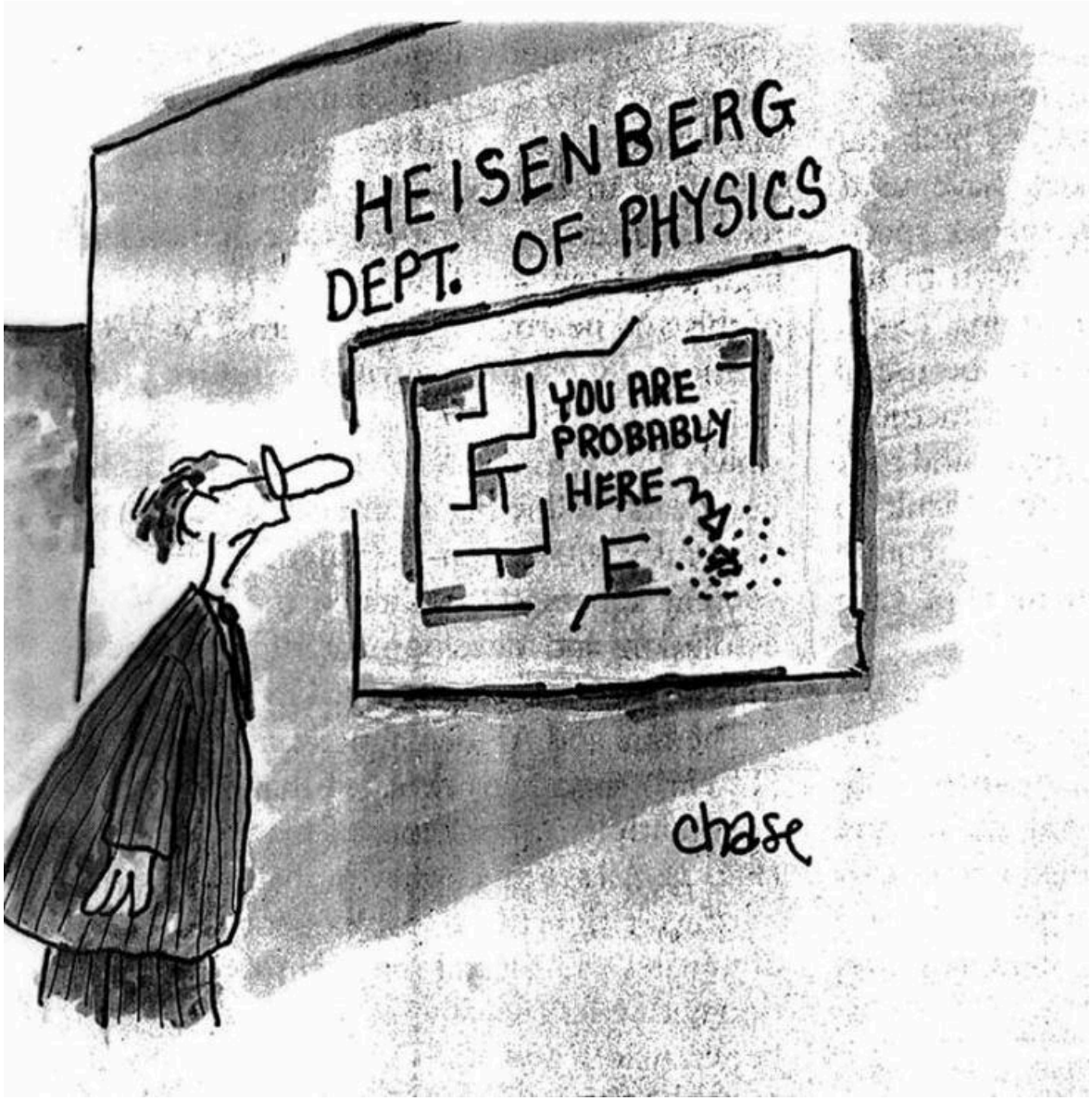
Security Now! #1035 - 07-22-25

Cloudflare's 1.1.1.1 Outage

This week on Security Now!

• Bypassing all passkey protections. • The ransomware attacks just keep on coming. • Cloudflare capitulates to the MPA and starts blocking. • The need for online age verification is exploding. • Microsoft really wants Exchange Servers to subscribe. • Russia (further) clamps down on Internet usage. • The global trend toward more Internet restrictions. • China can inspect locked Android phones. Use a burner. • Web shells are the new buffer overflow. An age verification protocol sketch. • What Cloudflare did to create an outage of 1.1.1.1.

"Uncertainty" is the nature of the Universe



Security News

Passkey Bypass in the Wild

The security guys with Expel Security have uncovered a passkey bypass using an adversary in the middle attack. The vulnerability of Passkeys to this attack is well known. It was a consession that needed to be made for the sake of cross-device login. The Expel Security guys have just three bullet points at the top of their blog's TL;DR:

- *Bad actors have figured out how to downgrade FIDO key authentication when compromising accounts.*
- *This technique is being leveraged in phishing attacks.*
- *The attack involves tricking a user into scanning a QR code with an MFA authenticator.*

Their blog posting is titled: *"PoisonSeed: downgrading FIDO key authentications to 'fetch' user accounts"* and they explain:

> *Our SOC (Security Operations Center) has recently spotted a novel attack technique that involves socially engineering a target to get around the security protections provided by FIDO passkeys. The attacker does this by taking advantage of cross-device sign-in features available with FIDO passkeys. These features are designed to help users sign into their accounts on systems without a passkey by using an additional registered device, like a mobile phone. However, the bad actors in this case are using this feature in adversary-in-the-middle (AitM) attacks.*
>
> *This is a concerning development, given that FIDO passkeys are often regarded as one of the pinnacles of secure multifactor authentication (MFA). And while we haven't uncovered a vulnerability in FIDO keys, IT and SecOps folks will want to sit up and take notice—this attack demonstrates how a bad actor could run an end-route around an installed FIDO key.*
>
> *We have reason to believe that this attack was carried out by PoisonSeed, an attack group known for large-scale phishing campaigns designed to steal cryptocurrency from their target's wallets. However, the technique described here could easily be leveraged in other attacks.*

And now they take us step-by-step through the details of the attack, writing:

> *The attack started with a phishing email sent to several employees at the company. The email lured these users to log into a fake sign-in page hosted at okta[.]login-request[.]com.*
>
> *This page mimicked the general look and feel of the company's normal authentication process, including an Okta logo and sign-in fields for username and password. However, not only is the domain hosting this fake login page suspicious, the domain itself had only been created a week before the attack.*

It's interesting that they provide that bit of detail. We've recently noted that the registration age of any domain a user is visiting should **always** be a massive red flag. At the very least, any visit to a "freshly minted" domain ought to be brought to the user's attention as an additional sanity check. Our web browsers, an add-on, or perhaps even highly security-conscious DNS resolvers, really should be checking the age of any domain names being resolved before they are visited. Or perhaps the page could be displayed and the user could begin filling-out any forms while the reputation is checked in the background and the form's "Submit" function would only be unlocked once a domain reputation, including the domain's age, passed scrutiny.

A user could, of course, bypass such a block, but only by forcing the browser to proceed. They wrote:

Both this domain, and the aws-us3-manageprod[.]com domain the user is redirected to if they enter their credentials, are hosted by Cloudflare. Leveraging reputable services like Cloudflare can make phishing scams appear more trustworthy, potentially lulling visitors into a false sense of security.

The targeted user in this case had a FIDO key registered to secure their account. Normally, the user would be required to physically interact with the FIDO key—touching it, for example, to confirm they're the ones logging in and are on the registered device or using a Passkeys app.

If a user whose account is protected by a FIDO key enters their username and password into the phishing page, their credentials will be stolen—just as with any other user. But with a FIDO key protecting their account, the attackers are unable to physically interact with the second form of authentication.

