and hardware standpoint, it costs the vendor more. The vendor can and often does charge more for this support of old gear, but at some point the cost of support will outweigh the cost that could be charged to a shrinking set of customers. Vendors will often discount or offer trade-ins for old gear to encourage customers to upgrade to new gear.

"Luckily, the vendors (well, the big iron guys) will give advance notices of EOL/EOS, and have the sales team always eager to engage the customer on new sales opportunities. As service providers we struggle with the never-ending notices of End of Life/End of Service of gear and will often have to fight for capital to do upgrades or replacements. These efforts will be taken on based on business objectives, risk, et cetera, and leads to the never-ending dance between the CTO, CFO, sales, and product development."

He said: "The service provider side: Hardware manufacturers will always EOL equipment and often give notice well in advance. Larger companies that sell 'big iron' will give notice years out. For example, Juniper, off the top of my head, provides three years for hardware support and one to two years on software support after the hardware is no longer supported for replacement support. So there's normally plenty of time for planning for obsolescence and replacement. Of course, these replacement plans are driven by business goals, which leads to point two.

"The CIO/CFO battles" - which of course this is what he's talking about that I talked about last week when I made up that dialogue between the CIO and the CFO, you know, and their competing priorities. "The CIO/CFO battles are the norm, and this battle is complex at best. Do we update now, later, never? Do we roll the dice? Are we doing a new build somewhere else that has our focus? These are endless. Just to say it's complex. The other side of this equation is the hardware manufacturer side, and this is what drove me to send this feedback.

"On the Hardware support side we've got discrete components (IC, chips, et cetera) can no longer be sourced. Discrete component replacement causes board redesign, and the cost of redesign is too high. Discrete component software support is End of Life due to the manufacturer End of Life of the IC. The IC, you know, Integrated Circuit library is no longer supported due to End of Life on the software support. The new replacement product is just cheaper, better, faster. Why keep the old one around, given its install base?" He says: "This is too complex, often political. You don't want to upset a long-time big customer with a hardware upgrade." Whatever.

"And on the Software support side, for example, see the issue with hardware support ICs, as this is part of the software chain. OS and supporting software no longer supported by vendors. New or upgraded replacement hardware uses different software for various reasons and thus is not compatible with the old hardware. This causes a complete new software support, development, and test chain. The cost of support is higher than the customer can sustain and can drive the customer to find other solutions.

Like the hardware side, this is complex and often political. Software licensing has a lifetime, limited in volume, developer seats, et cetera, that forces an EOL action."

Yeah. So obviously lots of things to consider. I thought this person's comments were worth sharing. For one thing, I would never expect ongoing hardware support for any device beyond the manufacturer's original commitment. If it might be available, okay, fine. You know, things like power supplies can often be somewhat generic and might be easily replaceable. But I get it that, like, if a circuit board dies, and the components are no longer available, then the thing's died. But if, for example, a port dies on an expensive router or on a switch that is out of warranty, then the calculus from my perspective is entirely different, and the conversation with the CFO is then very different. It's "The mission critical device just died. We're currently limping along, and we need it replaced ASAP."

You know, that's not the conversation that I hypothesized last week. I do really understand that maintaining old software has a decidedly non-zero cost. But the point I was making last week was that it felt like revenue was being left on the table. The manufacturer hopes, the vendor of the equipment hopes that a lack of ongoing support will force their customers to move to newer equipment because the vendor understands the security risk of not having security updates to old hardware. That's where the gap is. The customer doesn't quite understand the security implications. So their tradeoff is different. The reality is, most of those devices will remain out of warranty and out of support and will suffer the potential consequences from the security side. But great conversation and dialogue, and one that CIOs and CFOs should be having.

Dan Linder said: "Hi, Steve. In Security Now! Episode 1017 you made a comment about a Juniper router being unsupported and vulnerable, and then a hypothetical conversation between a CIO and CFO about replacing that otherwise hardware just because it was out of support. I, too, have some experience with U.S. Department of Defense rules. And one thing I haven't heard you discuss on the show are the STIG documents. STIG stands for 'Security Technical Implementation Guide.'" And of course you haven't heard me talk about them because I've never been in government, and hope to never be. I'm sure at this point there's no danger of that happening.

He said: "The STIG document is a series of checks or control and actions to take on a specific system that can harden it to some degree to mitigate threats to its overall security." So, okay, that sounds great. "Each control is given a category 1, 2, or 3 rating, with 'Cat-1' being the most important controls to implement. Within each control there are some check text steps and corresponding fix text steps" - which is why I'm glad I'm not in the government, no - "which list a simple command or action to take to validate that the control is in place; and, if not, what can be done to enable it." Okay, now, all seriousness, that sounds great because it's a check, you know, it's a checklist. It's like these things you have to do, and this is how you do them, and this is how you check that they're done.

