uBlock Origin & Manifest V3

Description: Meta was not bothering to hash passwords? PayPal to begin selling its users' purchase histories. 2021's record for maximum DDoS size has been broken. It's National Cybersecurity Month. When was the last time you updated your router's firmware? North Korean hackers are successfully posing as domestic IT workers. Why would a security-related podcast ever talk about Vitamin D? What's another way the recent Linux CUPS vulnerability might be weaponized? What's the secure consumer WiFi router of choice today? And what should be done to further secure it after purchase? Recent troubles with uBlock Origin's Lite edition shine a light on Chrome's coming content-blocking add-on restrictions. What's going on, and what can be done?

High quality (64 kbps) mp3 audio file URL: http://media.GRC.com/sn/SN-995.mp3
Quarter size (16 kbps) mp3 audio file URL: http://media.GRC.com/sn/sn-995-lq.mp3

SHOW TEASE: It's time for Security Now!. Steve Gibson, our guru of security, is here with some surprising news. Turns out Meta hasn't been bothering to hash its passwords for some time. PayPal's about to sell your purchase histories. Steve explains how to stop that. And then finally we're going to explain this whole kerfuffle over Manifest V3, the inability to use uBlock Origin with Chrome, and a little download that will keep you using uBlock Origin, at least for another six months. All that and a whole lot more coming up next on Security Now!.

Leo Laporte: This is Security Now! with Steve Gibson, Episode 995, recorded Tuesday, October 8th, 2024: uBlock Origin and Manifest V3.

It's time for Security Now!, the show where we get together and talk about your privacy, your security, your well-being online with our well-being professor, Dr. Steve Gibson.

Steve Gibson: Actually, because we're going to mention Vitamin D briefly today...

Leo: Uh-huh. See?

Steve: It is a bit of a well-being podcast. Actually...

Leo: Lisa's doctor said "I want you to do at least 1,000 IUs." I do 5,000 daily. I said, well, just use mine. He said: "Make sure it's a good provider."

Steve: Yeah.

Leo: But he says, and because she's a menopausal woman, calcium and Vitamin D are very important. In fact, for those of us who no longer - our skin no longer manufactures Vitamin D from the sun, and because we're told don't go in the sun whatever you do...

Steve: Or we'll be scraping things off of your skin later in life...

Leo: I'm going to the dermatologist at the end of the month. I asked my doctor, said "Do you think this is a problem?" He took a picture with an iPhone with a special lens on it. He said, "Let's get our camera in." It was an iPhone but it had a special lens on it. And they took a picture like that and sent it to the dermatologist. Got a call the next day from the nurse. She said, "It's not cancer, but we would like to see you." Okay. I think I'll be getting scraped at the beginning of the month.

Steve: Bring your wallet.

Leo: Bring your wallet. Steve, what's coming up today on Security Now!?

Steve: Okay. So we've got some follow-up on something we talked about several years ago, about Meta having been found not to be bothering to hash their login, their users' login passwords. Which it's just like, what?

Leo: In this day and age, really?

Steve: It's unbelievable, yes. Also, PayPal is going to begin selling its users' purchase histories, unless we turn that off. However, Leo, because you and I are both in California, we don't have to turn it off.

Leo: Oh, hallelujah.

Steve: Anyway, we'll be talking about that.

Leo: Yup.

Steve: There's also two other states that don't have to opt out. They are auto-opted out. We have broken - "we" meaning bad guys - broken 2021's record for the maximum DDoS size.

Leo: Not a good record.

Steve: Not a good record. It didn't last very long. But, boy, if those wires could melt, this would have melted them. It's also National Cybersecurity Month. When was the last time you updated your router's firmware? North Korean hackers, there's more news about these guys successfully posing as domestic IT workers. Also we're going to pose and answer the question, why would a security-related podcast ever talk about Vitamin D? Also, what's another way the recent Linux CUPS vulnerability has been found to be weaponizable?

Leo: Uh-oh. Oh, boy.

Steve: What's the secure consumer WiFi router of choice today?

Leo: Oh.

Steve: That's a listener question that we're going to answer.

Leo: I have an answer, too, which is what we use, but keep going, yeah.

Steve: Okay. And also what should be done to further secure it after its purchase. And recent troubles with Gorhill.

Leo: Our good friend Gorhill.

Steve: You know, if John Dvorak wrote software, that would be Raymond Hill.

Leo: Raymond's a little cranky. Just a little cranky.

Steve: Yes. So recent troubles with him. He's uBlock Origin's dad, and specifically its Lite edition has shined some light - and I don't know if you would say "shone." Is that shone?

Leo: Has shined. Has shone. Has shone some light.

Steve: Shined a light.

Leo: Yeah.

Steve: On Chrome's coming content-blocking add-on restrictions. It turns out I've discovered a way of postponing the inevitable.

Leo: Oh, good.

Steve: But at least you get till next summer. We're going to look deeply at what's going on and what can be done.

Leo: Oh, good.

Steve: And since fully half of the podcast is going to be that rather entertaining discussion, we'll move our ad inserts appropriately.

Leo: Well, I'm very interested in this Manifest V3. It feels like Google doesn't want you to run

an adblocker. I wonder why?

Steve: Uh-huh.

Leo: But, you know, and it would be a reason for me to abandon Chrome, frankly, if I can't run uBlock Origin.

Steve: Yup.

Leo: I don't want to go out on the web without it. All right. It's going to be a good show. Plus a Picture of the Week.

Steve: It's already had some great feedback. Again, I'll just note to all of our listeners that 10,100 and some odd of our listeners received the show notes, the Picture of the Week.

Leo: Last night. Last night.

Steve: Yeah, last night.

Leo: I'm sitting there watching a movie with Lisa, she said, "Oh, the show notes are here." So apparently Lisa subscribes, too.

Steve: Yeah, well, Lorrie has been bugging me for years to start sooner so that I'm less in a froth and a panic.

Leo: That's what I told her. I said, "This is the new Steve Gibson." She said, "It's probably Lorrie."

Steve: Yes, this is a married podcaster.

Leo: Awesome. Well, we love our wives, and thank goodness they're keeping an eye on us. All right, I'm ready, Steve. Picture of the Week time.

Steve: We didn't talk about this before, and I assume you have not seen it.

Leo: I have just seen the headline, "Modern Product Packaging Can Be a Challenge."

Steve: Yes.

Leo: All right. So [laughing]. Okay, okay, okay. Together, we'll look at this together. I'm sorry. It's hard not to laugh here. Wait a minute. Let me make it big.

Steve: No, you're supposed to laugh. That's the whole point.

Leo: Okay. Okay.

Steve: Yeah.

Leo: You have a pair of scissors, and you have those horrible blister packages.

Steve: Oh, my god. And, you know, I'm surprised there's not blood on the table somewhere.

Leo: I know. They're just awful.

Steve: Yes, yes. So for those who don't have the advantage of seeing the Picture of the Week from the show notes, this shows that some hapless individual used a pair of scissors to open their Logitech corded mouse.

Leo: Oh.

Steve: Unfortunately, where they chose to cut across the package with their scissors cut the mouse's tail. That is, its cord. A number of people have replied and said, well, that's one way to get a cordless mouse.

Leo: Not the right way.

Steve: Not the right way, no. Anyway, it's just a great picture because...

Leo: It's probably from a real person because who hasn't done this; right? This is just...

Steve: Actually, several people wrote and said, "Yeah, I've done something like that." It's like, I mean, they really are awful. Sometimes they, like, they will hide the instructions for using the thing inside so when you cut across it...

Leo: Right across it.

Steve: ...you're like cutting the instruction manual in half. I mean, it's just - it's very convenient for high-volume packaging, but all of the burden is transferred to the user, who is, as we said, you know, you have to, like - what I do is I carefully cut around the perimeter, yet then you've got to watch out that you don't get stabbed by the sharp edge of the packaging that has been cut by the scissors. It's just bad. So anyway, thank you. One of our listeners sent this to me. The Pictures of the Week are listener-sourced. So I very much appreciate them.

Leo: We're going to fix this lower third, Benito. It says Wednesday, and it is not Wednesday.

Steve: It is not.

Leo: So if anybody's watching and saying, "Oh, my god, it's Wednesday," no, it's not.

Steve: But it is the 8th, so that's...

Leo: It is the 8th, yes.

Steve: Okay. So Ars Technica carried the news that officials in Ireland have fined Meta $101 million US for their storing of hundreds of millions of user passwords in plaintext rather than hashing them, which of course as we know provides both breach and internal employee abuse protection. Ars first reported this conduct, and we talked about it five years ago, back in 2019. And at the time Ars used the headline: "Facebook apps logged users' passwords in plaintext because why not," with the subhead "Unencrypted user credentials stored on Facebook's internal servers as far back as 2012."

You know, and this sort of shows a problem in general that we see occurring in all different sorts of places because our technology, the way technology has been implemented is opaque. And, you know, I mean, it's true everywhere; right? Like we don't know the plastic that our seat cushions are made of and whether it's outgassing carcinogens. We just hope that they aren't. But, you know, how do you know? And we have no idea who is responsibly storing our credentials. We only find out that they haven't been when a breach occurs, and all of the passwords are in plaintext and not hashed.

Anyway, back in 2019, when we talked about this, Facebook said - I'm sorry, not Facebook, Ars reporting said: "Facebook has mined a lot of data about its users over the years - relationships, political leanings, and even phone call logs. And it now appears Facebook" - and this is in 2019 they're writing - "Facebook may have inadvertently extracted another bit of critical information: users' login credentials, stored unencrypted" - meaning unhashed - "on Facebook's servers and accessible to Facebook employees.

"Brian Krebs reports that hundreds of millions of Facebook users had their credentials logged in plaintext by various applications written by Facebook employees. Those credentials were searched" - and here's the point that - the numbers are just staggering. Those credentials, right, the Facebook users app login credentials stored in plaintext, Krebs reported at the time, "were searched by about 2,000 Facebook engineers and developers more than nine million times, according to a senior Facebook employee who spoke to Krebs. The employee asked to remain anonymous because they did not have permission to speak to the press on the matter." No, I would not think they would have permission.

And of course I recall this from when we talked about it five years ago because those numbers are so outrageous. So now Ars is reporting five years downstream currently that Facebook has spent these five years, these past five years "investigating" this. What? Five years? A heading in Ars reporting, they now said: "Meta investigated for five years." But as I said, this seems to me the term "investigated" should be put in air quotes because it's difficult to see how an "investigation" of non-hashing of login credentials could possibly require anybody five years.

Also, apparently they've got 2,000 engineers who have time to search through their own customers' passwords. You'd think they'd have some time to do some investigating of how they're, like, why aren't they hashing anything? How could this take five years is beyond me. And if anything, over that course of time, whatever trail there was would have only grown more stale year after year as people who knew the details became less accessible and more probably more forgetful, whether conveniently or not. So this feels a lot like Facebook dragging their feet internally and not wanting to give any final result from their investigation.