This is where things took a turn from your traditional phishing site. After entering their username and password on the phishing site, the user was presented with a QR code.

What happened behind the scenes is the phishing site automatically sent the stolen username and password to the legitimate login portal of the organization, along with a request to utilize the cross-device sign-in feature of FIDO keys. The login portal then displayed a QR code.

Under normal circumstances, when a user wants to sign in to their account from a different, unregistered device, they can still verify their identity if they've enrolled another authentication device. In most cases, this would be an MFA authentication app installed on a mobile device, most of which include a QR code scanner. The login portal displays a QR code after it receives the correct username and password, which the user scans with their MFA authenticator. The login portal and the MFA authenticator communicate to verify the login, and the user is granted access.

In the case of this attack, the bad actors have entered the correct username and password and requested cross-device sign-in. The login portal displays a QR code, which the phishing site immediately captures and relays back to the user on the fake site. The user scans it with their MFA authenticator, the login portal and the MFA authenticator communicate, and the attackers are in.

This process—while seemingly complicated—effectively neutralizes any protections that a FIDO key grants, and gives the attackers access to the compromised user's account, including access to any applications, sensitive documents, and tools such access provides.

As I noted, this attack is not novel. It's an acknowledged weakness of any cross-device authentication. SQRL had this weakness, too. I went to extreme lengths to eliminate this possibility from any same-device authentication. If you used SQRL's on-device app, any possible man-in-the-middle was excluded because the user's browser connected to the local SQRL client which performed the authentication. It then received the logged-in URL which it forwarded to the user's browser. No man-in-the-middle was ever able to obtain it. But this protection depends upon a link between the user's browser and the authenticator. And that's not available for cross-device authentication.

I wanted to share this with everyone so that this danger would be very clear. Passkeys are a huge step forward and they can prevent many other forms of abuse – if not all. But a determined attacker-in-the-middle that's able to engineer a spoofed phishing attack and convince a user to enter their valid username and password into a site, then intercept and forward their QR code for a cross-device passkey authentication can still get themselves authenticated even with passkey- protected authentication.

The Attacks Continue

For fear of allowing one of the biggest problems the cyber-community still faces: Ransomware attacks, I wanted to quickly note a couple of recent biggies:

South Korea's largest insurance company, Seoul Guarantee Insurance, got hit by ransomware last Monday. The incident has severely disrupted the company's operations and the company has been issuing handwritten loan guarantees to customers all week as it works to restore affected systems. This is the third major South Korean company to experience severe business disruptions this year due to a cyberattack. The country's largest telecom and its largest online bookstore suffered similar disruptions.

Also, the grocery distributor United Natural Foods expects to lose up to $400 million in sales this year following a ransomware attack last month which took multiple systems offline for days. That downtime affected its ability to fulfill and distribute customer orders.

Meanwhile, Australian airline Qantas obtained an injunction to prevent individuals and organizations from using or publishing data stolen in a recent ransomware attack. That's a new one. Since when do some foreign bad actors care about an Australian court order? The injunction suggests that the company is not willing to pay the ransom and is expecting the hackers to leak the data. But it's difficult to see what they expect to gain.

So it's business as usual in the cyber attack and ransomware world. And as we've noted before, there's not even any sign that we're making progress and improving our effective security.

"Error 451 - Unavailable for Legal Reasons"

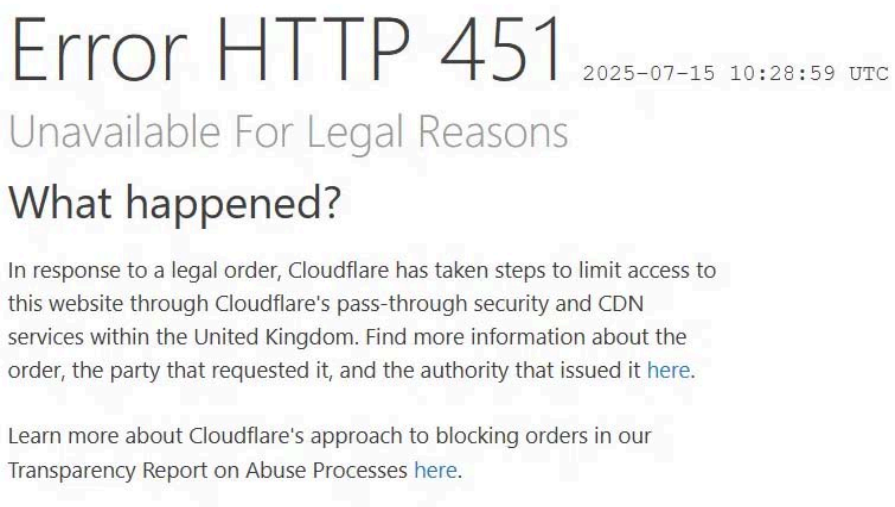
In what is being called a significant turn of events, Cloudflare appears to have changed their long-standing policy of total net neutrality within the UK. The TorrentFreak site, which covers these sorts of Net Neutrality-related events, writes:

Cloudflare has become the first internet intermediary beyond local residential ISPs, to block access to pirate sites in the UK. Users attempting to access certain pirate sites are greeted with [Cloudflare's] 'Error 451 - Unavailable for Legal Reasons'. In theory, ISP blocking should prevent UK users from even seeing this notice, but a combination of Cloudflare's blocking mechanism and choices made by some VPN users results in a piracy dead end.

To clarify, what they mean when they write *"ISP blocking should prevent UK users from even seeing this notice"* is that since the ISP is the entity who connects UK users to the Internet, ISP blocking would prevent users from ever connecting to a pirate website. The article continues:

Internet service providers BT, Virgin Media, Sky, TalkTalk, EE, and Plusnet account for the majority of the UK's residential internet market and as a result, blocking injunctions previously obtained at the High Court often list these companies as respondents. These so-called "no fault' injunctions stopped being adversarial a long time ago; ISPs indicate in advance they won't contest a blocking order against various pirate sites, and typically that's good enough for the Court to issue an order with which they subsequently comply.

For more than 15 years, this has led to blocking being carried out as close to users as possible, with ISPs' individual blocking measures doing the heavy lifting. A new wave of blocking targeting around 200 pirate site domains came into force Monday the 14th, but with the unexpected involvement of a significant new player. In the latest wave of blocking that came into force yesterday, close to 200 pirate domains requested by the Motion Picture Association were added to what was already one of the longest pirate site blocking lists in the world. The big change, is the unexpected involvement of Cloudflare, which for some users attempting to access the domains added yesterday, displays the following notice:



When we've previously covered this issue, and applauded Clourflare's adamant pro-net neutrality stance, we've cited Cloudflare's formal policy statement about this, which says:

Because Cloudflare cannot remove content it does not host, other service providers are better positioned to address these issues. Among other things, any blocking by Cloudflare is of limited effectiveness, as a website will be accessible if it stops using Cloudflare's network. Cloudflare therefore regularly pushes back against attempts to seek blocking orders.

