FREEDOM Administration Login

Description: Apple disables Advanced Data Protection for new UK users. Paying ransoms is not as cut and dried as we might imagine. Elon Musk's "X" social media blocks "Signal.me" links. Spain's soccer league blocks Cloudflare and causes a mess. Two new (and rare) vulnerabilities discovered in OpenSSH. The U.S. seems unable to evict Chinese attackers from its telecom systems. What are those Chinese "Salt Typhoon" hackers doing to get in? The largest (by far) cryptocurrency heist in history occurred Friday. Ex-NSA head says the U.S. is falling behind on the cyber frontlines. We have the winner (and a good one) replacement term for "backdoor." A look at a pathetic access control system that begs to be hacked (and will be).

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-1014.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-1014-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. We're going to talk about Apple, I don't know, giving in on the UK request for a backdoor? Maybe they were playing 3D chess? Steve has some opinions. We'll also talk about why it might be illegal to pay that ransomware, how the Spanish soccer league is blocking Cloudflare and causing quite a bit of a mess, and then why your apartment building access control system might not be all that secure. Hmm. It's all coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 1014, recorded Tuesday, February 25th, 2025: FREEDOM Administration Login.

It's time for Security Now!, the show where we protect you and your privacy and your security online. Did I say "we"? Pardon me. He protects you, Mr. Steve Gibson, the man of the hour.

Steve Gibson: Leo, you are inseparable from the podcast, from the network, from, you know...

Leo: Yeah, but in this case...

Steve: ...it will not go on without you.

Leo: I am a member of the audience in this case. I listen to Steve, and I hope you all do. What's coming up this week?

Steve: So I stumbled upon a - it started off as just a regular sort of like security announcement. But the more I looked into it, the more astonishingly - wow, too much caffeine. The more I was astonished...

Leo: Too many adverbs.

Steve: ...that anybody could be producing a system like this. And it is something that our listeners are going to be able to experience for themselves, the astonishing insecurity of, almost ironically, an access control system whose own access control just fails just miserably. Anyway...

Leo: Oh, my gosh.

Steve: The title of the podcast is that, "FREEDOM Administration Login," which we're going to have a lot of fun with when we get to it. But first we've got the news that - actually we sort of did a preview of it last week. In this case, it's Apple disabling the Advanced Data Protection for new users in the UK, and eventually all users, although they're not saying when, and they're not saying why they're not doing it yet. Anyway, my take on it is a little bit different than everybody else's. It looks like I'm probably going to be wrong, but I'll share it nonetheless.

We also have the news that, you know, we've been talking a lot recently about paying ransoms, like, oh, we've got these groups and those groups, and we've got attorneys, and we've got people who specialize in all this. Turns out paying ransoms, we should remember, is often illegal. So...

Leo: Oh, interesting.

Steve: ...there's that.

Leo: Yeah.

Steve: Also just a random piece about X blocking Signal.me links. Spain's soccer league has blocked an IP of Cloudflare. Unfortunately, they got much more than they bargained for when they did that, causing a big mess. We have two new and exceedingly rare vulnerabilities in OpenSSH, which is widely regarded as one of the most well-designed and most secure, thank goodness, open source projects that exists. But whoops, a problem was found. Not end of the world, but worth looking at.

Also the U.S. seems unable to evict Chinese attackers from its telecom systems. We've had a senator recently say, well, suggest what we should do in response because - as if saying "and we can't." It's like, what? What do you mean, we can't? And speaking of that, what are they doing to get in? What is Salt Typhoon? Is it some mastermind strategy? Turns out not so much. And our listeners will not be surprised to discover how China is getting into our networks. We have, oh, Lisa - Leo.

Leo: You called me Lisa. Hello.

Steve: I'm not confusing you. By far the largest cryptocurrency heist in history, which occurred just four days ago, on Friday. We have an ex-NSA, well, THE ex-NSA head, suggesting that the U.S. is actually falling behind on the cybersecurity frontlines. We have, as last week I put it out to our listeners, come up with an alternative term for "backdoor." The replacement term is a good one, suggested by many of our listeners. It does exactly what I was hoping it would do. It is both accurate and clear. We'll touch on that. And then, as I said, we're going to look at a pathetic access control system that just begs to be hacked. And it will be, maybe even by some of our own listeners, although not maliciously, maybe to help the poor schlubs who have purchased this thing and have just everything wide open.

Leo: Yeah, you poor schlubs.

Steve: You schlubs. And we've got a great, great Picture of the Week - a common theme, but a variation on that theme, a new entry into the ever-popular "Where there's a will, there's a way" contest.

Leo: Oh, that sounds like fun. That's the ones where you should be careful not to electrocute yourself.

Steve: Yeah.

Leo: Or fall off, or somehow...

Steve: I've had some great feedback about this. I did the mailing to 16,363 of our listeners last afternoon. And a bunch came back and said, now, this one is one I would not have thought of.

Leo: Nice. You have more subscribers than we have Club TWiT members. That's actually shifted. For a while we had more Club TWiT members. You have so many subscribers. Steve, I have not looked ahead. I have not seen the Picture of the Week. Should I scroll up now?

Steve: It's a good one. As I said, a new entry into the ever-popular...

Leo: Oh. Oh, dear. This does not look like a good idea at all. Holy moly. I like the way he's managed ground. I guess that's what he's doing with the screwdriver.

Steve: Yep, that's exactly right. He stuck the screwdriver into the VGA output in order to get it in touch with the shell of the VGA connector.

Leo: Oh, lord.

Steve: To establish ground. For those who are not seeing this picture, it looks like we have a case either of the power adapter connector of the laptop being loose, or maybe, you know that all of those barrel connectors, there are several different sizes of them.

Leo: They're proprietary, and I bet you he doesn't have one that fits, yeah.

Steve: Yes. And so we've seen before in similar pictures where, you know, somebody used fingernail clippers to jury-rig connecting an American outlet or American plug to European outlets or something.

Leo: Thank god laptops now all use USB-C. And you can tell this is a vintage picture. Look at the cell phone in the corner. This is a different era, thank god.

Steve: So this person was determined to, you know, the battery ran down on his laptop.

Leo: Yup.

Steve: He's like, okay, I've got to plug this in.

Leo: You've got to work, man.

Steve: But the adapter he has is the right voltage, but it's the wrong connector.

Leo: I hope it's the right voltage.

Steve: Oh, yeah, you definitely want to make sure of that. But those various connectors, there are some standards, but they're weak standards, and they have different numbers of millimeters of, like, inner and outer diameter.

Leo: Oh, yeah. I used to have a kit with all the different tips.

Steve: Right, exactly.

Leo: Remember that?

Steve: Right, exactly. So it looks like we have a situation here where he does, he has the wrong tip for his laptop. But he's like, that's not deterring him. So he's got a screwdriver stuck into the VGA output, wedged in there in the case, in order to obtain system ground. He's got the power adapter outer barrel, which is chrome, pulling against the screwdriver, so the ground of the AC adapter is connected to the shaft of the screwdriver, which then goes to the VGA shell to get ground. Then a paper clip has been opened up and stuck into the center of the coax of the power adapter. And then he's got a white piece, looks like a piece of insulation because he needs somehow to get the...

Leo: Oh, geez, this is so horrible.

Steve: He needs the opened up paperclip to go into and connect to the center pin of the power connector in the laptop without touching the edges, which of course is ground. I bet he does have to...

Leo: I bet he thought he was really smart doing that. I bet he...

Steve: I would argue that this guy gets an award, Leo, because the laptop is powered up, against all odds of this just not working.

Leo: It is? You can tell it's working?

Steve: Well, yeah. I mean, here it is. He took a picture, he was so proud. It's like, look what I did.

Leo: Look what I did, Ma.

Steve: It works. It works, yeah. And I can tell looking at it, as an engineer, yes, this would work. It's, you know, it's not going to survive an earthquake of any significance, but yeah. I think this is great. This is very clever.

Leo: Don't do this at home.

Steve: Where there's a will, there's a way.

Leo: Yeah, that's awesome. By the way, they're telling me in the chat that's not a cell phone, that is a cordless landline.

Steve: Yeah. Yeah, that looks - although still, the laptop's got some - it looks like that weighs - it's got some heft to it.

Leo: Oh, yeah. Well, you don't see VG - I'm thinking it's a ThinkPad.

Steve: Good point.

Leo: You don't see VGA often, yeah.

Steve: You're not seeing a VGA output, like, natively on the laptop, yeah.

Leo: You don't see ports like this anymore at all.

Steve: And there is microphone and headphone jacks there in the foreground.

Leo: Yeah, right.

Steve: So it does sort of date it, yeah.

Leo: Oh, this is good.

Steve: Nice piece of work.

Leo: Great picture, thank you, Steve.

Steve: Nice piece of work.

Leo: Great picture.

Steve: Okay. So I took Apple's decision as good news. Now, better news would have been for the UK to have decided to back off from their demand that Apple arrange to provide access to the encrypted stored iCloud backup data of anyone, anywhere, for whatever purpose they might have. But that hasn't happened, at least not so far. Apple took the next step in what I'm hoping is a bit of a dance, and that had to happen. You know, one way or another, I feel that, you know, this is the issue we've been perched on here for several years now. One way or the other, the world needs to work out this issue about governments believing that they have the right to breach the privacy of anyone they choose.

The question is, do they or don't they? This has been brought to the fore because the technology we have now prevents that. We have the technology, and Apple has implemented it, where there is just no way for Apple or a government to access data which has the, as Apple puts it, Advanced Data Protection, you know, all of the possible protections turned on.

BBC News reported that ADP stopped being an option for new users starting at 3:00 p.m. UK time last Friday. Other outlets have subsequently confirmed that ADP is no longer an option for new users in the United Kingdom. In response to the news, our Johns Hopkins cryptography professor, Matthew Green, posted on X. He said: "If you are not in the UK, you should turn on ADP now. The more people who use it, the harder it will be to shut it off this way."

Leo: Oh. I was about to turn ADP on. Then I thought, well, that just puts a big target on my back; right? That just announces...

Steve: Maybe it means that you're being counted as somebody who...

Leo: Yeah, it's a vote, yeah.

Steve: Exactly. It is a vote. Okay. So no one in the UK can now activate Advanced Data Protection, and existing users will be disabled at a later date. Now, that's the thing that I sort of found interesting. My own opinion is that this is Apple intentionally not yet dropping the other shoe. It's an incremental move which allows them to wait to see what the UK chooses to do next. There is little doubt that this move has been forced upon Apple and is not going to be widely embraced with great joy, I would think, among the UK's voting citizenry. You and I, Leo, were talking about this before we began recording. Your take is, you know, are people really going to care that much? You know, I mean, as evidenced by the fact that most people don't have it turned on.

Leo: No. It's kind of hard to turn it on, and you lose some features.

Steve: I would like to have it turned on. I can't, as I've said, I've got too many legacy Apple things around here that I'm still wanting to use, and you have to have more modern hardware in order to be able to turn it on. Because it has to be on universally on every device logged into that account, or no one gets to play.