But in any event, now Ars reports that Graham Doyle, Ireland's Deputy Commissioner of Data Protection, says: "It is widely accepted that user passwords should not be stored in plaintext, considering the risks of abuse that arise from persons accessing such data. It must be borne in mind that the passwords, the subject of consideration in this case, are particularly sensitive, as

they would enable access to users' social media accounts."

And of course the other thing we know, unfortunately, is that anybody who is still not using a password manager, and while the percentage of Internet users who today are using password managers has been going up significantly, still it's a minority. And we know then that there's a high incidence of password reuse. So passwords stored in plaintext can be used as a starting point for guessing the reuse of those credentials elsewhere.

Anyway, Ireland has been investigating the incident since Meta disclosed it, and their Commission of Data Protection, which is the lead European Union regulator for most U.S. Internet services, finally imposed a fine of $101 million, that's 91 million euros, this past week. So we can add that to the pile of fines that Facebook has incurred since the EU has been levying fines. Now, I have to say $101 million is not much compared to the more than $2.23 billion, that's 2 billion euros, for violations of the General Data Protection Regulation, the famous (or infamous) GDPR, which went into effect in 2018. So that amount includes last year's record $1.34 billion, which is 1.2 billion euro fine which Meta is now appealing.

So I presume, though I haven't looked into it since it's not frankly that interesting, that these fines - and we talked about them at the time - are due to Facebook storing EU citizen data outside the EU, likely in U.S.-based data centers. In any event, this is all a mess and demonstrates that, you know, as an industry we're still trying to figure out how to do all this stuff so that everybody's happy. And we're not there yet.

Okay. Now we have an action item for a lot of our listeners. A new, forthcoming PayPal default will be opting all of their customers, their users, into merchant data sharing. Two weeks ago, PayPal posted a 60-day notice warning of a forthcoming change to their Privacy Statement which will become effective at the end of November, on November 27th. The amendment says, under "Notices/Issued," dated September 23rd, 2024: "Amendments to the PayPal Privacy Statement," becoming effective November 27th.

And PayPal clearly explained: "We are updating our Privacy Statement to explain how, starting early Summer of 2025" - so not till next summer - "we will share information to help improve your shopping experience and make it more personalized for you. The key update to the Privacy Statement explains how we will share information with merchants to personalize your shopping experience and recommend our services to you. Personal information we disclose includes, for example, products, preferences, sizes, and styles we think you'll like. Information gathered about you after the effective date of our updated Privacy Statement, November 27th, 2024, will be shared with participating stores where you shop, unless you live in California, North Dakota, or Vermont. For PayPal customers in California, North Dakota, or Vermont, we'll only share your information with those merchants if you tell us to do so.

"No matter where you live, you'll always be able to exercise your right to opt out of this data sharing by updating your preference settings in your account under 'Data and Privacy.' We are also making other updates to our Privacy Statement including some additional disclosures related to your right, depending on the jurisdiction in which you reside, to ask us for a list of the third parties to which we've disclosed personal information, and to provide other clarifying information."

Okay, now, TechRadar carried the news of this by writing: "Another week, another online service silently changing its data collection and sharing practices by default." Now, I will argue, and I'll talk about this in a minute, that PayPal is in a different category, but okay. TechRadar said: "The good news is that you still have time to opt out before any of your information gets automatically given away without your consent," which is completely true.

"As per PayPal's policy updates page, issued on September 23rd for U.S. users, the service is set to exchange your data with third-party merchants to 'help improve your shopping experience and make it more personalized for you.'"

Leo: Yeah, right.

Steve: Uh-huh, yeah. Another way for PayPal to generate revenue, we understand. TechRadar said: "Starting in early Summer 2025, the new policy will not just come at the detriment of your privacy - even if you're using the best VPN apps - but PayPal will start gathering data as early as November 27th, 2024." Which is interesting. So, right, so they're going to start, they're officially going to start accruing all of the things that their purchasers, their users do, that purchase through PayPal, I guess so that there's a nice chunk of it available to offer when they officially start releasing it, and obviously selling it, this coming summer.

Leo: Do other credit companies do this? I mean...

Steve: No.

Leo: No.

Steve: No. And credit companies don't have access the way PayPal has with the merchant sites where they're present. You know, I use a credit card company, just their backend merchant services, and all they get from me is the minimum amount of information required to transact the credit card purchase, nothing, no other information. But PayPal has an information-sharing agreement with their merchants as part of all of this.

Anyway, TechRadar said: "Users appear to be opted in by default, which may be an issue under some privacy regulations like GDPR. After coming across some U.S.-based accounts complaining about this on Twitter, we decided to check," writes TechRadar, "if that was the case also for people in the UK. When we accessed privacy settings, the option was automatically toggled on.

"It's also important to bear in mind that the policy changes will not apply in the same ways across all jurisdictions and users. For instance, in the UK, the new data sharing is set to be enforced on October 10th, 2024." Which you know, in two days.

Leo: That's day after tomorrow. Oh, wow.

Steve: Yeah. "A policy update dated July 8th clarifies that, for the UK market, 'merchants are permitted to share customer personal information provided to them by PayPal with their service providers.' We suggest checking your profile settings as soon as possible to reverse the change if you don't wish your data to be shared."

Okay, now, I had to read that last part twice. In the UK, PayPal will be sharing its users' shopping histories with merchants; and, in turn, those merchants will be permitted to share this personal information provided by PayPal with the customers' service providers. So UK-based ISPs, who are not PayPal merchants, will nevertheless obtain this information indirectly through the merchants who are.

Leo: Oh, this is disgusting.

Steve: It is.

Leo: It's terrible.

Steve: It's unbelievable. And note that all of these information-sharing activities are pretty much guaranteed to be for-pay arrangements; right? PayPal is unlikely to be sharing this valuable

information with their merchants for free. Or if it is for free, then it represents an additional inducement for a merchant to offer PayPal payment. You know, the pitch would be: "Offer PayPal checkout, and as an added benefit we'll provide you with the detailed buying histories of the people who come to your website."

So as it happens, the people who participate in discussions over in GRC's "think tank" newsgroup know, because I was discussing the pros and cons of it there, that I had recently been considering reducing software purchase friction by adding PayPal checkout to GRC's eCommerce system.

Leo: Yeah, a lot of Europeans prefer it.

Steve: Yes. I decided not to, in the interest of remaining with a single universal credit card solution, since I've been using that for the past 25 years. Learning of this, I'm certain that I made the right decision since I would feel uncomfortable using a payment solution that defaults to profiling its users' purchasing. Since, I mean, that's deeply confidential information.

Now, I have to say I use PayPal myself, but fortunately I'm in California. And while the "nanny state" nature of California does occasionally annoy me and interfere with my choices, in this case I was glad to find that, indeed, that information sharing switch that almost everyone else will find is ON by default was OFF for me. For anyone who uses PayPal, after logging in, go to "Settings," which is a gear icon in the upper right if you're using a web browser. Under "Data & Privacy" you'll find the section "Manage shared info," and within that section you'll see "Personalized Shopping."

If you select that option, you'll be presented with some description and a big switch. And it says: "Let us share products, offers, and rewards you might like with participating stores." And then it says - and then there's a big switch. Mine was off because I'm in California. Other people will find theirs on. "Starting early summer 2025, we'll be building more personal experiences for you. You can opt in and out of sharing at any time by adjusting this setting." And then there's a link, "How personalized shopping works." If you click that, and I have pictures of all this in the show notes, it shows, it says: "How personalized shopping works. We're on a mission to help you find the most relevant products and styles." And it says: "We'll share recommendations with participating stores based on your shopping history and preferences. Your info helps participating stores show you products, offers, and rewards you might like."

So, yes, yet another privacy invasion. This is a new section and option that no PayPal user will have seen before. TechRadar explained that in the U.S., only residents of California, North Dakota, and Vermont will find this turned off by default, with it being on for everyone else, including those in the United Kingdom. Underneath that big switch, you know, I explained what it says.

And so, you know, I know how this audience, the audience of this podcast, feels about Internet privacy since I've long enjoyed plenty of two-way communication with our listeners, first through Twitter, now through email. So I wanted to be sure that everyone using PayPal in the United Kingdom, probably elsewhere in the world, and in the U.S., who does not reside in those three states, knew about PayPal's user purchase data sharing plans in time to preemptively say, gee, thanks, but no thanks. So flipping that off any time before the end of November will prevent PayPal from ever starting to do this.

So having said all that, I do also want to acknowledge that both this past Sunday, two days ago, and also the Sunday before, PayPal did very clearly notify me through email of these pending changes in a completely aboveboard fashion. In the identical email I received on those successive Sundays, they wrote: "Our updated Privacy Statement outlines how we'll use info collected about you after November 27th, 2024 to inform participating stores about what products, offers, and rewards you might like." So, you know, while we know that the "tyranny of the default" will work in their favor, and that defaulting to "opt-in" - defaulting to opt-in - will see most people simply glaze over, delete that email without pursuing it because, you know, we're constantly getting updates about this or that privacy statement being amended. In fact, during my walk yesterday evening with Lorrie, I mentioned this to her, and she just said, "Yeah, I don't ever read those." I said, yeah, no one does.

Leo: Right, yeah. That's why, I mean, you read your emails. People go, oh, it's more solicitations. I don't need it.

Steve: Right, exactly. So anyway, you know, to me this feels extra troublesome because this is a service that I have used simply because I prefer not spreading my credit card number and information around. It's why I was considering, you know, adopting it for GRC, because I recognize, you know, I see how glad I am when some random merchant I'm going to allows me to pay through PayPal because it is the lower friction transaction. Unfortunately, PayPal realized, wow, you know, look at all this information that we're getting about the people who use our service. We could be making some extra money by selling that. And so unless we say "no thank you," that's what they're going to begin doing. I knew our listeners would want to know. And Leo...

Leo: You should see all the comments in YouTube. Paul Reed: "I turned it off. Thanks, Steve." John Regan: "I just turned mine off, too." Let's see. Vagita: "I received the email today but skipped it until your story." I mean, thank you, Steve, is I guess the general sentiment. Because, yeah, who reads those emails?

Steve: Yup.

Leo: Do you want to take a break? Is that what I sense from you?

Steve: Yes.

Leo: Yeah, I would like to take a break right now. Well, good news, Steve, because we have sponsors. And they want to tell you about their product; okay? And by the way, I just want to tell you, we're not like PayPal. We know nothing about you. We can't know anything about you. This is an RSS feed that goes to an IP address, so we don't know who it is. So don't worry about it, we're not ever going to - we couldn't collect that kind of information. Unless you join the Club. And then we don't need to because you're giving us seven bucks a month; right? Now, let's hear about that DDoS record. What was the old record?

Steve: Oh ho ho ho, baby. Last Friday, Cloudflare disclosed that it had broken yet another record in fending off the largest DDoS attack ever seen on the Internet. Though the attack was brief, it lasted only 65 seconds from start to finish, during those 65 seconds Cloudflare's infrastructure was hit by an attack that peaked at 3.8 terabits per second.