So Cloudflare is saying *"don't ask us to take responsibility for the content we're hosting because there are many other hosting providers."* TorrentFreak explains:

> *Cloudflare notes that it may take steps to comply with valid orders if, among other things, "principles relating to proportionality, due process, and transparency" are upheld. Whether Cloudflare pushed back here isn't clear, but the information made available falls well short of that promised in the Error 451 notice.*
>
> *With no central repository of blocking orders and no legal requirement to share details of injunctions with the public, transparency in the UK is mostly left to chance. Some orders make their way online, but there is no guarantee. For those interested in finding out more about the order affecting Cloudflare, the company provides a link which promises to reveal "the party that requested it, and the authority that issued it." The link directs to the Lumen Database, which publishes information effectively donated by companies such as Google and Cloudflare, for the purpose of improving transparency.*
>
> *But in this case, there's no indication of who requested the blocking order, or the authority that issued it. However, from experience we know that the request was made by the studios of the Motion Picture Association and for the same reason the High Court in London was the issuing authority. To the general public, the information is just a short list of domains. If it wasn't for the efforts of Lumen, Google and Cloudflare, the situation would be significantly less clear than that.*

So TorrentFreak is noting and complaining that there's a real problem with a lack of transparency and accountability. They add:

> *The issue lies with dynamic injunctions; while a list of domains will appear in the original order (which may or may not be made available), when the MPA concludes that other domains that appear subsequently are linked to the same order, those can be blocked too, but the details are only rarely made public. From information obtained independently, one candidate is an original order obtained in December 2022 which requested blocking of domains with well known pirate brands including 123movies, fmovies, soap2day, hurawatch, sflix, and onionplay.*
>
> *What's also odd is that the notice linked **from** Cloudflare doesn't directly concern Cloudflare. The studios sent the notice to Google after Google agreed to voluntarily remove those domains from its search indexes, if it was provided with a copy of relevant court orders. Notices like these were supplied and the domains were deindexed, and the practice has continued ever since. That raises questions about the nature of Cloudflare's involvement here and why it links to the order sent to Google; notices sent to Cloudflare are usually submitted to Lumen by Cloudflare itself. That doesn't appear to be the case here.*

And as for VPN circumvention, TorrentFreak wrote: *"When blocking measures are required, Cloudflare digs in when requests concern its public DNS resolver (1.1.1.1). To achieve a similar effect, Cloudflare uses another technique instead."* So I assume they mean that Cloudflare still absolutely refuses to muck up their public DNS resolvers with filters. And thank God for that! We need a strong universal DNS resolver that's not subject to the whims and needs of any particular industry or government. So I'm very glad to know that they're not caving there. So what's the other technique Cloudflare uses instead?

TorrentFreak quotes Cloudflare: *"In countries with laws that provide for blocking access to online content, Cloudflare may geoblock websites to limit access in the relevant jurisdiction to those websites through Cloudflare's pass-through security and CDN services."* So in other words, Cloudflare will not filter DNS, but they will, when required by law (typically taking the form of court orders) filter access to the site they host based upon the location of the client.

TorrentFreak wrote: *"Cloudflare appears to be using geo-blocking in the UK, as some VPN users will soon find out. In normal circumstances, a VPN using a server in the UK will bypass ISP blocking no differently than a server located anywhere else in the world. Users attempting to gain access to domains currently blocked by Cloudflare, using a VPN server in the UK, will be greeted by Cloudflare's Error 451 blocking notice instead."* So what they're saying there is that whereas in the past a VPN may have been useful in jumping past a local ISP's block, and it didn't much matter where the VPN was terminated by its server, now that Cloudflare is implementing UK-wide geoblocking of their content, above and beyond what ISPs may also be doing, any UK-based VPN users will need to terminate their VPNs at servers outside the UK, which would not have been necessary when blocking was ISP-only.

The TorrentFreak site concluded by noting that the scale of this blocking appears to be large. They wrote:

> *Checking through the new domains blocked on the 14th, something else becomes apparent; they appear in multiple blocking orders, not just the one highlighted above. We're unable to check all 200 domains, but at least potentially, hundreds or even thousands of domains could be involved. And that may actually be a very good thing.*
>
> *Domains blocked by Sky, BPI and others, don't appear to be affected, at least as far as we can determine. All relate to sites targeted by the MPA, and the majority if not all trigger malware warnings of a very serious kind, either immediately upon visiting the sites, or shortly after. At least in the short term, if Cloudflare is blocking a domain in the UK, moving on is strongly advised.*

So I believe they're saying that the blocking Cloudflare has begun doing appears to relate to domains hosting malware, perhaps more than just those the MPA may be grumbling about. Whatever the case, it appears that Cloudflare is simply abiding by the law, though the evidence that even Cloudflare themselves link to doesn't directly explain exactly what's going on.

More age-related messes

The heat surrounding Internet user age continues to increase. I'm encountering an increasing level of pressure in the news I survey.

For example, last Thursday ROBLOX posted an update which included this under the headline "Age Estimation":

> *Roblox is investing an age estimation technology to help deliver tailored and developmentally appropriate experiences, while aiming to protect its community from those who might seek to do harm. To add contacts as a "Trusted Connection", users must be 13 and over and confirm*

their age using a video selfie, which is analyzed against a large, diverse dataset to estimate their age. Matt Kaufman, Roblox Chief Safety Officer said: "We know teens want more freedom to chat more freely with their friends. We believe that unfiltered chat should only be made available to users who have been age checked, which is why we're using new Age Estimation tools to unlock access to Trusted Connections for those 13 and over. We believe this additional freedom to chat more openly will reduce the incentive for teens to move interactions off platform, where they may be exposed to greater risk."

And Steam reports that they are being pressured over some of their content by the payment processors they use. In response, rather than risk losing their payment flow, Steam has reportedly removed thousands of games containing adult content, though what that is remains unclear. Last Friday, Eurogamer asked Valve for some clarification and wrote this:

In response to questions from Eurogamer regarding Steam's new guidelines preventing "certain types of adult content" from being distributed on the platform, Valve has provided some general background on the events leading to the decision.

A Valve spokesperson told Eurogamer: "We were recently notified that certain games on Steam may violate the rules and standards set forth by our payment processors and their related card networks and banks. As a result, we are retiring those games from being sold on the Steam Store, because loss of payment methods would prevent customers from being able to purchase other titles and game content on Steam."

So, in this case, thousands of titles are being removed – without regard for the age of the user – in what appears to be a case of blackmail censorship by Valve's payment providers.

I'm sure it must be clear to everyone by now that the need to verify the age of Internet users is not off someday in the future. It is right now, today. Yet the industry doesn't appear to be doing much of anything about it. We need the W3C or the IETF, or perhaps the FIDO Alliance – if any of them could move at anything above glacial speed – to whip up some standards.

Then, we need Apple and Google to implement them in their biometrically equipped devices. And someone like a next-generation Yubico needs to create a cute, inexpensive little spoof-resistant thumbprint authenticator that follows that specification (that doesn't yet exist). And we need all that yesterday, please.

Imagine that a Yubico-type thumbprint sensor/age-verifier existed. If you have a biometrically locked smartphone you don't need one. But high-end smartphones are expensive, so we need a $20 alternative. So if you don't have a suitably-equipped smartphone you purchase an inexpensive gizmo from Amazon or from your neighborhood electronics retailer.

So how do we arrange to create the binding between the user's biometric and an assertion of their age, and to do this at scale? Someone who wishes to enroll their iPhone, biometric Android device or inexpensive thumb-verifier, takes their chosen device to any U.S. post office, DMV, AAA or any notary like at any UPS store. You show them your government-issued ID proving your age. They check it carefully for forgery, etc., then have the user authenticate with their chosen biometric – their face or thumbprint – to their device, after which the agent uses their own

device, any NFC-equipped phone or terminal, to bless, activate and lock that biometric/age binding. Now this individual is in possession of a biometrically-locked assertion of their age which they can use, on demand, anywhere in cyberspace it's needed.

A bit later in today's podcast, in answer to a listener's question, I'm going to sketch out an example cryptographic protocol to provide some sense for some more of the details. But my overall point is that this problem is not intractable. But someone needs to get moving on it and there's no sign that's happening. Even though Yubico's co-founder Stina Ehrensvärd has moved onto other passions, I dropped her a note as I was writing this. She would be the perfect person to shake things up and to use her connections to get this moving.