He said: "While the STIGs give a specific fixed text to implement, most security organizations that review the application of these STIG controls allow for additional external controls that will mitigate a specific problem if it can't be addressed with the fix text suggested. For instance, if an insecure system is being used, but it is only used in an air-gapped environment, only accessible by a small number of people already vetted and trusted, they might well be willing to overlook a Cat-1 finding.

"In all the STIGs I have worked with" - and Dan, I'm glad you've maintained your sanity - "they all have a security question which requires confirmation that the system being secured can still receive updates from the manufacturer. If the company in your example was applying and enforcing the STIGS as written, then the CIO has quite a bit of leverage to go back to the CFO to get this system replaced." Yay. And that's why I want CISA to stay whole and functioning. He said: "I hope you can find time in a future episode to give a brief talk about the STIG documentation" - no, Dan, don't hold your breath - "and some of the potential" - please don't make me do that - "for securing anyone's environment regardless of government affiliation." Whew. Well, Dan, I'm glad you're there, and I'm glad you're following the STIGs to the letter.

Leo: Maybe that's why they use Signal, because they just couldn't bear to read the STIG.

Steve: Wow. And get in a SCIF, and then row, row, row your boat down whatever it is they do in the SCIF.

Leo: Oh, my.

Steve: Wow, yeah. Okay.

Leo: All right. Security Now! continues on. It is time to examine The Quantum Threat.

Steve: I think people are going to be surprised and interested by this. I really liked what HP had to share. We love showing up for this podcast every week, which, after all, Leo, we've been doing for nearly 20 years.

Leo: Whoo.

Steve: And as much as I would dearly love to be, I doubt we'll still be here the day a quantum computer first cracks actual, working-strength, public key encryption.

Leo: Oh. I was hoping it would open my wallet for me. But I guess if I'm dead it doesn't really matter.

Steve: Boy.

Leo: I'll leave it to the kids.

Steve: Actually, I don't know if your password is protected by public key. It's probably private key. It's probably just a password.

Leo: Just a password, yeah.

Steve: That generates a symmetric key, in which case you're still going to be locked up tight, even...

Leo: Thanks, Dad. You left me something completely useless.

Steve: But you could give the wallet to Hank. And, you know, in time...

Leo: Maybe in his lifetime.

Steve: That's right. Although he's doing so well with that salt. By the way, you know, we use the crap out of that stuff. Oh, my god, it is our...

Leo: It's good; isn't it?

Steve: It is our go-to present for our friends. We bought 20 bottles of the, what was it, it was the...

Leo: The flaky essential? With the garlic...

Steve: Truffle. The garlic truffle salt, yes.

Leo: The truffle salt is really good on popcorn and stuff.

Steve: Oh. Or a little bit on some filet, it makes a really nice...

Leo: Yes, it's excellent on a steak.

Steve: Yeah, yeah, yeah, we use it on steak.

Leo: You know, he's opening, in the next few months, a sandwich store in New York City. We should make a...

Steve: Hank?

Leo: Yeah. It's be Salt Hank's - it's on Bleecker Street, next to John's. Salt Hank's Sandwich Store.

Steve: Wow.

Leo: We'll go get a delicious juicy sandwich there.

Steve: Well, good for him. Good for him.

Leo: He'll probably be selling the salt. And now he does pickles, too, by the way. I only mention that because I am an investor in the pickle business.

Steve: Well, this was an unsolicited...

Leo: Thank you.

Steve: ...commercial. I mean, it's the truth. We use the truffle garlic salt. It's like our - we got 20 bottles. He was sold out for a long time.

Leo: Yeah, yeah.

Steve: And then it came back in stock.

Leo: I did the - it's funny that you did that. I did the same thing. I bought a case, yeah.

Steve: Yeah.

Leo: He - one last thing, though. To his credit, he made it on his own. He never used my last name. Nobody knew who he was. He didn't go - he didn't, you know, somehow ride my coattails. He did this all on his own. I'm very proud of him.

Steve: I've seen his TikTok stuff. It's astonishing.

Leo: It's good; isn't it?

Steve: He's got the gift.

Leo: Yeah, yeah.

Steve: Yeah, he's got it. Anyway, through the years of this podcast, we've all become students of the history of computer security. And one lesson we've all learned together is just how very, very long it's going to take to wash all of the old pre-quantum crypto out of our existing systems. Everything we have now is pre-quantum crypto. We know that there are a couple messaging systems that are mixing pre and post. That's good. That all leads to the simple and incontrovertible conclusion that there's no time like the present to begin.