Leo: Whoa.

Steve: 3.8 trillion bits per second. So...

Leo: Don't be reassured by the briefness of this. That just means they were testing it; right?

Steve: Yes.

Leo: It was just they test the weapon before they point it at somebody.

Steve: Yes. And what was interesting to me, because I saw the graph of this, was how steep the leading and trailing edges were. You know, I've seen a lot of DDoS attacks myself. And generally they sort of ramp up to full steam, and then they sort of fade out over time, you know, as the different agents get the news of where they should be attacking. This attack had really surprisingly sharp edges. It came on, went like right at full strength, 3.8 terabits per second. It went for 65 seconds, and then it just shut itself down. So to me that was really interesting. Maybe there's a new way these are being staged where, for example, the instructions go out to at this time launch an attack at this target. Yes. Now you've got it onscreen. And that is a sharp...

Leo: That's an on-off switch. That's incredible.

Steve: Yeah. It's really interesting. Yeah, look at that.

Leo: Wow.

Steve: 2.1 billion packets per second.

Leo: Now, they're coming from commandeered machines, from routers? I mean, it's not just from one guy's machine, obviously.

Steve: That's also interesting here. So I definitely - oh, no, that's not one guy, at all.

Leo: Yeah.

Steve: Because you can't, I mean, so the way Cloudflare, the only way Cloudflare is able to fend these off, and it literally, the target of the attack was not affected by this. Which is astonishing.

Leo: Mind-boggling, yeah.

Steve: You have to think in terms of Cloudflare's ability to absorb the attack. They're literally, they're absorbing it so that none of their conduits are saturated by that packet rate or that bitrate. So that valid traffic to the target of the attack is still able to get through Cloudflare's infrastructure and reach the servers that it's protecting.

Leo: It's a heck of an ad for Cloudflare.

Steve: That's, well, yeah. And in fact I was going to share their disclosure of this, but it was marketing speak. It was them bragging. It's like, okay, well...

Leo: Yeah, it was an ad, yeah.

Steve: You know, you do - I'm not saying you don't deserve to brag, but I'm not going to read your advertisement. So in the last month Cloudflare, which is no stranger to DDoS attacks because it's one of the services they offer, has fended off over 100 of these so-called hyper-volumetric Layer 3 and 4 DDoS attacks, many of which exceeded two billion packets per second.

Now, these so-called hyper-volumetric Layer 3 and 4 DDoS attacks have been occurring since the

start of September, and their targets have generally been customers in the financial services, the Internet, and the telecommunications industries who are hiding their servers behind Cloudflare specifically in order to remain on the air despite what would otherwise be wire-melting attack levels. This recent record-breaking 3.8 terabits per second attack broke the previous record, which had been set nearly three years ago in November of 2021. That attack peaked at 3.47 terabits per second, this one being at 3.8.

So, you know, we're sort of reaching - you sort of feel like there's a ceiling maybe that we're beginning to hit. And that one, that November 2021 attack, was blasting an unnamed Asian-based Microsoft Azure customer, trying to blast them off the 'Net. The attacks are using UDP packets aimed at a fixed port. And though there wasn't any reporting about this, it turns out that DNS reflection attacks are like what a lot of these DDoS services are using. The problem is - and that is to say, well, UDP packets bouncing off of DNS servers. The reason is DNS servers are one of the most prevalent servers that need be publicly accessible in order for their services to be offered. So they're out there.

So the floods were originating from Vietnam, Russia, Brazil, Spain, and the U.S. Cloudflare said that the high bitrate attacks likely originate from a large botnet comprising infected ASUS home routers that have been exploited using a recently disclosed critical flaw, which is CVE-2024-3080. And that's got a CVSS of 9.8.

Leo: Ouch.

Steve: Yeah, that's up there. According to statistics shared by Censys, you know, that's C-E-N-S-Y-S, which is - it's a new Internet vulnerability apprising service. It's like Shodan. Their IPs have reverse-DNS that points to their domain. And I'm seeing GRC's network being probed by Censys all the time. That's how I know it's Censys is that their probes identify them.

Leo: And they're looking for the vulnerability. Yeah.

Steve: Yes, exactly. In the same way that...

Leo: Shodan is, yeah.

Steve: ...the probes that my own ShieldsUP! port scanner sends out, they have reverse DNS set to shieldsup.grc.com so people who care know that it's, you know, a benign half-open TCP probe. It doesn't actually connect to anything.

Anyway, Censys said, of this 9.8 ASUS flaw, a little over 157,000 ASUS router models were potentially affected by the vulnerability when they did their scan in June, June 21st of this year, of 2024, with the majority of these devices located in the U.S., Hong Kong, and China. So DDoS isn't going away. It's not going to go away. It is a, you know, we've spent a lot of time over the years talking about DDoS attacks, why they happen and why they are unblockable.

For a long time I was, like in the early days, I was lobbying for ISPs to filter the packets leaving their networks, you know, egress filtering, as it's called, because we had bots that were spoofing their source IPs in order to cause packets to bounce off of some server and go to the target. And I said, hey, this problem can all be solved if ISPs just won't let these bogus packets that should never originate from within their networks leave their network. Well, that was then. What's happened is now we have these Layer 3 and 4 attacks which are very often HTTP queries. So they're not spoofing their IP because, if you've got hundreds of thousands of bots...

Leo: Because it's a million ASUS routers.

Steve: Yeah.

Leo: Hey, it's me. What are you talking about?

Steve: Yeah, doesn't matter. And so now the packets leaving are valid, and they're like making very expensive queries of servers that are heavily script laden and take a long time to respond. And it just - so it's a server CPU exhaustion, where they just can't serve, they can't generate that many high-cost pages.

Leo: Now, you mentioned the abrupt on-and-off profile of this attack.

Steve: Yeah.

Leo: That's interesting because that means you've got a command-and-control server that can trigger all of these routers instantly.

Steve: Yeah. And that's why I'm thinking maybe they are time-synched, and the command is on...

Leo: Ah, at 3:00 p.m., yeah, yeah.

Steve: Yes.

Leo: Your site was down briefly this week.

Steve: Yup.

Leo: I was wondering if you were hit by DDoS or it was just...

Steve: Yup, it was Sunday morning. It started a little after, like about 9:15, and lasted for an hour. And it was a flood attack. And, you know, I just - actually I was working on the podcast, and so I just - and I said, "Lorrie, GRC's down." And she said, "Oh, no, what are you going to do?" I said, "Well, I've got Google Docs open. I'm working on Tuesday's podcast. So, you know."

Leo: Nothing. The answer is nothing. Steve does not negotiate with terrorists, just so you know.

Steve: Well, and it takes, like, nothing to knock me off the 'Net. I'm not protected. I'm not hiding. I don't have Cloudflare.

Leo: Have you thought of becoming a Cloudflare customer?

Steve: No.

Leo: You're not mission critical. It's not worth it.

Steve: Well, and I'm offering a lot of services for free. And if I start doing things that cost me money...

Leo: Right.

Steve: Then the whole tradeoff between what I can choose to do and what doesn't make sense begins to change.

Leo: Right, right.

Steve: So...

Leo: We do have - our servers are behind, I'm not going to be specific about what we do, but we are behind DDoS protection. Of course, that's one of the things Club TWiT pays for; you know? We do have some revenue, and so we're able to do that. Does Cloudflare not offer some sort of free tier? I believe they do. But I don't know if it includes DDoS.

Steve: So the other thing is that my bandwidth is complex because I'm...

Leo: Yeah, you're not normal.

Steve: ...sending out ShieldsUP packets. I'm using DNS in order to version checking for all of the freeware that's able to check for different versions. And it just makes life more complicated. I believe in keeping it simple when I can. And, you know, we're mostly on the 'Net. And when we're not...

Leo: It's not mission-critical. That's what I tell my staff. They say, why don't you have generators? Because we're not mission-critical. If we're down for an hour or two, no one's going to die. Although, you know, since we closed the studio I no longer have anywhere to put my server. It used to be running in the studio. So my website, Leo.fm, has been down, as have been the Minecraft servers. And I think what I'm going to do is use Cloudflare pages to host my website because then you get all those - and it's completely free. You get all those benefits. It's a little tricky to set it up. I've been trying for three months to do it. But as soon as I figure it out I will do it. Cloudflare's a pretty impressive service, I have to say. I will...

Steve: I like them. And, you know, I think Microsoft has a service, Akamai has a service, I mean, there are, you know...

Leo: Amazon does, yeah, there are a lot of companies that do this, yeah.

Steve: Yeah.

Leo: They have to have a lot of bandwidth; right?

Steve: Well, and so what they have to have is geographic spread.

Leo: Yes.

Steve: So the idea is that there are these bots scattered all over the world, which means they are entering Cloudflare's infrastructure at access points all over the world.

Leo: Right.

Steve: So even though the total amount of bandwidth is high, the local amount of bandwidth is lower than Cloudflare's bandwidth at that location. And that's the key is that no part - so Cloudflare is so spread geographically that even though the total attack is huge, there's no saturation, no point of saturation. Cloudflare's technology allows them to identify and block the attack at all of the different points across its infrastructure before the routing concentrates the attack down to the server where it's being targeted.

Leo: Perfect. That's why it's often CDNs that do this.

Steve: And that's the key to them. Yes, exactly, you need a big content delivery network-style protection. And I've got a wire. I've got a 100-base-T connection.

Leo: GRC isn't in 30 countries all over the globe, in every continent? No? I don't understand why not.

Steve: Okay. So speaking of these ASUS routers, I use an ASUS router for WiFi service at my place with Lorrie. And even if that router were not safely perched behind a separate pfSense firewall appliance which connects it to the Internet, the last thing I would ever do would be to open a publicly accessible remote admin portal, or media server, or file server, or any of that nonsense.

Leo: Right.

Steve: Which consumer routers now offer as bullet points for themselves.

Leo: And a lot of people do it. They put their Plex server on the network or whatever.

Steve: Yeah, like some poor clown at LastPass.

Leo: [Theatrical throat-clearing]

Steve: So I'm sure that listeners of this podcast have similarly protected themselves. But the Censys survey reveals that around 157,000 other ASUS owners may not have been so circumspect. You know, so seeing this story, I checked in with my router, which I hadn't for a

while. I don't have automatic updates enabled, although the ASUS allows it, since my network has other security provisions, like, galore. But it turned out that when I checked, my router's firmware was a bit behind. It was running v3.0.0.4, and 3.0.0.6 was available.

Leo: Well, that's not too behind. That's just...

Steve: I have no trouble with the router, but updating always makes sense. And also having layers of security is always a good thing, so the more the merrier. Since this month of October is National Cybersecurity Awareness month, let me take this occasion to suggest that everyone listening just take a moment to check their router's firmware to see whether there's an update available beyond what's running now. I'm glad I did. And I would recommend that everybody turn on automatic firmware updating, since that's a feature that is now available in consumer routers, and it just makes sense.

