Chrome Web Store Is a Mess

Description: U.S. lawmakers respond to the UK's outrageous demand about Apple's encryption. What, exactly, is a "backdoor," and can a "backdoor" NOT be secret? Highlights from last week's Windows Patch Tuesday. A look into RansomHub, the latest king of the Ransomware hill. TOAD: Telephone-Oriented Attack Delivery. The State of Texas v. DeepSeek. Disabling Apple's "Restricted Mode." Where did I put that $800 million in Bitcoin? A sci-fi author update. And a deep dive into the misoperation of Chrome's critically important Web Extension Store.

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-1013.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-1013-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson is here. We'll talk about the U.S. response to the UK's request that Apple stop encrypting your data. Why is everybody calling this a "backdoor"? Steve has got a rant. He doesn't like that word, and he's looking for a better one. We'll also talk about TOAD. Did you know that TOAD stands for Telephone-Oriented Attack Delivery? What's Google doing to stop that? And then we will talk a little bit about what a terrible job Google's doing managing the Chrome Web Extension Store. When you hear this, you're going to - you won't believe it. Coming up on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 1013, recorded Tuesday, February 18th, 2025: The Chrome Web Store Is a Mess.

It's time for Security Now!, the show where we cover the latest security news, privacy news, with a gentle dollop of science fiction and fun, with this guy right here - maybe a little math even - Steve Gibson from GRC.com.

Steve Gibson: Hello, my friend. It's great to see you.

Leo: Good to see you.

Steve: And actually it's funny you should mention sci-fi because I'm going to - we are going to swing in briefly, and I'm going to update our listeners on the recommendations that I accepted from ChatGPT when I asked it for - as we may remember, about four or five weeks ago I said here are the things that I've read that I've enjoyed. What else do you recommend?

Leo: Yes; right.

Steve: And first of all, it guessed a bunch that I hadn't told it about that I also have loved in the past, and recommended some others. Anyway, so we're going to talk about that. Now, I should explain that the title of today's podcast, "Chrome Web Store Is a Mess," is not my title. It's the title given to a jam-packed with information and experience blog posting by a very well-known Chrome and more broadly web extension developer who's been active for more than 20 years, believe it or not, before this podcast began.

Leo: Wow.

Steve: So that was his title. And by the time we're done, rather than people saying, oh, yeah, well, it's a mess, everyone is going to know why. And I contend that understanding the reason why is much more useful than just saying, you know, stating it as a fact. So a lot of really interesting information, which is going to leave us with some questions also about why it's a mess because it's a bigger mess than it arguably needs to be. I mean, like, provably. So what's Google up to? Because it's not like they lack resources. Anyway, so that's our main topic for this Episode 1013 for, here we are in the middle of February already.

We're going to talk about U.S. lawmakers responding to last week's topic or discussion point, which was the UK's outrageous demand about Apple's encryption. Also, I want to just touch on what exactly do we mean when we say "backdoor." What is a backdoor?

Leo: Careful.

Steve: Yeah. Can a "backdoor" not be a secret? Because I don't think so. Also we have highlights from last week's Windows Patch Tuesday. A look at RansomHub, the latest king of the ransomware hill.

Leo: Oh, boy.

Steve: We've not taken a close look at one of these operations for a while because we kind of OD'd on it a few years ago. But there's some interesting stuff here. We also have something called TOAD, which stands for Telephone-Oriented Attack Delivery, which we're going to describe. Also we have Texas v. DeepSeek, which is now a thing. The disabling of Apple's Restricted Mode. And the question - now, this is not I speaking - where did I put that $800 million in Bitcoin? My bitcoin is not worth 800 million, but there is some guy whose is.

Leo: Oh, yeah.

Steve: As I mentioned, we've got the sci-fi author update. And then a deep dive into the misoperation of Chrome's critically important Web Store. You know, 90% capture of the market has Chrome, and extensions are an important part of that ecosystem. But, you know, installer beware because we're going to really understand what's going on there by

the time we're done. And of course one of our great pictures of the week, thanks to our terrific listeners.

Leo: I only can see some peanuts at the top of the screen.

Steve: That's good.

Leo: So I haven't seen the whole thing yet.

Steve: That would suggest that you've seen the caption I gave it, "Lest there be any doubt."

Leo: Well, that's not exactly a giveaway.

Steve: No, it's not. That was my point. That's why I said it, "Lest there be any doubt." And then you see a little row of peanuts, yes. The punchline is down further.

Leo: We'll scroll up together in just a moment. All right, Steve. Let's scroll up together. The Picture of the Week.

Steve: With the caption "Lest there be any doubt."

Leo: Lest there be any doubt. A well-known anti-allergy warning, I guess; right?

Steve: That's right. You definitely want to be notified if what you're eating contains peanuts. If the equipment ever processes peanuts in the past, if peanuts were being eaten by someone walking down the corridor near you...

Leo: I was on an airplane where the flight attendant said we're taking all your peanuts back. There's a kid onboard who's allergic, deathly ill. So we're going to come around and collect your peanuts. So even in the air, if you're really allergic, I guess.

Steve: Yeah. So for those who don't have the benefit of video, we have a large bin, probably like a self-serve bin of peanuts in the shell, so they're those...

Leo: Pretty clearly peanuts.

Steve: It's very, you know, remember the old Planters guy that was like a big peanut?

Leo: Mr. Peanut, yeah.

Steve: Yeah, Mr. Peanut, thank you. Yeah, like there's actually two peanuts in most shells, you hope.

Leo: Sometimes there's three, you never know.

Steve: Yeah, that's a - yeah. Anyway, we've got a big bin of that, leaving no doubt in anyone's mind what this contains. And there is of course a warning sign in front of it, letting everyone know that "This product contains peanuts."

Leo: Really. Well, that's, you know, it could be good news if you like peanuts.

Steve: This product is peanuts, in fact.

Leo: Yes. There you go. This product is peanuts. Oh, boy.

Steve: Okay. So U.S. lawmakers have responded. Last Thursday, Engadget gave their updated coverage of the UK decryption order that headline, "U.S. lawmakers respond to the UK's Apple encryption backdoor request." And the subhead was "Senator Ron Wyden and Representative Andy Biggs said the order is 'effectively'" - they're speaking of the UK's order - "'effectively a foreign cyberattack waged through political means.'"

Leo: Wow. They're not far wrong. I mean, it affects Americans' data, too.

Steve: Yeah. So what Engadget said was: "The UK's shockingly intrusive order for Apple to create a backdoor into users' encrypted iCloud data doesn't only affect Brits; it could be used to access the private data of any Apple account holder in the world, including Americans. Less than a week after security experts sounded the alarm on the report, the U.S. Congress is trying to do something about it." Now, actually, if the U.S. Congress was able to do anything, that would be good.

They continued: "The Washington Post reported on Thursday that, in a rare show of modern Capitol Hill bipartisanship, Senator Ron Wyden" - who is a Democrat - "and Representative Andy Biggs" - an Arizona Republican - "wrote to the new National Intelligence Director Tulsi Gabbard, asking her to take measures to thwart the UK's surveillance order, including limiting cooperation and intelligence sharing if the country refuses to comply." I mean, we're talking about breaking our allegiance with the UK over this, you know, allegiance as in ally.

"Biggs and Wyden wrote" - okay. So this is like the official from Congress. "'If Apple is forced to build a backdoor in its products, that backdoor will end up in Americans' phones, tablets, and computers, undermining the security of Americans' data, as well as of the countless federal, state, and local government agencies that entrust sensitive data to Apple products. The U.S. government must not permit what is effectively a foreign cyberattack waged through political means.'

"The pair," writes Engadget, "told Gabbard that if the UK doesn't retract its order, she should 'reevaluate U.S.-UK cybersecurity arrangements and programs, as well as U.S. intelligence sharing with the UK.' Wyden sits on the Senate Intelligence Committee, and

Biggs is on the House Judiciary Committee and chairs the Subcommittee on Crime and Federal Government Surveillance." So those are the right two guys.

"Wyden began circulating a draft bill that, if it were passed, could at least make the process harder for UK authorities. The proposed modification to the 2018 CLOUD Act would make information requests to U.S.-based companies by foreign entities more onerous by requiring them to first obtain a judge's order in their home country. In addition, it would forbid other countries like, say, the UK, from demanding changes in encryption protocols to the products or services of companies in the U.S. Request challenges would also be given jurisdiction in U.S. rather than in foreign courts." So, you know, basically, if we create a law demanding that changes in encryption products are basically forbidden, then, whoops, okay.

"The UK order, first reported by The Washington Post" - and of course this is what we discussed last week - "requires Apple to create a backdoor into its Advanced Data Protection, a feature introduced in iOS 16.2 back in 2022. Advanced Data Protection applies end-to-end encryption to many types of iCloud data, including device backups, Messages content, notes and photos, making them inaccessible even to Apple. The order demands a blanket ability to access a user's fully encrypted data whenever and wherever the target may be located.

"The order was issued under the UK's" - here comes the word - "Investigatory Powers Act of 2016, known not so affectionately as the 'Snoopers' Charter,' which expanded the electronic surveillance powers of British intelligence agencies and law enforcement. It would be a criminal offense for Apple to publicly confirm receiving the order" - so, like, they can't talk about it - "so the company hasn't commented," writes Engadget, "on the matter. Security experts warn that implementing this backdoor would needlessly expose anyone with any Apple account to foreign spying, hackers, and adversarial countries.

"Apple received a draft of the order last year when UK officials debated the changes. In a written submission protesting them, the company said the planned order 'could be used to force a company like Apple, that would never build a backdoor into its products, to publicly withdraw critical security features from the UK market.' The company can appeal the notice, but cannot use the appeal to delay compliance. Ciaran Martin, former chief executive of the UK's National Cyber Security Center, told The Washington Post: 'Most experts in the democratic world agree that what the UK is proposing would weaken digital security for everyone, not just in the UK, but worldwide.'"

Okay, now, I wanted to take a moment to focus upon the use of the term "backdoor," which has appeared about 20 times so far in what I've read, and even in Apple's own response, which was quoted. Unfortunately, its original meaning is being lost and stretched through reuse for other purposes. As I noted, the term was liberally used throughout the original Washington Post article, and also in Engadget's own reporting, mostly because we don't have another term like that.