Leo: Yeah. Right now my son has a laptop that he hasn't updated, and I can't get rid of it because it needs his password to remove it. So I'm kind of stuck.

Steve: So the UK's Parliament now realizes that, if Apple is also forced to take the next step, which they haven't yet, of disabling all existing ADP-enabled encryption across the UK, that's going to have a far greater negative impact with the UK's politicians being directly blamed for forcing Apple to take away privacy guarantees that those citizens of the UK previously enjoyed. And, right, they're going to be singled out. Other people, you know, the world over get to have this. Not people in the UK. So since enabling ADP is something that one needs to do deliberately, and as we said, it can be a little, you know, you have to work at it in some cases, it will be those who most want it who will be having it removed.

Now, I'm sure Apple is holding out hope that that won't be necessary. If this first move by Apple is sufficient to have called the UK's bluff, to very clearly demonstrate that it's not joking about this and that it will proceed with removing all remaining iCloud ADP encryption - and only then for disadvantaged UK citizens - then Apple can avoid backtracking on existing encryption and can simply resume allowing those who want to turn it on to do so. I don't know what's going to happen. But I'm sure it's quite clear to everyone now that Apple holds all the cards here. I mean, they can be forced to turn it off, but then they're just going to disadvantage UK citizens.

The BBC's reporting said: "It is not known how many people have signed up for ADP since it became available to British Apple customers in December 2022. Professor Alan Woodward - a cyber-security expert at Surrey University - said it was a 'very disappointing development' which amounted to 'an act of self harm' by the government. He told the BBC: 'All the UK government has achieved is to weaken online security and privacy for UK-based users,' and that it was 'naive,'" he said, "of the UK to 'think they could tell a U.S. technology company what to do globally.'

"Now, opinions on this are mixed, however. The BBC reported that online privacy expert Caro Robson said she believed it was 'unprecedented' [well, she's right] for a company 'simply to withdraw a product rather than cooperate with a government.'" And of course,

you know, we know it's unprecedented, which is precisely why the world has desperately needed this precedent to be set. We don't know which way it's going to go. "Robson told the BBC: 'It would be a very, very worrying precedent if other communications operators felt they could simply withdraw products and not be held accountable by governments.'"

So of course that's a different take than we have. I don't think there's anything "worrying" about it. This is precisely what Apple needed to do. And we already know that Signal and others have said they would follow in Apple's footsteps. I don't, you know, what can Signal do? They can't. There's nothing they can do except to leave if the UK says you must build, you know, a means of monitoring your users into your product.

The BBC said: "Meanwhile, Bruce Daisley, a former senior executive at X, then known as Twitter," they wrote, "told BBC Radio 4's PM program: 'Apple saw this as a point of principle. If they were going to concede this to the UK, then every other government around the world would want this, too.'" And that's a really good point. My feeling is we could not ask for a better test case setup than what we have. New users are being told they can't have something that they may want. Existing users are at risk of losing it. So your move, UK.

Now, of course, there is a downside and dark side to this, you know, which tempers my enthusiasm. What if the democratically elected politicians within the UK decide that they know better than their own citizens? What if they shrug off this first step toward Apple's removal of ADP, forcing Apple to take the next step of requiring all existing UK users who have ADP enabled to disable it? What then?

So some other reporting on this quoted Mike Chapple, an IT professor at the University of Notre Dame's Mendoza College of Business and a former computer scientist at NSA. He noted that this episode illustrates "one of the fundamental flaws in government efforts to undermine encryption. Faced with having to choose between security and complying with government regulations, companies like Apple tend to remove security features entirely." And here's the worry. Chapple noted that: "The net effect is reduced security for everyone. If other governments follow the UK's lead, we risk a future where strong encryption is functionally outlawed, which puts all of us at risk of not just government surveillance, but also to eavesdropping by other bad actors."

So in other words, I've been assuming,, hoping, that the UK's elected parliament would lose this fight with Apple and, you know, their own citizens, and that the rest of the world would take note of that. You know, as I said last week, France is getting ready to push some of their own legislation forward to the same end. But maybe I'm the one who's being naive. You know, we learn that people don't really care all that much about encryption so long as they're able to check out how many "likes" they've received, and that they're fine with trusting their government to do the right thing.

Obviously on this podcast we're focused on these issues. Maybe most people aren't. We need to accept that this Apple/UK standoff might very well break in that direction, and that other governments would then learn exactly the wrong lesson, and immediately make similar guarantees or make similar demands, thus forcing a general global retreat on all encryption privacy guarantees.

Leo: So this is like glass is half full and half empty, I guess.

Steve: Right.

Leo: Because I have a completely different take. In my view, Apple capitulated, and the UK government got most of, they didn't get all of what they wanted, but they got most of what they wanted.

Steve: Well, yes.

Leo: There's no end-to-end encryption available from Apple in the UK. So how is that a win for Apple or anybody else? You can no longer do end-to-end encryption in the UK.

Steve: Right.

Leo: That seems, strikes me as a capitulation on Apple's part, and that this [crosstalk] UK's part.

Steve: Well, this is probably just the first shoe to drop on the UK's part.

Leo: Well, you're assuming there's going to be some...

Steve: [Crosstalk] demand from everybody else.

Leo: Yeah, you're assuming that the British citizens are going to stand up, say no, I want my ADP. But they're not going to do that. They're not going to do that. Because as you point out, people aren't even aware of the issue. And I think what this is going to give is a license to every other government to do exactly the same thing. Oh, good, Apple was glad to back down on this. Apple will turn off ADP. It's as simple as sending them a secret letter saying we want a backdoor. They don't need a backdoor anymore in the UK. They don't need a - they've always had a backdoor into iCloud.

Steve: Right. Right. As long as you don't have ADP.

Leo: I mean, it's a legal backdoor. They have to subpoena it. But it's the same...

Steve: Right, as long as you don't have ADP turned on, there is a means by which Apple is able to comply with the demand from the UK courts; whereas with it turned on, Apple is unable to comply.

Leo: Right.

Steve: I mean, they're able to honestly say, you know, on the stand, "We're unable to give you what you want."

Leo: This is what scares me. This is what I thought would happen, which is that governments are eventually going to tell people, no, you cannot provide end-to-end encryption to your customers. And then when Apple says, okay, fine, that sounds like a capitulation to me.

Steve: So what could they have done, or nothing? I mean, is this inevitable, Leo?

Leo: Whether, that's the problem, they have to withdraw from the UK is the only thing they can do.

Steve: Encryption or their product? They can't...

Leo: Yeah, completely withdraw. And by the way, that's not unprecedented. Google withdrew from China. And Apple has mostly withdrawn from Russia for similar reasons.

Steve: Wow.

Leo: But yes, you're right, I mean, Apple [crosstalk] in the UK. That's not going to happen.

Steve: No, no. And the other thing is that this is sort of a fuzzy line. So is it a phone registered by a UK citizen? What about them traveling out of the UK? Talking about a U.S. citizen in the UK?

Leo: This is why I said Apple partly capitulated. The request from the UK government - and again, this has never been published...

Steve: Is everybody...

Leo: ...is everybody globally. Not just citizens. We want a backdoor to all ADP accounts globally, including for U.S. citizens.

Steve: Well, all iCloud backup storage, you know.

Leo: Yeah.

Steve: Yeah, yeah. They want you to - they want to - oh, very good point.

Leo: So Apple didn't comply fully. Apple only did it in the UK.

Steve: Yes. They can't get your - well, they can get yours and mine because we don't have ADP turned on. But they can't get any non-UK person.

Leo: And physically we don't need it. But what I worry about is the dissidents, the political opposition, political leaders, intelligence agencies, all of these people, if they want to use an iPhone, and they want to use iCloud...

Steve: Legal use cases for...

Leo: ...should be using ADP.

Steve: ...needing strong encryption, yes.

Leo: Right. Now, we talked about this on MacBreak Weekly, and it is possible to use an iPhone without iCloud. And that's what you have to do if you want to be private at this point is you turn off iCloud backup. You just don't use iCloud because Apple has the keys. Just as Google has the keys to Google Drive and Microsoft has the keys to Microsoft's OneDrive.

Steve: And I think we did learn that, when you turn off iCloud backup, within a short period of time...

Leo: It bugs the hell out of you.

Steve: Apple, well, yeah, they're...

Leo: What do you mean you're not backing up?

Steve: I took a picture with this, and it's not over here. It's like, wait.

Leo: No, Apple will - you were going to say I think Apple will delete it.

Steve: Yeah, they will scrub your data from the cloud.

Leo: It's going to be a while, though. And we have to trust that they're going to do that. That's another thing. They might not. How would we know?

Steve: Oh, it's Apple, though. They want to.

Leo: Yeah. I don't think they want to store it.

Steve: No.

Leo: That's why ADP exists, because they wanted a way to say to governments, no.

Steve: Yes. And...

Leo: How did that work out?

Steve: And essentially it brings them to parity. Remember that Android has had this. Android has end-to-end encrypted cloud backup for a while now. And it's on by default.

Leo: What we don't know, this leaked out through - and I wish I could - I've forgotten which, was it Bloomberg with the information...

Steve: It was The Washington Post that first covered this.

Leo: Oh, it was the Post.

Steve: Yes.

Leo: So the Post found it. It was then confirmed by several other sources. But this is the equivalent of our national security letter in the U.S.

Steve: Right.

Leo: The government can request this, and the rules are you can't say that the government's asked for this. So Apple never said, oh, yeah, we've got - they just turned off ADP.

Steve: Thus the existence of warrant canaries.

Leo: It's a warrant canary, in effect.

Steve: Yes. And if we stop telling you we've never received a warrant, then draw your own conclusions.

Leo: So the question is did, and why wouldn't they, the UK government also send this to everybody else, Google and Microsoft and Signal? And why haven't we heard from those parties? They're by the way, enjoined from saying anything about it, as well.

Steve: Yeah.

Leo: You know, if you're going to obey the law, you can't say a word about it.

Steve: And again, this is why, regardless of what happens, this is what we've - this is - everything has been building to this for the last several years.

Leo: I just fear it's not going in the right direction.

Steve: It's - eh.

Leo: See, I changed your mind. It's half empty, Steve.

Steve: I'm an optimist. I want the good guys to win.

Leo: I do, too.

Steve: Yeah.

Leo: Well, you'd better darn well make sure you get some end-to-end encryption on your stuff and start thinking about this if you want to protect your privacy.

Steve: Well, and if Apple is just the first target, then the other chips are going to fall; right?

Leo: They've got to.

Steve: I mean, it's...

Leo: By the way, look, I don't want to get political on this. But do you think Kash Patel will hold back in any way? The new director of the CIA?

Steve: He's FBI.

Leo: I mean of the FBI.

Steve: Yeah.

Leo: Or Bongino or whatever his name is?

Steve: Hold back in complying with the UK? Or...

Leo: No, the FBI is going to go full speed ahead. And do you want the FBI...

Steve: And demand the same thing from Apple.

Leo: This is a weapon, we now have a weaponized law enforcement in the United States. This is the time to download some secure encryption and start paying attention to your privacy because law enforcement's going to go after their enemies. And frankly, I'm probably, if they knew about me, I would be one of them. Not Steve. Steve's, no, Steve's a good guy. He would never. I'm going to shut up right now. Go ahead.