Leo: You should only have it off if you're Steve Gibson, and you know what you're doing. I mean...

Steve: You know, if you really - essentially, if you're willing to take responsibility for it being off, and you know what that means, and the idea of having your router updating itself for some reason makes you queasy, and I don't think it should.

Leo: Yeah.

Steve: So. We've recently been looking at the growing problem of spoofed identities by remote workers. The news just this past week is that more than a dozen blockchain companies have inadvertently hired undercover North Korean IT workers. Because that's what you want in your cryptocurrency companies. Wow. You know? We wonder what is the problem with these blockchain companies? Why can't they get their security right? Well, according to a CoinDesk investigation, these companies include well-established blockchain projects such as Injective, ZeroLend, Fantom, SushiSwap, Yearn Finance, and Cosmos Hub.

Leo: Well-established brand names in crypto space.

Steve: All happily employing North Korean IT workers.

Leo: Wow.

Steve: In every case, the workers passed checks using fake IDs and fake job histories. And, you know, aside from it being an obviously bad idea for any cryptocurrency company to allow an agent of a foreign government inside your sensitive organization, it also happens to be completely against the law in the U.S. and any other companies that have North Korea under sanctions, which include you can't hire anybody who's from North Korea. Wow. I guess that's a consequence of everything going virtual. Unfortunately, you've got virtual employees now, and Korean may be their first language.

Leo: Yikes. By the way, I wanted to mention this. I know you're very interested in bitcoin. We covered it. You had some and so forth. And there's always been a question about the person who invented it. You did a couple of really good pieces on that.

Steve: Satoshi.

Leo: On the mathematician or group involved behind it, Satoshi Nakamoto. No one knows who that is, or if he or they are still alive. But I'm very curious. Tonight there will be a documentary coming out on HBO, by the same guy who kind of blew the lid off Q, remember, the whole Q thing. Cullen Hoback is purporting that he knows who Satoshi is, and he will reveal it in this documentary on HBO tonight. So I'm very curious what that's going to be. And I guess that's where I'll be tonight, watching that show.

Steve: We made some millionaires.

Leo: Yeah. And, you know, lately, with the news of this, some of the very earliest bitcoin wallets have been opened and transferred out. And so there is some thinking that maybe he did come upon the true, I mean, so many people have done this, including Newsweek, announced incorrectly who Satoshi Nakamoto was. It could just be another one of those. It could be an Al Capone's safe, or it could be really a big story.

Steve: Wasn't there some guy they outed, and he kept saying over and over, I'm not him, please, I'm not him.

Leo: It was some poor Japanese guy named Satoshi. Newsweek put it on the cover. It was not a good - they never - I don't think they ever retracted it, even. It was just terrible. Anyway, I'll let you know next week what I think.

Steve: Cool. I'll make a point of watching it. It sounds fun.

Leo: It might be worth watching yeah. This guy absolutely figured out who Q was. So, and it was a really good documentary. This one's called "Money Electric: The Bitcoin Mystery."

Steve: Nice. So Chris said: "Hi, Steve. I'm a longtime listener to Security Now!, but last week as I was hiking in the White Mountains," he said, "it occurred to me that there is one episode of this podcast that literally changed my life, and that was the Vitamin D episode."

Leo: Me, too, I think. Yeah. I agree.

Steve: And actually many of our listeners have said the same. He said: "Ten years ago I would listen to podcasts while lying in bed suffering from debilitating back pain. My doctor had prescribed a big bottle of opioids, and I was desperate for an alternative, when I heard you and Leo mention Vitamin D and your past episode. I went back to the archive and listened to the Vitamin D episode, then went to my doctor and made him test me. My Vitamin D level was extremely low.

"I started taking 4,000 IU daily, and over the course of a year I threw out the pain meds and started to feel much better. I would likely be bedridden and addicted to painkillers, rather than hiking in New Hampshire, had I not started taking Vitamin D. I think it's been a couple of years since I heard you mention Vitamin D on the podcast, so I want to urge you to remind people about that episode and your Vitamin D page, in case there is anyone else out there facing a similar situation."

Leo: And this would be the place where I would mention that neither Steve nor I are medical doctors, and that we, you know, this is not medical advice.

Steve: Yes. I have in the show notes, I said: "Everyone should keep in mind that I have no formal medical training of any kind. I'm a self-taught health hobbyist.

Leo: Which should say something right there. And Chris's story, while amazing, is purely anecdotal.

Steve: Absolutely.

Leo: However, the good news is Vitamin D is not toxic. So at worst you're throwing money away; right?

Steve: Well, it is toxic at extremely high doses.

Leo: You have to take a lot of it.

Steve: You have to take a lot.

Leo: Yeah.

Steve: So it was our audio podcast, actually it was an audio-only podcast, Leo, 209, recorded on August 13th of 2009. And at the time I had been spending a lot of time researching health and nutrition. I would take something - a vitamin or a mineral - and read one or more entire books about it, cover to cover.

And I have to say that that research, which was done 20 years ago, before I turned 50, it's had a profound effect upon the lives of myself, my family, and my friends. I have no way of knowing whether I would feel as fantastic as I do today if I had not been consuming a wide range of supplemental nutrition for the past 20 years. You know, we'll never know. But I do know that there's still a lot more that I want to accomplish, so I'm going to keep doing what I've been doing since, if nothing else, it certainly doesn't appear to be hurting.

However, I know that for many people consuming lots of supplements may not be practical for a number of reasons. Many dislike taking pills. They can upset stomachs, and there's an added cost, of course, above one's normal diet. And for that reason, I've been extremely selective, like down to one, about, you know...

Leo: I keep begging Steve to tell me what else he knows, but he won't tell me.

Steve: So, you know, so I've been selective about what I've shared of my research. I mean, Leo, there's just there's some fascinating things. But anyway. I felt compelled to steal an early episode of Security Now! to explain what I had learned about Vitamin D. What you will find, our listeners who don't already know, will find in that podcast is an explanation of the science and the biochemistry of Vitamin D, why it's not actually a vitamin, and the many reasons why it's so crucial to human health.

And interestingly, this was done in August of 2009. The spring following that podcast, so the

spring of 2010, I started receiving notes from many of our listeners who separately, individually reported that for the first time in their lives they and their family, who were also taking a useful - who had started taking a useful amount of Vitamin D had sailed through the winter months without so much as a sniffle. And years later we saw an example of Vitamin D's powerful benefits for our immune system during the world's struggle with COVID-19. Multiple studies revealed - and again, we know that correlation is not causation. But there was a strong correlation shown between people's Vitamin D status and their COVID outcomes.

So anyway, the reason I chose to talk about Vitamin D is that only micrograms of it are required. It's extremely potent. So that means that a useful daily dose of four to 5,000 IU is delivered in a little, tiny, easy-to-swallow capsule of olive oil - or, as I like to refer to them, "little drops of sunshine." And Vitamin D is also very inexpensive. About a year's supply is $15.

So anyway, I just - thank you, Chris, for putting this back on everyone's map. Again, I'll say I have no formal medical training. I'm just curious about the way my body works. And I feel a little guilty that there's so much more I could share, but I am self-taught.

Leo: Can we just - can we have a little private chat sometime, and you can tell me what else I should be doing?

Steve: Well, you know, two of my very best friends, my high school buddies, are MDs. And they're always saying, okay, Steve, what should we be taking? Because of course...

Leo: Well, I do C because of you, and megadoses of C. You do more than I do. But I do three grams a day.

Steve: Yeah, that's not enough. But it's better than none.

Leo: It's a lot.

Steve: Here's an example, Leo. There is an enzyme, L-Gulonolactone oxidase.

Leo: Yes, of course.

Steve: I know. We know the chromosome on the human genome which codes for the creation of that enzyme. If that enzyme were being created, our livers would be synthesizing, based on our weight, around 20 grams of Vitamin D a day.

Leo: Whew.

Steve: Yes. And here's the other weird thing is all the other animals in the animal kingdom.

Leo: They make it.

Steve: Yes, except guinea pigs, some fruit bats, and a couple primates that we're very closely related to. But the dogs and cats that people have as pets, all the animals in the zoo, everything is synthesizing their own Vitamin C because it's so important. And the other thing is that our liver, our livers are trying to make it. The first five steps of the synthesis process, it's a six-step

process, they're all present and working. But the lack of that one enzyme causes it to fail.

Leo: Wow.

Steve: And if you inject that enzyme into someone, they suddenly start producing Vitamin D until the enzyme ends up being destroyed over...

Leo: Vitamin C.

Steve: Vitamin C, yeah.

Leo: We're talking about C now. We talked about D. So I put, I have a liquid Vitamin C that's three grams per capful I put in my beverage.

Steve: That's, I mean, that's absolutely...

Leo: But maybe I'll do a couple of those then.

Steve: It's absolutely a good thing to do.

Leo: You think I need 20 grams of Vitamin...

Steve: I take 10. I take five in the morning and five in the evening.

Leo: That's a lot. Okay.

Steve: It's water soluble, so it doesn't stay with you.

Leo: It just goes right - that's why I do it in here, in this, because it's titrated. So I'm sipping all day, so kind of a constant flow of C. Because it does, it goes right through you. It doesn't...

Steve: That is a good thing.

Leo: Yeah.

Steve: And, you know, I know there's lots of people who say, oh, supplements don't do anything, it's just a scam to take your money. It's like, okay, I get it. And as I said, I'll never have any proof that I wouldn't be in the same condition I am in.

Leo: That's the problem, yeah.

Steve: If I hadn't been doing this.

Leo: We don't know if you'd be exactly as you are today having never taken a supplement at all. There is no way of knowing that.

Steve: Right.

Leo: By the way, maybe, and they're suggesting this, you and I can get together, we do this little Friday off-the-cuff kind of broadcast where we could talk about the other things that you recommend? If we had big disclaimers?

Steve: The problem is I would have to spend so much time researching it and getting back up to speed, I mean, I think one of the things our listeners like about this podcast is that I'm...

Leo: It's deeply researched.

Steve: I spend a lot of time putting it together.

Leo: Yeah, yeah.

Steve: And I may get around to it. I mean, get around to doing something more.

Leo: The invitation's always here.

Steve: Thanks.

Leo: Just so you know. We have this - Fridays I do kind of an oddball thing. I'm going to do coffee again. We did a coffee thing. It was a lot of fun, cost me huge amounts of money in coffee equipment. Do you want to take a break?

Steve: Yeah, let's do it.

Leo: Okay.

Steve: Perfect.

Leo: And then we will go on and talk about CUPS. And I am still very interested in the recommendations for the best routers. That'll be now, Steve. On we go.

Steve: Shane Overturf, an IT Consultant who listens to the podcast, said: "Steve, you've probably already seen this article by Akamai regarding the CUPS vulnerability; but in case you haven't, I thought it would be of interest to you." And he gives me a link.