Now, in the past I've pedantically objected to the use of the term "backdoor" in these cases, and I'm going to take this opportunity to be at least as pedantic about this again today, but maybe for the last time because I'm going to have to give up. I've previously suggested that what's being asked for is a locked, yet unlockable, front door. That's what they're asking for. Now, I suppose the trouble is that this stuff can be confusing for those who don't inhabit the security space for a living. You know, the term "backdoor" sounds bad; right? And "bad" is often the way someone wants it to sound when they're trying to say, oh, this is what they're asking for is bad. Well, okay. Backdoor.

So what's wrong with using the term "backdoor"? My problem is that words in general need to have and to hold onto their meaning, although we also see that blurring with misuse; right? The term "backdoor" already, I want to say, has - maybe I'd have to say

had - an extremely specific and exact meaning. You know, I mean, we've been around since its early use. It was originally used to describe any sort of security measure bypass, and it was definitely meant to be a secret. Period. A backdoor is, by definition, a secret. So the UK cannot possibly mandate the inclusion of a "backdoor" into anything, because anything mandated could never be a secret. The UK could certainly mandate that Apple have some means for complying with their demands for a user's data. And if that data was initially encrypted for the user's privacy, then Apple would need to have some means for decrypting it in order to comply with the UK's demand.

But nothing about that suggests the use of any sort of "backdoor." And in fact, from where we are now, Apple would need to deliberately design-in a new "front door," for which only they possess the key. Apple clearly objects to doing this, and for that I salute them. As has been previously mentioned, Google has supported full similar end-to-end, device-to-device encryption of cloud-stored data from Android 9's "Pie" edition, and in this case "Pie" referred to a dessert...

Leo: Mmm.

Steve: ...rather than to Pre-Internet Encryption, even though that's what it offered. So that had double meaning there. So if we should not refer to designed-in decryption capabilities as "backdoors," what should they be called? The problem is the security industry doesn't have any sufficiently pithy and engaging term for this. So "backdoor" it is, for better or for worse, even though that isn't at all what anyone is asking for, whether they know it or not.

Anyway, I did say I was going to be pedantic about this, and I'm sure I haven't disappointed on that account. Every time I see the term "backdoor," which again has a very specific meaning, its meaning being used as a generic term for obtaining otherwise-inaccessible information, I think to myself, yeah, but a backdoor is not what it is. Unfortunately, that's what everybody's going to be calling it, and I think we've collectively lost control of the term.

Leo: Do you want to propose another one? I mean, it's basically they want the keys. You have talked before about some sort of...

Steve: They want Apple to be holding keys.

Leo: Yeah.

Steve: I mean, that's really it. They want Apple to be holding keys. Apple has said, "We don't want to be holding keys."

Leo: Right.

Steve: Because, you know, we don't want that responsibility. And also we're selling the fact that we're not holding the keys.

Leo: Right.

Steve: I mean, that's a sales point for Apple technology.

Leo: Well, it's only for the Advanced Data Protection version because they do hold the keys for everything else. And this is important.

Steve: Yes.

Leo: Because most Apple users do not use ADP.

Steve: You and I don't.

Leo: Because it's a pain in the butt, yeah.

Steve: You and I don't. I can't because I still have an iPad where I wait about an hour for it to turn on, but it works. I'm kidding, but...

Leo: Let's be clear. What the UK Snoopers' Charter or the, as you say, the Investigatory Powers Act - now you know why they call it the Snoopers' Charter. Really what they're saying is we want clear text of any message ever, of any file ever. We want access to it when we ask for it.

Steve: Privacy bad. Privacy bad.

Leo: Privacy bad. And we want you to be able to give us the information should we ask for it. And Apple's, you're right, saying we don't want to.

Steve: We don't like encryption. We don't like encryption. You know, we used to be able to put a wiretap on somebody, and we'd get all of the content from them.

Leo: Well, and we saw what happened because of CALEA, that now the Chinese are in our phone system.

Steve: Right. Using that backdoor, for lack of a better term.

Leo: Right. It's up to you to come up with a better name.

Steve: We need, okay, so here it is, this is - here it is. I've asked for a caption on a photo before, so now...

Leo: We need a better name.

Steve: ...this is our listeners' challenge. You all heard that. Backdoor means a secret. So what would be a fun, pithy, catchy, successful term for this, for an encryption bypass, essentially, is what we're asking for.

Leo: That's what it is, isn't it.

Steve: It's an encryption bypass, yeah.

Leo: Yeah. So there is no such thing as real encryption. That's what they want.

Steve: Well, it'll, you know...

Leo: You've mentioned in the past you had come up with - and this is some years ago - the notion of some sort of key escrow system that might allow this without really compromising people's privacy. Do you remember that? Way back when?

Steve: There are. A lot of work has been done. For example, there are ways to take a single key and divide it up among some number of people.

Leo: Right.

Steve: Where you need some subset of those people to provide their content in order to recreate the whole key. So, I mean, there's all kinds of, I mean, cryptographers have solved all these problems before. But when we start getting tricky, and anything seems muddy, you end up, like, no one wanting those CSAM image hashes on their phone.

Leo: Right.

Steve: They're like, they're not the images. No, no, no. We don't want anything to do with that. So I respect Apple for being very sharp-edged about this. It's, you know, yes or no. It's either we cannot do it, or we're not going to try.

Leo: Well, the real issue here, if it were just the UK saying we want that for UK traffic, traffic inside the UK for UK citizens, Apple would just say, okay, fine. UK citizens, you don't get Advanced Data Protection. And that's maybe what will end up happening is the UK might back off and say, okay, just for the UK.

Steve: But then how do you define that border? That's the problem.

Leo: It's very flexible.

Steve: What about a UK phone traveling outside of the UK?

Leo: Or if I'm having a conversation with somebody from the UK.

Steve: Right.

Leo: That's my data, too. So it is very tricky. Asking for it globally, though, Apple is not going to say, okay, we'll turn off Advanced Data Protection globally. They're not going to do that.

Steve: No.

Leo: And they shouldn't.

Steve: No, not because the UK says we want the right to have access to anyone's data. No.

Leo: Yeah. Ron Wyden's right.

Steve: And, I mean, so for a couple years now, right, we've been talking about and following and chronicling the inherent tension. In fact, it's why I dropped the development of CryptoLink, which was my, you know, I mean, absolutely uncrackable cryptographic networking technology. And I just decided I don't want to invest heavily in creating something that the government may tell me is making me an outlaw.

Leo: And this is back in the Obama days.

Steve: Yeah.

Leo: Right? I mean, this is well before this was an issue.

Steve: And so it is really good that the UK has come down like this because now, I mean, what they've asked for is such overreach, as you said, so much - they're asking for complete decryption of anything they want. They need to just be told no. And other governments who are watching this are going to go, oh, okay, well, let's not try. I mean, France, as I mentioned last week, France has got some of their own legislation moving forward through their own parliament. And if the UK just gets slapped down and says, you know, if you want to do that, we're just, you know, not going to give encryption to anybody in the UK, see how your citizens like that.

Leo: And honestly, if our Congress asked for that in the UK, if the U.S. Congress said, oh, and we want to be able to look at anybody's conversations anywhere in the world, people in the UK would be just as upset as we are.

Steve: Yeah.

Leo: It's not okay. It's UK.

Steve: It's UK. I saw that coming.

Leo: There's a slogan.

Steve: That's right. Okay. So compared with last month's massive batch of software fixes, it didn't break a record. That's, what is it, 163 or something? But it was a local record. February's updates last week were mild. They addressed a mere - merely 63 flaws and eliminated a pair of less severe, though still actively exploited, zero-days in Windows. Of those 63 flaws, three were rated critical, 57 were deemed to be merely important, one was moderate, and the last two were rated as low severity, so don't be in a big hurry for that. But of course they all come as a big bundle.

In addition to those 63, Microsoft also separately resolved 23 flaws over in their Chromium-based Edge browser. The two resolved zero-days had CVSSes of 7.1 and 7.8, respectively. The 7.1 was an elevation of privilege in Windows Storage. Microsoft's alert said: "An attacker would only be able to delete targeted files on a system." That's interesting. "This vulnerability," they said, "does not allow disclosure of any confidential information, but could allow an attacker to delete data that could include data that results in the service being unavailable." Thus the 7.1. It's like, well, that's not good. But it's not going to, you know, it's not a 9.8 house-on-fire CVSS.

However, Mike Walters, the president and co-founder of Action1, noted that the vulnerability could be chained with other flaws to escalate privileges and perform follow-on actions that can complicate recovery efforts and allow threat actors to cover up their tracks by deleting crucial forensic artifacts. So, yeah, deletion, if that's all you can do, that can still be good, if you want to delete logs of you poking around in someone's system which you would otherwise not be able to delete.

The second zero-day, having the higher CVSS of 7.8, also created an elevation of privilege vulnerability, this time in Windows Ancillary Function Driver for WinSock. WinSock is short for Windows Sockets and is part of the operating system's networking subsystem. Due to the fact that the AFD.sys driver is down in the kernel, the successful exploitation of this vulnerability, you know, good old networking vulnerability, would allow an attacker to obtain system privileges. So, you know, yes, escalation all the way up to full system.

Now, a similar flaw in AFD.sys was disclosed by General Digital last August after they found that it had been weaponized by North Korea's Lazarus Group. A year ago, in February of 2024, Microsoft plugged a Windows kernel privilege escalation flaw affecting the AppLocker driver (that's appid.sys) that was also being actively exploited by the same group. These attack chains stand out because they do not rely upon the Bring Your Own Vulnerable Driver (BYOVD) approach, which we've talked about, like an old signed printer driver which has known flaws. The bad guys will bring that in. It's signed, so Windows says, oh, a signed driver, let's load it. And then they exploit the vulnerability down in the kernel that that driver created. That's the Bring Your Own Vulnerable Driver.

Instead, what's happening here is that they take advantage of the comparatively rare security flaws that still can be found, and these two were just patched, in native Windows drivers to eliminate the need to introduce vulnerable drivers into their targets. And really locked-down systems can even prevent, not surprisingly, the Bring Your Own Vulnerable Driver. They're locked down so much they won't allow any new driver to be installed. Of

course that creates lots of headaches for people who just want to use Windows a little more casually, but you can't have it both ways.

Now, it's not known whether the abuse of last month's zero-day is also linked to the Lazarus Group. Remember, both of these drivers are zero-days. They were under abuse. So somebody had found them, and they were found being exploited. CISA has added both of the flaws to its Known Exploited Vulnerabilities (KEV) catalog. Their presence in CISA's KEV catalog does require federal agencies to apply patches by the 4th of March, so within like four weeks of this thing happening.