Steve: I'm just glad I'm not a teenager now, Leo, or the history would be written differently because...

Leo: Oh, man, what a world to grow up in.

Steve: I got myself into some trouble with, you know, escapades. But, boy, I didn't have the Internet to tempt me. So I'm glad for that. Let's talk about our sponsor, who's going to tempt our listeners.

Leo: Oh.

Steve: And I'm going to sip on that $9.50 latte.

Leo: Now, there are other ways you could spend that money, Steve. I'm just saying. You're automatically a member of the club. Is that what's in there, by the way, is a quinti venti...

Steve: No. This is a smaller cup. It's only got three shots. And I did...

Leo: You made it yourself.

Steve: I made it here before the podcast.

Leo: So it cost you much less. It's an idea whose time has come, shall we say.

Steve: I can tell you that people care who listen to this podcast. You know I have the GRC.sc link shortener just to make it easy to refer people to things. The number one shortcut taken of all time was to the National Public Data breach, just shy, eight shy of 13,000 clicks on that. And to give you a sense, the second most popular - so that was

12,992, that one. The second most popular is the credit freeze shortcut. And that's only got 3630.

Leo: Oh. Holy cow.

Steve: So four times the number of clicks. I mean, people really did care about that National Public Data breach.

Leo: Good. Just because I don't, I'm like the canary in the coal mine. I'm the guy who's like, take it all, and let's see what happens. But that's just because I've been doing broadcasting for 50 years. I mean, how could I have anything to hide by this time? Nothing. On we go.

Steve: So podcast 1012 topic, its topic was "Hiding School Cyberattacks" two weeks ago. And last week we took a look at the latest rising Ransomware-as-a-Service startup, well, they started last February, but still they're now number one, and that's RansomHub. One thing we didn't touch on at all during either of those recent discussions was the question of the legality of all these ransomware payments that are being made. An editorial about this appeared in a recent Risky Business Newsletter, which opened with a reminder regarding the legality of paying ransoms.

The newsletter's author wrote: "A recent CISA report, and a series of tweets from Equinix's threat intel analyst Will Thomas, clarified that quite a few infosec and adjacent cybersecurity experts are not fully aware that paying ransoms to a rising ransomware crew named RansomHub carries quite a high risk of breaking U.S. sanctions. The group," he reminds us, "launched in February 2024, when it started advertising its Ransomware-as-a-Service offering in underground hacking forums. They got incredibly lucky because, just three weeks later, law enforcement agencies across the globe dismantled LockBit, which was, at the time, the largest RaaS (Ransomware-as-a-Service) platform on the market."

Okay, now, just to intersect here, to interject what the editor meant about their being incredibly lucky was that RansomHub had established itself and its presence in the sector just as the current number one RaaS provider, LockBit, was being taken down. This left the RaaS affiliates without any base of operations. But as luck would have it, the new kid on the block, RansomHub, just happened to be there to step in to fill LockBit's abandoned role.

The editorial continues: "Throughout the year, many of LockBit's affiliates slowly found their way to RansomHub. By the end of the year, the platform rose to become 2024's most active ransomware operation, with its leak site listing more than 530 victims. A CISA report published last August warned of the group's rise in popularity and increased operations. But as Will Thomas noticed, RansomHub also appears to have attracted some unsavory affiliates, namely the members of a cybercrime cartel known as Evil Corp. Evil Corp appears to have begun using RansomHub as a final payload around July of last year, dropping the ransomware onto systems previously infected via the FakeUpdates (SocGholish) botnet per reports from both Microsoft and Google.

"Between late 2017 and '18, Evil Corp previously developed and ran its own ransomware strains, such as BitPaymer, WastedLocker, DoppelPaymer, Hades, and PhoenixLocker. The group abandoned its own tools after it was sanctioned in the U.S. in December of 2019, sanctions that forced companies to flat-out refuse to pay ransoms, they didn't

have any choice, fearing that they would break sanctions and face the wrath of U.S. authorities.

"Since then, Evil Corp has been jumping between different RaaS platforms as part of a clever strategy of hiding their tracks and as a way to avoid scaring their victims with the possibility of sanction violations. With a fresh new coat of both U.S. and UK sanctions issued in October of last year, the risk of breaking sanctions in the case of a RansomHub infection is higher than ever." So they finish this saying: "But still, the TLDR here is that, if you get hit by RansomHub, you better check with your legal team before even thinking of opening your wallet."

So, you know, we know that the rise of ransomware is entirely fueled by the prospect of the bad guys getting ransom payments. They don't care, the bad guys could not care less about any random enterprise's network insecurities, nor their databases full of proprietary customer crap. They couldn't care less. The only thing they care about is cash. And the realization that vulnerable enterprises do care absolutely about their own crap-filled databases, and about them not being publicly exposed, created today's modern ransomware nightmare.

So the point being, if it was ever actually possible to pinch the cash flow, the ransomware problem would slow down a lot. But as we observed also last week, that just doesn't appear to be happening. I think what we're seeing is there are still enough companies that are able to avoid the problem of sanctions, for example, not in the U.S., where this is a problem, but are operating in countries either with loose regulations or are not able to enforce sanctions and so forth that are able to create this cash flow into the bad guys' wallets.

This is kind of odd. I'm unsure why exactly the security and privacy industries are all up in arms over last week's news that X has started blocking its users from including links containing the "Signal.me" domain. But I saw this, like, all over the place.

Leo: Yeah. And I don't even, you know, this is one of those things where - by the way, I just, to test it, just now posted my Signal address. Now, I see it, and I did get one person message me. But so maybe they're shadow banning it. But I don't see them blocking this. Now, that doesn't mean they didn't. They may have changed - this is often the case, as with, like, Mark Zuckerberg, where you do stuff, and they say, oh, never mind, that was my mistake.

Steve: Okay. So it could already be gone.

Leo: Yeah. Anyway, I was able to post this without being...

Steve: And do we know if anybody has been able to click it? Because...

Leo: At least one person has messaged me on Signal, yes, saying "Welcome."

Steve: Oh, okay.

Leo: So maybe, yeah.

Steve: Okay.

Leo: It could be that, you know, it could be that there are ways of slowing it down.

Steve: Well, and it did seem really strange.

Leo: Yeah.

Steve: You get all kinds of weird messages. The blocking was supposed to cover public posts, private DMs, and even personal X profiles. And the messages about like when a Signal.me domain was encountered were never clear. You might see "Sending Direct Message failed" without further explanation. Attempting to post publicly may result in "We can't complete this request because this link has been identified by X or our partners as being potentially harmful." Or you might see "This request looks like it might be automated. To protect our users from spam and other malicious activity, we can't complete this action right now. Please try again later." Oh, and at the time of this being reported, which was late last week, an attempt to add a Signal.me link to a profile bio resulted in an error message saying "Account update failed. Description is considered malware."

So, okay. Anyway, maybe that's already gone. Maybe that was, you know, as you said, Leo...

Leo: Sounds more like a bug.

Steve: ...it's like, oh, sorry, we didn't really mean to do that.

Leo: Yeah.

Steve: Because of backlash that was created.

Leo: You never know. We don't know.

Steve: And for me, you know, the fact that this was a big deal, you know, the incredible inertia that X has is another - I think it's an interesting object lesson in the inertia we often observe throughout the tech sector and elsewhere. As we know, today there's been an explosion of alternate messaging platforms, you know, like Signal in the case of Signal.me. But, you know, there's Mastodon, Bluesky, Discord, Meta's Threads, WhatsApp, Instagram, Signal, Telegram, and more.

Unfortunately, what this has created is a dispersion from what was a valuable single-platform concentration which Twitter originally provided. Like, you know, having everyone on different platforms is far less useful for, obviously, for contacting everyone, than having everyone in the same place. But that's the way things have evolved. And it was probably inevitable, right, that there would be alternatives, and people would migrate off into their own areas. But for what it's worth, it's why I returned to email for my own purposes. As I mentioned at the top of the show we have 16,326 subscribers at

this point. I think now it's - I actually got a few during the mailing. Some additional people signed up yesterday.

Leo: Bravo. Good for you. Yeah.

Steve: So anyway, I'm not surprised it's gone. And we've seen, you know, Twitter flailing back and forth. It's not the first time that - I'm still calling them Twitter. You know, X has blocked something and then backed off of their blocking.

Leo: Oh gosh. For a long time they blocked Mastodon links; you know?

Steve: Right.

Leo: So it could easily be that they saw Signal as a competitor. As X gets into more and more things and becomes the everything app, that might also be. But...

Steve: Yeah. And, you know, we know Elon. He's prone to doing things and then, you know, changing his mind. So whatever.

Leo: By the way. I don't post on X, and I only did this for you. But I figured posting my Signal address is probably a good thing to do.

Steve: Well, and actually I went to X. I'm signed out of it on my browser on my other desktop. And I tried on Sunday to log in. I logged in with my username and password. It prompted me for my six-digit one-time password. I put it in, and it said "invalid." And so I'm unable to log in there. So yesterday...

Leo: Lot of people have reported that, by the way. Don't let your X account log itself out because it's hard to get back in.

Steve: Oh, really.

Leo: Yeah.

Steve: That's nuts. Well, anyway, so I'm still logged in.

Leo: It's just broken. I don't think it's intentional. I think it's broken.

Steve: Okay, good. Because I'm still logged in in my other - my desktop. And when I came here yesterday morning after the weekend, I, like, I went to X to see whether I was going to be able to get back in. And I did discover that the last, the previous two weeks I had forgotten to post my weekly show note summary. It used to be only to X where I was...

Leo: Right, that's where I would get it, yeah.

Steve: So I apologize to everybody. I said, I'm sorry, my bad, I will - and I'm posted there now for today's podcast already.

Leo: So that was a device that you hadn't been logged out of yet.

Steve: I never logged out of X on that other machine.

Leo: I know.

Steve: I would not have done that deliberately.

Leo: Well, it could have timed out. Maybe. I don't know.

Steve: Yeah. That's a very good point. Because I'm in it on this workstation more often than I am over there.

Leo: That's the one you use, yeah.

Steve: So it could have been just so many months that I didn't go there that, yeah, you're right, the cookie expired.

Leo: Yeah.

Steve: Which I would like to be able to login there, so hopefully.

Leo: I think if you keep trying you'll get in eventually.

Steve: I first encountered a short, worrisome blurb which read: "Cloudflare blocked in Spain on the weekends." And it read: "Spanish Internet service providers have started blocking access to some Cloudflare IP addresses on the weekends. The blocks were put in place this month after Spain's soccer league won a lawsuit against Cloudflare for hosting pirate streaming sites. According to reports in local media, the blocks are indirectly blocking access to many legitimate websites, including GitHub, Reddit, and many private Spanish businesses."

So this news was accompanied by a tweet. Some guy on Twitter, @TheXC3LL, tweeted: "If you are an APT using Cloudflare as CDN, and you see your beacons disappearing every weekend in Spain, it's because football. ISPs are blocking Cloudflare during weekend to avoid people..."