And he said: "While it's true that most people aren't going to be exposing port 631 to the Internet" - this is the CUPS vulnerability that we talked about last week - "and I can't think of a valid reason to expose it, it's apparent that there are a fair number of those who do have it exposed. The Akamai article shows how trivial it is to leverage this vulnerability into a much more

serious and widespread attack," he said, "something you alluded to in the last podcast. So for the devs to dismiss it as 'not so bad' seems to be a dangerous attitude. Looking forward to Security Now!," he says, "'boldly going where no man has gone before' to 999 and beyond."

So I'm glad that Shane brought this to my attention. Last week I did note in passing that a handful of other security researchers had also examined the CUPS vulnerability, but I did not bother to dig into them. Akamai's findings are a bit chilling because they note that the presence of the CUPS-browse service, which is the thing that listens on port 631, allows it to be used in amplifying reflection attacks.

They gave their write-up the title "When CUPS Runneth Over: The Threat of DDoS." Akamai wrote: "Akamai researchers have confirmed a new attack vector using CUPS that could be leveraged to stage distributed denial-of-service attacks. Research shows that, to begin the attack, the attacking system only needs to send a single packet to a vulnerable and exposed CUPS service with Internet connectivity.

"The Akamai Security Intelligence and Response Team (SIRT) found that more than 198,000 devices" - so just shy of 200,000 devices - "are vulnerable to this attack vector and are accessible on the public Internet. Roughly one third of those, 34% of those could be used for DDoS abuse," they said, "58,000-plus. Of the 58,000-plus vulnerable devices, hundreds exhibited an 'infinite loop' of requests. The limited resources required to initiate a successful attack highlights the danger. It would take an attacker mere seconds to co-opt every vulnerable CUPS service currently exposed on the Internet and cost the attacker less than a single U.S. cent on modern hyperscale platforms.

"While reviewing the technical write-up about the vulnerabilities, we discovered that another attack vector was not discussed: DDoS. DDoS continues to be a viable attack vector used to harass and disrupt victims across the Internet, from major industries and governments to small content creators, online shops, and gamers. Although the original analysis focused on the RCE - the Remote Code Execution - which could have a more severe outcome, DDoS amplification is also easily abused in this case.

"The problem arises when an attacker sends a crafted packet specifying the address of a target as a printer to be added. For each single packet sent, the vulnerable CUPS server will generate a larger and partially attacker-controlled IPP/HTTP request directed at the specified target. As a result, not only is the target affected, but the host of the CUPS server also becomes a victim, as the attack consumes its network bandwidth and CPU resources.

"We should note that many of these identified machines were running" - get this - "on very old versions of CUPS, such as version 1.3, which was initially released in 2007. It is not uncommon for some organizations to leave machines running on extremely outdated hardware and software, and it is unlikely that such devices will be updated anytime soon. This presents a prime opportunity for malicious threat actors. They can take advantage of the outdated hardware for DDoS amplification or, given the RCE in this scenario, build botnets for many purposes, including DDoS." So yes, as we say, vulnerabilities and exploits never get worse, they only ever get better.

Oh, and to the issue of consumer routers, a listener who requested anonymity wrote: "Hello, Steve. I've been listening to your show for a few years, thanks to the recommendations of my former coworker. I am following more than I could at first and think I catch the general gist, but still miss significant bits of the technical know-how. Could you please recommend what is the most secure out-of-the-box residential router for non-technical folks, please? I want to replace my parents' router for multiple reasons, primarily since I can longer access the online admin portal to update the firmware, which is HTTP, and concerns about TP-Link on the backend. I've heard suggestions, such as use pfSense, but I've also heard that it would be easy to misconfigure something.

"I'm in a non-technical role, and I might be able to follow a YouTube video potentially, but I'm concerned about missing configurations. Would greatly appreciate it if you or the community could please recommend a budget-friendly residential router that is secure by default without needing end-user configuration. Thank you." And then she finished, "I'd appreciate not having my name mentioned on the show."

Leo: I think that's really a great question because you're a sophisticated user. You can run pfSense, and maybe many of our audience members are. But I think it's - for instance, people say, why don't you host your own password vault? And I'm not an expert on this. Bitwarden is. I let Bitwarden do it. And I think even though it's not Trust No One, it's safer to do that. I wish I had your skills, but I don't. So it's appropriate, I think, for somebody to say, well, what's a safe, effective solution that doesn't require a lot of tweaking and fiddling and knowledge?

Steve: Right. And that's exactly the case. And I liked this listener's question because I believe that today's mainstream consumer routers are all going to be secure by default.

Leo: Well, that's good news.

Steve: And, you know, after enabling automatic firmware updates, which today's routers have, that will keep themselves updated in the event of anything significant happening. Now, having said that, disabling UPnP and WPS, which are the two things that are generally enabled by default, that's a good idea, too. But my point here that consumers primarily get into trouble when they enable the additional extra fancy features that are being promoted to sell these routers today; things like remote WAN-side admin or any sort of Internet accessible media, file, or other types of servers. A media server, a file server or anything like that.

We've seen over and over and over there is no safe and secure way to do any of that. There are secure ways to accomplish those things, but they're more complex. They're more complex because more complexity is required to do those things securely. So in other words, don't do them at all unless you're going to do them the right way. Don't just flip a switch in your router to turn that stuff on. That's where you get into trouble.

So, you know, in this case our listener's parents, for whom she's getting this router, they don't need any of that crap. They need a NAT router. And, you know, NAT is secure unless you do something to make it insecure. Unfortunately, UPnP can make it insecure, and WPS can make it insecure. They just need a generic SOHO (Small Office Home Office) NAT router. I'm partial to ASUS, and I don't think I'd look any further than that since something in ASUS's line would likely be a good match. You know, I just looked at Amazon last night because I was curious. There's a nice-looking ASUS WiFi router for $66. You know, so that's definitely budget-friendly.

And the ASUS firmware supports disabling WPS and UPnP. It offers isolated WiFi guest networks, so that you can put your guests and your IoT devices on a network isolated from the rest of the Intranet. Also a listener of ours, Michael Horowitz, maintains a terrific website over at routersecurity.org, all just one word, R-O-U-T-E-R-S-E-C-U-RI-T-Y, routersecurity.org. And I recommend Michael's site without reservation for any additional router security research someone would want to do.

Leo: It's really a short list. I think this is exactly what I've recommended for years.

Steve: Yup. Yup.

Leo: I used to have a five-step thing I did on the radio show. Before you use any wireless router change the password, the administrative password. Change the default SSID. Turn on WPA2 encryption. As you said, turn off WPS and turn off UPnP. And you're pretty good right there. You've got some other things to do, like look for port-forwarding and make sure that that's not turned on.

Steve: But again, it won't be by default.

Leo: Right, right.

Steve: So, yeah.

Leo: And I do think that that recommendation now that we make nowadays, which is turn on auto updates and make sure it's doing that, has become more and more important. Stacey Higginbotham, for a long time, our IoT expert, said don't buy any IoT device that will not automatically wirelessly update because you're going to need updates. There is no device that's perfect. And if you turn those updates, if it has the updates in the first place, and you turn them on, that's pretty good. You agree?

Steve: Yup. I think that's right. And so I guess the main thing I wanted to say was that when we talked about the ASUS 9.8 CVSS problem, well, that was because somebody turned on one of those extra features. That's where you get into trouble. An out-of-the-box ASUS router is a strong NAT router. It's going to be fine.

Leo: And if you turn on automatic updates, you wouldn't have had that problem either; right?

Steve: Right.

Leo: That would automatically fix it. The other thing I love about ASUS is they use their own customized version of DD-WRT, which is an open source router firmware. You can put DD-WRT on your ASUS router, as well. And that's nice because, again, open source means there are a lot of eyes looking at it, lot of people working at it, and a lot of fixes out there. Yeah, I agree with you on ASUS. We use Ubiquiti. We've always used Ubiquiti as a kind of a prosumer home system here.

Steve: Yeah, Michael likes Peplink, pep something, but it's like a $300 router, and it's - he thinks it's more secure.

Leo: Synology makes excellent routers, too, by the way.

Steve: Yes, Synology's got some nice routers, too.

Leo: If you want to pay the - honestly, all the good routers, including ASUS now, are well over $200. $300 is not an unusual amount of money. Used to be you could buy a $59 Linksys router. That route is pretty much shut down, as it should be.

Steve: Well, and the reason is they've - a lot of them are all these fancy gaming things, and they've got quality of service and...

Leo: And 18 antennas.

Steve: And, yeah. I just think there's a lot of stuff you're paying for that most people don't need.

And I would say that our listener's parents, who just need something for their home, I'd spent 66 bucks for that bottom-of-the-barrel ASUS. There's nothing wrong with it.

Leo: Does ASUS have a $66 router?

Steve: Yeah.

Leo: That's good to know. The other thing I would add, we often come across this on The Tech Guy, is that larger installations, bigger homes, mesh systems are often a good way to go. And Eero makes a very good, a very easy-to-use mesh system with excellent security, as well. So if you do need more than - sometimes a single ASUS in the middle of the house isn't enough to get to the corners.

Steve: And what do they call it, AI mesh, ASUS has a whole, a very mature mesh technology.

Leo: They do have a mesh system, yeah, yeah. Actually, that wouldn't be bad, either. I haven't tried it, but I'm sure it's good. ASUS is good, yeah.

Steve: Okay. We're at our main topic, uBlock Origin and Manifest V3. Why don't we take our last break, and then we will do this unbroken.

Leo: Which was the name of Kevin Rose's, as you may remember, Kevin Rose's hacker podcast for a long time, The Unbroken. So this is a subject I've been very interested in for some time because Google's move towards Manifest V3 seems to be very self-serving and may be enough for me to abandon using Chrome.

Steve: Well, we talked about it before, and it is the case that it's more secure. But it comes at the cost of neutering features of the add-ons that many of us have come to rely on.

Leo: A beneficent side effect, one might say.

Steve: Yeah. So it's been several years since we talked about this, you know, the web browser content blocker that's heavily favored by the Internet's more tech-savvy users. It's what many of the listeners to this podcast, and you and I, Leo, are using. I have it installed everywhere possible. And I've often commented, when I see unfiltered websites, like other people are using a browser...

Leo: How do you use that stuff?

Steve: I can't imagine, I mean, like stuff's jumping up and down, and things are popping up and sliding across the screen, and I just - I cannot imagine not having uBlock Origin filtering the mess that the Internet has become.

Leo: I mean, we're ad supported. I'm not against ads. Ads are vital to the ecosystem. But there's ads, and then there's ADS. And some of this is a security issue, as well.

Steve: Yeah, the little monkeys jumping up and down with the barbells, it's crazy.

Leo: Yeah. No. Yeah.

Steve: So unfortunately, web browsers are gradually tightening the screws on the freedoms that add-on extensions such as uBlock Origin have traditionally enjoyed and upon which they depend. The Chrome browser's eventual shift from Manifest V2, you know, version 2 to version 3 promises to make life much more difficult, if not impossible, for add-ons like uBlock Origin to continue to provide the features we've grown to depend upon.