So the most severe flaws addressed by Microsoft in this month's update were not zero-days. There's of course CVE-2025-21198. That's got a CVSS of 9.0, allowing a remote code execution in the so-called High Performance Compute, or the HPC Pack. Microsoft documented that, saying: "An attacker could exploit this vulnerability by sending a specially crafted HTTPS request to the targeted head node or Linux compute node granting them the ability to perform remote code execution on other clusters or nodes connected to the targeted head node or Linux compute node granting them the ability to perform remote code execution in other clusters or nodes connected to the targeted head node."

Okay. So although this is bad, it wasn't known to be abused at the time of its patching. So, you know, now the vulnerability is known. And remember, CVSS of 9.0, and it's a remote compute in something network, remotely network accessible. So the bad guys could potentially reverse engineer the update, discover the vulnerability, weaponize it, and start using it. So now would be a good time to apply this month's patches, if you haven't already.

There's also an 8.1 CVSS which affects Windows LDAP, its Lightweight Directory Access Protocol. The flaw allows an attacker to send a specially crafted request and to execute arbitrary code. Now, since that's really not good, the LDAP flaw would normally have a higher CVSS, right, network-accessible remote code execution. So why only in 8.1? Because it involves a race condition that has to be one in order to succeed.

Even so, Ben McCarthy, the lead cybersecurity engineer at Immersive Labs, said: "Given that LDAP is integral to Active Directory, which underpins authentication and access control in enterprise environments, a compromise there could lead to lateral movement, privilege escalation, and widespread network breaches." In other words, you know, the precursor to ransomware in your company, and nobody wants that.

Oh, and speaking of authentication, because that's what this problem was is a very low probability of success authentication bypass. There's also a CVSS 6.5 NT LanMan v2 hash disclosure vulnerability which, if successfully exploited, would permit an attacker to authenticate as the targeted user. So not any "sky is falling" updates; but, as usual, updating as soon as practical would be a good idea. RansomHub.

Leo: Oh. With a "u." Misspelled. Is it, or no? No, it is spelled with an "o." Okay.

Steve: Yeah.

Leo: At the top, at the top you spelled it with a "u." And I thought...

Steve: Oh, you're right, I did notice that the spelling...

Leo: That's a good way to spell it.

Steve: Yeah, sum.

Leo: It's RansomHub.

Steve: RansomHub. So this 2024's, as in last year's, Top Ransomware Group, they hit more than 600 organizations.

Leo: This is the email you do not want to see.

Steve: "We are the RansomHub. Your company servers are locked, and data has been taken to our servers. This is serious."

Leo: Yeah.

Steve: Then they have "Good news: Your server system and data will be restored by our Decryption Tool. For now, your data is secured and safely stored on our server." Oh, that's nice.

Leo: What a relief.

Steve: We're your backup system.

Leo: Yeah.

Steve: That's right. "Nobody in the world is aware about the data leak from your company except you and RansomHub."

Leo: Oh, boy.

Steve: In other words, we got it. We encrypted it. We wiped all of yours out because obviously you're not able to hold onto it. And it's been decrypted, and we haven't told anybody. So now's the time to pay.

Leo: Look at their address. Holy cow.

Steve: Yeah, well, those are Tor nodes.

Leo: Ah. Okay. So that's a GUID. Okay.

Steve: Yeah. So under the FAQ section of their ransom note they have: "Who we are." And then they've got a normal browser link, and then a Tor browser link that will take you to their site on the dark web in order to learn about these nefarious cretins.

Leo: Well, I'm going to go to the authorities immediately.

Steve: That's right. And then they say: "Want to go to the authorities for protection? Seeking their help will only make the situation worse." And then they go on to explain how you will be prevented, you know, they will try to prevent you from seeking help, and they're incompetent, and incident reports, and blah blah blah blah blah.

Leo: Wow.

Steve: So, yeah, and they even give a Wikipedia link to the General Data Protection Regulations to show how you could get in trouble if you do anything except open your bitcoin wallet to these guys.

Leo: Wow. Wow.

Steve: Well, so what we have is a new and quite effective Ransomware-as-a-Service, which of course is the way to do this now, RaaS, Ransomware-as-a-Service group, calling themselves Ransom, with an "o," Hub. They had risen in prominence to become last year's number one perpetrator after compromising the networks and data of more than 600 organizations worldwide. And no doubt a bunch of them were the school districts that we talked about recently. The RansomHub bad guys have been observed leveraging now-patched security flaws in Microsoft's Active Directory and the Netlogon protocol to escalate privileges and gain unauthorized access to a victim network's domain controller as part of their post-compromise strategy. So, you know, larger organizations that have a domain controller around.

Analysts at Group-IB write in a report published last week that "RansomHub has targeted over 600 organizations globally, spanning sectors including healthcare, finance, government, and critical infrastructure. This has firmly established them as the most, currently the most active ransomware group through 2024."

Now, the group first surfaced exactly a year ago, in February of 2024, after acquiring the source code associated with the now-defunct Knight, K-N-I-G-H-T, formerly known as Cyclops, Ransomware-as-a-Service group from the RAMP cybercrime forum. Five months later, an updated version of the locker, as it's called, you know, the encryption software, the locker, was advertised on the illicit marketplace with capabilities to remotely encrypt data via the Simple File Transfer Protocol (SFTP). The group's updated malware comes in multiple variants that are capable of encrypting files on Windows, VMware ESXi, and SFTP servers. RansomHub has also been observed actively recruiting affiliates from LockBit and BlackCat groups as part of the partnership program.

Leo: This is very professional. Wow.

Steve: Unfortunately, indicating an attempt to capitalize on law enforcement actions targeting its rivals. Remember that we've talked about how, you know, when you get

stomped on, all the rats scurry, and some of them take the source code with them and set up new operations. Some of them just switch over to using, you know, like merge with other groups. In the incident which was analyzed by Group-IB, RansomHub unsuccessfully attempted to exploit a critical flaw impacting Palo Alto Networks PAN-OS devices. That was using a flaw 2024-3400, and they were trying to use a publicly available proof-of-concept. But then they ultimately breaching the victim network by means of a brute-force attack against the VPN service.

The Group-IB researchers said: "This successful brute force attack used an enriched dictionary of over 5,000 usernames and passwords. The attacker finally eventually gained entry through a default account frequently used in data backup solutions, which then allowed them to breach the network perimeter." So don't reuse usernames and passwords from anywhere. Make your own from scratch, everybody.

The initial access was then used to carry out the ransomware attack, with both data encryption and exfiltration occurring within 24 hours of the compromise. The attack weaponized two known security flaws in Active Directory, one from 2021. Now, okay. Anybody who's getting compromised today, or I should say in 2024, through an Active Directory flaw that was patched in 2021? Again, I will never tell anybody they deserve it, but wow. Come on.

So that was 2021-42278, also known as noPac, and the Netlogon protocol, that flaw dates from 2020, the year before, that CVE-2020-1472, also known as ZeroLogon, that we've talked about. And so here's a network, again, just nobody is giving it any thought, any maintenance, any updates. I mean, you know, you have to try not to have your system updated by Microsoft. It takes work for that to be the case. So, yikes. And that, of course, allowed the attacker to seize control of the domain controller and then conduct lateral movement within and across the network. So, trouble.

The researchers said that: "The exploitation of these vulnerabilities enabled the attacker to gain full privileged access to the domain controller, which is the nerve center of a Microsoft Windows-based infrastructure. Following the completion of the exfiltration operations, the attacker prepared the environment for the final phase of the attack. The attacker operated to render all company data saved on the various Network Attached Storage systems completely unreadable and inaccessible, as well as impermissible to restore, with the aim of forcing the victims to pay the ransom to get their data back."

The researchers added: "The origins of the RansomHub group, its offensive operations, and its overlapping characteristics with other groups confirm the existence of a still-active cybercrime ecosystem. This environment thrives on the sharing, reusing, and rebranding of tools and source code, fueling a robust underground market where high-profile victims, infamous groups, and substantial sums of money play central roles." Ransomware-as-a-Service affiliates are incentivized with an 80 [eight zero] percent share of ransom proceeds.

Leo: Whew. Wow.

Steve: Yeah, that was always the thing that, from the first moment this appeared, Leo, you and I noted that that's so smart, that the affiliates that are doing essentially the upfront work of getting into people's networks and creating, you know, opening those doors, be they front or back, that they get 80% of the proceeds. That's just, dare I say, smart.

Leo: These guys, they take a smaller cut than Apple does. You know, oh, we're only going to take 20%. But, you know, if you've got a thousand affiliates, that adds up.

Steve: Yeah. So after originally being saturated in ransomware stories, you know, I've been actively avoiding them since there hasn't really been that much new to report, except just incidents [crosstalk] incidents.

Leo: Ongoing, yeah. Yeah, yeah.

Steve: Law enforcement has successfully tracked down, when they've been, like, really motivated by the big embarrassing breaches, tracked down and stomped out many of the larger and highest profile groups. But, exactly as was predicted, any members who managed to escape law enforcement sweeps, or those who were more peripheral to the operations, changed groups, moved, merged into others, or formed new groups. The problem is, as we saw during last week's detailed look into attacks on K-12 school systems, there's just too much money potentially waiting to be collected from insurers for bad guys to ignore the chance to get some of that.

So ransomware, in one form or another, promises to remain a cybercrime staple for the foreseeable future. It's not going away. It's, you know, I would argue, maybe it became too high-profile and learned a lesson from that, you know, all of that, you know, shutting down the East Coast's oil pipeline, that roused the giant, and those groups no longer exist today. But it as a source of extortion and revenue through extortion, that's not gone away, and it's not going to.

Leo: You can kind of see why. I mean, not only is it lucrative, it's probably pretty fun to try to find a way to get into these systems; right? It's like a game. And you get paid.

Steve: I would always be too afraid. On the other hand, I'm not in Russia aiming at the West.

Leo: Well, that's it. If you're in Belarus, nobody's going to arrest you. You know? You're safe.

Steve: Yeah.

Leo: And, you know, you're underemployed. They probably are highly educated. Maybe not. Maybe they're just script kiddies. But...

Steve: A lot of these, they're, I mean, this does show some ingenuity.

Leo: It's clever.

Steve: Yeah. And how many ways are there to socially engineer an attack? I mean, and now you've got GPT making your letters sound really good.

Leo: That's right. You can no longer look at a phishing attack and say, well, that's clearly phony because of the bad grammar. No, they're perfect.