Leo: Oh, my god.

Steve: "...watching football from pirate streamings. As a side effect, you cannot use GitHub on weekend."

Leo: Oh, my god. So do you blame the pirates, or do you maybe blame the Spanish authorities or ISPs?

Steve: Before I go any further...

Leo: Geez.

Steve: ...let me remind everyone that the reason using a crude packet-level firewall to perform "IP-based blocking" no longer works is SNI, Server Name Indication. What SNI enables in practice is IP sharing at scale. So, for example, GRC, my little company, has a handful of IPv4 IPs which I treasure. But I now have many more websites and services than I have IPs. I'm being saved by SNI, Server Name Indication, which allows the incoming connecting client, as part of its TLS negotiation, to specify which remote server the client intends to access at that IP.

Leo: Is that like port forwarding?

Steve: Well, it's just you could think of it as multidomain hosting at a single IP. So there might be hundreds or thousands of domain names whose DNS all resolves to that same single IP.

Leo: Interesting.

Steve: So that means that access to hundreds or thousands of individual websites and services would be erroneously blocked if some court were to order the IP that also shares that, you know, some copyright infringers with all the other legitimate sites. So this is a mess. Cloudflare's headline, Cloudflare's own headline read: "LaLiga Understood Dangers, Went Ahead Anyway."

Leo: Oh, boy.

Steve: And Cloudflare wrote: "Cloudflare provides security and reliability services to millions of websites, helping to prevent cyberattacks and make the Internet safer. Like virtually all major cloud service providers, Cloudflare uses shared IP addresses to manage its network, meaning that thousands of domains can be accessed with a single IP address." You know, of course, this is how we've solved the IPv4 depletion problem, too, right, is by - it's like we can have lots of domains, all sharing a single IPv4 address.

Leo: I get the difference. It's like port forwarding except you don't - since all websites use the same port, you can't just do port forwarding. You have to do name, forward by name.

Steve: Exactly.

Leo: Yeah.

Steve: Exactly. And that's what's exchanged during the TLS handshake. During the TLS handshake, the browser says I'm hoping to hook up, to connect to this website at this IP. And so then the proper server responds with a certificate for that domain, and which the client, the web browser then looks at and goes, oh, yeah, okay, that's a good certificate. Let's go with a secure connection.

So Cloudflare said: "Cloudflare has repeatedly warned about the consequences of IP blocking that fundamentally ignores the way the Internet works. Indeed, other governments in Europe have acknowledged these concerns and concluded that IP blocking violates Net Neutrality. Although LaLiga clearly understood that blocking shared IP addresses would affect the rights of millions of consumers to access hundreds of thousands of websites that do not break the law, LaLiga went ahead with the blocking. This appears to reflect a mistaken belief that its commercial interests should take precedence over the rights of millions of consumers to access the open Internet.

"At the same time, Cloudflare regularly speaks with rights holders and policymakers about better ways to combat illegal piracy and online abuse. While Cloudflare cannot remove content from the Internet that it does not host, we have well-developed abuse processes in place to help by connecting rights holders with service providers who can take effective action. We will continue to push for rational solutions to combat illegal piracy that do not impact the rights of millions of Europeans to browse the Internet."

In other words, they're saying, we're not hosting this content. We're just part of the Internet's infrastructure. So don't blame us. We're not the problem. We're offering a solution.

Leo: Sigh.

Steve: So some reporting on this explained: "Cloudflare's statement needs no explanation, but two issues deserve highlighting. According to LaLiga's statement, its target behind Cloudflare was a web page with instructions" - get this, Leo - "on how to download an Android app." Not even the content. Not even pirated content. Instructions on how to download an app. "If that app was the means of accessing the content, that raises an important question. When Cloudflare's IP address was blocked, did that 'deactivate' both the app and the pirated content available through it? If not, blocking many innocent websites appears to have been weighed against the benefit of blocking an instructional web page."

They also wrote: "Cloudflare's suggestion that this was done deliberately could make this a matter for the European Commission, at minimum. Perhaps even more remarkable was the unwillingness of the ISPs to do anything, despite having the power to do so. The complication, of course, is that Telefonica and Movistar have licenses to distribute LaLiga content, and very little incentive to step in. Ultimately, customers of Movistar have suffered the most as individuals. This means that a decision was made to block

Cloudflare, in the knowledge that Movistar subscribers would face the most disruption, and then Movistar was instructed to carry out the blocking against its own customers. As the court envisioned, apparently."

Okay. So again, just to be clear, it's the customers of these Spanish ISPs that have taken to blocking websites by IP address that are being impacted because these customers are behind their ISPs' IP-based firewalls. After all of this, Spain's LaLiga soccer league replied. They wrote: "Over the last few days, multiple websites across Spain have experienced disruptions, an issue linked to the blocking of a few IP addresses by Internet service providers." Now, just to note, under the court order that LaLiga got from some judge somewhere.

They wrote: "These blocks were implemented following requests from LaLiga to combat illegal access to its content, which Cloudflare has facilitated by knowingly protecting criminal organizations for profit. Through this conduct, Cloudflare is actively enabling illegal activities such as human trafficking, prostitution" - I know - "pornography, counterfeiting, fraud, and scams, among other things. In fact, LaLiga identified two IP addresses covered by Cloudflare, which provided access to child pornography. This evidence has been fully documented and submitted as part of a formal police report."

Okay, now remember, what LaLiga is objecting to is a web page that provides instructions for downloading an Android app which, in turn, allows streaming of live soccer matches. And Cloudflare made clear that it has mechanisms in place for dealing with illegal content. LaLiga's statement says: "Cloudflare is actively enabling illegal activities such as human trafficking, prostitution, pornography, counterfeiting," blah blah blah.

But it would be more accurate to say: "The Internet is actively enabling illegal activities such as human trafficking, prostitution, pornography, counterfeiting, fraud, and scams, among other things" because, yes, the Internet as a whole does passively enable these things, right alongside all the positive things it also enables, the Internet also enables. And this is, of course, the Net Neutrality issue at the heart of Cloudflare's argument. They are functioning as part of the Internet's content conduit, and they are determined to remain as neutral as possible.

LaLiga's statement continued. They wrote: "This action specifically targets IP addresses used to illegally access LaLiga content, which were shielded by Cloudflare. Just like other major U.S. tech corporations, Cloudflare enables criminal organizations" - so now they've broadened this; right? "Just like other major U.S. tech corporations, Cloudflare enables criminal organizations to digitally launder stolen illegal content, making them a complicit party in intellectual property crimes as defined in Article 270.2 of the Spanish Penal Code."

Wow. Okay, now, you know, there's really a simple solution to this. LaLiga could simply decide not to stream their soccer matches to the Internet at all. Just like in the old days. Have fans attend their games. Then there's no problem. But, no. They, of course, want all the benefits of this magical technology without any of the technologically-enabled downside.

They continue. "It's important," they wrote, "to emphasize that this is not a broad or indiscriminate block." Right. All evidence to the contrary, you can't get to GitHub on the weekends, and despite the need to issue this explanation in the first place. They said: "LaLiga is absolutely certain and has proof that these IPs are being used to distribute illegal content alongside legitimate material." So they know they're also blocking legitimate content. They said: "Legal businesses affected by these blocks are those that Cloudflare has deliberately used as a digital shield..."

Leo: Oh, please.

Steve: "...to obscure illegal activity, without their knowledge and while profiting from it." Wow. They said: "More than 50% of pirate IPs illegally distributing LaLiga content are protected by Cloudflare. Despite multiple formal requests from LaLiga for Cloudflare to cease its collaboration with pirate sites, the company has refused to cooperate, instead continuing to profit from the criminal activity it helps to conceal.

"LaLiga has repeatedly reached out to Cloudflare, requesting voluntary cooperation. However, on Friday, February 7th, the U.S. tech company responded in a surprising manner, defending its actions with implausible and incoherent technical excuses." This is probably just the fact that it's...

Leo: They don't understand it.

Steve: ...doing IP sharing, yes, exactly. "This left LaLiga with no other option but to take direct action. This issue is not unique to Spain; similar measures have been taken in other countries to combat piracy of sports content. LaLiga fulfilled its due diligence obligations before resorting to this step." And then they said: "Google, Cloudflare, VPN providers, and other entities facilitating piracy are responsible for the illegal activities they enable and profit from. LaLiga, backed by the justice system, will not relent in its efforts to protect football and the interests of its clubs against criminal action related to audiovisual fraud and digital laundering."

So, you know, "Don't shoot the messenger" is a long-understood principle. To call out Google, Cloudflare, VPN providers and other entities is to say "The Internet." LaLiga wants to have all the benefits that derive from having the Internet, which they did not create, carrying their content for effectively no cost, while also wishing to somehow prevent that no-cost carriage from being used in ways they disapprove of.

It's understandable that, when served with an IP-blocking court order, those ISPs within the Court's reach had no choice other than to block access to that IP for all of their customers. And given LaLiga's feelings, it's also understandable that they would have made such an appeal to the court. What's missing from the equation is the legal precedent that would prevent the court from producing the ruling that they did. As Cloudflare said in their statement: "Cloudflare has repeatedly warned about the consequences of IP blocking that fundamentally ignore the way the Internet works. Indeed, other governments in Europe have acknowledged these concerns and concluded that IP blocking violates Net Neutrality."

So hopefully this issue will escalate and have this lower court ruling overturned with a higher Spanish court so that precedent will be created in Spain; LaLiga's and all others' current and future appeals will then be thwarted; and the principles of Net Neutrality, which is clearly the only way a sane Internet can function and thrive, will prevail in the end. So I guess we chalk this up to "growing pains." Another one of these, you know, problems which technology has created and hasn't yet, you know, the legal system hasn't yet decided how it's going to completely settle on this. We just need more - we need more legal precedent.

Leo: And a better understanding of how technology works.

Steve: Yes, exactly.

Leo: Clearly, yeah.

Steve: We need another break.

Leo: You want some help here? You want a little help from...

Steve: I need some coffee.

Leo: I'm glad to offer it. Steve is now fully caffeinated, hydrated, and ready to continue the program.

Steve: So, indeed. Through the years we've noted that vulnerabilities discovered in OpenSSH are vanishingly rare. And this project as a whole is widely regarded as one of the most secure of any open source project. And this is, of course, that's a good thing, it's crucial, since OpenSSH's role is to be positioned on the frontline, exposing itself to the Internet while warding off all attackers. So when Qualys announces the discovery of two new and potentially weaponizable vulnerabilities in this crucially important remote access technology, it gets everybody's attention.

Last Wednesday, Qualys disclosed. They said: "The Qualys Threat Research Unit (TRU) has identified two vulnerabilities in OpenSSH. The first, tracked as CVE-2025-26465, allows an active machine-in-the-middle attack on the OpenSSH client when the VerifyHostKeyDNS option is enabled. The second, CVE-2025-26466, affects both the OpenSSH client and server, enabling [oops] a pre-authentication" - well, okay, it's a denial-of-service attack. So it's not access.