And there's been some recent interesting turbulence involving uBlock Origin, Mozilla, and uBlock Origin's cantankerous creator and developer and maintainer, whose real-world name is Raymond Hill. He goes by the moniker "Gorhill." And we'll get to the recent trouble between Mozilla and Gorhill in a minute where some seven million installations of uBlock Origin are currently installed. But let's first look at what's going on with uBlock Origin and the future of the Chrome browser, which has around 37 million installations.

The Neowin site recently published a nice summary with the background titled "uBlock Origin developer recommends switching to uBlock Lite as Chrome flags the extension." So Neowin wrote: "Google recently released Chrome 127 into the Stable Channel, and the update caused some commotion among certain customers. Those using the uBlock Origin extension, one of the most popular and well-received adblockers, noticed that the browser now flags the extension with the following message. It says: 'uBlock Origin: This extension may soon no longer be supported. Remove or replace it with similar extensions from the Chrome Web Store.'"

They wrote: "Makers of the uBlock Origin extension [meaning Gorhill] published an article on GitHub that explained why Google Chrome claims uBlock Origin 'may soon no longer be supported.' Long story short," they wrote, "the message appears due to Google's plans to deprecate Manifest V2-based extensions in favor of Manifest V3. For those unfamiliar," they said, "Manifest is a set of rules that defines how extensions integrate into browsers and interact with their web pages. Migration from Manifest V2 to V3 has been long in the making. It faced tremendous criticism from users and developers, forcing Google to delay its plans and implement various changes to address the complaints.

"Despite multiple changes, Manifest V3 still imposes significant limitations on browser extensions, especially content blockers. There is no Manifest V3-based uBlock Origin, so the developer recommends uBlock Origin Lite, a 'pared-down' Manifest V3-compliant version of the extension. Like uBlock Origin, uBlock Origin Lite prioritizes reliability and efficiency, but it has to compromise some features that are now impossible under Manifest V3. There's a dedicated web page that describes the difference between uBlock Origin and uBlock Origin Lite.

"Since the switch to Manifest V3 cripples the extension quite a lot, the developer does not plan to implement an automatic upgrade in the Chrome Web Store." Basically, these are separate products. It doesn't make any sense for uBlock Origin the full version to upgrade to the Lite version. Gorhill's not going to do that. "Therefore, users can either stick to it until the bitter end or," they write, "look for Manifest V3-compliant alternatives, such as uBlock Origin Lite or others."

Okay. So on this point Gorhill wrote: "Manifest V2 uBlock Origin will not be automatically replaced by Manifest V3 uBlock Origin Lite. uBlock Origin Lite is too different from uBlock Origin for it to silently replace uBlock Origin." He said: "You will have to explicitly make a choice as to which extension should replace uBlock Origin according to your own prerogatives. Ultimately, whether uBlock Origin Lite is an acceptable alternative to uBlock Origin is up to you. It's not a choice that will be made for you." And we have to say that that's sort of a refreshing approach; right? After we saw...

Leo: Kasparov...

Steve: Yes, thank you.

Leo: Not Kasparov, Kaspersky.

Steve: Kaspersky.

Leo: Or Kaspersky.

Steve: After we saw Kaspersky just automatically give people a replacement and surprise them, thinking that their computers have been infected with malware.

Leo: Is better. You like this.

Steve: So anyway, Neowin's coverage finishes, saying: "According to the most recent announcement, Google plans to finish the migration to Manifest V3 by the end of this year, 2024. However," they said, "enterprise customers will have the ability to continue using Manifest V2" - the ones we want - "extensions for an additional six months. Interestingly, Mozilla, the only mainstream browser maker that does not use Chromium" - I suppose that's true if you ignore Apple browsers - they wrote, "does not plan to ditch Manifest V2 extensions." In other words, we can stay with what we want on Firefox. They said: "Therefore, uBlock Origin will continue working in Firefox and other browsers that do not deprecate V2 extensions."

Okay. So although Chrome is reported to already be deprecating Manifest V2 in favor of V3, I just checked, and my Chrome is running the full uBlock Origin without any complaint. But that might not last long since Google has said it will be finished with this migration three months from now. In Google's own Manifest V2 support timeline document, which I tracked down, they wrote: "On June 3rd of this year, 2024, the Manifest V2 phase-out begins."

They said: "Starting on June 3rd, which was the date of this announcement, on the Chrome Beta, Dev, and Canary channels, if users still have Manifest V2 extensions installed, some will start to see a warning banner when visiting their extension management page." Okay, and everybody can do that now, anybody with Chrome. "Up in the URL put chrome://extensions. That informs them that some Manifest V2 extensions they have installed will soon no longer be supported. At the same time, extensions with the Featured badge that are still using Manifest V2 will lose their badge."

So reading that, I fired up my Chrome, which I don't normally have running any longer, and went over to chrome://extensions. And sure enough, there it was. For uBlock Origin it said: "This extension may soon no longer be supported. Remove or replace it with similar extensions." And then a link to the Chrome Web Store. And also down below, where it specifically shows the uBlock Origin little red shield icon, there's a link to "Find alternative." Okay, I didn't do any of that, and I'll tell you why in a second.

So Google said: "This will be followed gradually in the coming months by the disabling of those extensions. Users will be directed to the Chrome Web Store, where they will be recommended Manifest V3 alternatives for their disabled extension. For a short time after the extensions are disabled, users will still be able to turn their Manifest V2 extensions back on, but over time that toggle will go away, as well." So they're trying to softly force everyone off of V2 extensions. But eventually, like by turning them off, then you can go back and turn it on if you want to, then they'll turn it off again, so you can fight with Chrome that way for a while.

And they said: "Like any big launches, all these changes will begin in pre-stable channel builds of Chrome first - Beta, Dev, and Canary. These changes will be rolled out over the coming months to Chrome Stable, with the goal of completing the transition by the beginning of next year, meaning 2025."

And that timeline document ended with the statement: "Enterprises using the ExtensionManifestV2Availability policy will be exempt from any browser changes until June of 2025." Well, that, I thought, was interesting. What's this "ExtensionManifestV2Availability" policy, and where can I get one? So I tracked that down. It applies to Windows, Mac, and Linux builds of Chrome, the desktop versions. Google's description for the policy, Google's, you know, the maker of Chrome, their description of the policy is: "Control if Manifest V2 extensions can be used by browser." Which sounds like exactly what we want.

So the details are, they said, under their description of this policy: "Manifest V2 extensions support will be deprecated, and all extensions need to be migrated to V3 in the future. More information and timeline of the migration can be found at" blah blah blah. "If the policy is set to Default, or not set, V2 extensions loaded are decided by browser, following the timeline above." Not quite well written, but fine. "If the policy is set to Disable" - that's setting number one - "V2 extension installations are blocked. Existing ones are disabled. The option is going to be treated the same as if the policy is not set after V2 support is turned off by default." Meaning you could do it now if for some reason you wanted to, or if your corporation did it to you or something.

"If the policy is set to Enable" - that's setting two - "V2 extensions are allowed. The option is going to be treated the same as if the policy is not set before V2 support is turned off by default." In other words, you get to keep them. Then they said: "Extensions' availability are still controlled by other policies." So we have 0 is the default, 1 is they're disabled, 2 is they're enabled, and 3 is that they're enabled for forced extensions only.

Chrome's "forced extensions," as a reminder, are those that are installed by enterprise policy. They're installed silently without user interaction, bypassing the normal installation process, and they're not removable by users. So setting this to two sounds like exactly what we want. That gives any savvy Chrome users an additional six months of access to their current V2 extensions, not just uBlock Origin by anything else that you might want which is sensitive to this V2/V3 switchover.

For Windows systems, this policy can be applied by adding a 32-bit DWORD value to the Windows registry. It can be done by hand or by executing a .REG registry file. And you know this is coming; right? To make this as easy and foolproof as possible for our listeners, I've created a GRC shortcut which will allow you to instantly obtain a three-line, it's very simple, registry file from me. So the shortcut is grc.sc/v2. That will offer your browser a file to download named "V2Extension.reg." You can open it in a text editor to verify its contents or to get, if you want to do it by hand, which you're certainly welcome to, to get the exact spelling of everything because that's got to be exactly right. Either way, you can double-click on the file to execute it.

Since the file has come to you from the Internet, it will carry the "Mark of the Web," which will cause Windows to scrutinize it further. Since .REG files are just text files, I cannot digitally sign that. So I was unable to give it GRC's blessing. So Windows will inform you that the source of the file cannot be verified, and ask if you're sure. Once you say, "Yeah, it's okay, I know that guy," you'll get another pop-up, this time from the Registry Editor explaining that running .REG files can mess things up, and that you should only proceed if you know and trust the source of the file and you're sure you want to continue. If you click "Yes," your system will have added a policy to Chrome instructing it to continue allowing Manifest V2 extensions to run without harassment until next summer.

A cool thing you can do, either before or after, actually it'd be fun to do it both, is there's a different URL you can put into Chrome, chrome://policy. That will show you any policies that are set in Chrome. I didn't have any before. After I ran this registry tweak, sure enough, there it displayed the policy that was in place. And when I went back to chrome://extensions, that warning message about uBlock Origin was gone. So Chrome is no longer nervous about me running a V2 extension. And now I get to keep uBlock Origin for Chrome, not that I use Chrome very much. But sometimes I do. I get to keep it until June of 2025. Yup, and there that is, the "Are you sure you want to do it?"

Leo: Good. So now I'm safe on Windows.

Steve: Yup.

Leo: Not so much anywhere else, but...

Steve: No. The same policy is available on Mac and Linux.

Leo: Ah.

Steve: There they call it a "preference." And I didn't track down how to set a Chrome browser preference.

Leo: Yeah. We'll figure that out.

Steve: But it is available on all of the desktop platforms.

Leo: Good to know. Thank you, Steve. That's great.

Steve: Yeah. Okay. So this brings us back to the question: "What features does V2-compatible uBlock Origin sacrifice in the transition to V3-compatible uBlock Origin Lite? Because after June of 2025 Chrome and all Chromium-based browsers...

Leo: Well, that's the question. Do they all have to do it? Like does Brave have to do it? Does Arc have to do it? I mean, these are all - Edge?

Steve: It looks like Edge is going to be terminating V2 support. Brave, I have learned from one of our listeners, appears to be willing to go to some effort to continue with V2 support. So I think we'll be a little bit on pins and needles.

Leo: Possible, anyway.

Steve: Well, maybe. I mean, it is pretty core to the Chromium architecture. It may be that they're not going to rip out V2. They're just going to, like in Chrome, they'll shut it down but leave it there. So Brave may be able to turn it back on. It's just we don't know at this point.

Okay. So the questions are, what's happening? The uBlock Origin Lite GitHub repository has an FAQ page which answers this question in some detail, and actually with lots of technical jargon. Wikipedia actually offers a more accessible summary. So here's what Wikipedia says. They said: "In 2023, Google made changes known as 'Manifest V3' to the WebRequest API used by adblocking and privacy extensions to block and modify network connections. Following Google's implementation of Manifest V3 and the end of support for V2, uBlock Origin's effectiveness is drastically reduced in Google Chrome and other Chromium-based browsers."