In other news: Exchange gets 6 months of ESUs

It appears that Microsoft remains unsure what to do about the fact that no one wants their new crap – especially in light of the fact that Exchange Server is switching to a subscription. Wow. So it shouldn't be too surprising that no one is in any big hurry to switch to subscription mode. Everyone just wants to keep using the crap they already have that's working just as well as any of the new crap probably would – especially when they already paid for the crap they have that's all installed and working just fine. So we're talking about the Exchange 2016 and 2019 servers, whose End Of Life is scheduled for that same fateful day in October – the 14th – when Windows 10 and other Microsoft products no one wants to be forced to stop using were originally scheduled to stop receiving security updates.

But because users of Exchange Server are not rando consumers, anyone who has, so far, refused to jump at the opportunity to switch to the marvelous new pay-as-you-go subscription plan, is going to need to pay up. And Microsoft says, that's it. We're serious this time. No, really, we're not kidding. This is the last time. Seriously. They actually wrote: "Don't even bother asking for more." Wow. Last Tuesday's Exchange Team Blog posting headline was: *"Announcing Exchange 2016 / 2019 Extended Security Update program"*. They wrote:

> *With both Exchange 2016 and 2019 going out of support in October 2025, we've heard from some of our customers that they have started their migrations to Exchange Subscription Edition (SE) but might need a few extra months of Security Updates (SU) for their Exchange 2016 / 2019 servers while they are finalizing their migrations.*
>
> *We are announcing that we now have a solution for such customers. Starting on August 1st, 2025, customers can contact their Microsoft account team to get information about and purchase an additional 6-month Extended Security Update (ESU) for their Exchange 2016 / 2019 servers. Your account teams will have information related to per server cost and additional details on how to purchase and receive ESUs, starting August 1st, 2025.*

Logic suggests that the "stay right where I am for the next 6 months" plan will cost more than the "that subscription sounds great!" plan. And no one ever accused Microsoft of leaving any money on the table. So it will almost certainly cost those foot draggers more than getting with the new plan. Microsoft's posting continued:

> *What does this mean?*

- *This ESU is not an "extension of the support lifecycle" (Microsoft Lifecycle Policy | Microsoft Learn) for Exchange 2016 / 2019. Those servers still go out-of-support on October 14, 2025, and you will not be able to open support cases for them (unless directly related to an issue with a SU released to ESU customers during the ESU period).*

- *This ESU is a way for customers who might not be able to finalize their migrations to Exchange SE before October 14, 2025, to receive Critical and Important updates (as currently defined by Microsoft Security Response Center (MSRC) scoring) as SUs that we might release after October 2025. If there are SUs that we need to release, we will privately provide such SUs to ESU customers. Exchange 2016 / 2019 SUs will not be released on public Download Center or Windows Update after October 2025.*

- *We are not committing to actually releasing any SUs during the ESU period. Exchange Server does not necessarily receive SU updates every month on Patch Tuesday (2nd Tuesday of the month) as SUs are released only if there are Critical or Important security product changes. Therefore, if there are no SUs that we need to release during the time of ESU, there will be no such updates provided. We will, however, confirm with ESU participants each Patch Tuesday whether an SU was provided or not.*

- *This ESU will be valid for 6 months only (through April 14, 2026). This period will not be extended past April 2026 (you do not need to ask).*

Who is Exchange 2016 / 2019 ESU for?

This program is intended only for customers who are unable to finalize their migrations to Exchange SE before end of support lifecycle for Exchange 2016 / 2019, already use Exchange 2016 CU23 or Exchange 2019 CU14/CU15, and still need Critical and Important security coverage for the older servers still in operation.

- *We recommend that customers do not rely on this ESU, but instead upgrade their organizations to Exchange SE in time.*

- *Customers using Exchange 2019 should in-place upgrade to Exchange SE quickly and switch to the Exchange SE modern lifecycle policy.*

Ahhhhhh, yes! The "modern lifecycle policy" – also known as the "we'll no longer allow you to purchase it. In these modern times you now keep paying for it forever."

For what it's worth, the wonderful and clever folks over at 0patch **do** provide patches for Exchange Server. So it might be more cost effective to consider remaining with the already paid for Exchange Server you already own and having the 0patch folks keep it up to date for you until the April 14th sure and final drop-dead date for patches arrives in 2026.

Perform an Internet search in Russia, pay a fine.

Yikes! A new Russian law has criminalized online searches for controversial content. Russia previously criminalized the sharing of such content, but with officials saying censorship during wartime is justified, restrictive digital laws are being tightened. The Washington Post reported last Thursday:

Russian lawmakers passed controversial legislation Thursday that would dramatically expand the government's ability to punish internet users — not for sharing forbidden content but for simply looking it up. The new measures, which sailed through the Russian parliament and will take effect in September, envision fining people who "deliberately searched for knowingly extremist materials" and gained access to them through means such as virtual private networks, or VPNs, which let users bypass government blocks. VPNs are already widely used in Russia to circumvent the many blocks on websites.

Russia defines "extremist materials" as content officially added by a court to a government-maintained registry, a running list of about 5,500 entries, or content produced by "extremist organizations" ranging from "the LGBT movement" to al-Qaeda. The new law also covers materials that promote alleged Nazi ideology or incite extremist actions. Until now, Russian law stopped short of punishing individuals for seeking information online; only creating or sharing such content was prohibited. The new amendments follow remarks by high-ranking officials that censorship is justified in wartime. Adoption of the measures would mark a significant tightening of Russia's already restrictive digital laws.

Similar legislation passed recently in neighboring Belarus, Russia's close ally ruled by authoritarian leader Alexander Lukashenko, and has been used to justify prosecution of government critics. The fine for searching for banned content in Russia would be about a $65, while the penalty for advertising circumvention tools such as VPN services would be steeper — $2,500 for individuals and up to $12,800 for companies.

Sarkis Darbinyan, an internet freedom activist whom the Russian authorities have labeled a foreign agent said: "The fines imposed for searching for extremist materials in this iteration may be minor, but this can be grounds for detention, pressure, a pretext to be escorted to the police station. I am most afraid that in the next iteration, administrative fines will turn into criminal cases."

Previously, the most significant expansion of Russia's restrictions on internet use and freedom of speech occurred shortly after the February 2022 full-scale invasion of Ukraine, when sweeping laws criminalized the spread of "fake news" and "discrediting" the Russian military.

The new amendment was introduced Tuesday, attached to a mundane bill on regulating freight companies, according to documents published by Russia's lower house of parliament, the State Duma. Net Freedoms, an advocacy group, said in a statement: "Lawmakers have repeatedly used this 'cunning' tactic of quietly inserting repressive measures into dormant, previously introduced bills. It allows them to accelerate the legislative process — moving through the second and third readings in a single day — and to avoid public scrutiny."

On Wednesday, as news of the censorship amendments sparked widespread concern in Russian media, lawmakers pushing the bill sought to downplay fears that citizens would be penalized for browsing the web. Sen. Artem Sheikin, one of the bill's authors, told state-controlled news agencies that the new measures are not intended to punish individuals for accessing prohibited websites using VPNs. Reading Facebook or scrolling through Instagram, Sheikin said: "does not constitute an administrative offense. The main focus is on regulating providers. … There is no plan for mass punishment of users." He claimed that liability would only attach in cases of knowingly searching for and accessing content officially designated as extremist by a court and added to a Ministry of Justice blacklist. However, Sheikin did not explain how authorities would determine whether an individual knew the accessed content was deemed extremist.

Russian internet activists have warned that the vague language of the amendments creates significant potential for misuse. It also remains unclear how regulators intend to monitor search queries or enforce the new rules. Net Freedoms said that telecom operators and Russian platforms such as VK, which are already obligated to store and share user data with law enforcement, could be asked to turn over such information.

User search activity can also be exposed through unprotected public WiFi networks, search engine histories or data stored on devices, such as browser logs and autofill entries.