Steve: Yeah.

Leo: Spelling, grammar, everything.

Steve: And you can also say, well, you know, this is a company involved in remarketing, you know, flimwizzles, and so please write a letter that would induce a flimwizzle purchasing agent to click on this link.

Leo: I think I can write that letter for you. Wow. Wow.

Steve: Yeah. Here's something I didn't realize was a thing until I learned that Google was beta testing its prevention. There's a class of attack using the acronym TOAD, which stands for Telephone-Oriented Attack Delivery. This forthcoming feature of Android 16 blocks fraudsters from sideloading apps during phone calls. Now, when I read that, I thought, sideloading apps during phone calls?

Leo: What?

Steve: That's a thing? Anyway, the Hacker News explains. They wrote: "Google is working on a new security feature for Android that blocks device owners from changing sensitive settings when, that is to say while, a phone call is in progress."

Leo: Wow.

Steve: Which they're directed to do by the fake tech support guy.

Leo: Oh, so it's not automated. Somebody says, oh, you know...

Steve: Yes.

Leo: Can you see this?

Steve: It's like, oh, to do this you have to - anyway. Specifically, they said, new in-call anti-scammer protections include preventing users from turning on settings to install apps from unknown sources and granting accessibility access. The development was first reported by Android Authority. Okay. So apparently scammers are - as we can like reverse engineer the attack from this; right? Scammers are instructing unwitting users to do things during phone calls, such as, I suppose, when calling a fake technical support hotline for assistance.

The Hacker News continues, saying: "Users who attempt to do so during phone calls will now be served the message: 'Scammers often request this type of action during phone call conversations, so it's blocked to protect you. If you are being guided to take this action by someone you don't know, it might be a scam.'" Furthermore, it blocks users from giving up app access to accessibility over the course of a phone call.

The feature is currently live in Android 16 Beta 2, which was released last week. With this latest addition, the idea is to introduce more friction to a tactic that has been commonly abused by malicious actors to deliver malware. Dubbed telephone-oriented attack delivery, TOAD, got to love that acronym...

Leo: I love that, yeah.

Steve: Yeah. These approaches involve sending SMS messages to prospective targets and instructing them to call a number by inducing a false sense of urgency. Last year, NCC Group and Finland's National Cyber Security Centre disclosed that cybercriminals were distributing dropper apps using a combination of SMS messages to initiate scam calls, followed by phone apps calls to trick users into installing malware such as Vultr.

The development comes after Google expanded restricted settings to cover more permission categories in order to prevent sideloaded apps from accessing sensitive data. So, like, so Google added protections, and then the bad guys realized, oh, we've got to get those to be turned off. So let's get the guy on the phone and explain why, oh, you need to turn this off just for just a second. We just need to make a few little changes here in order to solve your problem. So Google has also rolled out the ability to automatically block sideloading of potentially unsafe apps in markets like Brazil, Hong Kong, India, Kenya, Nigeria, Philippines, Singapore, South Africa, Thailand, and Vietnam.

So anyway, this seems like a very useful feature, and I think it's the sort of thing that our phones could obviously very easily do. How often do you actually need, would you legitimately be fiddling with app access permissions while you're on the phone? I mean, it could even be, like, sorry, this is not available while the phone is in use. So, you know, like a deliberate shutdown in the phone's multitasking system.

Leo: The problem is that sometimes it's legit; right? If you called your...

Steve: Could be.

Leo: ...help desk at your company, and they want you to do this...

Steve: Yup.

Leo: ...that's the problem. So all they can really do is warn you and say...

Steve: Yeah, and I think this should serve us as a reminder of just how effective social engineering attacks remain. You know, as I've often said, most people have no idea how any of this stuff works. You know, they're just like, okay, what, you know, how - I can turn it on. And, you know, when a knowledgeable-sounding voice at the other end of the

phone explains how to fix some made-up problem, you know, many people will just follow along.

Leo: Sure.

Steve: Especially when this is, you know...

Leo: Especially older people; right?

Steve: Yes. And, right, when it's spoken with authority, I mean, notice how even ChatGPT's voice of authority, it's like, it's seductive. It's like so sure that it's correct. I loved how - it wasn't Andy, it was Alex who was mentioning that he asked about the specs for some router for he had like the 16-port version. And he asked for the specs for the 8 and the 4. And the 8 exists. There is no 4-port version. But it just produced a four-port specification sheet that was beautiful.

Leo: Yeah.

Steve: For a completely fictitious router.

Leo: "Confidently wrong" is the term.

Steve: Yeah.

Leo: You saw, I mean, this is such a common problem that Zelle, which is the electronic payment system used by very many banks, Chase just started blocking Zelle payments through social media contacts because there are so many scam social media systems; right?

Steve: Yup.

Leo: And older people go, oh, yeah, I saw this guy, a thing on Instagram. And so they're going to stop it because 50% of fraudulent wire transfers from Zelle originate on social media.

Steve: Wow.

Leo: I mean, we're sitting ducks out here, Steve. Help us. It's amazing. It's just amazing. Good, good on Google for doing that. That's probably the least they can do, you know.

Steve: Yeah. I mean, again, it makes so much sense. It's a simple thing to do. And I'm sure there's an, you know, if you're really sure, then okay. But, you know, but for that to come up on your phone, even some oldster is going to go, oh.

Leo: Sure.

Steve: That didn't occur to me. Ooh, you know?

Leo: Oh, right.

Steve: Sonny? Who do you say you were with again?

Leo: Yeah, yeah. I see that. Zelle does that now if you use it a lot, which I do. It'll warn you. It'll even show you sample spoof messages and things, say, you know, this happens. You can't - so they're doing - I guess they're really a vector.

Steve: Let's take a break, and we're going to talk about Texas v. DeepSeek.

Leo: Oh. Okay. That should be - that'll be interesting. All right.

Steve: Under the heading "Because why not?," we have the news, reported by The Record, that Texas is investigating DeepSeek.

Leo: Of course they are.

Steve: Because why not?

Leo: It comes from China; right?

Steve: Which, you know, yeah, DeepSeek comes from China.

Leo: It's got to be bad.

Steve: What did they do wrong? Well, they embarrassed the U.S. by making a better AI. So we've decided that they probably violated the state's data privacy laws, and we need to find out, says Texas. In their reporting, The Record wrote: "Attorney General Ken Paxton's office has also requested relevant documents from Google and Apple, seeking their 'analysis' of the inexpensive and open source DeepSeek app and asking what documentation they required from DeepSeek before they made the app publicly available for download on their app stores."

Leo: Oh.

Steve: In other words, the Attorney General in Texas has no information of any sort whatsoever.

Leo: Well, that's obvious.

Steve: But just thinks that it's kind of probably a bad idea.

Leo: Tell us about it. You tell us.

Steve: Yeah, exactly. That's right. Paxton said in a statement: "DeepSeek appears to be no more than a proxy for the CCP." Oh, those commies.

Leo: That's a little much. Okay, yeah.

Steve: Those commies, yeah, to undermine American AI dominance. And, you know, and they did it better than we did - we don't like that - and steal the data of our citizens. That's why I am announcing - mostly it's the announcement. "I'm announcing a thorough investigation and calling on Google and Apple to cooperate immediately by providing all relevant documents related to the DeepSeek app." In other words, their AI is better than ours, and we can't have any of that. So we're going to investigate them in order to hopefully find some evidence of some misbehavior somewhere.

The Record wrote: "DeepSeek, Google, and Apple did not immediately respond to requests for comment." And maybe even not not immediately. "On January 28th, Paxton banned DeepSeek's use on all devices owned by members of his staff due to security concerns and what a press release from his office called 'the company's blatant allegiance to the CCP, including its willingness to censor any information critical of the Chinese government.'" Oh, that's right, because it doesn't have the right to censor information that's critical of China, even though it's from China.

"This week, New York State and Virginia both blocked the use of DeepSeek on government devices; and on Monday, Representatives Josh Gottheimer, a Democrat from New Jersey, and Darin LaHood, an Illinois Republican, introduced a bipartisan bill that would ban federal workers from using DeepSeek on government devices."

Leo: Josh Hawley has proposed a bill that would fine anybody a million dollars, or as much as 20 years in prison, for downloading DeepSeek. You know, you can run DeepSeek in the U.S. explicitly; right? It's just a model that people can download. There are a number of places you can run DeepSeek around here.

Steve: So, sadly, yes. Any Chinese...

Leo: Without any access to China. Without, you know, completely locally.

Steve: Right. Any Chinese technology backlash has become predictable, with DeepSeek just being the latest example. Since it's exceedingly difficult to prove that China is not

using their DeepSeek app, you know, the smartphone, the mobile app, to monitor the questions, behavior, and who knows what else of U.S. citizens, it appears that we're inevitably heading into a world of increasing mistrust, you know, basically a technology cold war, where everyone is going to be trusting, only going to be trusting the hardware, software, and firmware produced by their own country and their close allies. And even close allies are having trouble, as we're seeing with the emerging standoff between the UK and Apple.

That this was where we were headed appeared to be clear for years. As tensions between the U.S. and both China and Russia have been gradually mounting, everyone listening to this podcast has heard me wonder on many prior occasions how it is that China and Russia were still using Microsoft's Windows, an operating system that could so easily be hiding pro-Western capabilities. As we know, both of those countries have felt similarly and are now working to remove Windows from their critical enterprises and industries. And as we know, that's a feat that's much more easily ordered than accomplished. It's sad, Leo, but it's the direction we're headed in; you know?

Leo: Well, here's the thing.

Steve: Having a technological dtente for a while.

Leo: The reason this was embarrassing the U.S. is because this was an open model.

Steve: Yes.

Leo: And so you can run DeepSeek v3. Here it is on Together AI, but there are plenty of places you can do this, running completely on United States servers. By the way, you can ask about Tiananmen Square because it doesn't have that block.

Steve: Yup.

Leo: It will respond. You don't need the app. And this is great. It's good it was open source. Even Sam Altman said, yeah, we might be on the wrong side of history with this.

Steve: Yeah, well, I mean, they are. This was a breakthrough. This was, without a question, it caught a lot of people flatfooted in the more traditional, I mean, and I say "traditional" with air quotes because, yeah, that's a month ago was traditional.

Leo: Let me just quickly query this DeepSeek running at Together.ai to see if it will tell me about this famous photo of a man standing in front of a tank. Oh, yeah, absolutely.

Steve: Un-huh.