Okay. And I'll just interject that, while this sounds bad, and is, this is not any failing in uBlock Origin. It's true universally for all content control add-ons under MV3. This is why Google has been met with significant pushback, and why, for example, the EFF is apoplectic.

Anyway, Wikimedia elaborates. They wrote: "As a result, uBlock Origin Lite was created and designed to comply with Manifest V3 extension framework. uBlock Origin Lite differs significantly from uBlock Origin in several key aspects, primarily due to the constraints and design goals

associated with MV3. Specifically, it lacks filter list updates outside of extension updates, and has no custom filters, strict-blocked pages, per-site switches, or dynamic filtering. Non-Chromium browsers," they wrote, "such as Firefox are unaffected. Google has been criticized for implementing some of these features due to its dominance in the online advertising market."

Gorhill's FAQ page for uBlock Origin Lite asks and answers this question. Question: "If I install uBlock Origin Lite, will I see a difference from uBlock Origin?" And his answer: "Maybe. Maybe not. It depends on websites you visit, how you configured uBlock Origin, and how you configured uBlock Origin Lite." And he says: "In short, only you can tell." He says: "It's very possible that the sites you visit do not require any of the filtering capabilities specific to uBlock Origin, in which case you won't see a difference.

"Also, mind that by default there's no cosmetic filtering or scriptlet injection in uBlock Origin Lite, while these occur by default in uBlock Origin. In uBlock Origin Lite, you will have to raise the blocking mode to either Optimal or Complete to benefit from cosmetic filtering and scriptlet injection. Furthermore, uBlock Origin Lite requires the default mode to be Optimal or Complete for some advanced filtering capabilities to take effect, while they're enabled by default in uBlock Origin. In general, uBlock Origin Lite will be less effective at dealing with websites using anti-content blocking, or minimizing website breakage."

Okay. So it doesn't sound like the end of the world for uBlock Origin Lite on Chrome, which Chrome users will at least be able to delay using now, using this policy change, until June of 2025. So that's the story with Chrome and all the closely related Chromium-based web browsers. The great news for the seven million of us who are currently using the full uBlock Origin on Firefox is that Mozilla has officially stated that they have no plans to remove support for Manifest V2 from Firefox.

Leo: Oh, that's great.

Steve: And Leo, as you said, you know, that's going to put some pressure, I think, on people who really do care about controlling their Internet browsing experience.

Leo: They should have been using Firefox all along, anyway, in my opinion.

Steve: Yes, agreed.

Leo: Yeah.

Steve: Yeah. So the good news is Mozilla has no plans to do the same for Firefox. Okay. However, uBlock Origin is so popular and well known that a recent kerfuffle between Mozilla and Gorhill regarding uBlock Origin Lite received a great deal of attention online. There's a bunch of coverage of it in the tech press. A bunch of our listeners said, hey, what's this about? Can you figure this out?

So, okay. You may be thinking, did I say Mozilla and uBlock Origin Lite?

Leo: Yeah.

Steve: And if so, why is there a Lite edition of uBlock Origin on Firefox when Mozilla has said that Firefox's support for Manifest V2 is safe and will never be removed? The reason is that Gorhill just wanted to release the same add-on feature-set for Firefox and Manifest V3 that he had created for Chrome. He wanted to have a uBlock Origin Lite available for both major web browser platforms.

A little over a month ago, Gorhill posted to GitHub that he had received two emails from Mozilla Add-Ons, you know, addons.mozilla.org, also known as AMO, you know, the abbreviation of that domain, addons.mozilla.org. And he posted the entire content of the emails that he had received.

Mozilla Add-Ons wrote: "Hello. Your Extension uBlock Origin Lite was manually reviewed by the Mozilla Add-ons team in an assessment performed on our own initiative of content that was submitted to Mozilla Add-ons. Our review found that your content violates the following Mozilla policy or policies. First, consent, specifically, nonexistent: For add-ons that collect or transmit user data, the user must be informed and provided with a clear and easy way to control this data collection. The control mechanism must be shown at first-run of the add-on.

"The control should contain a choice accompanied by the data collection summary. Depending on the type of data being collected, the choice to send cannot be enabled by default. If data collection starts or changes in an add-on update, or the consent and control is introduced in an update, it must be reshown to all new and upgrading users. For the exact requirements, refer to" - and then they have a URL. "For an example of how to provide a consent and control dialog, see" - and another URL. "Also, if your add-on is listed on addons.mozilla.org, the listing needs to include a privacy policy, and a summary of the data collection should be mentioned in the add-on description."

Leo: You can't blame Mozilla for saying that; right? I mean...

Steve: Right. Yeah, absolutely.

Leo: But Gorhill probably doesn't want to do that.

Steve: Well, yes. And so point number two, they wrote: "Sources, specifically Sources or instructions are missing." They wrote: "Your add-on contains minified, concatenated, or otherwise machine-generated code. You need to provide the original sources, together with instructions on how to generate the exact same code used in the add-on. Source code must be provided as an archive and uploaded," blah blah blah blah blah. Okay. And this refers to a bazillion affected versions. He's got, like I can't even count, like I don't know, like a huge number of affected versions.

Leo: Well, that's reasonable, too, because if there's hidden code in there...

Steve: Completely reasonable. Completely reasonable. So, and the second email listed exactly the same add-on policy failures, none of which applied to uBlock Origin Lite, or uBlock Origin, for that effect. But that one only showed the oldest of the versions and gave him 14 days to cure the problem. The other ones immediately yanked all of those previous ones including the most recent one from the add-ons site, the Mozilla add-ons.

Gorhill predictably reply wrote in the thread, he said: "Contrary to what these emails suggest, the source code files highlighted in the email have nothing to do with data collection. There is no such thing anywhere in uBlock Origin Lite. There is no minified code in uBlock Origin Lite, and certainly none in the supposed faulty files. There is a privacy policy link in uBlock Origin Lite's add-on page," meaning these manually reviewed emails were 100% bogus. Like whoever did this couldn't have actually looked at what was being supplied. They probably assume that every add-on now is doing data collection. And so when they saw that this thing didn't pop up a data collection notification, they said, oh, it's missing. Well, yes.

Leo: But Gorhill doesn't collect any data?

Steve: None whatsoever. Zero.

Leo: All right.

Steve: That's not what uBlock Origin does; right?

Leo: Right.

Steve: I mean, he's old-school. He's, you know, he's one of us.

Leo: But could it be said you're collecting data if, I mean, I wonder if some of the activities of an adblocker kind of imply that maybe you have to look at the this - for instance, you might have to look at the site somebody's visiting to know what extension to enable. Or there may be, it may be that in fact the extension sees the sites that you're visiting, in which case there is a theoretical possibility of data collection; right?

Steve: Well, that's why he provides the source. And we've talked about this. Firefox requires that you provide the full source, no minification, and instructions on how to build it from scratch. So that it's like...

Leo: Good.

Steve: Yeah. I mean, they've done everything right. Unfortunately, they have accused Gorhill of using minified code, no ability to build it, and data collection, none of which is true.

Leo: So he doesn't do any of that.

Steve: Doesn't do any of that.

Leo: He doesn't minify code?

Steve: No.

Leo: Oh, so this was some automated thing that didn't know what the hell it was talking about.

Steve: It was completely bogus. It was completely bogus. And the problem is you don't give bogus stuff to Gorhill.

Leo: Not to Gorhill. No, no.

Steve: So he responds: "I don't have the time or motivation to spend time on this nonsense, so I will let AMO do whatever they want with uBlock Origin Lite."

Leo: Oh, lord.

Steve: "I will probably publish a self-hosted version which auto-updates, like how dev build of uBlock Origin is self-hosted, when I find the time to arrange all that." Okay. So that was his first posting. The following day, on September 5th, someone with the handle "Rob-W" posted in this discussion thread over on GitHub, he said: "@gorhill The review decision looks inaccurate to me. Could you reply to the email to let the original reviewers know that the assessment is inaccurate? What you wrote above in the comment is sufficient." Gorhill did not reply to that in the thread. But nearly two weeks later...

Leo: I don't know who Raymond Hill is. I see him as something like Ted Kaczynski, in a shack somewhere with a really long beard.

Steve: Like I said, if Dvorak wrote code.

Leo: This would be...

Steve: What are you talking about?

Leo: God bless him, and we are very grateful. And, you know, I don't blame him for not wanting to engage in bureaucratic back-and-forth.

Steve: That's just exactly it. So two weeks go by. And on September 18th Gorhill posted: "Starting with uBlock Origin Lite," and it was 2024.9.12.1004, "the Firefox version of the extension will be self-hosted and can be installed from the release section. The extension will auto update when a newer version is available."

And then, on September 26th, Gorhill posted that he had changing his mind. He wrote: "The Firefox version of uBlock Origin Lite will cease to exist. I am dropping support because of the added burden of dealing with AMO's nonsensical and hostile review process. However trivial this may look to an outsider, it's a burden I don't want to take on; since the burden is on me, I make the decision whether I can take it on or not. It's not something up for discussion."

He said: "The burden is that even as a self-hosted extension, it fails to pass review at submission time, which leads to having to wait an arbitrary amount of time, where time is an important factor when all the filtering rules must be packaged into the extension. And once I finally receive a notification that the review cleared, I have to manually download the extension's file, rename it, then upload it to GitHub, then manually patch the update URL to point to the new version. It took five days after I submitted version 2024.9.12.1004 to finally be notified that the version was approved for self-hosting. As of writing, version 2024.9.22.986 has still not been approved.

"However often I look at all this, every time I can only conclude the feedback from Mozilla Add-ons Team to have been nonsensical and hostile, and as a matter of principle I won't partake in this nonsensical and hostile review process."

Leo: I can't say I blame him.

Steve: "It only takes only a few seconds to see how this is nonsensical. Keep in mind that this

'was manually reviewed by the Mozilla Add-ons team'." And then he says, he quotes them: "For add-ons that collect or transmit user data, the user must be informed and provided with a clear and easy way to control this data collection." And then he says: "Where is the 'data collection' in this file?" And he provides the URL to the JavaScript of his code Then he quotes them again. "Your add-on contains minified, concatenated, or otherwise machine-generated code." And then he says again, "Where is the 'minification' in these files?" And then he gives us four URLs to the open source JavaScript of his code.

Then he quotes them again: "Also, if your add-on is listed on addons.mozilla.org, the listing needs to include a privacy policy, and a summary of the data collection should be mentioned in the add-on description." And he said: "Right. It's always been there since the first version published on AMO more than a year ago."

Leo: Oh dear.