The proposal drew ire even from some Kremlin loyalists who called the amendments an overreach. The daughter of a Russian senator and head of the League of Safe Internet, a group known for denouncing anyone criticizing the government, said the legal changes would prevent her organization from doing its work as her group would technically be breaking the rules by opening the flagged content. She wrote in a Telegram posting: "It turns out that under the new law, the League for Safe Internet will not be able to transfer data on extremist communities to the Ministry of Internal Affairs. They will ban us from monitoring extremism."

In recent years, the Russian government has intensified its crackdown on digital freedoms by targeting VPN usage and other tools that allow citizens to bypass state censorship. A law passed in early 2024 criminalized the promotion of such technologies, making it illegal to share information about these services or to post guidelines on how to bypass restrictions.

Authorities have since sent hundreds of takedown requests to app stores, pressuring Western tech giants such as Google and Apple to remove VPN apps. According to the GreatFire research project, Apple removed about 60 applications following the restrictions, but Google complied with only six out of 212 removal requests.

Russia has also expanded its use of deep packet inspection (DPI) technologies, enabling more precise blocking of traffic, and committed millions of dollars to fortify its "sovereign internet" infrastructure, aiming for extensive control over online activity.

Telecom providers have been ordered to log detailed user data, while citizens are being pressured to use domestic platforms instead of foreign ones by throttling or restricting platforms such as YouTube, X and Instagram as the Russian government seeks to limit access to independent information and dissenting voices.

The use of the term "throttling" reminded me that we just recently talked about how Cloudflare was being "throttled" by limiting any request to Cloudflare to 16K bytes.

This news is disturbing because Russia is an extreme example of a general tendency we're seeing globally from the world's governments. The UK and the EU are chafing over encryption and arguing against fundamental privacy rights. Here in the U.S., the Supreme Court has approved the means various extreme special interest groups will be using to criminalize any Internet speech they dislike or deem to be unwholesome.

It feels as though for the first 50 years of the Internet, it was not understood and thus remained somehow out of bounds for the world's governments and politicians. Or perhaps it just didn't matter all that much until the past decade or so. We enthusiasts were having a great time playing in our sandboxes with our technologies. But now the adults have returned and they're scowling at the things we've been up to.

Take a burner phone to China
You may want to pick up a temporary "burner" Android phone when traveling into China. Chinese authorities are using a new forensics toolkit to extract data from Android phones. The new tool, named "Massistant" is being used at border checkpoints and by local police forces. It can extract geolocation data, images, SMS messages, contacts, and data from third-party messaging apps. According to the mobile security firm Lookout, Massistant appears to be the successor of a previous tool used by authorities named MFSocket.

I'll also note that anyone switching to the use of a burner phone should begin using it some days before their trip so that it can accrue some believable history. There have been instances of people being further harassed when their use of a burner was made obvious by its very lack of any extracted historical data.

Fortinet in the Doghouse
After encountering the following bit of news, it occurred to me that perhaps remote web management access of any kind, regardless of how well authenticated its designers and deployers probably believe it to be, really has risen to the status of the buffer overflow or overrun. It's tops recurring, ubiquitous and really dumb thing to do.

So the news is that security researchers with the Shadowserver Foundation have found webshells on almost 80 Fortinet FortiWeb firewalls. The Shadowserver Foundation believes the webshells were installed after hackers exploited a recently patched vulnerability (CVE-2025-25257). The bug – here it comes again – is a pre-auth SQL injection in the firewall's web panel. Fortinet has not yet confirmed in-the-wild exploitation. Apparently they're the last to know, since 80 individual instances of a Fortinet FortiWeb firewall compromise ought to be pretty easy to confirm. Sounds a bit like they might not be in any big hurry to confirm it officially.

Sci-Fi

Hail Mary
Last night, I finished my very pleasurable re-read of Andy Weir's Project Hail Mary novel. I have absolutely no idea how anyone could possibly turn this into a hyper-condensed two-hour movie that's in any sense faithful to the book. I wouldn't want to be that screenwriter or director. We'll find out next March 20th. I don't doubt that people who have never read the book will love the movie. But the book was really terrific and whatever the movie will be, I can't see how it could possibly be anything but a rough outline of the events in the book.

I immediately purchased Andy's second novel, "Artemis" and it's loaded into five Kindles – one Kindle device, one iPhone and three iPads – that I move among from day to day. So I'm going to plow into Artemis and I'll let everyone know what I think of Andy's second book.

Listener Feedback

Bob VanMeeteren

Hi Steve, Just wanted to write that a SpinRite Level 3 refresh of my 2017 kindle fixed my issue. Thank you for this amazing product. Also I am a loyal Security Now listener since 2019 and grew up with a Speak and Spell so thanks for that too!

We can infer from Bob's note that he has an eight year old Amazon Kindle that developed some sort of problem. During the three and a half year SpinRite v6.1 development we learned much more than we knew there was to learn about the surprising age-related decline in the performance and reliability (which are closely related) of solid state storage. We also learned that SpinRite's ability to recover data that's become marginal, coupled with its re-writing of solid state data, more often than not completely reverses this decline and rejuvenates storage.

As an avid Kindle owner who often exports books from the device for archiving, I'm well aware that connecting a Kindle to a PC allows the PC to view the Kindle as a solid state drive. And that's all SpinRite needs to be able to work its magic on any device such as a Kindle.

We sometimes hear from people asking whether SpinRite is able to similarly repair and restore Android smartphones and other devices. We tell such people that if their device allows itself to be placed into a mode where its storage is visible to a PC then the chances are very good that, as Bob found with his well-used Kindle, SpinRite can restore the device's proper operation and performance.

Alan Hague

Hi Steve, Love the podcast (for decades now) and Spinrite. The new version really helps with my TiVo drive, which is large.

In a recent Security Now you mentioned that you no longer worry about AI since it has no intent. Like the "I want a lollipop" scenario. But it seems to me that if AI has ingested ALL Sci-Fi books, then it has many ideas of what a human might do when threatened. Could AI simply respond to a stimulus by using what its "learning" shows could be a proper response? Couldn't it therefore replicate itself, disable electronic controls, or worse, without intent? Thanks for all you do for us all! Alan Hague / Indianapolis

Alan's note reminded me of my TiVos, which I still miss to this day. That company got so much right. While we have vastly more options today than we once did, it was once so nice having everything gathered in one place. Today, it's necessary to go hunting around for shows among so many separate services. But in any event, it's very cool that SpinRite is still useful in keeping Alan's TiVo alive. And as he says, TiVo's drive being large means that before SpinRite v6.1, a full drive recover and refresh cycle could have taken quite a while, during which there would be no media recording or playback. So, v6.1 being so much faster means much less downtime.

As for AI's possible negative reactions, I am 100% happy having settled upon the statement that mankind has not yet created an artificial intelligence. What we've been working toward, for the past 100 years, amounts to increasingly good ***simulated intelligence***. I like this definition because it delineates true "intelligence" in exactly the right way, and I believe that it helps us to disentangle ourselves from our struggle to understand exactly what it is that we have most recently created.

We clever monkeys have managed to create an extremely convincing and compelling simulation of true human intelligence. But no matter how good that simulation may be, it's fundamentally different from the actual human intelligence that created it. A recording of an opera singer can be indistinguishable from the original singer, but the recording is not the opera singer. A simulation is not the real thing.

So, to your point, Alan, if an AI trained on Sci-Fi (as they all will have been if they've been trained on Internet-accessible material) were to be prompted with language that's threatening, and if was not otherwise restrained from answering without filtering, it would be likely to respond according to its training, which might be as we would expect a truly intelligent machine to respond. But that would only be because what we have today are extremely high-fidelity simulations of truly intelligent machines.

40 years ago, Edsger Dijkstra, the quite famous Dutch computer scientist and professor who's considered to be the father of "structured computer programming" wrote an essay about the similar claims being made of intelligent machines during **his** time (40 years ago) and before. One of the things he wrote in his takedown was so pithy that it stuck with me. He wrote that the question of whether computers can think is just as relevant and just as meaningful as the question of whether submarines can swim.