Last Tuesday, Hewlett-Packard's "Threat Research" group posted a terrific piece called "From False Alarms to Real Threats: Protecting Cryptography Against Quantum." That's what I want to share today. In their opening, they make some great points that are well worth appreciating. They wrote: "Quantum computers could break asymmetric cryptography, which would be catastrophic for society's digital infrastructure." I mean, and truer words have never been written.

"Quantum computers powerful enough to break cryptography do not exist today, but the threat of one being created steadily advanced in 2024." So they're talking about last year, of course. "With multiple quantum computing technologies overcoming development obstacles, the security community is now more sure than ever that sufficiently powerful quantum computers will come. Some think it could be ten years; but with the speed of recent innovation, an unexpected breakthrough could accelerate that. This has created a significant security risk because we rely on protections for a long time and need them in place before threats arise.

"Since we last wrote on this topic a year ago, authorities around the world have increased efforts to urge organizations to start migrating systems to quantum-resistant cryptography. Critical industries are especially advised to mitigate these quantum risks given they are high-profile targets. Particular priorities for migration include sensitive data vulnerable to capture-and-decrypt attacks, and protections rooted in hardware." That's a key, "protections rooted in hardware." Without upgraded protections at the hardware and firmware foundation, quantum attackers can compromise devices even if the software running on the hardware is quantum-resistant.

"2024 also saw several false alarms of quantum breaks to cryptography. We expect that" - that is, false alarms - "to become a trend as innovation in quantum computing progresses. What we have seen is that such false alarms will elicit panic from some, but only complacency from others. But they also proved useful in raising the conversation about readiness and an understanding of the consequences of a real alarm. In short, we must stay vigilant and prepare for the real threat.

"Over the last year, we at HP also made progress to protect customers from the threat of cryptography being broken by quantum computers. Last year we announced the world's first business PCs to provide firmware integrity against quantum computer attacks. Today, we are announcing the world's first printers to protect firmware integrity against quantum computer attacks. These security innovations demonstrate our dedication to safeguarding our customers against future threats."

They then quoted Boris Balacheff, the head of the HP Security Lab, an HP Fellow and Chief Technologist for Security Research and Innovation. Boris said: "As innovation progresses toward more powerful quantum computers, it is urgent to prepare for the threat this represents to the asymmetric cryptography we depend on in our daily digital lives. This starts with migrating systems that cannot be updated easily once deployed. After the introduction of quantum-resistant firmware integrity protection in PCs last year, today we are announcing the launch of printers with similar capability to protect against future quantum computing threats. We continue with our commitment to lead the way with endpoint security innovation, and keep our customers safe into the future."

Now, this is not something we've focused upon or talked about previously. And of course they're correct. As we know, all of the secure booting technology we have today is based upon the motherboard's firmware being able to verify the digital signatures of the software that the motherboard's UEFI firmware first loads. And all of that secure boot technology is currently pre-quantum. It's embedded into the hardware with technologies such as the TPM, the Trusted Platform Module, that dates from 2003.

Listening to what HP has to say here really serves, I think, to put a much finer point on this looming issue. I've edited the piece which follows to remove HP's non-technical self-promotion - there was a lot of it in here - and for its length because it went on longer than it needed to. But there's a great deal of information here still. I want to share it.

They wrote: "In the past 12 months, the cryptography and security community has experienced heightening concern over the progress of quantum computing. The last year has been marked by key developments in quantum computing technology, as well as multiple instances of false alarms over potential quantum breakthroughs that put cryptography at risk. Although these alarms were ultimately disproven, when considered alongside genuine advancements in quantum computing, they highlighted the fragility of society's digital infrastructure. A sufficiently powerful quantum computer could break much of the cryptography relied upon globally. Given how fundamental cryptography is to security everywhere, a quantum computing breakthrough before the world is ready would jeopardize security. It could allow attackers to run riot across our digital infrastructure, giving them freedom to access network services, take over devices, steal blockchain assets, decrypt sensitive data, and more.

"In reaction to these advances, there has been an increased sense of urgency to fortify cryptography, driven by technical authorities and experts. This urgency has led to accelerated timelines and new policies to address the looming quantum threat. Against this backdrop, the security community has intensified its preparations. Academia, standards bodies, governments, and industry are collaborating and making concerted efforts to migrate technologies to being quantum-resistant.