Steve: And then he gives us the URL. And he said: "Incidentally, all the files reported as having issues are exactly the same files being used in uBlock Origin for years, and have been used in uBlock Origin Lite as well for over a year with no modification. Given this, it's worrisome what could happen to uBlock Origin in the future given it uses the exact same files." He says: "Steps taken by Mozilla Add-ons Team as a result of the (nonsensical) 'issues' was to disable all versions of uBlock Origin Lite except for the oldest version, first published by AMO on August of 2023. That oldest version is also reported as having the same 'issues' and was set to be disabled by Mozilla Add-ons Team unless the 'issues' were addressed." He said: "Based on that finding, those versions of your extension will be disabled in 14 days."

So he wrote: "I disabled this version myself to prevent new users from ending up with a severely outdated version of the extension to avoid a subpar first experience of uBlock Origin Lite. So essentially," he says, "it was deemed that all versions of uBlock Origin Lite were having 'issues.' But instead of disabling all of them except the most recent one, they disabled all of them except the oldest one. This is hostile, considering that whoever installed uBlock Origin Lite at that point would be installing a version of uBlock Origin Lite with severely outdated filter lists, along with an outdated codebase." He said: "Many issues were fixed in the codebase since August 2023.

"I am unable to attribute good faith to both the nonsensical review feedback and the steps taken as a result of this nonsensical review feedback, and I am unable to take on the added burden of having to deal with nonsense. This is unfortunate because despite uBlock Origin Lite being more limited than uBlock Origin, there were people who preferred the Lite approach of uBlock Origin Lite, which was designed from the ground up to be an efficient suspendable extension, thus a good match for Firefox on Android. From this point on, there will no longer be a package published in the release section for Firefox, except for the latest one, uBlock Origin Lite 2024.9.22.986, if and when it's approved."

So then Raymond apparently received some additional non-sympathetic feedback...

Leo: Oh, boy. Don't poke the bear.

Steve: Uh-huh, about his decision to completely drop uBlock Origin Lite from Firefox since he final posted on October 1st, last Tuesday, was: "Looks like the sentence 'however trivial this may look to an outsider, it's a burden I don't want to take on' is lost on many who want to have an opinion about all of this. I dropped support for uMatrix years ago because it had become a burden I could not take on. This is such a case here, where the unwarranted de-listing of uBlock Origin Lite and the requirement of having to deal with this caused the support to maintain a Firefox version to cross the line into the 'burden I cannot take on' territory. Amount of burden to take on is a personal decision, not something to be decided by others."

And just to add a bit of objectivity, since Gorhill has clearly taken a stand on this, here's a

sympathetic comment I found six days ago over on Ycombinator, where somebody completely different said: "I manage a medium-size browser extension at work. We also offered it on Firefox. But I have spent the past year struggling to get back into Mozilla store after a manual review. As far as I can tell, there are maybe two reviewers that are based in Europe (Romania?). The turnaround time is long when I am in the U.S., and it has been rife with this same kind of 'simple mistake' that takes two weeks to resolve."

He says: "You need a privacy policy." We already have one. "You are using machine-generated code and minified code." No, you are looking at the built code, not the included source. "We cannot reproduce your source." Right. That's because you didn't follow the instructions and are in the wrong directory.

Leo: Oh, boy.

Steve: He says: "Very frustrating." And there were a number of other similar comments. So it appears that Mozilla really does currently have a problem with this aspect of their bureaucracy; and that Gorhill, someone who has, shall we say, an extremely low threshold of tolerance for any sort of incompetence that's impeding him, finally just decided that it wasn't worth his time or energy to fight a frustrating battle.

Leo: He doesn't take fools lightly. And god bless him.

Steve: No, exactly.

Leo: You know what, I don't blame him. And god, I'm so grateful that he writes this and gives it away for free. It must be a significant amount of work.

Steve: Yeah.

Leo: And I don't blame him for saying it's just not worth additional effort.

Steve: No. So we have the full story. Under Chrome we get an extra six months of the use of full uBlock Origin with the addition of that little policy tweak in Windows, and something equivalent is available on Mac and Linux. Again, grc.sc/v2 will deliver the .REG file to a Windows user. Double-click on it, say yes a couple times, and you're all set up.

I'll finish today's discussion with something you mentioned, Leo, at the top, which is, you know, we've got an evolving technology in our browser add-on ecosystem. We have not talked about this large and significant question of the ethics surrounding editing received web pages to remove content, any content, that the website wishes to deliver and push on its visitors.

Leo: That's a very good point. That's a very good point.

Steve: Tracking scripts are one thing, but the more controversial removal is that which produces revenue for the site. We know that today there are many websites that wholly depend upon the revenue from advertising to survive. And we need look no further than this podcast's own hosting network TWiT to see firsthand the effects of advertising revenue becoming less available than it once was.

Leo: Right, right.

Steve: So I will finish today's discussion by quoting the author of uBlock Origin. Raymond Hill, Gorhill, says the following on his GitHub page for his original full-spectrum content blocker, uBlock Origin. He writes: "uBlock Origin is a CPU and memory-efficient wide-spectrum content blocker for Chromium and Firefox. It blocks ads, trackers, coin miners, pop-ups, annoying anti-blockers, malware sites, et cetera, by default using EasyList, EasyPrivacy, Peter Lowe's Blocklist, Online Malicious URL Blocklist, and uBO filter lists. There are many other lists available to block even more. Hosts files are also supported. uBlock Origin uses the EasyList filter syntax and extends the syntax to work with custom rules and filters. You may easily unselect any preselected filter lists if you think uBlock Origin blocks too much. For reference, Adblock Plus installs with only EasyList, Adblock Plus filters, and Acceptable Ads enabled by default.

"It is important to note that using a blocker is NOT" - he has in all caps - "theft. Do not fall for this creepy idea. The ultimate logical consequence of blocking = theft is the criminalization of the inalienable right to privacy. Ads, 'unintrusive' or not, are just the visible portion of the privacy-invading means entering your browser when you visit most sites. uBlock Origin's primary goal is to help users neutralize these privacy-invading methods in a way that welcomes those users who do not wish to use more technical means."

So we've spent a lot of time through the 19-plus years of this podcast, as this industry has evolved, looking at this issue. If advertisements were visually static and non-intrusive, if they were not planting cookies in my browser and running code in an active attempt to fingerprint me for the purpose of tracking my movements and compiling a list of everywhere I go and everything I do, and if the websites hosting these obnoxious privacy invasions were not actively complicit in this, then I would feel far more sympathetic to the need for websites to generate revenue by forcibly exposing me to things I do not want.

Leo: And we should point out that there are many websites, Jason Snell's website is a good example, that have first-party ads that are plaintext, that are not blocked by uBlock Origin or any other adblocker.

Steve: Yup.

Leo: They can't because they're first party. It's part of the content.

Steve: Right.

Leo: And so it is possible to have advertising that goes right through any adblocker because it's not invasive. It doesn't invade your privacy.

Steve: Right. And, you know, I do not believe that where we are today in the year 2024 is where we'll be 10 years from now. If nothing else, we can see how the industry and government are struggling to come to an agreement and compromise. I was disappointed that European regulators forced Google to abandon its significantly privacy-enforcing Privacy Sandbox technology. The fact that they were forced to give it up because it would have been so privacy-enforcing tells you all you need to know about the state of today's web technology.

Leo: We talked about that on MacBreak weekly today, that you can't assume governments are going to always act in your favor and in favor of protecting your privacy. In fact, they may be acting in favor of advertisers' right to invade your privacy, as in this case. Yeah.

Steve: Yes. And we know content control add-ons do not completely prevent tracking and profiling, but they do mitigate it. And they do make the use of the web significantly more pleasant. One thing seems clear: If individual end users - the consumers of the ads and the targets of this tracking - do not push back within their means against this abuse of our attention and privacy, it's likely to take much longer for it to change. So we're voting by saying no thank you, you know, fix your technology, and we won't have a problem.

Leo: Cory Doctorow has called the widespread use of adblockers the largest consumer boycott in history. Almost 50% of people who use the Internet now use adblocking technology. And that's a pretty strong vote against. Now, some people don't like ads, period. I mean, there are really people who will just say, I'm not going to listen to an ad. I'm not going to look at an ad. I will block every ad. I don't care what your monetization strategy is. And so I think there is a percentage of people who just don't like ads.

Steve: Well, and websites have the option of sensing that somebody is refusing to look at ads and then refusing to show them content.

Leo: Yeah, that's true. Don't adblockers trying to get around that stuff? No?

Steve: Yeah. Again, you know, the controversial thing is that we're editing what our browser is doing.

Leo: Yeah, right.

Steve: And you argue, hey, why do I not have the right to do that?

Leo: Yeah, I mean, it is...

Steve: To decide what I want my browser to do on my computer.

Leo: Yeah. It's your screen, your computer.

Steve: Yup.

Leo: This is a tough, this is a really difficult one. And I do have to point out that a lot of websites have gone out of business this year, including AnandTech, iMore, because there was no way to get around this consumer boycott. There's no way to make a living. We're faced with that, as well. I understand people don't like ads. I don't know what the answer is to this. Our ads are not - they may be intrusive. I don't think they're non-intrusive, but they do not spy on you, and they're not malware in any form. They're just audio. A lot of people fast-forward through them. There's no real way to block them, but they might fast-forward through them. I don't know what the answer is, Steve. I really don't. This is a tough one because we want journalism; right?

Steve: And part of the problem is, I mean, ads really are obnoxious. They have discovered that if you turn the volume up, then your dollar amount goes up. So the moment you see that, everyone's going to turn the volume up. And then they're competing with each other to see who has the most volume.

Leo: It's a vicious circle.

Steve: And a lot of them are really obnoxious.

Leo: I agree.

Steve: I can't watch television without being able to fast-forward past the ads.

Leo: But Steve, do you want everything to have a paywall? Because that's the option.

Steve: That's a problem, too.

Leo: I mean, that's really the option is that you can't read it unless you pay for it.

Steve: So I would have no problem paying for something that I use routinely. That is, you know, for example, the Washington Post, The New York Times, some site. But I'm not a person who is consuming a great deal of focused online content. I'm not reading The New York Times or the Washington Post or any online content in a go back and, like, to it constantly. I'm annoyed that my iPhone keeps offering me news that I can't read because when I click on it I have to be Apple Plus or Apple News Plus. It's like, don't show this to me if I can't read it.

Leo: So there's the large issue. You live in a small town. I live in a small town. The New York Times and the Washington Post are not going to cover our city council meetings or school board meetings, the initiatives we're voting on in a couple of weeks because it's not national news. And yet we don't have local newspapers anymore because there's no money, there's no support, no financial support.

Steve: Yeah.

Leo: So that means we've got an electorate that is fundamentally, unless they really go out and look, ill-informed on the issues of the day. That's a problem, too. So this is a very thorny issue. I am very - I do want to be clear, though. I am grateful to Raymond Hill for uBlock

Origin. I use it on every darn computer. I'm not happy that Google is making it useless on Chrome. I hope that Firefox continues to support it. And I understand that there is definitely a contradiction in my use of an adblocker and my making my living through an ad-supported network. I don't know what the answer is.

Jump To Top