He wasn't a believer, and at least as regards what we have today, I believe he is still just as correct today as he clearly was 40 years ago. Today, we may have far better submarines, but that does not make them fish.

Eric Southwell

Hello Steve (and Leo). LONG TIME listener of the show. I eagerly await each episode.

Getting to the point, I don't understand why this 'age verification' problem is so intractably hard to solve. The US government has several databases that must include all of us. For citizens, the Social Security Administration has all of our info. For non-citizen residents the government has other databases that have unique numbers associated with people, and importantly their birthdays.

Can't we invent a secure process where we people somehow generate a hash, or are provided a hash, of just our name and birthday? Possibly we generate this hash on a government website that asks for other data to 'prove' who we are. Later when asked to prove our age to a different website, we provide the hash. The hash can be checked against the database of hashes for proof of age. The only data transmitted is the hash data. By design, the response from the age verifying service would only be Yes to allow access or No to prevent access.

I'm probably missing something obvious. It's just that it seems like we could use cryptography to provide data that is anonymous to a requester, but can be verified against a database (that already exists) in order to prove our age, or identity. Heck, maybe a QR code would do the trick ;-) Or even TOTP from an authenticator app. Or public / private keys pairs. Anxious to hear your thoughts. /Eric

There are two primary issues: The first is spoofing. As long as there have been age-based restrictions on what someone can or cannot do, there has been pressure to spoof one's age. The concept of the "fake ID" is so ubiquitous and deeply rooted into our culture that it's not even a meme any longer; it's way beyond that.

The primary classic reason for having and using a "fake ID" is so that its holder may fraudulently assert that they're older than they truly are. In the physical world, a higher-quality fake ID will sport a photo of its underage holder. This makes contesting the ID when it's presented much more difficult. The other use case is the use of someone else's, some other older person's actual ID. In that case, the question is whether the photo on the ID is that of the person presenting it. In the first case we have a falsified identifier for the person holding the ID and in the second case we have a legitimate identifier for a different person.

So the first and largest problem, as we transition to the cyber realm, is how to prevent the spoofing of anyone's age assertion. This is why I've consistently referred to the need for tight biometrics as a necessary component of any effective online age verification system. If someone simply has a hash or a QR code or a public/private key pair, nothing prevents any of those technologies, which are all inherently anonymous, from being shared with others. The time that would be required for an underground market in fake online age assertions to be established would best be measured in microseconds. Therefore, any technology that asserts someone's age must, absolutely must, somehow be tied to unspoofable biometric parameters that uniquely identify that person. This suggests that facial and fingerprint recognition pretty much need to go hand-in-hand with any form of online age verification. And this, of course, presents a sticky wicket because not everyone has uniform access to such biometric technology.

But I said there were two primary issues. The second one is no less important, and that's privacy. It will almost certainly be very important to people who wish to authenticate their age, for whatever reason, that they not be individually identified as part of the requirement for doing that. This is where last week's zero-knowledge proof business comes in. We need the ability to make a go/no-go – over 18 years of age or not – assertion without revealing anything else about ourselves. This suggests that we need some sort of proxy, to which we biometrically authenticate, to make this assertion on our behalf. But we also don't want that proxy to obtain any information about the website to which we wish to authenticate.

The cryptographic tools we already have provide the framework for a solution. For example, just off the cuff, some site that must authenticate our age before we're permitted to enter could present a large cryptographically unique random token. We've talked many times about how trivial this is to generate: The site simply encrypts a counter which only ever counts up using a secret per-site key. The output of that encryption will be a pseudo-random token that has never been seen before and will never be seen again. To this token we append the age-assertion that the site requires its visitor to validate.

The user then needs to arrange to have that compound token signed by an age-assertion provider. This could be anyone who participates in this system, like Apple, Google, or Samsung who have the necessary biometrics, or anyone who's able to assert that they will somehow arrange to only ever sign an age assertion for someone whose age they have verified matches that assertion. Note that the entity that's being presented this age assertion to sign knows nothing about the entity or website that generated the assertion. So the user's privacy is preserved.

The signed assertion is then returned by the user to the website which verifies that the assertion is one that ***it*** recently issued, that it has not yet been used – since these must be single use – and that it matches the token that was issued for this user's current session. The asserter's signature is verified against the root certificates in what would become the industry's common age-assertion root store, and the user is then admitted to the age-controlled website. With some additional thought it would be possible to automate and streamline this process using QR codes and more. My point is, this problem **can** be solved.

It’s extremely annoying that the U.S. Supreme Court ruled that no one’s first amendment rights to protected free speech would be abridged by the imposition of this quite onerous requirement. As we all know, at present the industry has no means whatsoever for asserting anyone’s age without sacrificing all privacy and their individual identity.

This imposition significantly changes the nature of the Internet. Some of our listeners have forwarded links to commentary written by authors of websites containing salacious adult content that’s far more tame than the legislation’s initial targets. Yet that adult content falls within the very broad legislation’s scope. So the point has been made that this is only the initial foray and that the underlying goal is to force the removal from the Internet of any content that a minority of the U.S. public finds unacceptable. Tomorrow’s Internet may look much different from today’s. In many ways it will be better. But control can always be misused.

Cloudflare's 1.1.1.1 Outage

https://blog.cloudflare.com/cloudflare-1-1-1-1-incident-on-july-14-2025/

I haven't mentioned anything about my discoveries resulting from my pretty much incessant use of the new and still developing GRC DNS Benchmark. But what I suspect most users of this new tool are going to discover, is that if you didn't have something like the Benchmark to more carefully customize and personalize or confirm your own choice of optimal DNS resolvers, you probably could not go very wrong choosing any of Cloudflare's DNS solutions. Although they are not alone among the Benchmark's top-rated resolvers, they are always near the top and I've been quite impressed by what I've seen. I'll have a lot more to say about that before long.

I'm mentioning this today, because exactly one week ago, on July 14th, while we were recording this podcast, from just before 3pm to just before 4pm, Cloudflare suffered a significant outage incident which caused their wildly popular primary DNS resolver, accessed at the IP [1.1.1.1] to disappear from the Internet for an hour. The details surrounding this event are extremely interesting and I thought everyone would enjoy learning about not only what happened, but also why and how.

Before I start by sharing the introduction of their report, I want to note that this is precisely why standard best practice on the Internet has always been to configure a pair of DNS resolvers for use by every connection to the Internet. "Stuff happens" as they say. So anyone whose Internet connection was configured to use both of Cloudflare's IPs: 1.1.1.1 and its secondary backup of 1.0.0.1, would only have noticed a brief "stutter" when 1.1.1.1 stopped responding. Operating systems will first reissue their UDP DNS queries under the assumption that the UDP packet may have been dropped either to or from the resolver. Then, once the primary resolver has failed to respond to several queries, all DNS resolvers that are configured for that Internet interface will be queried in parallel and the OS will then switch to using the first one to reply. So a nearly transparent switchover from 1.1.1.1 to 1.0.0.1 would have occurred for many people during that hour-long outage.

One last point: Lest anyone worry that their LAN network border router may only be assigning a single DNS IP – aimed at itself – to their PCs inside the LAN, this is a common configuration and should not be any cause for concern. In these scenarios, the LAN's router is serving as the proxy for the public-facing DNS resolvers and is using DHCP to configure the client machines on its LAN to ask it for any DNS resolution. It will then, in turn, forward those DNS queries to one or more of its configured public resolvers – which are often configured and provided by the connection's ISP.