"The first attack, the 26465, succeeds regardless of whether the VerifyHostKeyDNS option is set to 'yes' or 'ask.' Its default is 'no.' This attack requires no user interaction and does not depend on the existence of an SSHFP resource record (that's an SSH fingerprint) in DNS." In other words, "VerifyHostKeyDNS is an OpenSSH client configuration option that lets the SSH client," you know, the one connecting to an SSH server, "look up and verify a server's host key using DNS records," which that's very cool, another example of DNS being so useful just as an Internet addressable database. So here you can ask for a given domain's SSH host fingerprint.

"The vulnerability was introduced" - they know exactly when this happened - "in December [whoops] of 2014," so 10 years ago, "just before the release of OpenSSH 6.8p1. Although VerifyHostKeyDNS is disabled by default" - that is, normally set to "no" so it's not a problem, it's only a problem if it's set to "yes" or "ask" - "it was enabled by default in FreeBSD from September 2013 until March of 2023."

Now, although I don't use the OpenSSH client on my own FreeBSD instances, when I saw that the date range included my most recent installation of FreeBSD, I checked. And sure enough, FreeBSD's default, in a config file for the client, is indeed set to "yes." So for what it's worth, you know, it is the case that you want to make sure VerifyHostKeyDNS, I mean, especially when you're not using DNS Host Key Lookup is set to "no." But, okay, it's not a huge problem if it is. We'll get there in a second.

In the second vulnerability, both the OpenSSH client and server are vulnerable to this 26466 CVE. It's a pre-authentication denial-of-service attack. It is an asymmetric resource consumption of both memory and CPU. So it can be used to bring down the

system that the OpenSSH server is sitting on. And that's not good. That was introduced in August of '23, so not that far back, shortly before the release of OpenSSH 9.5p1.

On the server side, this attack can be mitigated by leveraging other existing mechanisms that OpenSSH provides such as LoginGraceTime, MaxStartups, and the more recent PerSourcePenalties options. The recommended action for this is just upgrade. OpenSSH 9.9p2 addresses all these vulnerabilities. And, you know, that's what everybody should do.

Qualys underscored OpenSSH's terrific security record. They wrote: "Despite these two vulnerabilities" - which again, they're not the end of the world, but be good to update - "OpenSSH's overall track record in maintaining confidentiality and integrity has made it a benchmark in software security, ensuring secure communications for organizations worldwide."

Okay. So what do these two things mean? Qualys writes: "In the first instance, if an attacker can perform a man-in-the-middle attack via 26465, the client may accept the attacker's key instead of the legitimate server's key. This would break the integrity of the SSH connection, enabling potential interception or tampering with the session before the user even realizes it. SSH sessions," they wrote, "can be a prime target for attackers aiming to intercept credentials or hijack sessions. If compromised, hackers could view or manipulate sensitive data, move across multiple critical servers laterally, and exfiltrate valuable information such as database credentials and so on. Such breaches can lead to reputational damage; violate compliance mandates such as GDPR, HIPAA, PCI-DSS; and potentially disrupt critical operations by forcing system downtime to contain the threat.

"In the second case, SSH is a critical service for remote system admin. If attackers can repeatedly exploit that second flaw, 26466, being a denial of service, they may cause prolonged outages or prevent administrators from managing servers, effectively locking legitimate users out. An enterprise facing this vulnerability could see critical servers become unreachable, interrupting routine operations and stalling essential maintenance tasks."

They said: "When the Qualys research team confirmed the vulnerability, Qualys initiated a responsible disclosure process and worked with OpenSSH to coordinate its announcement." And of course its remediation. So bottom line is anyone who's worried about this and who uses the OpenSSH client may wish to make sure that their client's config file has that VerifyHostKeyDNS set to "no." And anyone who relies on OpenSSH should look for and install updates which are now available.

And I just to mention that Qualys provided a truly beautiful write-up of the details of this bug. If this were a podcast that looked at the details of software vulnerabilities, then this would be the topic of the week. They show some small snippets of OpenSSH code, directly from the source, and carefully describe how they went about discovering the problem which became a vulnerability after they were able to engineer its exploitation. So the reason I bring this up is anyone who considers themselves to be a bit of a codesmith I think would be well served looking at that excellent page. I've got the link to it at the bottom of page 10 of the show notes. So I recommend it highly.

Okay. So some sobering news was made during last week's Munich Security Conference, as reported by Politico, who wrote: "The State of Virginia's Senator Mark Warner is working to build support on the Hill" - meaning, you know, in Congress - "for major changes to America's offensive cyber policy, amid the government's continuing failure to fully evict China's Salt Typhoon hackers from U.S. phone networks." It's like, what? It's like, we know they're in there. And, like, this is a problem somehow? What?

"Speaking to reporters on the sidelines of the Munich Security Conference last week, Warner said he now does not believe the U.S. can ever fully oust the elite, Beijing-backed hacking group Salt Typhoon from its telecommunications backbone" - meaning the U.S.'s telecommunications backbone...

Leo: Holy cow.

Steve: Like, what? "...without unleashing U.S. hackers inside China, or at least credibly threatening to." In other words, our technology is so weak that we give up. And so we're simply going to threaten China to get out or else.

Leo: Scare them out. You need a rat catcher.

Steve: Wow. Wow.

Leo: Holy cow.

Steve: Mark Warner said: "Your diplomatic pushback on the Chinese would be a hell of a lot stronger if the U.S. could tell China: 'We're going to go into your networks the exact same way you go into ours.'" And "Warner is the first Democrat," Politico wrote, "to come out so clearly in support of punching back harder in cyberspace against China in the aftermath of the Salt Typhoon breaches, with congressional Republicans and members of Trump's new administration having already signaled their support for that shift.

"Warner said that replacing aging and vulnerable networking equipment could cost the telecom companies tens of billions" - just wait till you hear what the vulnerability is - "tens of billions, while evicting the Chinese from every nook and cranny inside the nation's sprawling phone system could take '50,000 people' - wait, don't we have a whole bunch of people out of work now, Leo? Maybe we could use them - '50,000 people and a complete shutdown of the network for 12 hours.'"

Leo: Oh, no phones at all.

Steve: Because, yes, we're just that lame that we're just - we give up. China, just, you know.

Leo: Wow.

Steve: Warner said that he has been in talks with the heads of the congressional intelligence committees, and that "consensus was already there" for a new, more hawkish hacking strategy. The next step, he said, was "putting meat on the bones" of that idea something that might require the formation of a bipartisan expert commission, he said. He also emphasized that he believed working through the Hill and building support among Democrats was critical to a more robust cyber deterrence strategy. Warner argued that "If it comes from Trump, you know, any Democrats will just say, 'He's just going over the top.'"

Warner did say he felt part of the long-term solution was the promulgation of new cybersecurity regulations for the telecom sector. Yeah, that'd be good. That's something the Biden administration and several congressional Democrats have supported, but the Trump administration has at least for now pooh-poohed. Overall, Warner said that he was apoplectic that so few people seem to be paying attention to Salt Typhoon. He said: "The fact that people's heads are not exploding still makes me crazy."

Leo: Wow.

Steve: Okay, now, as we've often noted, we must assume that the NSA has just as much penetration into Chinese networks as they have into American networks. I just, you know, we're not going to hear that news; right? But you have to assume that. It strikes me as a sad state of affairs that our political leaders are now suggesting that we're incapable of securing our own networks, and that the only way to "get them out of ours" is to credibly threaten to do more damage to them through theirs.

Okay. So speaking of Salt Typhoon, we've not gone in and done any sort of a deep dig. So I decided to figure out, like, what the heck? Salt Typhoon has been on the radar of several cybersecurity threat tracking groups for some time. The commonly known "Salt Typhoon" name is the one it received from Microsoft's Threat Intelligence group. But the same group, Salt Typhoon, is also known as RedMike by the Insikt group, which is the Recorded Future Network Intelligence Group's name. Meanwhile, Kaspersky calls them "GhostEmperor," and ESET tracks them and their activities as "FamousSparrow."

Now, although Microsoft has not chosen to share their findings within the broader security community, others have. The news from Recorded Future's network intelligence group is somewhat dispiriting because it turns out that RedMike, as these guys call it, is exploiting - get this, Leo - two very well known, long since patched, two-year-old vulnerabilities in Cisco's IOS XE Web UI. Yes, you heard that right. The infamous Salt Typhoon has been gaining entry into the world's telecom carriers using an exposed web management user interface. And not only that, they are a pair of privilege escalation vulnerabilities, 2023-20198 and 2023-20273. And, yes, both dating back to 2023.

The 20198 privilege escalation vulnerability was found in version 16 and earlier of Cisco's IOS XE web UI, and the patch for it was published by Cisco in October of 2023. Attackers exploit this vulnerability to gain initial access to the device and issue a Cisco IOS "privilege 15" command to enable them to then create a local user and password on the device. Following this, the attacker uses the new local account on the device to access it. They then exploit the associated 20273 privilege escalation vulnerability to gain root user privileges. And once that's done, the group uses this new privileged user account to change the device's configuration and add a GRE tunnel, which is similar to an encrypted VPN link, which then gives them persistent access and data exfiltration.

And all of this pain because those telecom carriers have not bothered to update their Cisco IOS firmware to fix this 18-month-old vulnerability, both of which were fixed in October of 2023, not to mention leaving a web management UI exposed to the Internet. And that's the underlying cause of all of this mess is non-updated Cisco IOS gear for 18 months and exposed web management user interface that allows the bad guys, these Chinese hackers, to get in, set up a persistent tunnel back out to them, and then they have unrestricted access to the network of the telecom provider. If we'd simply - I don't know how it takes 50,000 people to update the firmware on some Cisco devices that are still being supported because this is only a year and a half ago. Government.

Leo: Yeah, it's mindboggling, yeah.

Steve: Government. Let's aim Elon at that. Elon, here. I mean, he would understand all of that. Elon, go fix this. Update the firmware on the Cisco routers. Just make it so.

Leo: Yeah, you know, take all those DOGE kids and send them out updating firmware. I could get behind that. That's not a bad idea.

Steve: Okay, now, Leo. For a while I'm sure we were all somewhat intrigued by the news of this or that, never heard of them before, cryptocurrency exchange being hacked and losing millions of dollars worth of never heard of it before cryptocurrency, or contracts, or I don't know, monkey icons or whatever. But as also eventually happened with the constant torrent of ransomware attacks, over time they turned out to just be so much background noise; you know? And for the sake of our own sanity, we stopped talking about every one of these because it was just constant.

Leo: Yeah, but this one's different.

Steve: But this one is different.

Leo: Holy cow.

Steve: Not this time, folks. Under the headline "Boy, that's gotta hurt!" is the news that the world's second largest by trading volume, second largest major cryptocurrency exchange was, as they say, taken to the cleaners by a group of quite determined North Korean hackers to the tune of - is everybody sitting down? Grip your steering wheel firmly if you're listening to this during your morning commute - $1.5 billion worth of completely liquid Ethereum tokens. $1.5 billion. Wow. This makes it the largest crypto heist ever in history.

Leo: Probably the largest heist in history; right?