Leo: Tiananmen Square protest, 1989, Tank Man. This is DeepSeek, the so-called "censored Chinese AI."

Steve: Yeah.

Leo: Never mind.

Steve: Yeah.

Leo: Somebody should call Ken Paxton and show him this.

Steve: Well, and I would imagine somebody will surface a non-Chinese DeepSeek-based U.S. app.

Leo: Well, that's what this is. It's not an app, but it's a website, Together.ai.

Steve: Well, but an app because it is the app that Texas is upset about.

Leo: Yeah, well, yeah. I took the app off. I don't need the app; right?

Steve: Right. Right. But I would imagine somebody will do an app based on domestic hardware running, you know, DeepSeek.

Leo: You could right now, yeah.

Steve: Because it's a great model.

Leo: Yeah.

Steve: Yeah. Okay. I wanted to note that eight days ago, as I'm sure you covered on MacBreak, Apple announced that they had updated all of their operating systems to fix a bug that they said may - and of course they always say "may" - may have been used in "extremely sophisticated attacks against specific targeted individuals." Which is to say we know that it was, but we're not going to say that.

Back when it was introduced, we covered the introduction of so-called "Restricted Mode." It further locks down Apple devices wherever it's enabled. On the one hand, it makes those devices much less fun to use because they can't do as much. But that's the whole point; right? With more capability comes more opportunities for vulnerability. We once talked about how it's actually like a - it's not a multiplicative, it's a squaring function because anything you add that interacts with everything else has all those new interaction possibilities. It's not just twice as much, it's the square of number of interactions.

So in return, however, for making the devices much less fun to use, it also makes them far less easy to compromise. And I strongly endorsed the addition of this option at the time since we still haven't figured out how to make highly complex products 100% secure and bulletproof. So this allows an individual who is a high, you know, a highly likely to be targeted target of interest person to make their phone less functional in return for making it much less easy to compromise.

The flaw that was fixed, this flaw that Apple just fixed eight days ago, which is now fixed, would have, and presumably did at the time, allow sophisticated attackers to employ the flaw in an attack chain. Its role in the chain was to disable restricted mode, which should not have been possible. That should have been a UI thing only, on a locked device. So the phone was locked. Restricted mode was enabled. With this flaw as part of the attack chain, restricted mode would be turned off, even though the phone was locked.

The vulnerability, as described, could have been used to enable unlocking technology similar to that that's in Cellebrite's products, which as we know allow snoopers to break into devices when they have physical access to them. And what I loved is that Apple's restricted mode also helps with this by proactively blocking data access to iPhones and iPads when they've been locked for more than an hour. So after the phone's been locked for more than an hour, the physical access through the external port is restricted so that, you know, you can't plug it in and have it be a drive or connected to your car or whatever. You know, very cool.

The vulnerability in Apple's iOS and iPadOS affects iPhone XS and later, iPad Pro 13-inch, iPad Pro 12.9-inch 3rd generation and later, iPad Pro 11-inch 1st generation and later, iPad Air 3rd generation and later, iPad 7th generation and later, and iPad mini 5th generation and later, said Apple. So across the board that's been fixed. And, you know, just a good thing that they're doing that, staying on top of this.

In other news we have, Leo, James Howells. That's the poor guy who lost his hard drive...

Leo: Oh, I know where I know that name, yeah.

Steve: ...containing the only copy of the 51-character private key which he needs to unlock his cryptocurrency wallet.

Leo: Sounds familiar. His wife threw it out, by the way. Did you see that?

Steve: Yeah. The wallet contains 8,000 - yes, you heard me right - 8,000 bitcoins.

Leo: $800 million.

Steve: $800 million.

Leo: Give or take.

Steve: With bitcoin now worth around $100,000 each.

Leo: Wow.

Steve: Ouch. That's got to hurt. James is certain that the drive was mistakenly thrown out with the trash and is now lurking somewhere in a landfill in Newport City, Wales.

Last month he lost a court battle with the Newport City Council in Wales, which may have been his last shot at excavating the dump since, soon after, the city council revealed that it would be closing the landfill and building a large solar farm on the site. He offered to purchase the landfill. He was going to get investors who would all be willing to gamble that he was going to be able to find the drive somewhere, and so they would invest in subsidizing his purchase of the entire landfill property so that he could go through it, gunky bit by gunky bit, I mean, we're talking old bananas and, ugh, to find the hard drive and then recover his $800 million.

Anyway, the city council said no, we're not going to offer it for sale. We're going to set up a solar farm there because we want to replace our fleet of diesel garbage trucks with EVs to help the city transform itself into a renewable energy, lower carbon footprint environment. So, sorry about that. The opportunity is closing. You know, unless you're going to tunnel underneath the solar farm. I don't think they're going to allow him to do that. So, ouch. Looks like that chapter is closing. And of course stories abound, right, of people who, well, and my own, and yours, Leo, who didn't take those early bitcoin wins very seriously.

Leo: Somebody we know very well bought, I think he said three bitcoin for $6 back in the day. It's right around when we were talking about it. He heard the show. He has kept them all this time.

Steve: Nice.

Leo: And he is about to buy a car. He calls it his "$6 car."

Steve: Nice.

Leo: It will be a nice car.

Steve: Nice.

Leo: But you have to keep it. That's the problem. When it gets to a hundred bucks you might be tempted. When it gets to 150.

Steve: Well, I remember that spike at $17,000.

Leo: Yeah.

Steve: That set me on my first complete check of every hard drive, every drive image, everything I had where it might have been around. And yes, had I found it, I would have said "Woohoo!"

Leo: You would have sold it; right.

Steve: Absolutely. Absolutely.

Leo: And now you'd be kicking yourself. I'm just figuring I'm going to hold onto that wallet until quantum computers can crack the RSA encryption, and then I'll have some money.

Steve: That'd be cool.

Leo: Might be worth millions by then.

Steve: It absolutely could because, as I covered, you were on vacation when Tom and I did the bitcoin...

Leo: The intro to bitcoin, yeah.

Steve: You know, the whole podcast was on the topic of the bitcoin blockchain, and I explained how it worked and how the number of bitcoins were asymptotically approaching a limit. It was designed-in scarcity, which is the reason we've seen what's happened happen. And I should have taken my own advice.

Leo: Oh, Steve.

Steve: I've been waiting to gain sufficient experience with a new-to-me sci-fi author before mentioning my recent science fiction reading enjoyment. As I mentioned at the top of the show, I don't remember if it was before we began recording or not, I took ChatGPT up on its advice about other authors who were similar to those whose novels I'd previously enjoyed more often than, you know, sometimes I've enjoyed them more often than once. As we recall, ChatGPT not only produced a list of recommendations, but among those were others of my favorites that I had never mentioned, or like didn't ask in that proposal to ChatGPT. And, you know, being cautiously suspicious of AI, we wondered whether ChatGPT might have previously ingested my own published sci-fi reading list, or even the transcripts of this podcast. Who knows how it came up? But it did suggest others that, you know, I had already read.

But in any event, I obtained a handful of new author recommendations. Since I had seen Neal Asher's name around a lot, I purchased a copy of "Gridlinked." And I do mean purchased. It wasn't free as part of the - it wasn't offered as part of the Kindle Unlimited plan which I subscribe to. Everything else I've been reading recently has been. But given that inflation has jacked the price of, Leo, a five-shot Starbucks Venti Latte is $9.50.

Leo: Whoa. Are there eggs in it? Whoa.

Steve: No, but it's the shots. Somehow espresso got every expensive.

Leo: We ate at the Waffle House in Tucson. There's a 50-cent-per-egg surcharge. So everything's more expensive these days.

Steve: Wow. Anyway, paying $7 for a novel that will give me weeks of true enjoyment, it works for me.

Leo: Yes. And you're supporting the arts. You're supporting creativity. That's good.

Steve: Yes. Yes, thank you. That's a good point, too.

Leo: Buy stuff, yeah.

Steve: You know, but the novel has got to be good. You know, remember that awful thing that I tried reading where the first sentence was "The starship Zigawatt dropped into orbit."

Leo: Immediately. I drop those immediately.

Steve: No, no, not Zigawatt.

Leo: Not Zigawatt, no.

Steve: Anyway, I started with "Gridlinked" because it was Asher's early work, and I prefer to start at the beginning of an author's work. But if the critics on Reddit know what they're talking about, this five-novel series, the series of which Gridlinked is the first, pales in comparison to Asher's later work. Someone who finished "Gridlinked" asked on Reddit whether the other four in the series were worth reading, and someone replied: "I think he was finding his feet in the Polity universe with 'Gridlinked.'" They said: "His following works are miles ahead. Keep at it. You won't be disappointed."

Well, that sounds great to me because I'm already not disappointed. You know, I've mentioned that I seem to be quite sensitive to an author's ability to write. You know, it's not just the plot and the characters for me. They need to be able to express themselves. And Neal Asher really can. It is a little disturbing that Brits spell "ass," as in someone's rear...

Leo: Arse?

Steve: ...arse. It's like, that's, okay. It's like, do you actually, you know, do you say "arse"?

Leo: Yeah, they say "arse."

Steve: You do.

Leo: I don't think it's a different spelling. I think it's just a different way of saying...

Steve: No, it is A-R-S-E.

Leo: Yeah, yeah, no, I know. But, I mean, I think it's just another - I don't think it replaces, well, I don't know. We don't need to get too deep into this.

Steve: Anyway, Goodreads described "Gridlinked" by writing: "'Gridlinked' is a science fiction adventure in the classic, fast-paced, action-packed tradition of Harry Harrison and Poul Anderson, with a dash of cyberpunk and a splash of Ian Fleming added to spice the mix. Ian Cormac is a legendary Earth Central Security agent, the James Bond of a wealthy future where 'runcibles,' matter transmitters controlled by AIs, allow interstellar travel in the blink of an eye throughout the settled worlds of the Polity. Unfortunately, Cormac is nearly burnt out, having been 'gridlinked' to the AI net for so long that his humanity has begun to drain away. He has to take the cold-turkey cure and shake his addiction to having his brain on the 'Net."

Okay, now, it's a bit freaky that Neal Asher wrote about 'Net addiction and the tendency to lose one's humanity through being over-connected back in 2001, 24 years ago, when this book was first published. So anyway, I'm not going to say much more other than that I'm now 67% through the second of the five-book series, and I am really enjoying them. And in fact I've been reading the second book since I saw that sort of like pooping on his work stuff over on Reddit, and being, like, willing to be more critical of it? I really like it. I'm sorry. I like it.