"In this blog post, we discuss two false alarms that percolated through the community over the last year, and what we learned from them. We explore the current state of the quantum computing threat to cryptography and how the community is preparing a response.

"The first alarm took place in April of 2024 during the NIST 5th PQC (Post Quantum Computing) standardization conference, which had convened to discuss cryptography designed to withstand quantum computer attacks. The trigger for the alarm was an academic paper, newly published and not yet reviewed or corroborated, describing a new quantum computer attack that could have been effective at breaking the new post-quantum cryptography the technical community had been working on for almost a decade. This cryptography was meant to become a global standard to protect digital infrastructure, should quantum computers break traditional asymmetric cryptography like RSA and most Elliptic Curve Cryptography.

So they said: "A claim it was broken was shocking and would leave the quantum-resistant migration in disarray, if confirmed true. Speculation about the paper, entitled 'Quantum Algorithm for Solving Lattice-Based Cryptosystems,' lit up our technical social media networks. One of our team was at the conference. While the talks continued and the audience listened attentively, attendees gradually started to form small huddles, trying to make sense of the publication. Remarkably, no one was sure the paper was incorrect. Most hoped it probably was incorrect, but at face value it was convincing, presenting a credible nine-step algorithm that put quantum-resistant lattice-based cryptography in a very precarious position.

"For eight days, there was furious analysis among cryptographers and quantum computation experts. With very few people claiming to be experts in both fields, many researchers wrestled with analysis beyond their areas of expertise. A Discord community sprang up, crowd-sourcing a comprehensive analysis and triage of the paper's claims. This intense assessment-phase ended when two researchers found an inconsistency in the final step of the nine-step algorithm. The paper's author engaged with this critique and confirmed the final step had an irreconcilable error.

"And thus the community breathed again. But for an entire week, the community responsible for developing the cryptography that will protect much of our digital lives into the future had seriously considered the possibility that they had got it wrong. Because this was so technical and didn't impact the cryptography we currently use, the news didn't make the broader security community panic. And the doubt didn't last long enough within the cryptography technical community to gain momentum and spread." And of course our podcast listeners may recall that we did touch on the fact of this having happened at the time. We will keep you in the loop.

HP continues: "The second moment of 2024 when the broader security community thought that cryptography was broken was also triggered by an academic paper. The paper, 'Quantum Annealing Public Key Cryptographic Attack Algorithm Based on D-Wave Advantage,' was published in May of 2024 in the Chinese Journal of Computing. This false alarm caused more widespread uncertainty and panic within the technical community and beyond, with several reports stating incorrectly that some researchers were able to break RSA encryption using a D-Wave Advantage quantum computer." And, again, that news made it into this podcast because it would be difficult to overstate just what havoc would ensue if that were to be true.

HP wrote: "With a general audience unable to assess the original paper (only the abstract was published in English), the reports generated real anxiety. However, there was little credibility in the claim that RSA had been broken, and expert consensus rapidly emerged. With a bit of scrutiny, it was established that the researchers had only broken a very small-scale, simplified RSA, and their solution did not scale to the kind of numbers used for security and was therefore not a credible threat. Again, after a week or so, concerns about pre-quantum cryptography having been broken were largely quelled. However, for several months afterwards, incorrect reports still appeared, sparking fresh waves of concern among those who had missed the initial reporting.

"One benefit of these events is that they test the security community's preparedness for the sudden removal of some fundamental underlying cryptographic primitive. From that perspective, these alarms have been like the safety briefing before an airplane flight, forcing the community to grapple with what to do in the worst-case scenario. If the event were real, are we ready? What preparations should be in place, and are they?

"The fact that a broad audience was alarmed tells us that there is a growing understanding of the critical impact of the quantum threat, and that action will increasingly be called for. The successful resolution of these incidents underscores the importance of a measured and collaborative approach to evaluating cryptographic research, for the community has shown it can be relied upon to robustly evaluate these complicated ideas. Unfortunately, analyzing such academic papers is inherently complex, requiring expertise that is rarefied and spans multiple fields - cryptography, mathematics, quantum algorithms, quantum computer engineering, and physics. So we should anticipate regular moments of doubt in the security of our cryptography and have the patience to wait for assessment before panic-induced reactions.

"One day, there could be surprise news, or even a significant rumor, of a real breakthrough. Rather than panic, we should instead ensure we're prepared and have put in place quantum-resistant protections, starting with our priorities. This said, there's also concern that too many false alarms related to quantum computing breakthroughs could eventually lead to a false complacency and inaction. This might cause people to believe the quantum threat is not yet a serious concern when it is. If too many incidents lead to unwarranted panic, a genuine threat might be ignored as just another false alarm when it finally does arrive."