Steve: It is the largest heist...

Leo: How do you steal $1.5 billion from a, you know, armored car? I mean, or a bank.

Steve: Yes. It is the largest heist of any kind in history of the world, and it's nearly 2.5 times larger than the previous record, which was the theft of $625 million from the Ronin Network back in April of 2022.

So I have a link in the show notes, the bottom of page 12, showing the fraudulent transaction event on the Ethereum blockchain where 401,346.76888, I mean, it goes on forever, you know, with decimal, ETH are being transferred. That transfer was fraudulent. Ethereum peaked at around $4,000 each in early December of last year and is currently trading around $2,800 U.S., which if you multiply 2,800 by 401,346, you get around $1.5 billion of liquidity that the second largest group, which is BitPay, lost.

Okay. So the hack took place just last Friday, February 21st. And in addition to being the single largest crypto heist ever, it's also considered to be one of the most complex crypto heists ever.

Leo: You know, parenthetically, kudos to Bybit because we wouldn't know all these details if they hadn't been very transparent.

Steve: Yes, they were. And they have not been sunk. They said we've got the liquidity to cover this, you know, this does not put us out of business. But they're not happy about it.

Leo: Yeah, no.

Steve: But they were very upfront. So the most, not only the biggest, but the most complex crypto heist. The blockchain analytics firm Arkham Intelligence and also the intelligence firm Elliptic have independently claimed that they were able to track the hack to the Lazarus Group, which is a well-known North Korean advanced persistent group, an APT group.

What we know is that Lazarus first infiltrated Bybit's network some time ago. They then quietly studied the company's internal procedures, identified and then infected with malware all of the multiple employees who are now required to mutually sign off on any major movement of the company's funds. This multi-sign-off requirement is obviously designed to solve the problem of any single employee being hacked or phished or scammed or whatever. But that didn't thwart the attack this time.

The hackers specifically targeted the process of replenishing the company's active wallets, known as hot wallets, where the company's daily operational funds are stored. When hot wallets run dry, or low, crypto exchanges will move funds from their reserves, from the so-called cold wallets, to make sure there's enough liquidity to cover users' withdrawals and token inter-exchanges. The same goes for when hot wallets hold too much money. In those instances, crypto exchanges will move funds back to the offline cold reserves to safeguard those reserves from malicious actors and exploits, and limit possible losses.

So, you know, that all makes sense. And actually, that's what saved these guys; right? Because they've got something like 10 billion in total reserve, only 1.5 - "only," I'm saying. But still, not all of it because they did have a bunch in cold storage, and the bad guys didn't get that. But they did capture one massive transfer of 1.2 billion.

Bybit's CEO Ben Zhou says that when his staff wanted to replenish the hot wallets with new funds on Friday, the hackers altered the user interface of the crypto wallet software the company was using to move their funds. The modification appeared on the systems of every one of the multiple engineers who needed to simultaneously sign off, in what is known as a "multi-sig transaction." A tweet describing what happened reads - I have a tweet in the show notes from some random person who said: "The attacker somehow," and then we've got four points. First, "Identified every multi-sig signer." Second, "Infected each signer's device with malware." Third, "Made the UI show a different transaction than what was actually being signed." Fourth, "Got all signers to approve without suspicion." And then he finished, saying "Cold wallet security just got redefined."

Now, not surprisingly, Bybit's loss of that $1.5 billion in Ethereal tokens did not go unnoticed. And since this makes many investors nervous about other potential

weaknesses in and about Bybit's security, the company did say said that news of the hack had led to a surge in withdrawal requests. CEO Zhou wrote that the company had received more than 350,000 requests from customers to withdraw their funds, and that this surge of departing money could lead to delays in processing.

In response, Bybit set up a bounty for the recovery of the stolen funds - get this - offering to pay anyone who is able to recover the funds 10% of anything they're able to recover.

Leo: I'll take it.

Steve: Uh-huh. This has, in turn, set off the biggest bounty hunt on the Internet, with the winners being eligible to earn up to a whopping $150 million. Right? 10% of 1.5 billion. At the same time, not surprisingly, the perpetrators, who were naturally standing by and ready to deal with this massive windfall, quickly began laundering their funds in the hopes of hiding their tracks and diffusing the proceeds of their theft among the world's cryptocurrency exchanges. They're moving quickly because, if they leave the funds in their normal wallets, they risk having them hacked back by multiple parties including law enforcement, bounty hunters, and other threat actors.

Another tweet observed, and this was from a VXDB tweeted: "Lazarus has started laundering the $1.4B stolen ETH." And they said: "Exch.cx, a no-KYC exchange, has recorded an abnormal spike in ETH volume - 20K ETH in the past 24 hours versus its usual 800 ETH. Their Bitcoin reserves are also empty, but their ETH reserves have increased by 900%." So, yes, that 1.5 billion is, you know, sloshing around within the Internet's exchanges while North Korea tries to tuck it away in random corners of the Internet so that it's not all in one place and hopefully, you know, can't easily be tracked and recovered. And we know, since blockchain activity can be monitored and tracked, we now have a bit of a shell game underway.

So what's our takeaway from this? If we're wise, every event teaches a lesson that prevents its recurrence. And hopefully others are also able to learn and gain from seeing what has befallen others, and take away the same lessons without needing to first fall off the same cliff. In this case, I think the lesson here is that the systems which manage these massive cryptocurrency reserves need to be far more isolated from everyday systems than they currently are. In other words, they need to be fully air-gapped, with nothing less being sufficient.

These are lessons that the professional intelligence community and those practicing the highest security in the world learned decades ago. And nothing we've done since with our computer and networking technology has served to make air-gapping any less necessary. We could easily argue that, in fact, the reverse is true, and that air-gapping systems that absolutely and positively must never be compromised has grown more necessary today than ever before.

I would bet that Bybit has just learned the same painful lesson. They obviously felt that requiring a multi-person, multi-keyed funds transfer authorization process would be sufficient. It's certainly better than requiring just one person. They just learned a $1.5 billion lesson, though, that it wasn't enough.

Leo: That's amazing. Wow.

Steve: Wow. Okay. We're going to talk about some sadness about us falling behind in cyberspace after another word from a sponsor, Leo.

Leo: Okay. Very good. Thank you, Steve. And now back to Steverino.

Steve: Okay. So we have North Korean-backed hackers stealing around $1.5 billion of cryptocurrency...

Leo: By the way, that's not the first. They've stolen many billions of dollars over the years. That's how they get hard cash.

Steve: Yeah. It is, unfortunately, it's a profit center for North Korean hackers.

Leo: Yeah, yeah.

Steve: They're good at it. Speaking at the, well, I was going to say that the former head of the NSA, and who's also the ex-Cyber Command head, said in a wide-ranging speech and subsequent interview just this past Saturday, three days ago, that the U.S. is falling behind its enemies in cyberspace. Wonderful.

Speaking at the DistrictCon cybersecurity conference in Washington, D.C., retired General Paul Nakasone said that "our adversaries are continuing to be able to broaden the spectrum of what they're able to do to us." And he said, "and that the United States is falling 'increasingly behind' its adversaries in cyberspace." Unfortunately, he would be in the position to know, having led the NSA and then been in charge of Cyber Command. So, you know, that's the guy whose opinion you care about.

Here's what CyberScoop wrote in their coverage of the event, and in fact they were the people who interviewed him. They said: "Nakasone said incidents like Chinese government-backed breaches of U.S. telecommunications companies and other critical infrastructure as well as a steady drumbeat of ransomware attacks against U.S. targets illustrate 'the fact that we're unable to secure our networks; the fact that we're unable to leverage the software that's being provided today; the fact that we have adversaries that continue to maintain this capability.'

"Nakasone, who led NSA and CYBERCOM from 2018 until early last year and is now founding director of Vanderbilt University's Institute of National Security, said he fears the threats of the future are going to get more dangerous. One example is 'We are starting to see the beginnings of the bleed from non-kinetic to kinetic for cyber operations,' he said, referring to actual physical damage.

"Nakasone said: 'What's next is that we're going to see cyberattacks against a series of platforms being able to actually down platforms with ones and zeros.' A board member for OpenAI, Nakasone also talked about how artificial intelligence could make cyber offense more potent. Specifically, he mentioned the notion [oh god] of generative targeting, such as the idea of physical drones choosing their targets powered by AI." Because, Leo, what could possibly go wrong?

Leo: Yeah.

Steve: He should read some Daniel Suarez to see how he thinks about the wisdom of autonomous AI-powered drones. CyberScoop continues, writing and quoting him: "'We're starting to challenge this idea of humans in the loop, and I also offer to you, as we think about artificial intelligence needs, think about cyber weaponry,' he said. 'How far are we talking to this idea of being able to create an agent that's going to move through your network, that's going to change based upon topology of the network, being able to evade the defenses that are there, choosing targets of the future?'

"Members of the Trump administration, and some members from both parties in Congress, have called for the United States to get more aggressive with offensive operations in cyberspace. In a separate conversation with reporters, Nakasone said he agreed with those sentiments. Nakasone's Cyber Command conducted operations dating back to at least 2018 to disrupt Iranian and Russian hackers in conjunction with more defensive 'hunt forward' missions in other nations designed to fortify allies' defenses and detect future threats against the United States. He also advocated for a philosophy of 'persistent engagement,' to be in constant contact with cyber enemies proactively rather than reactively.

"Nakasone said of offensive operations: 'We need to do more of that, certainly. It's not just the only thing we need.' He said that one of the points of persistent engagement was to ensure anyone who attacked U.S. election infrastructure knew they would suffer consequences from the United States. He said: 'Can we be more forthcoming in terms of some of the things we did? Yeah, I think there's opportunity.'" Okay, so that's interesting. That suggests that we did something in response to foreign interference with our national elections, but that whatever it was was kept on the down-low.

"In his speech, Nakasone said the top priority for the United States should be hiring top talent. Under President Donald Trump, the government has been removing some of those who were in the cyber talent pipeline. Eventually, Nakasone said: 'We're going to have to be able to engage folks again and say, "Hey, please come and work in government." It's an open question how long any damage to the trust of potential hires will last,' he said.

"Another change under Trump is that Defense Secretary Pete Hegseth has reportedly sped up the implementation of a Cyber Command overhaul, from 180 days" - in other words, half a year, you know, six months - "to 45 days," just a month and a half. "In response to a question from CyberScoop, Nakasone said: 'How doable is it? It's really doable when you can get the direction from the Secretary.' Asked if he was worried about whether the tightened timeline would lead to that implementation suffering, Nakasone answered only that the concepts of Cyber Command 2.0 have been in the works for a while already." And actually that's true. I'll just add that the Cyber Command 2.0 initiative was started toward the end of Biden's administration. So that was already underway.

And finally they wrote: "During a question-and-answer session with the DistrictCon audience, Nakasone did not voice any criticisms of Trump's purge of top military officials, such as General Charles 'CQ' Q. Brown, chairman of the Joint Chiefs of Staff. While praising Brown's work, Nakasone said: 'At the end of the day, the President gets to choose his own principal military adviser.'"