So what's really interesting is this particular Polity universe is run by dispassionate AIs because humans cannot be trusted to wield such power. Basically the people said, okay, you know, sorry, politics corrupts. So we're just going to turn this over to AIs because we can't be trusted with it. Within the Polity, life is sweet and orderly, with no crime, and everyone has something interesting to do. So what it reminded me of is Star Trek's Federation of planets. Remember, like where there isn't even any currency anymore. You just, you know, do things that are good. So of course there are those who chafe under the bit of authority and who prefer the freedom that, you know, is anarchy. So there's plenty of adventure and war and opportunity to be found out on the fringe beyond the control of the Polity.

Anyway, mostly, Neal Asher can write, and I think he's a terrific storyteller. I will definitely keep paying $7 each for the next three books. And given the Reddit comments about Neal's follow-on works, and there are, like, 15 of them at least, I mean, he's been very prolific because he started writing in 2001, and he's been going steadily, you know, I'm going to be very glad that I took ChatGPT up on its suggestions for similar authors.

And I have one piece of listener feedback because I had so much that I wanted to share about the Chrome Web Store. Bob McNaughton, he said: "This might be obvious, but surely if you configure DNS over TLS in your browser, you will miss out on the caching performed by any of the more local DNS resolvers, such as the one in your router? Wouldn't it be better to use DNS over TLS in the router, thus hiding your DNS queries

from your ISP, but getting the advantage of cached lookups other people on the same LAN have performed?"

So Bob is 100% correct, of course. In all of our discussion, I had not mentioned that, if a user configures their local web browser to use any form of encrypted DNS service - which seems to be the way things are evolving - some loss of local caching, for example by the local router if it does DNS caching, although a lot of them don't, would be lost. The flip side of this is that the emerging DNS Benchmark code, which I'm working on, continues to show that once a TCP and TLS connection have been negotiated and brought up, which browsers typically do once per page, the individual flurry of DNS lookups being offered by the Internet's major providers over those encrypted TLS connections, are actually being resolved FASTER by them than, for example, by my own ISP's local resolvers.

So, I mean, it's like it's still faster to do it. As we noted last week, this might be due to the fact that encrypted DNS servers are still lightly loaded because the use of DNS over TLS or DNS over HTTPS is still the exception by far more than the rule. But I'm going to be very interested to learn what everyone else discovers once the Benchmark can, you know, start to be more widely used.

So, okay. Leo, our last break, and then we're going to dig into the really information-packed posting by somebody who knows the Chrome Web Store inside and out.

Leo: Okay. I'm excited. Well, no. That would be a lie. I am anticipating with great interest. How about that? Our show today is - I mean, it's good stuff. I'm not saying it's bad stuff. I'm just I'm not, like, jumping up and down with excitement for it. I just want to hear it.

Steve: I get it. Thank you, Leo, for clarifying that.

Leo: All right, Steve. I am now excited.

Steve: There you are, intrigued, interested...

Leo: I am, uh, thrilled. Thrilled, I tell you.

Steve: [Crosstalk] through this, yes. Okay. As I said, "Chrome Web Store Is a Mess" is the exact title someone who should know gave to a recent blog posting of his a few weeks ago. Wladimir Palant, his posting caught my eye, both due to his pedigree and due to the importance of his message. Anyone who's been following this podcast for more than a few years could probably reduce the number of major security trouble sources to a high single digit. And among those most important would be the security of web browser extensions because web browsers are the way we interface to the Internet and the rest of the world so much.

Extensions to the basic functionality of our web browsers have been with us since nearly the beginning. And 20 years ago, back when there was much less to do on the Internet, the security of an add-on was much less critically important. In fact, the very first extensions didn't have any security. Mozilla created an extension mechanism, and you really needed to trust the source of that code completely.

But every year since then, more and more of our lives have moved online. This has meant that the overall security and privacy offered by the web browsers we use to interact with the Internet has become increasingly important. And no one who has listened to more than a couple of this podcast's episodes could entertain any doubt that, disheartening though it might be, the world is apparently filled with an astonishing number of total strangers who would hurt us without a second thought to obtain any advantage.

Several times in recent weeks I've focused our attention upon the security and privacy issues surrounding web browser add-ons. Sadly, there are many. So when I saw that Wladimir Palant had taken the time to push back a bit from the entrails of specific add-ons to survey the larger picture, I knew that was something I wanted to share.

Earlier I mentioned Wladimir's pedigree, but his name may not ring any bells right off. So here's how he explains himself on his blog site. He writes: "My name is Wladimir Palant, and I'm mostly blogging about security topics these days. You will often see me taking apart browser extensions because I've been developing those myself since 2003. One particularly well-known project of mine is Adblock Plus, which I originally developed. Eventually, I co-founded eyeo, a company to take care of this project. I'm still developing the browser extension PfP: Pain-free Passwords, while my other extensions have become obsolete over time.

"My writing is meant to help people learn. So I aim to provide information on both how vulnerabilities can be found and how they can be prevented in your own code. I won't merely discuss security issues, but also try to draw generic conclusions from those and give recommendations. Despite researching security topics since at least 2007, I still do it as a hobby rather than my job. I experimented with earning money via bug bounty programs, which resulted in acceptable income. However, other aspects eventually turned me away from bug bounties. In particular, I want to write about my research, and don't want to be prevented from it by a company taking years to fix an issue."

Okay. In other words, he was becoming annoyed that after finding and reporting some problem, and being paid for his responsible disclosure, the bug bounty agreement would require that he never reveal anything about the problem until after it had been fixed. This differs, of course, from unpaid security researchers who are able to set 90-day "fix it before we publish it" deadlines. So Wladimir was becoming annoyed that bugs were being purchased, and he was being effectively gagged when he wanted to be able to document the problems and use them as illustrative teaching examples.

In any event, here's a highly technical developer who created one of the earliest and most popular and successful privacy extensions, who has been at this for more than 22 years. So when this guy titles his blog posting "Chrome Web Store Is a Mess," I want to understand why he thinks so.

Wladimir wrote: "Let's make one thing clear first: I'm not singling out Google's handling of problematic and malicious browser extensions because it is worse than Microsoft's, for example. No. Microsoft is probably even worse. But I never bothered finding out. That's because Microsoft Edge doesn't matter. Its market share is too small. Google Chrome, on the other hand, is used by around 90% [nine zero], 90% of users world-wide, and one would expect Google to take their responsibility to protect its users very seriously; right? After all, browser extensions are one selling point of Google Chrome, so certainly Google would make sure they're safe?

"Unfortunately," he writes, "my experience reporting numerous malicious or otherwise problematic browser extensions speaks otherwise. Google appears to take the 'least effort required' approach towards moderating Chrome Web Store. Their attempts to automate all things moderation do little to deter malicious actors, all while creating

considerable issues for authors of legitimate add-ons. Even when reports reach Google's human moderation team, the actions taken are inconsistent, and Google generally shies away from taking decisive actions against established businesses. As a result, for a decade my recommendation for Chrome users has been to stay away from Chrome Web Store if possible." Again, he writes: "As a result, for a decade my recommendation for Chrome users has been to stay away from Chrome Web Store if possible."

He said: "Whenever extensions are absolutely necessary, it should be known who is developing them, why, and how the development is being funded. Just installing some extension from Chrome Web Store, including those recommended by Google, as we'll see, or 'featured,' is very likely to result in your browsing data being sold or worse. Google employees will certainly disagree with me. Sadly, much of it is organizational blindness. I am certain," he says, "that Google meant well and that they did many innovative things to make it all work. But looking at it from the outside, it's the result that matters. And for the end users, the result is a huge and rather dangerous mess."

Okay. So some recent examples. He said: "Five years ago I discovered that Avast browser extensions were spying on their users." That was he who discovered this. Remember we covered that at the time. It was a big deal. It's this guy who made the discovery, which may be why his name is at least some familiar to some of us. He continues: "Mozilla and Opera disabled the extension, that is Avast, the Avast browser extension listings immediately," he says, "after I reported it to them. Google, on the other hand, took two weeks, where they supposedly discussed their policies internally.

"The result of that discussion was eventually their 'no surprises' policy, which says: 'Building and maintaining user trust in Chrome Web Store is paramount, which means we set a high bar for developer transparency. All functionalities of extensions should be clearly disclosed to the user, with no surprises. This means we will remove extensions which appear to deceive or mislead users, enable dishonest behavior, or utilize clickbait-y functionality to artificially grow their distribution."

Okay. So he says: "So when dishonest behavior from extensions is reported today, Google should act immediately and decisively; right? Let's take a look at two examples that came up in the last few months. In October," he says, "in October I wrote about the refoorest extension deceiving its users. I could conclusively prove that Colibri Hero, the company behind refoorest, deceives their users on the number of trees they supposedly plant, incentivizing users into installing with empty promises. In fact, there is strong indication that the company never even donated for planting trees beyond a rather modest one-time donation.

"Google got my report and dealt with it. What kind of action did they take? That's a very good question that Google won't answer. But refoorest is still available from Chrome Web Store, it is still 'featured,' and it still advertises the very same completely made up numbers of trees they supposedly plant. Google even advertises for the extension, listing it in the 'Editors' Picks' extensions collection, probably the reason why it gained some users since my report. So much for being honest. For comparison, refoorest used to be available from Firefox Add-ons, as well, but was already removed when I started my investigation. Opera removed the extension from their add-on store within hours of my report.

"But maybe that issue wasn't serious enough. After all, there's no harm done to users if the company is simply pocketing the money they claim to spend on a good cause. So also in October I wrote about the Karma extension spying on users. Users are not being notified about their browsing data being collected and sold, except for a note buried in their privacy policy. Certainly, that's identical to the Avast case mentioned before, and the extension needs to be taken down to protect users.

"Again, Google got my report and dealt with it. And again I fail to see any result of their action. The Karma extension remains available on Chrome Web Store unchanged. It will still notify their server about every web page its users visit. The users still aren't informed about this. Yet their Chrome Web Store page continues to claim 'This developer declares that your data is not being sold to third parties outside of the approved use cases,' a statement contradicted by the extension's own privacy policy. The extension appears to have lost its 'Featured' badge at some point, but now that's back.

"Note: Of course Karma isn't the only data broker that Google tolerates in Chrome Web Store. I published a guest article today by a researcher who didn't want to disclose their identity, explaining their experience with BIScience Ltd., a company misleading millions of extension users to collect and sell their browsing data. This post also explains how Google's 'approved use cases' effectively allow pretty much any abuse of users' data.