So what becomes clear is that where we need to be, and as soon as is practical, is at a point where we're no longer reliant upon classical pre-quantum crypto so that the eventual announcement of a true breakthrough is just met with a yawn and a shrug. So where exactly are we today? What is the current true level of alarm we should be feeling? HP addresses that, and we will address it after this final break.

Leo: Well, fascinating, and I take it, well, I don't know. Cause for concern?

Steve: Cause for real caution.

Leo: Yeah.

Steve: I think when I'm done here, after this next piece, our listeners will understand that, as soon as post-quantum stuff, post-quantum solutions are made available, they really should switch. For example, there will be, you know, here we were talking about obsoleted Juniper routers. Well, they're all pre-quantum.

Leo: Right.

Steve: So when Juniper offers post-quantum protected router technology, you don't want to wait until, you know, let's hope there's enough time between the availability of post-quantum safety and that breakthrough, that the natural lifecycle of router death will have, you know, taken all of the pre-quantum technology out of, you know, out of service. But we know, Leo, there are some dusty back cabinets and, you know, some backrooms that have stuff running, you know, there's still a windup key on some of these things. So...

Leo: Well, we'll talk about preparing for an I guess inevitable future in just a bit. You're watching Security Now!. Steve Gibson, Leo Laporte. We do this show every Tuesday. We're glad you're here watching. A reminder you can watch live if you tune in right, you know, it's right after MacBreak Weekly, and that time varies. Roughly 1:30 p.m. Pacific, 4:30 Eastern, 2030 UTC. The livestreams are, well, there's eight of them. Discord for the Club members. There's YouTube, Twitch, TikTok, X.com, Facebook, LinkedIn, and Kick. Watch wherever you like. But of course the best thing to do is download a copy of the show. You can get it from Steve's site. I'll tell you more about that in a bit. Our site, of course. Or subscribe, and that way you'll get the audio or the video the minute it's available. I'll have more information about that in a second. But now let's get back to Security Now!. Steve?

Steve: Okay. HP said: "With so many possible quantum breakthroughs to be assessed, and uncertainty about what is credible, it can be difficult to understand the landscape of quantum computing and separate fact from fiction. Let's take a closer look at the reality. To gauge the true alarm level, we should examine the process of quantum computing technology. Over the past year, there has been impressive advancement in several technologies, with multiple promising pathways emerging. Even if some fail, others may succeed." And of course remember we only need one to succeed to be in trouble. They said: "Compared to a year ago, large-scale quantum computing now seems more likely. We look to experts to qualify this likelihood.

"The Global Risk Institute's 2024 report highlights a 'significant chance' of a quantum threat emerging by 2034, posing an 'intolerable risk from a cybersecurity perspective.' So a significant chance of a quantum threat emerging in 10 years posing an intolerable risk from a cybersecurity perspective. Okay. So how significant? Nearly one third of the 32 experts surveyed estimate a 50% or greater chance of quantum computers breaking cryptography by 2034. Okay. One third of 32 experts. So 10 of the 32 experts estimate a 50% or greater chance of quantum computers breaking cryptography by 2034, with an average estimate of 27%. So the experts on average think there's a 27% chance of crypto being broken in 10 years. They said the highest in the six annual surveys conducted so far, so they've been polling every year.

"To summarize recent changes, the report states: 'The progress in the last year has induced many people both within and outside the quantum research community to realize that the quantum threat may be closer than they thought.' The German Information Security authority, BSI, recently updated their comprehensive assessment of quantum computer technologies. The report concludes that, due to major roadblocks being resolved, quantum computers are likely to break cryptography within at most 16 years, but recognizes that new developments could lead to a breakthrough as soon as a decade.

"Progress has been made, not only in various quantum computing candidate technologies, but also in aspects like scalability, scale, inter-connectivity, and operating software. Stability is a major challenge for current quantum technologies, as they do not hold their state for long before deteriorating. Reducing noise and using effective error-correction, where more errors are corrected than introduced, is crucial for long-term stability. Demonstrating this effectiveness is a milestone that has been achieved by four technologies: Superconducting Transmons, Ion Traps, Neutral Atoms, and Color Centers." Of course.

"Sizes of systems have increased as production processes mature, with Google announcing their 105-qubit Willow, IBM introducing the 156-qubit Heron along with a roadmap for processor scaling, and Microsoft and Quantinuum upgrading the H2 Trapped Ion processor to 56 qubits.