So, yikes. We're apparently not giving as well as we're getting, as I was assuming and hoping we were; you know? The NSA is as annoyed as we all are over our inability to secure our own networks, and the future planners are seriously considering AI-powered attack drones without any of those pesky slow humans in the loop, you know, having second thoughts and gumming up the works. And again, it's just so easy to pose our favorite rhetorical question: "What could possibly go wrong?" Wow.

I wanted to announce the achievement of another of my own milestones for the work that I'm doing on the DNS Benchmark. Friday evening I dropped the fifth pre-release of the DNS Benchmark. And just to be clear, these are not betas or even alphas. They are incremental works-in-progress. You know, for example, the first of the pre-releases was the day after Christmas, where the Benchmark was first able to query and benchmark remote DNS nameservers over IPv6. Until then it was only IPv4. So December 26th it got IPv6 capability.

Last Friday evening's fifth pre-release published its new ability to also query nameservers using DNS over HTTPS and DNS over TLS, so the two encrypted protocols that it will be supporting once it reaches its final version 2 completion. All of that is now working. And as always, the reason for this wide-spectrum testing is so valuable, even though everything appeared to be working perfectly for me, the result of that fifth release has been the discovery of a bunch of things that I had missed, a handful of bugs.

So that's what I want. I could not be happier. The Benchmark is coming along nicely, and I have a terrific proving ground of pre-release testers who will help me to assure that the Benchmark's final release will be as completely bug-free as version 1 of the Benchmark was when I released it 16 years ago. So, onward.

And finally, the great "backdoor" replacement, Leo. Last week's call for a replacement for the term "backdoor"...

Leo: Oh, yeah, good.

Steve: ...produced the expected massive wave of replies. So first, thank you everyone. As I mentioned earlier, we now have 16,350, I think it's actually 353, subscribers to the weekly podcast emails. So I'm receiving all the feedback I could ever ask for from all of these listeners. Among the suggestions for backdoor's replacement were many fun ideas. But the one that I saw multiple times, from multiple suggestions from our listeners, and the one that feels best, is simply "Master Key."

Leo: Oh. Duh. Yeah.

Steve: The idea that Apple, or any other similar provider, when put in this position, would arrange their technology so as to have a master key that, implicitly, only they would know. I think that term, you know, it's well understood. It's immediately understood. It's clear. And it offers precisely the concept that I was looking for, you know, since while the key itself is a secret, the designed-in existence of such a key, and such a capability, is not. So as we know, Apple may decline to ever put, ever support any form of master key. They just may say no. We never want that. But that's the right term. I like it way better than a backdoor.

Again, backdoor just doesn't sound right. It doesn't have the right meaning and connotation; whereas Apple holding a master key, that's, you know, that's exactly the right thing. And we know they don't want to; right? They don't want the responsibility. And all of the crypto people will argue, if you have a master key, then somebody can pick the lock.

Leo: Didn't we use to call it, like, "key escrow"?

Steve: Yeah. And you can arrange a key escrow. You can take a big key and break it up in pieces in order to, like, you know...

Leo: Well, you don't have to, to do escrow. You just have to...

Steve: Correct.

Leo: ...give it to somebody.

Steve: You just have to hide it somehow.

Leo: Right, right, right.

Steve: Protect it somehow, yeah.

Leo: So maybe the key escrow is the key that is given to the - not quite.

Steve: Okay, Leo. We are going to talk about the most egregious access to an access control system imaginable after our final break.

Leo: Great.

Steve: And this is just going to - in fact, everyone's going to be able to play along with this. I'm going to - you will, too, Leo. Just wait for this.

Leo: Good.

Steve: This is unbelievable.

Leo: Steve, let's find out, what is FREEDOM? And I want to know more about this. Sounds fascinating.

Steve: Okay. So I assume you have a browser in front of you.

Leo: Yes.

Steve: Open it and search the Internet for the phrase which is the title of today's podcast, FREEDOM Administration Login.

Leo: Okay.

Steve: And I did that a couple days ago, and I got a full page of search results.

Leo: That's not a good - not a good sign.

Steve: I happened to click on the one that began, it was an IP address, 98.174.254.140. Do you see that there?

Leo: Well, let me - I was actually using my AI search engine, which was giving me instructions. So let me just go to Google because that's probably the better place to just get the raw results.

Steve: Yup, yup. Kind of what I did.

Leo: FREEDOM Administration...

Steve: FREEDOM Administration Login.

Leo: Okay. Oh, look.

Steve: There it is.

Leo: It's been asked for so many times. Okay. Oh, yeah, lookit, there's the IP addresses. Wait a minute. These are actual servers.

Steve: Page after page after page. I clicked on the 98.174.254.140. Do you see, is that one there?

Leo: Well, it probably is. It's hard to find it. It's a needle in a freakin' haystack.

Steve: Yeah, well...

Leo: There's 98.191, is that one?

Steve: Oh, try it. I don't know. I just...

Leo: Let's see what we get. So this is a login - okay.

Steve: Now, I don't want you to go any further.

Leo: Because I don't want to be...

Steve: You don't want to break the law.

Leo: ...prosecuted under the Computer Fraud Act.

Steve: Today's main story just makes you shake your head, but the underlying lesson is too important to ignore. Even so, if it weren't already so public I would not be shining any brighter light on it.

Leo: This is that bad.

Steve: It's that bad. But I guess I'm glad others have, even if I would have probably passed. The first sign of something having gone very wrong was the following short news blurb, which read: "Default password in Hirsch building entry systems: Hirsch Enterphone building entry systems contain a hardcoded username and password for their web admin panel that can allow threat actors to unlock doors via the Internet."

Leo: See, this is a little suspicious, this page I pulled up, because the copyright ends 2013. So this is one of those, it's just been left there for 12 years.

Steve: That one probably is. The IP that I found was 98.174.254.140. It was prettier looking than that one.

Leo: Yeah.

Steve: I did see - I did...

Leo: Yeah, there's different - this is the more modern look, yeah.

Steve: Right. Really nice big blue screen with a 3D cube on it is the one that I ended up with.

Leo: Well, see, they all look a little different, depending, I guess, on the vintage.

.STEVE: Yeah. So, again, it's been around for a long time, which, again, sad. Okay. So the hardcoded username and password for their web admin panel, reads this news, that can allow threat actors to unlock doors via the Internet. The default creds are for an admin account named "freedom" that uses the password "viscount."

Leo: Which is the company that makes this.

Steve: Yes.

Leo: Okay.

Steve: According to security researcher Eric Daigle, there are more than 700 Hirsch Enterphone systems available over the Internet, with most used by apartment blocks across the U.S. and Canada. Hirsch says customers did not follow their instructions to change the default passwords. However...

Leo: Who reads the manual these days anyway? Really? Come on.

Steve: Yes, that pesky manual. Hey, look, it works, Martha. We're done.

Leo: Oh, my gosh.

Steve: Fire it up. Let's, okay.

Leo: What is FREEDOM used for?

Steve: It unlocks all the doors of all these apartment buildings.

Leo: Oh, no.

Steve: And it manages all the entries and all the key fobs.

Leo: Oh, that's not good.

Steve: And logs everything. Just wait. I mean, just wait, Leo.

Leo: Oh, that's not good.

Steve: Hirsch says customers did not follow their instructions to change the default passwords. However, the misconfiguration's discoverer, Eric Daigle, says customers are never prompted to change the password during the setup process. Tracked as CVE-2025-26793, the vulnerability has a 10 out of 10 severity score and, okay, the news says is very likely to be exploited. I'll be surprised if listeners to this podcast haven't already thought, well, I'm in a coffee shop. Anyway, that's likely the understatement of the year.

Eric gave his blog posting the title "Breaking into dozens of apartment buildings in five minutes on my phone." And the subhead is "What a place to use default credentials." In his posting, Eric shared his entire process of discovery, which is so fun that it bears sharing here. He explained: "A few months ago I was on my way to catch the SeaBus when I walked by an apartment building with an interesting-looking access control panel.

I wrote down the 'MESH by Viscount' brand name and made a note to look into it when I had a chance. I ended up just missing my ferry." He says, parens, "(the 30-minute Sunday headways are brutal." He said: "So I decided to see if I could find anything promising on my phone while waiting at Waterfront for the next boat.

"Googling the name of the system brings up a sales page advertising 'TCP/IP capability to remotely program and maintain the system.'" He says: "That sounds promising, so let's try to find a manual. 'Mesh by viscount' filetype:PDF" - that's a search - "gets us an installation guide. Page 4 explains how to log into the system's web UI." Eric attached the screenshot he took of his Android mobile phone, from which we learn, among other things, that his location has very good 5G coverage, but that he's also in rather desperate need of recharging his phone's dying battery.

On that page we see the statement: "The default logon information for the Freedom Web Application, as well as the underlying Linux operating system, are listed in the table below. Both are case-sensitive." You know, and you want to be sure to point that out to the hackers. "These should be changed from the default during the software configuration process. And below that is a table showing that the Freedom Login has the username 'freedom' [all lower case] and the password 'viscount' [all lower case]." And that the underlying Linux system has the username, guess, yes, "administrator," and the password is blank. So don't need to bother with that pesky Linux password.

Eric's blog posting notes: "Default credentials that 'should' be changed, with no requirement or explanation of how to do so. Surely no building managers ever leave the defaults; right? And even if they did, they'd surely have no reason to expose this thing to the Internet; right? The screenshot from the manual tells us the web UI login page's title is 'FREEDOM Administration Login,' which gives us something to search for."

Okay. In other words, this web portal's login page has the title "FREEDOM Administration Login," which means that Google will have discovered and happily indexed all of them, sitting there wide open on the Internet. You know, I was hoping that the server might have used some non-standard port. Silly me. And everyone can do this, right now from home, or from your mobile phone, just like Eric did while he was waiting for the ferry and desperately hoping that his phone's battery would last. Just search the Internet for the phrase "FREEDOM Administration Login," and you'll be rewarded with countless hits. I clicked on one. The web server is using port 80, not 443, so it's HTTP and not HTTPS, which, you know, makes it cheesy for an application like this, but, you know.

So I told Firefox that, yes, I wanted to go to this old-school HTTP site, and I have the link in the show notes for anyone who cares. And sure enough, I was greeted with a beautiful big login page for Viscount Systems FREEDOM. And there in the upper-left was the prompt for the system's administrative login username and password. Naturally, that's as far as I took it.

But Eric went in. Here's what he shared. Under "Part 1" of his blog posting, "Personally Identifiable Information Galore," he wrote: "Exposing the panel to the Internet is dumb." That's one word for it. That's a four-letter work, that's good.

Leo: Dumb.

Steve: Dumb. "But fortunately, none of these systems were accessible using the default." And then he says, "Just kidding, of course they were. The very first result happily lets me in with the freedom:viscount login. That's the old-school way of putting a username and password in the URL," he says, "where you put freedom:viscount." He said: "The first interesting thing here is the Users section." Eric shares another

screenshot, from which we learn that he's now on WiFi, and his phone's battery is much happier. The screenshot he shares has blanked out the site's URL for the sake of his blog posting, the building's physical address, and the full building residents' names. But they're all there in their full glory, alongside each resident's unit numbers, so anyone can see exactly who lives where.