"Neither refoorest nor Karma were isolated instances. Both recruited or purchased other browser extensions, as well. These other browser extensions were turned outright malicious, with stealth functionality to perform affiliate fraud and/or collect users' browsing history. Google's reaction was very inconsistent here. While most extensions affiliated with Karma were removed from Chrome Web Store, the extension with the highest user numbers and performing affiliate fraud without telling their users was allowed to remain for some reason. With refoorest, most affiliate extensions were removed or stopped using their Impact Hero SDK. Yet when I checked more than two months after my report, two extensions from my original list still appeared to include that hidden affiliate fraud functionality, and I found seven new ones that Google apparently didn't notice.

"As for the reporting process, you may be wondering, if I reported these issues, why do I have to guess what Google did in response to my reports? Keeping developers who report in the dark is Google's official policy." And he quotes a popup that he received that says: "Hello Developer. Thank you again for reporting these items. Our team is looking into the items and will take action accordingly. Please refer to the possible enforcement actions and note that we are unable to comment on the status of individual items. Thank you for your contributions to the extensions ecosystem. Sincerely, Chrome Web Store Developer Support." In other words, you explicitly receive no feedback as somebody who reports a problem to the Chrome Web Store.

He says: "This is the same response I received in November after pointing out the inconsistent treatment of the extensions. A month later, the state of affairs was still that some malicious extensions got removed, while other extensions with identical functionality were available for users to install, and I have no idea why that is. I've heard before that Google employees are not allowed to discuss enforcement actions, and your guess is as good as mine as to whom this policy is supposed to protect.

"Supposedly, the idea of not commenting on policy enforcement actions is hiding the internal decision-making process from bad actors, so that they don't know how to game the process. If that's the theory, however, it isn't working. In this particular case the bad actors got some feedback, be it through their extensions being removed or due to adjustments demanded by Google. It's only me, the reporter of these issues, who is left guessing. But this is a positive development. I've received a confirmation that both these reports are being worked on. This is more than I usually get from Google, which is silence. And typically also no visible action either, at least until reports start circulating in media publications forcing Google to then act on it.

"But let's take a step back and ask ourselves, how does one report Chrome Web Store policy violations? Given how much Google emphasizes their policies, there should be an obvious way. In fact, there's a support document for reporting issues. And when I started asking around, even Google employees would direct me to it." And he shows a bunch of

radio buttons on this where the radio buttons are "Did not like the content; Not trustworthy; Not what I was looking for; Felt hostile; Content was disturbing; and Felt suspicious." And then it's highlighted with "If you find something in the Chrome Web Store that violates the Chrome Web Store Terms of Service, or trademark or copyright infringement, let us know." And then those were the radio button options.

But Wladimir notes, he says: "This doesn't seem like the place to report policy violations. Even 'Felt suspicious' isn't right for an issue you can prove is a violation." He says: "And unsurprisingly, after choosing this option, Google just responds with: 'Your abuse report has been submitted successfully.' No way to provide any details. No asking for my contact details in case they have questions. No context whatsoever, merely 'Felt suspicious.' This is probably fed to some algorithm somewhere which might result in, I don't know, what, actually? Judging by malicious extensions where users have been vocally complaining, often for years, nothing whatsoever results. This isn't the way," he says, "you know, to do this right."

He says: "Well, there's another option listed in the document. If you think an item in the Chrome Web Store violates a copyright or trademark, fill out this form." And he says: "Yes, Google seems to care about copyright and trademark violations, but a policy violation is neither. If we try the form, that is, try to use this form nevertheless, it gives us a promising selection. We have two options: Policy, meaning a non-legal Reason to Report Content; or Legal Reasons to Report Content." He says: "Finally. Yes, policy reasons are exactly what we're after. Let's click that. And here comes another choice." And there's only one. It's under "Select the reason you wish to report content," and it has a radio button. "Child Sexual Abuse Material. Report images or videos involving a child under 18 engaging in sexually explicit behavior."

He says: "Well, that's really the only option offered. And I have questions. At the very least those are in what jurisdiction is child sexual abuse material a non-legal reason to report content? And since when is that the only policy that Chrome Web Store has?" He says: "We can go back and try 'Legal Reasons to Report Content,' of course; but the options available are really legal issues: intellectual properties, court orders, or violations of hate speech law. So that's another dead end." He says: "It took me a lot of asking around to learn that the real (and well-hidden) way to report Chrome Web Store policy violations is Chrome Web Store One Stop Support." He says: "I mean, I get it that Google must be getting lots of nonsense reports. And they probably want to limit that flood somehow. But making legitimate reports almost impossible can't really be the way.

"In 2019 Google launched the Developer Data Protection Reward Program (DDPRP) meant to address privacy violations in Chrome extensions. Its participation conditions were rather narrow for my taste. Pretty much no issue would qualify for the program. But at least it was a reliable way to report issues which might even get forwarded internally. Unfortunately, Google discontinued this program in August of 2024.

"It's not that I am very convinced of DDPRP's performance. I've used that program twice. First time I reported Keepa's data exfiltration. DDPRP paid me an award for the report but, from what I could tell, allowed the extension to continue unchanged. The second report was about the malicious PDF Toolbox extension. The report was deemed 'out of scope' for the program, but forwarded internally. The extension was then removed quickly, but that might have been due to the media coverage it received. The benefit of the program was that it was a documented way of reaching a human being at Google who would look at a problematic extension. Now it's gone."

And what about the Web Store and their spam issue? He says: "In theory, there should be no spam on Chrome Web Store. The policy is quite clear on that. 'We don't allow any developer, related developer accounts, or their affiliates to submit multiple extensions that provide duplicate experiences or functionality on the Chrome Web Store.'" That's

what Wladimir considers spam. Spamming the store with essentially identical apps. He says: "Unfortunately, this policy's enforcement is lax at best. Back in June of 2023 I wrote about a malicious cluster of Chrome extensions." He says: "I listed 108 extensions belonging to a single cluster, pointing out their spamming in particular. Thirteen were almost identical video downloaders; nine almost identical volume boosters; nine almost identical translation extensions; five almost identical screen recorders - definitely not providing individual value."

He said: "I have also documented the outright malicious extensions in this cluster, pointing out that other extensions are likely to turn malicious, as well, once they have sufficient users counts. And how did Google respond? The malicious extensions have been removed, yes. But other than that, 96 extensions from my original list remained active in January 2025, and there were of course more extensions that my original report did not list. For whatever reason, Google chose not to enforce their anti-spam policy against them. And that's merely one example. My most recent blog post documented 920 extensions using tricks to spam Chrome Web Store, most of them belonging to a few large extension clusters. As it turned out, Google was made aware of this particular trick a year ago, before my blog post already. And again, for some reason Google chose not to act.

"What about extension reviews? Can they be trusted? When you search for extensions in Chrome Web Store, many results will likely come from one of the spam clusters. But the choice to install a particular extension is typically based on reviews. Can at least these reviews be trusted? On the topic of moderation of reviews, Google says: 'Google does not verify the authenticity of reviews and ratings, but reviews that violate our terms of service will be removed.' And the important part of the terms of service," he writes, "is your reviews should reflect the experience you've had with the content or service you're reviewing. Do not post fake or inaccurate reviews, the same review multiple times, reviews for the same content from multiple accounts, reviews to mislead other users or manipulate the rating, or reviews on behalf of others. Do not misrepresent your identity or your affiliation to the content you're reviewing.

"Now, you may be wondering how well these rules are being enforced. The obviously fake review on the Karma extension is still there, three months after being posted. Not that it matters, with their continuous stream of incoming five-star reviews." He says: "A month ago I reported an extension to Google that, despite having merely 10,000 users, received 19 five-star reviews on a single day in September, and only a single negative review since then." He says: "I pointed out that it is a consistent pattern across all extensions of this account. For example, another extension with only 30 [three zero], 30 users received nine five-star reviews on the same day. It really doesn't get any more obvious than that. Yet all these reviews are still online."

And I actually, for what it's worth, have a picture of them. "Sophia Franklin, September 19th, 2024, five stars: Solved all my proxy switching issues. Fast, reliable, and free. Robert Antony, same day, September 19th, 2024, five stars: Very user-friendly and efficient for managing proxy profiles. Liz Berry: Works like a charm! A must-have for anyone using multiple proxies. Godwin Max: No more digging through setting. This extension makes proxy switching so much easier. Five stars. Also Aaron Brookly, five stars, September 19th" - all of these the same day: "Excellent proxy tool flexibility, perfect for my needs. Going Kate, five stars: Smooth performance and no issues switching between different proxies. Dady Max: Makes proxy management hassle-free. Simple and effective."

Wow. So I have a lot to say in reaction to what Wladimir is observing and reporting. But I'm holding that for a minute until he's finished. Still, I wanted to note, and I hear you laughing and chuckling, Leo, in the background, and I understand. I want to note that the automated clean-up of clearly bogus reviews would be trivial to implement. Wladimir

is made suspicious when an extension with 30 users acquires nine five-star reviews all on the same day. Right. One wonders whether they were all posted from different accounts at the same IP address. Google would know. But even if not, the fraudulent pattern is glaringly obvious.

And remember that it's more than likely that this conduct is also reflected in the operation of the extension itself. Someone who's unwilling to honestly earn a reputation for their extension is more likely to have ulterior motives for creating it in the first place. So if Google were to automate extension review clean-up - which, again, would be trivial for them to do - they would be reducing the damage being done through the fraudulent over-promotion of less savory extensions. Because no trivial clean-up is happening, we need to wonder whether review spamming may be something Google doesn't mind, despite the policy publicly posted to the contrary; you know. And they don't mind it, even if it's actually clearly hurting Chrome's users, because it's the spammy reviews that are going to have the unsavory actions against their users, selling their browsing histories.

Wladimir says: "And it isn't only fake reviews. The refoorest extension incentivizes reviews which violates Google's anti-spam policy which says: 'Developers must not attempt to manipulate the placement of any extensions in the Chrome Web Store. This includes, but is not limited to, inflating product ratings, reviews, or install counts by illegitimate means, such as fraudulent or incentivized downloads, reviews, and ratings."

He says: "It's been three months, and they are still allowed to continue. The extension gets a massive amount of overwhelmingly positive reviews, users get their fake trees, and everybody is happy. Well, other than the people trying to make sense of these meaningless reviews. With reviews being so easy to game, it looks like lots of extensions are doing it. Sometimes it shows a clearly inflated review count. Sometimes it's the overwhelmingly positive or meaningless content. At this point, any user ratings with the average above four stars is likely to have been messed with."