"The stability and size of the relatively new Neutral Atom technology, whose key elements were only demonstrated as recently as 2022, has shown a massive improvement with potential for acceleration. The QuEra start-up that came out of this research has just this February been backed with a $230 million investment, providing an indication of the high interest in this research. Of very recent note, a new technology with greater natural stability - the topological qubit - has been demonstrated for the first time as a proof of concept by Microsoft, who claim the technology offers a 'clear path to fit a million qubits on a single chip,' which would be needed for scaling.

"Advances in inter-connected quantum states between different chips are starting to show promise for enabling the distributed quantum computation needed for large-scale quantum computers. Additionally, an ecosystem of organizations are developing the necessary developer tools and software stack for operating quantum computers and creating quantum programs. This stack, like the classical computation stack, ranges from physical machine instructions to higher-level programming languages, allowing specialists to effectively use their expertise and enhance progress.

"Given all these advancements, Scott Aaronson, a quantum computing expert, recently said he believes that 'the race to build a scalable fault-tolerant quantum computer is actually underway.' His position on the urgency of addressing the quantum threat to cryptography has shifted from 'maybe' to 'unequivocally, worry about this now. Have a plan.'

"In summary, in just the past year, breakthroughs in quantum computing have strengthened the consensus that quantum computers capable of breaking today's cryptography may become feasible soon. It may only take a surprise acceleration from one of the promising technologies to break cryptography in less than a decade. Therefore, it's crucial to assess our preparedness and take action to ensure we're fully ready."

And then HP notes almost needlessly, under "Migrating Quantum-Vulnerable Cryptography Is on a Whole New Level Compared to Patching a Zero-Day Vulnerability." Although I'm sure our listeners are aware that we're talking about a sea change that requires us to scrap everything we've built, it's worth hearing HP out on this. They write: "It's tempting to think the problem of fixing" - and of course they're writing for a different audience than ours. "It's tempting to write the problem of fixing quantum-vulnerable cryptography is like patching a zero-day vulnerability in code. However, this analogy under-represents the scope of the quantum threat. A zero-day vulnerability is an error in a specific sequence of computer instructions in a specific program or library, which can typically be identified and then patched. Even if the error occurs in a pervasively common library, such as the Log4j vulnerability, it is still fixable by developing a patch.

"Unlike a zero-day, the quantum threat does not apply to a specific sequence of computer instructions, but instead applies to all implementations of vulnerable asymmetric cryptography. These implementations vary widely, potentially manifesting in millions of different code sequences. When quantum computers become viable, each of these will need replacement individually, by upgrading the cryptographic algorithms and keys used, requiring a global effort and collaboration by security practitioners, business leaders, and cryptographic experts."

And, you know, the more I think about it, the more I'm glad that this podcast will probably not be around to see this disaster befall humanity.

Leo: It's going to be worse than Y2K, that's for sure.

Steve: Oh, Leo. Oh, every light switch and router and webcam and toaster and microwave oven, I mean, we're IoT'ing everything.

Leo: Yeah.

Steve: And it's all bad because none of this stuff, this is all, you know, $5...

Leo: You forget how widespread this would be. I mean, this is...

Steve: It's everything.

Leo: Yeah, yeah.

Steve: It's everything. Given, you know, the reluctance to change that we've witnessed throughout the past 20 years, what chance is there that we're going to be the least bit prepared for this? We're talking about replacing everything, and doing it even while it's not obviously necessary that it needs to be done at all. That's the problem is that, you know, it's working great. What's the problem here?

Leo: Yeah, and unlike Y2K or 2038, we don't know when this is going to be.

Steve: Right. Exactly. It is not an approaching deadline. We knew when the elevators were going to stop running on Y2K.

Leo: Wow. I'm glad you, you know, I didn't - I hadn't really thought about how widespread this issue would be. I thought, oh, it's just encryption. It's not a big deal.

Steve: And remember that security is only as strong as the weakest link. You know? Who's not going to have some old webcam, light switch, thermostat, router lying around that continues relying upon pre-quantum crypto? And that's the bad guys' way in.

Leo: Right.

Steve: HP wrote...

Leo: Go ahead. No, you go ahead, I want to hear more.

Steve: Okay. HP wrote: "This process of patching has already started and is part of the migration to quantum-resistant cryptography that the security community is currently undertaking. But how should organizations be responding? Across government, industry, academia, and standards bodies, mechanisms to protect against quantum attacks are being put into place with some urgency. Our advice is to start by inventorying what would be vulnerable to quantum attackers." What wouldn't be? "Then prioritize what needs migrating and protecting first. The most urgent priorities for most organizations include protecting data with long-term confidentiality requirements - that's right, everything backed up and stored in the cloud is vulnerable; protecting long-lived systems by upgrading cryptography in hardware because all of their hardware is vulnerable today.