Okay. So what happened at Cloudflare to cause a massive hour-long worldwide outage of their flagship 1.1.1.1 DNS resolution? Here's what they shared:

> *On 14 July 2025, Cloudflare made a change to our service topologies that caused an outage for 1.1.1.1 on the edge, resulting in downtime for 62 minutes for customers using the 1.1.1.1 public DNS Resolver as well as intermittent degradation of service for Gateway DNS.*
>
> *Cloudflare's 1.1.1.1 Resolver service became unavailable to the Internet starting at 21:52 UTC and ending at 22:54 UTC. The majority of 1.1.1.1 users globally were affected. For many users, not being able to resolve names using the 1.1.1.1 Resolver meant that basically all Internet services were unavailable. This outage can be observed on Cloudflare Radar.*

This Cloudflare Radar page of theirs is very cool. I have its link in the show notes and I've also made it this week's GRC Shortcut. So you can go to: grc.sc/1035.
https://radar.cloudflare.com/dns?dateStart=2025-07-14&dateEnd=2025-07-15

Anyone who is interested in DNS at scale will find this page quite interesting.

For example, the second chart shows the overall usage ratios of the four DNS protocols for their 1.1.1.1 resolver. Traditional DNS over UDP currently commands an 86% share. In a very distant second place is DoT at 7.1%, then DoH at 4.7% and plain unencrypted TCP at 2.2%. Although modern browsers have settled upon DoH for their use of privacy-enforcing DNS, when Android devices are configured to use private DNS with Cloudflare that's DoT. And DoT is often preferred by IoT devices and enterprises.

Another interesting data point is that Cloudflare's 1.1.1.1 resolver receives 62.6% – just shy of 2/3rds – of its requests for IPv4 addresses whereas queries for IPv6 addresses make up 18.8%. So while IPv6 is nearly 1/5th of the total, it's clear that IPv4 still rules.

I'll note that the DNS Benchmark tends to favor resolvers with IPv6 addresses. It consistently finds that they respond slightly faster than resolvers addressed with IPv4 addresses. Cloudflare does have a similar pair of IPv6 resolvers, though their IPv6 IPs are not nearly as cool as 1.1.1.1 and 1.0.0.1.

Anyway, lot's of interesting stuff on that page. Let's continue with Cloudflare's explanation of who tripped over what cord at headquarters. They wrote:

> *The outage occurred because of a misconfiguration of legacy systems used to maintain the infrastructure that advertises Cloudflare's IP addresses to the Internet. This was a global outage. During the outage, Cloudflare's 1.1.1.1 Resolver was unavailable worldwide.*
>
> *We're very sorry for this outage. The root cause was an internal configuration error and not the result of an attack or a BGP hijack. In this blog, we're going to talk about what the failure was, why it occurred, and what we're doing to make sure this doesn't happen again.*
>
> *Cloudflare introduced the 1.1.1.1 public DNS Resolver service in 2018. Since the announcement, 1.1.1.1 has become one of the most popular DNS Resolver IP addresses and it is free for anyone to use.*
>
> *Almost all of Cloudflare's services are made available to the Internet using a routing method known as anycast, a well-known technique intended to allow traffic for popular services to be served in many different locations across the Internet, increasing capacity and performance. This is the best way to ensure we can globally manage our traffic, but also means that problems with the advertisement of this address space can result in a global outage.*

Let's pause again to talk about "Anycast" for a second.

Several weeks ago we mentioned that the European Union had introduced a set of its own DNS resolution services for its EU member citizens. I immediately added all of their DNS IP, DoT and DoH addresses to GRC's Benchmark and I was a bit put off by their sluggish performance. In retrospect this was to be expected since the Benchmark was actually communicating with DNS resolvers operated by Whalebone and located in the Czech Republic. And while that may be right around the corner for users in the EU, it's on the far side of undersea cables and many router hops from my location in Southern California.

I confirmed with many of our EU-located DNS Benchmark testers that these same DNS4EU resolvers operate quite acceptably well for anyone located near them. In other words, for those DNS4EU resolvers, their actual real-world performance will be a direct function of how far away the client is from the location of those physical servers whose IP addresses the client is accessing. These resolvers have so-called "UNICAST" IP addresses where traffic addressed to those IP addresses will be routed across the Internet to them. This is completely fine for EU citizens since those servers will be close by. And the EU certainly doesn't wish to expend their resources making their DNS4EU fast for me in the States.

So what's different about Cloudflare and their 1.1.1.1 IP? The 1.1.1.1 Cloudflare IP is an "ANYCAST" address where that IP does not refer to any specific physical resolver hardware. So any traffic addressed to that IP is NOT routed to some resolver located at a single specific location. Instead, "anycast" addresses will automatically route to the closest Cloudflare data center. This means that whereas the performance of the DNS4EU IPs is determined by the client's location and their distance from the EU, Cloudflare, being a major global network provider, will have a data center that's close to anyone, and hat single ubiquitous 1.1.1.1 IP will automatically cause any client's DNS lookup traffic to be routed to that closest data center for resolution. It's an extremely slick system and it explains how Cloudflare is able to offer their super-high performance DNS services from a single universal IP, no matter where its clients may be located.

Okay, back to Cloudflare. They wrote:

> *Cloudflare announces these anycast routes to the Internet in order for traffic to those addresses to be delivered to a Cloudflare data center, providing services from many different places. Most Cloudflare services are provided globally, like the 1.1.1.1 public DNS Resolver, but a subset of services are specifically constrained to particular regions.*
>
> *These services are part of our Data Localization Suite (DLS), which allows customers to configure Cloudflare in a variety of ways to meet their compliance needs across different countries and regions. One of the ways in which Cloudflare manages these different requirements is to make sure the right service's IP addresses are Internet-reachable only where they need to be, so your traffic is handled correctly worldwide. A particular service has a matching "service topology" – that is, traffic for a service should be routed only to a particular set of locations.*
>
> *On June 6, during a release to prepare a service topology for a future DLS service, a configuration error was introduced: the prefixes associated with the 1.1.1.1 Resolver service were inadvertently included alongside the prefixes that were intended for the new DLS service.*

Okay. Just to be clear, that fundamental configuration error which lumped the universal 1.1.1.1 IP in with some others occurred back on JUNE 6th. Not in July. So it was more than a month old. They explain:

> *This configuration error sat dormant in the production network as the new DLS service was not yet in use, but it set the stage for the outage on July 14. Since there was no immediate change to the production network there was no end-user impact, and because there was no impact, no alerts were fired.*

Their report then lays out a detailed minute by minute and hour by hour timeline of the event.

At 21:48 UTC, just before 3pm during last week's podcast recording, the "you know what" started to hit the fan. They detailed this:

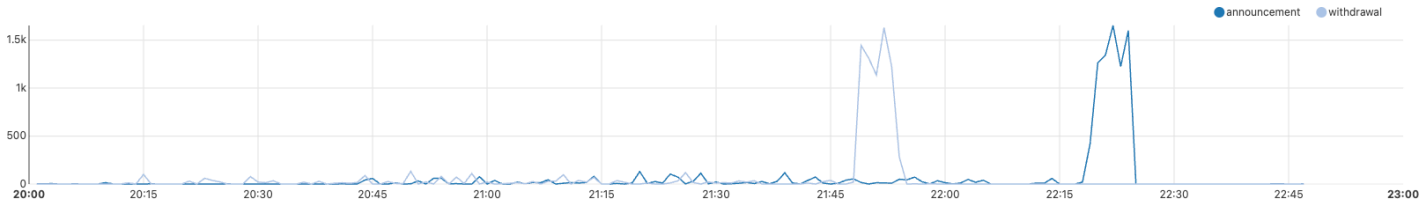
> *A configuration change was made for the same DLS service. The change attached a test location to the non-production service; this location itself was not live, but the change triggered a refresh of network configuration globally.*
>
> *Due to the earlier configuration error linking the 1.1.1.1 Resolver's IP address to our non-production service, the 1.1.1.1 IP was inadvertently included when we changed how the non-production service was set up. The 1.1.1.1 Resolver prefixes started to be withdrawn from production Cloudflare data centers globally.*

Everything we're talking about is BGP – the Border Gateway Protocol – which we've covered a number of times in the past, generally when something goes very wrong with the Internet due to its misconfiguration, such as attempting to route all of the Internet's global traffic through a pawn shop in lower Slabovia. That never turns out well for anyone. So something similar happened again, and with a similar outcome. Internet traffic is great and it works incredibly well, right up until it utterly fails. And it generally fails big.