And he said: "What about 'featured' extensions?" He said: "But at least the 'Featured' badge is meaningful; right? It certainly sounds like somebody at Google reviewed the extension and considered it worthy of carrying the 'Featured' badge. At least Google's announcement indeed suggests a manual review." They say: "Chrome team members manually evaluate each extension before it receives the badge, paying special attention to the following." And we've got two points.

"First, adherence to Chrome Web Store's best practices guidelines, including providing an enjoyable and intuitive experience, using the latest platform APIs and respecting the privacy of end-users. And second, a store listing page that is clear and helpful for users, with quality images and a detailed description." He says: "Yet looking through 920 spammy extensions I reported recently, most of them carry the 'Featured' badge. Yes, even the endless copies of video downloaders, volume boosters, AI assistants, translators and such. If there is an actual manual review of these extensions as Google claims, it cannot be thorough. To provide a more tangible example, the Chrome Web Store currently has Blaze VPN, Safum VPN, and Snap VPN extensions, all carrying the 'Featured' badge.

"These extensions, along with Ishan VPN, which has barely any users, belong to the PDF Toolbox cluster which produced malicious extensions in the past. A cursory code inspection reveals that all four are identical; and are, in fact, clones of Nucleus VPN which was removed from Chrome Web Store in 2021. And they also don't even work. No VPN connections succeed. The extension not working is something users of Nucleus VPN complained about, which the extension compensated for by loading it up with fake reviews.

"And again, all of these carry the 'Featured extension' badge. So it looks like the main criteria for awarding the 'Featured' badge are the things which can be easily verified automatically, like user count, Manifest V3, claims to respect privacy - not even the privacy policy, merely the right checkbox was checked - and a Chrome Web Store listing with all the necessary promotional images. Given how many such extensions are plainly broken, the requirements on the user interface and general extension quality don't seem to be too high. And providing unique functionality definitely is not on the list of criteria.

"In other words, if you are a Chrome user, the 'Featured' badge is completely meaningless. It's no guarantee that the extension is not malicious, not even an indication. In fact, authors of malicious extensions will invest some extra effort to get the badge. That's because the website algorithm seems to weigh the badge considerably towards the extension's ranking."

So finally, how did Google get into this mess? "Google Chrome," he writes, "first introduced browser extensions in 2011. At that point the dominant browser extensions ecosystem was Mozilla's, having been around for 12 years already. Mozilla's extensions suffered from a number of issues that Chrome developers noticed. Essentially, unrestricted extension privileges necessitated very thorough reviews before extensions could be published on Mozilla's Add-ons website. And since these extension code reviews largely relied on volunteers, they often took a long time, with publication delays being very frustrating to the add-on developers."

He says: "Note that I was an extension reviewer on Mozilla Add-ons myself between 2015 and 2017." He says: "Google Chrome was meant to address all these issues. It pioneered sandboxed extensions which allowed limiting extension privileges. And Chrome Web Store focused on automated reviews from the very start, relying on heuristics to detect problematic behavior in extensions, so that manual reviews would only be necessary occasionally, and after the extension was already published." And of course I remember we talked about all of these things when Chrome first happened on this podcast because it was during the podcast this all happened.

He says: "Eventually, market pressure forced Mozilla to adopt largely the same approaches." He says: "Google's over-reliance on automated tools caused issues from the very start, and it certainly didn't get any better with the increased popularity of the browser. Mozilla accumulated a set of rules to make manual reviews possible. For example, all code should be contained in the extension, so no downloading of extension code from web servers remotely. Also, reviewers had to be provided with an unobfuscated and unminified version of the source code. Google didn't consider any of this necessary for their automated review systems. So when automated review failed, manual review was often very hard or even impossible. You couldn't fall back."

He says: "It's only with the recent introduction of Manifest V3 that Chrome finally prohibits remotely hosted code." Like, in other words, until then an extension could just download whatever it wanted afterwards. He says: "And it took until 2018 to prohibit code obfuscation, while Google's reviewers still have to reverse minification for manual reviews." He says: "Mind you, we are talking about policies that were already long established at Mozilla when Google entered the market in 2011. And extension sandboxing, while without doubt useful, didn't really solve the issue of malicious extensions. I already wrote about one issue back in 2016." He says, quoting himself: "The problem is useful extensions will usually request 'give me the keys to the kingdom' permission. So these permissions always need to be granted.

"Essentially, this renders permission prompts useless. Users cannot possibly tell whether an extension has valid reasons to request extensive privileges. So legitimate extensions have to constantly deal with users who are confused about why the extension needs to 'read and change all your data on all websites.' Eventually, users become desensitized

and trained to simply accept such prompts without thinking twice. And then malicious add-ons come along, requesting extensive privileges under a pretense. Monetization companies put out guides for extension" - get this. "Monetization companies put out guides for extension developers on how they can request more privileges for their extensions while fending off complaints from users and Google alike. There is a lot of this going on in the Chrome Web Store, and Manifest V3 is unable to change anything about it.

"So what we have now is, one, automated review tools that malicious actors willing to invest some effort can work around. Second, lots of extensions with the potential for doing considerable damage, yet little way of telling which ones have good reasons for that, and which ones abuse their privileges. Third, manual reviews being very expensive and unreliable thanks to historical decisions. And finally, fourth, massively inflated extension count due to unchecked spam. Those last two, 'Manual reviews being very expensive and unreliable thanks to historical decisions' and 'Massively inflated extension count due to unchecked spam,'" he says, "further trap Google in the 'it needs to be automated' mindset." Because after all, you know, there's 135,000 extensions now, and it's completely, they've completely lost control.

He says: "Yet adding more automated layers isn't going to solve the issue when there are companies which can put a hundred employees on devising new tricks to avoid triggering detection." And he says: "Yes, hundreds of employees because malicious extensions make a lot of money and are big business.

"So what could Google do? If Google were interested in making Chrome Web Store a safer place, I don't think there is a way around investing considerable manual effort into cleaning up the place. Taking down a single extension won't really hurt the malicious actors. They have hundreds of other extensions in the pipeline. Tracing the relationships between extensions on the other hand, and taking down entire clusters, that would change things. As the saying goes, the best time to do this was a decade ago. The second best time is right now, when Chrome Web Store, with its somewhat less than 150,000 extensions, is certainly large, but not yet large enough to make manual investigations impossible. Besides, there's probably little point in investigating abandoned extensions, those whose latest release is more than two years ago, which make up almost 60% of the Chrome Web Store."

And he finishes: "But so far, Google's actions have been entirely reactive, typically limited to extensions which already caused considerable damage. I don't know whether they actually want to stay on top of this. From the business point of view, there is probably little reason for that. After all, Google Chrome no longer has to compete for market share, having essentially won against all competition. Even with Chrome extensions not being usable, Chrome will likely stay the dominant browser."

Okay. So as we so often observe on this podcast, it's certainly useful to tell someone, as I noted at the top, to be careful when they may be considering some action that might have negative consequences for them. But at least for me, if I'm told not to do something, in order to really accept that I want to understand why. I want to understand exactly why something would be bad for me. You know, actually I think that's why I grew up to respect my father. He was an explainer. So I suppose I come by that honestly.

Leo: Ah. That's where you got it; huh?

Steve: Yeah. His explaining approach always made so much sense to me because, armed with an understanding, no one needs to tell me anything about what to do or not to do, since I'm able to judge that for myself. So in the case of Google Chrome Web

Store extensions, I'm not going to tell anyone not to download and install extensions they feel they need. Rather, everyone who's reached this point in today's podcast is now fully equipped to judge for themselves whether anything that's there may be worth their time. It would be great if Google were able to function as a reliable curator of the 135,000 Chrome Web Store extensions that are currently available for download. We now absolutely know that, for whatever reason, they are unable and/or unwilling to do so. So we're individually on our own.

Knowing all the things that are wrong - rampant spamming of code-identical extensions under different names, the return of previously removed hostile extensions under different names, an essentially broken extension permissions system, totally bogus five-star reviews, conscientious developer reports going completely unheeded, "Featured" extensions having no additional value whatsoever, and more, you know, the title Wladimir gave to his extremely informative blog posting of "Chrome Web Store Is a Mess" seems entirely fitting.

I author these show notes in Google Docs every week. So I'm in a web browser while I'm writing this. And at one point while I was writing this yesterday, I looked up at the top of my browser with the intention to enumerate the browser extensions I'm using. Then I realized with a smile that none of this applies to me, since I don't use Chrome at all. I'm happily using Firefox, where the full-strength uBlock Origin still continues to work.

While I'm sure that many of the same issues plague Mozilla's extension repository, Wladimir's comments did indicate that Mozilla and Opera may have been far more responsive to abuse reports. And that's important. If nothing else, it's Chrome that has by far the largest target painted on its back. In this case, I'd rather stick with an "also ran" browser, where the browser I'm using is not as big a target as Chrome.

Leo: Yeah. And I think also it's probably the case that, if you stick to a handful of well-known extensions, you're okay. I mean, look at the dopy extensions he's talking about.

Steve: Yes, yes. You know, Privacy Badger, uBlock Origin, obviously...

Leo: I'm on Arc, which is a Chromium derivative.

Steve: Yup.

Leo: But so I am using Chrome extensions. But I stick, I mean, I guess it's always possible. I have Bitwarden, that's safe.

Steve: Of course.

Leo: Kagi Search, that's safe. Raindrop.io.

Steve: Yup.

Leo: Snowflake, which I forgot I put on here. That's cool. That's the Tor reflector. And uBlock Origin. I think they're probably all fine.

Steve: Yes.

Leo: I don't need a browser extension to set my proxies.

Steve: And Leo, it's not clear you can even get one.

Leo: Yeah. It wouldn't do anything.

Steve: There may not be one that actually does that.

Leo: I'm actually much more concerned, and it's true that this is a problem in apps, as well, with malicious SDKs that either used to be okay and have been co-opted, or always had a little bit of...

Steve: So supply chain attacks.

Leo: Yeah. I mean, there are so many of those, and so many - very few developers write all their code. Almost all apps, and I'm sure all extensions, too, use libraries and other SDKs that could well be malicious, yeah. That's why you've got to use stuff that's trusted. Steve, once again, another fabulous episode of Security Now!. Thank you so much.

Steve: Thanks, my friend.