"The cost of upgrading hardware is expected to be significant. In July of 2024 the U.S. Office of the National Cyber Director published a report estimating the total cost of quantum-resistant cryptography migration for prioritized U.S. government systems" - this is only the U.S. government - "between 2025 and '35 at somewhere around $7.1 billion. In their calculation, they specifically call out that migrating the cryptography hardwired into hardware or firmware would constitute a significant portion of that overall cost. Government authorities are uniquely positioned with expert insights and the responsibility to protect national assets. Understanding their strategy and policies for critical systems and infrastructure should help any organization plan for migration with appropriate urgency." And let's hope that we have a vital and functioning CISA to keep this on the forefront of everyone's mind.

HP continues, saying: "Let's start with the U.S., who have a comprehensive plan and set of actions in place. In 2022, U.S. authorities established a tempo for migration. This has led to all federal agencies planning, taking inventories, and reporting on progress annually. A timetable to migrate National Security Systems was also established, with all new acquisitions" - get this - "with all new acquisitions from 2027 needing to be quantum-resistant, and all non-migrated products to have been phased out by the end of 2030." So just five years hence. That's great.

They said: "Migration of firmware signing is prioritized as even more urgent, with migration of firmware roots of trust - the firmware integrity protections in the hardware - expected to be 'implemented for some long-lived signatures this year,' in 2025. Since 2022, authorities have put in place guidance, including a guide published by CISA, NSA, and NIST, and organized outreach to help engage and ready the industry. Most recently, the Executive Order on 'Strengthening and Promoting Innovation in the Nation's Cybersecurity' of 16th of January this year, 2025, further emphasized the urgency to migrate. It specified that when procuring products, federal agencies must require quantum-resistant cryptography when it is widely available in a product category and require quantum-resistant protection in networks 'as soon as practical.'"

Now, that's cool because that means it becomes a competitive advantage and requirement. As soon as any is available in a category, that's the one that must be purchased, which means one early mover forces the movement of all of their competitors.

HP said: "Alongside this, NIST recently released its draft plan to deprecate classical asymmetric cryptography - deprecate classical asymmetric cryptography (RSA and relevant ECC) - from the end of 2030, the plan to deprecate asymmetric crypto, RSA and ECC, from the end of 2030, five years, and entirely disallow it for security purposes after 2035. Assuming this plan is confirmed, this will be highly influential in establishing migration urgency because it means there is an end date within the lifetime of many current systems." Maybe even this podcast. "Even during 2031-2035, data owners will only be able to use quantum-vulnerable cryptography by exception, where they evaluate and accept the risk.

"Beyond the U.S., the Australian Cyber Security Centre (ACSC) is also setting an urgent timeline for migration. The ACSC recently updated its Cryptography Guidelines for government and industry to disallow quantum-vulnerable cryptography after 2030." Five years. Disallow its use.

"In Europe, the security authorities of the UK, France, Germany, the Netherlands, Sweden, Norway, and Switzerland all urge preparation and are giving increasingly comprehensive guidance on how to migrate and prioritize. In April of last year, 2024, the EU recommended establishing a strategy to migrate public services and critical infrastructures as soon as possible. Building on this, in November of last year, 2024, 18 EU Member States issued a Joint Statement urging nations to make the transition to quantum-resistant cryptography a 'top priority'" - however, we want to be able to see your texts - "and protect the most sensitive data as soon as possible, latest by the end of 2030." Again, five years.

"The last 12 months have seen an intensification of the calls to migrate by national authorities. This underlines the need to act: assess cryptography dependencies, plan and prioritize for migration, and start to migrate priority assets. The heightening of the quantum threat to cryptography and the intensification of national calls to action during the last year have fortunately been met with significant progress in the range and availability of migration solutions.

"New quantum-resistant cryptographic algorithms were released as NIST Standards last year to celebration of government, academia, and industry following a collaborative selection process spanning nearly a decade. These new algorithms offer quantum resistance suitable for general use in protocols and applications. They also complement existing standardized quantum-resistant hash-based signatures suitable for special purposes, such as code signing. With this suite of standards, it has now become possible for industry to migrate in many scenarios.

"Standards capture community consensus and security best practice, while enabling interoperability between different elements across a system. As such, standards are a crucial part of industry migration to quantum resistance. From standards that define new cryptographic algorithms, through to protocols that use these algorithms and applications that adopt them, the community is carefully and steadily integrating quantum resistance into the technology stack and making resistance available to customers in products.