Eric notes: "This maps residents' full names to their unit numbers. The building address is also used as the site title. That's already not great, but it's worse in conjunction with the Events section. This is a multi-year log of every time a fob associated with a certain suite number accessed an entrance or an elevator. So we can now easily determine that, say, Jon Snow of Unit 999, at 123 Bear St. in Vancouver, BC comes home every day at 6:00 p.m."

Leo: Oh.

Steve: "For good measure, there's also a Users section which exposes every resident's phone number." Then we get to "Part 2: Breaking In," where Eric writes: "The Personally Identifiable Information leaks are pretty wild, but the most interesting thing we have access to is the Controlled Areas section. In here I can apparently register new access fobs, disable existing ones, and change the doors they're authorized for. The system for this is somewhat convoluted. Fortunately I don't need to understand it at all because I can just unlock any entrance I want through an override function."

And I have a screenshot of that page from the show notes showing main entrance, door, main entrance access, and a dropdown list box with very pretty colorful icons, Leo, showing Unlock with a green hasp open, and then Lock, and then LOCKDOWN. And I suppose LOCKDOWN means that it will no longer unlock for individual users. But, yes, you are able to simply choose the green Unlock icon. You will hear a clunk at the front door, and then you can just walk right in. So an attacker has the ability to unlock any of the doors - any of the doors, elevators, everything - controlled by this otherwise rather high-end building access control system. And Eric notes: "So I can break into this building in about five minutes without attracting any attention whatsoever. Neat."

And then we get to Eric's "Part 3: How widespread is this?" Eric writes: "Maybe I just got lucky that the default credentials worked on the first result, and this is actually really rare. Let's get back to a desktop and scan more properly," he says. Which he then does. He uses some semi-automated scripting to attempt logging into the 742 exposed instances that his quick search turned up. It might be that using a more robust scanner would find many more. But of those 742, Eric's script was able to successfully log into the building's access control system of 43% of them, just shy of half, leaving them completely vulnerable and unprotected while also disclosing information about the building's residents that many would find quite objectionable.

So why is Eric sharing all this, despite the fact that this is significant and far from being merely a theoretical vulnerability? Presumably because he first tried to do the right thing, but the vendor who indirectly created this mess in the first place could not be bothered to address it. Eric's responsible disclosure timeline shows that last year, the end of last year, on December 20th, he discovered this. So five days before Christmas he was looking - he was waiting for the ferry. A week later, on the 27th, he wrote: "Current vendor of MESH identified as Hirsch, a subsidiary of Vitaprotech Group, contacted them. On January 9th, the CEO of Identiv, former vendor of MESH, was contacted."

Two days later, Hirsch product security responds requesting details and are asked if they intend to alert their clients. On the 29th, okay, so that was the 11th. So 18 days go by.

"Hirsch replies, stating that these vulnerable systems are not following manufacturers' recommendations to change the default password."

Leo: Or they're holding it wrong. It's their fault.

Steve: Right. The next day - I know, I love that. The next day, on January 30th, Hirsch was asked for an update as to whether clients running vulnerable systems have been alerted. No response to that. On February 14th, the CVE 26793 was assigned as a 10 out of 10. Yes, everyone knows why. And on the 15th this was published. So anyone who's been listening to this podcast for long will be well aware that there are several fundamental design flaws present here.

Leo: Really. Huh.

Steve: First and foremost, as Eric briefly noted, there's almost certainly no need for an apartment building's access control system to be exposed to the public Internet.

Leo: No.

Steve: So while the Linux-based web server on the network would need to have its web server bound to the internal LAN interface to allow for administrative access by management on the LAN, it should never be bound to the WAN interface. Even Cisco is unable to do this correctly and expose web UI to the public Internet. So certainly these clowns can't.

The second thing that's wrong with this picture is the entire concept of built-in factory-supplied usernames and passwords. Those days MUST come to an end, and that should have happened long ago. The lesson the industry has learned the hard way, over a span of decades of trying very hard not to learn it, is that usernames and passwords is a place where security MUST trump convenience and the associated annoyance of the "I cannot login to my management portal" tech support calls which will result.

Deal with it. There must be no default username and password, and also no form of manufacturer-hidden backdoor username and password. As we know, any of those will be discovered the first time anyone goes looking. The system simply needs to generate a long unique username and password the first time it is started. When it discovers they are blank, it needs to use whatever entropy it's been able to gather from the universe up to that point - which is trivial for any connected device given unpredictable network packet timings - then use that entropy to initialize the username and password to pseudorandom gibberish.

This cannot be left to chance or to someone reading "Please change the username and password from their initial default," and then presumably thinking "Yeah, I'll get back to that once everything else has settled down." You know, it is absolutely important for the system to enforce their being changed just once, or being set just once to something completely random and unguessable. Given that the username and password will initially be gibberish, an administrator should be free to change them immediately if they wish, or the gibberish can be written down. Or the user's password manager can be used to record it. Or the browser's automatic built-in offer to remember it for its user can be accepted. The point is today's ubiquitous tools mean that gibberish is no longer the daunting problem it once was. So let's have gibberish.

We've learned that doing what these clowns have done, of shipping their system with a publicly documented and thus publicly known username and password, while also allowing the system to be accessed from the Internet, is asking for exactly the sort of trouble that will now be visited upon every one of this system's owners. Guaranteed. And finally, adding insult to injury, the damn things all have the same web portal page title, meaning that a simple Google search...

Leo: It's too easy.

Steve: ...brings up hundreds and hundreds of potential victims, with, as Eric's login testing script discovered, a 43% chance of those publicly-known usernames and passwords allowing any casual passerby to see who lives there, where exactly they live, to view detailed historical logs of their comings and goings, and to unlock any of the doors that are controlled by the system's so-called security.

Lord only knows how many other similarly insecure systems exist in the world today. There's no way the owners of these systems, who are obviously not IT trained and focused admins, will ever be made aware of this trouble, until they begin suffering from mysteriously unlocked doors and mysterious thefts that cannot be explained because there's no sign of break-in. At that point, who's ultimately responsible for the damage that results? Well, yes, the bad guys. You know, it's criminal to do this. But it's going to happen.

The saddest thing is that all this is so avoidable by better system design. It would be tempting to conclude that the coders who are designing and implementing such security systems must have no security training. How could they? But who knows? Perhaps the coders did have security training, but when they presented a secure system with a strong password policy system built-in and no public access, they were overridden by management demanding an easier-to-use system that would not burden them with tech support calls and would allow them to have remote access for easier support?

Leo: That's the bingo, right there.

Steve: Yes.

Leo: It's about support, reducing support expenses.

Steve: Yes. That worrisome Log4j vulnerability that was discovered back in December of 2021, which kicked off our 2022 podcast year, turned out to be more worry than reality for exactly one reason. It was difficult to do. Its fruit was not low-hanging. It was up at the top of a very tall tree, well out of reach for all but the most determined and capable hackers. We've learned that not all would-be hackers are rocket scientists. There is indeed an upper crust of elite hackers who can hack anything, but their numbers are blessedly few. The great mass of hackers are those who need to be following a script.

My point here is that this FREEDOM Administration Login catastrophe doesn't even require a script. It's not low-hanging fruit. The fruit has fallen off the tree and is lying on the ground, waiting to be picked up or kicked around. A governing rule of computer abuse is "The easier it is to abuse, the more often and likely it is to happen." I came to full attention when I encountered this story this week because it's been a long time since we've encountered anything that's been begging this loudly to be abused. And there's no

doubt that it will be, especially when you add in the fact that the physical street address for the building being managed by these systems is loudly presented at the top of every logged-in page.

Leo: Come on in, guys.

Steve: It's unbelievable. There's no need to guess which buildings may as well have left all their doors permanently unlocked and the schedules of their tenants posted publicly. Given that it's trivial to log into these portals to determine their physical address, and that the majority of these facilities appear to be located in Canada - so said Eric - a good Samaritan among us might take it upon themselves to login, determine the building's address, and notify the building's management of this glaring security trouble. If anyone listening to this podcast wishes to do so, despite having the best intentions, I would advise taking some anonymizing precautions.

Leo: Oh, yeah.

Steve: Since we've seen instances where white-hat hackers are still being accused of wrongdoing. And technically, using even publicly posted credentials to log in, when you don't have permission, that's a crime. But it would make for a nice security project for anyone interested in doing some good, and it's somewhat astonishing that the publishers of this atrocity, this, you know, it's an atrociously insecure access control system, replied to Eric that, "Well, you know, vulnerable systems are not following manufacturers' recommendations to change the default password" - of course it's their fault - rather than taking any proactive measures to cure these and any future "recommendation failures." Well, that's a recommendation failure. For anyone who might be interested in pursuing this, I've included the link to Eric's blog posting on the last page of this week's show notes.

I haven't mentioned that, even if these systems' default username and password are changed, you know, we're still looking at the always questionable security presented by exposed Internet-facing web UI portals. Right? We know how challenging their security can be. It's some Java, some JSP is the thing that answers this login, that generates this login page. So who knows, you know, where that came from, and whether that can be bypassed. There well might be some, you know, albeit less trivial means of bypassing these systems' login security. Having them exposed to the Internet at all, and readily indexed by anyone who looks, is just such a bad idea.

In any event, no matter what happens from here, this did make a great case study for our 1,014th Security Now! Podcast. And Leo, you and I will see everyone back here next week for number 1,015.

Leo: Wow. Yes, we will. What a great story, and not at all surprising. There are so many like that; you know? And you didn't even have to use Shodan. Just Google. That's all it took.

Steve: Nope, Google.

Leo: Wow. I hope I don't get in trouble for showing those Google search results. How could you? I mean, it's...

Steve: Yeah. It's Eric's blog posting. I found it referred to in a different news site. So it's out there.

Leo: Yeah.

Steve: Otherwise I wouldn't have talked about it. But it's such a good object lesson.

Leo: It is.

Steve: In like, how bad, I mean, just how bad it can be.

Leo: Yeah.

Steve: This is just egregious.

Leo: And I think to some degree this happens again and again because companies want to save money on support. And so they know that somebody's going to forget the password that they set on their login screen to control all the locks in their apartment building, and they're going to call them, and they say, oh, well, good news.

Steve: And you're bragging that you can access it over the Internet. You should not be able to access it over the Internet. Who needs to? In the rare case that that's necessary, then enable it. But don't have it on by default.

Leo: Yeah. Yeah. I mean, I think in some cases that's probably something they want, the manager's offsite or something. I don't know.

Steve: And somebody paid a bunch of money for this, Leo. It's not like this is free.

Leo: Right.

Steve: You know, this was an expensive access control system. It's got controls on the elevators and all the doors, and it's logging people's fob use, I mean, I'm sure it's tens of thousands of dollars.

Leo: Well, if there's any justice, people will sit up and take notice, and the next time somebody needs a security system for their apartment complex, they may not buy FREEDOM.

Steve: Talk about leaving the backdoor unlocked.

Leo: Yeah. Excitement.