- **At 21:52:** DNS traffic to 1.1.1.1 Resolver service begins to drop globally.
- **At 22:01:** Internal service health alerts begin to fire for the 1.1.1.1 Resolver and a formal incident is declared.
- **At 22:20:** A fix is deployed – A "revert" was initiated to restore the previous configuration. To accelerate full restoration of service, a manually triggered action is validated in testing locations before being executed.
- **At 22:54:** The "impact" ends – Resolver alerts are cleared and DNS traffic on Resolver prefixes return to normal levels.

So what was the "impact" of this? There are some interesting details there, too. They write:

> When the impact started we observed an immediate and significant drop in queries over UDP, TCP and DNS over TLS (DoT). Most users have 1.1.1.1, 1.0.0.1, 2606:4700:4700::1111, or 2606:4700:4700::1001 configured as their DNS server.
>
> It's worth noting that DoH (DNS-over-HTTPS) traffic remained relatively stable as most DoH users use the domain cloudflare-dns.com, configured manually or through their browser, to access the public DNS resolver, rather than by IP address. DoH remained available and traffic was mostly unaffected as cloudflare-dns.com uses a different set of IP addresses. Some DNS traffic over UDP that also used different IP addresses remained mostly unaffected as well.
>
> As the corresponding prefixes were withdrawn, no traffic sent to those addresses could reach Cloudflare. We can see this in the timeline for the BGP announcements for 1.1.1.0/24:

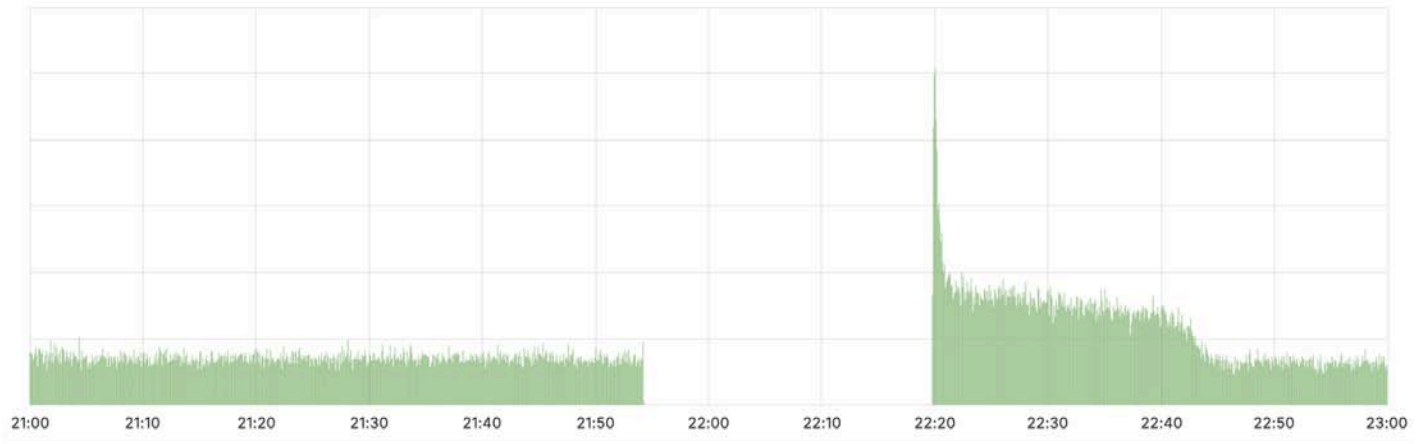


The show notes include the chart from their write-up. We see a first burst of Border Gateway Protocol traffic that's busy updating all of the Internet's global BGP routers with the latest routing tables and, unfortunately, withdrawing all of the Internet's routing for the 1.1.1.1 IP. After that, the Internet's routers have no idea where to send any of the traffic bound for the 1.1.1.1 IP. So when any 1.1.1.1-bound packets hit the first big iron router, there's nowhere for it to go. It's treated as an unroutable IP. It goes nowhere and is just dropped.

Then, shortly after they realize that something truly horrible has just happened, they emergency revert to the previous global network configuration and we see another burst of BGP "Announcement" traffic going out and spreading across the Internet's global routers. They're all then learning about the 1.1.1.1 IP and where they should send any traffic that declares 1.1.1.1 to be its destination.

There's one lost bit of interesting charting that they provide. They write:

> *When looking at the query rate of the withdrawn IPs it can be observed that almost no traffic arrives during the impact window. When the initial fix was applied at 22:20 UTC, a large spike in traffic can be seen before it drops off again. This spike is due to clients retrying their queries. When we started announcing the withdrawn prefixes again, queries were able to reach Cloudflare once more. It took until 22:54 UTC before routing was restored in all locations and traffic returned to mostly normal levels.*



The chart shows the 90 minutes before the event, with query traffic puttering along on a more or less straight line. Then it just utterly disappears. It drops to zero, which is what we would expect once the entire Internet has forgotten what to do with that IP.

Then, at 22:20 UTC, the traffic just as suddenly skyrockets to about six or seven times normal. As they wrote, DNS clients that were just discovering the outage would have been frantically retrying their queries, creating an artificial tsunami which could be seen at the Cloudflare resolvers once routing had been restored.

Their postmortem flagellation posting then digs deeper into how and why this happened. I'll share a paragraph of it ... and see if this doesn't sound hauntingly familiar to what we heard CrowdStrike explain almost exactly one year ago after they cause the crash of 8.5 million Windows machines. Cloudflare wrote:

> *The way Cloudflare manages service topologies has been refined over time and currently consist of a combination of a legacy and a strategic system that are synced. Cloudflare's IP*

ranges are currently bound and configured across these systems that dictate where an IP range should be announced (in terms of datacenter location) on the edge network. The legacy approach of hard-coding explicit lists of data center locations and attaching them to particular prefixes has proved error-prone, since (for example) bringing a new data center online requires many different lists to be updated and synced consistently.

And here it comes, they wrote:

This model also has a significant flaw in that updates to the configuration do not follow a progressive deployment methodology: Even though this release was peer-reviewed by multiple engineers, the change didn't go through a series of canary deployments before reaching every Cloudflare data center.

In other words, just as with CrowdStrike, there was what turned out to be too much confidence placed in the automation side of the system. So deployment was all at once and not incremental or tested before it was let loose upon the entire planet. As they say, lessons learned.

After sharing a bunch more detail, including how the inadvertent withdrawal of the 1.1.1.1 routing revealed an underlying, but inconsequential, BGP hijack originating from Tata Communications in India, they conclude:

Cloudflare's 1.1.1.1 DNS Resolver service fell victim to an internal configuration error.

We are sorry for the disruption this incident caused for our customers. We are actively making these improvements to ensure improved stability moving forward and to prevent this problem from happening again.

They were already moving toward a better and less error-prone system to support their future growth. If nothing else, this mishap showed them the value of that planning and investment.

I have the link to the full incident report, GRC's short of the week and the very interesting page of DNS resolver statistics at the end of the show notes for anyone who's curious to know more:

Full incident report:
https://blog.cloudflare.com/cloudflare-1-1-1-1-incident-on-july-14-2025/

The Cloudflare Radar page of graphs:
https://grc.sc/1035
https://radar.cloudflare.com/dns?dateStart=2025-07-14&dateEnd=2025-07-15