"This is why collaborating with other vendors and participating in standardization efforts is essential. Notably, HP is engaged in NIST's National Cybersecurity Center of Excellence Migration to Post-Quantum Cryptography project. This NCCoE project was convened to bring industry and end-user organizations together to help solve the practicalities of quantum resistance adoption and transition.

"To stay ahead of the quantum threat to cryptography, we cannot afford to take a 'wait and see' approach. At HP, our strategy is to prioritize quantum resistance from the hardware up and securely migrate from there. When prioritizing and planning what protections to migrate, it is crucial to consider the cost, effort, and difficulty of engineering the change. Migrating hardware - and the solutions baked into hardware - often requires changes to physically-engineered parts, which can be slow and needs a lot of forward planning, and sometimes years ahead."

So all that makes a lot of sense. We've seen, for example in the case of HP's printers, how printers can become the home to advanced persistent threats. You don't want your printers to get taken over by bad guys. So having them be proof against that is super important.

So anyway, HP's excellent state-of-the-race overview was heavily resourced with links to back up everything they said. I've included the link to their full article in the show notes for anyone who wants to follow and get more background information.

We really are in a time of significant change. Governments are tackling the tough problem of wanting to protect their citizens' privacy while not wishing to allow criminals to evade responsibility for their crimes by abusing absolute privacy. The move from the physical to the cyber world has parents and guardians wishing to protect their children from online harms, which means there's no way getting around knowing at least something about who's who on the Internet. And on top of all this the fundamental technology that underlies any of our ability to do these things is strongly expected to collapse and be rendered completely useless once quantum computers, whose arrival now appears to be inevitable, are brought to bear. So we certainly are living through interesting times. And Leo...

Leo: I mean, is it so severe a problem that I should from now on only buy IoT devices that say "NIST Approved Cryptography"? Can I buy anything like that?

Steve: I don't think it's percolated down there yet.

Leo: No. No.

Steve: No. And it will be a selling point where at some point, you know, there will be a consumer seal that says, you know, PQC, Post Quantum Computing.

Leo: Yeah, Post Quantum Crypto.

Steve: Or Post Quantum Crypto.

Leo: We've really got to get the word out. I'm really glad you brought this in and shared it with the class because it's clearly an oncoming train.

Steve: It is a looming, yes, a looming problem. It went from academia, like oh, look, lattice-based crypto, you know, we've got some new algorithms to replace what we have, you know. And it was like you and me joking about, okay, well, they managed to factor four bits, so...

Leo: Right.

Steve: I guess we're safe for now. That was a few years ago, and they've been working hard on this problem.

Leo: There are a number of technologies looming - artificial superintelligence, fusion, quantum crypto, quantum computing - all of which would change the world drastically. And it's kind of hard...

Steve: Are changing the world drastically; right?

Leo: Yeah. It's hard, well, but none of those three...

Steve: I mean, AI is. AI is changing the world.

Leo: Yeah. But ASI is not here yet.

Steve: No.

Leo: And it's also possible to say that it seems unlikely that we'll get any of those three - ASI, quantum computing, or fusion. It's speculative. And it's easy to say, well, it's not going to happen so I'm not going to worry about it. But it's prudent to say, but what if it does happen? I still don't know, I mean, they gave it a 100% probability in the next 50 years or something; right? I mean, but we don't know. Could be 10 years, could be five years, could be 100 years.

Steve: Could be a breakthrough. A breakthrough could happen.

Leo: Could be tomorrow.

Steve: Yes. Could be tomorrow.

Leo: And I guess the thing to point out is that companies are spending lots of money to make this happen. Big companies are spending lots of money to make all three happen; right? We had a guy on Intelligent Machines the other day who was very concerned about ASI. He said it's the equivalent of five or six Manhattan Projects. We're spending hundreds of billions of dollars to develop this thing without any regard to the consequences. We are living in interesting times. You're right, Steve. I'm glad we won't be around to report on it. A retirement's looking better and better. No, no, we need to, we have to stay here. You all, you know, you're here so that we can cover this stuff. We appreciate it.

Steve: We will be back here next week on April Fool's Day.

Leo: Oh. Worst day of the year for tech journalists.

Steve: I will not take advantage, I have never taken advantage of April Fool's Day.

Leo: No, nor have I.

Steve: I don't think that's fair to our listeners.

Leo: It's cheesy.

Steve: So, yeah.

Leo: And I strongly encourage - the problem is that I'll read stories in the next week, and I will not know, are these legit? I really have to dig deep to figure it out. I hate April Fool's Day. All right, Steve. Have a wonderful week. You could find this show on Steve's site.