Security Now! #1046 - 10-07-25

Google's Developer Registration Decree

This week on Security Now!

• Qantas says no one can releak their stolen data. • Brave's usage is up. But is it really 3 times faster. • Next Tuesday the EU votes on "Chat Control". • Microsoft formally launches a "Security Store". • Outlook moves to block JavaScript in SVG's. • A new release of Chrome. • Gmail will no longer pull external email via POP. • Googe Drive starts blocking ransomware encryptions. • The UK issues another order to Apple. • Researchers create a "Battering RAM" attack device. • HackerOne's significant bug bounty payouts. • The Imgur service goes dark across the UK. • The Netherlands plans to say NO to "Chat Control." • Discord was breached and government IDs leaked. • Salesforce says it's not another new breach. • Signal introduces a new post-quantum ratchet. • Your motherboard MIGHT support TPM 2.0. • Google to force Android app devs to register and pay.

This is **so** clever!

Security News

Qantas Airlines Permanent Injunction

We touched on this weird story in July ago after the Australian airline Qantas, obtained a temporary injunction to prevent the use of data stolen in a recent ransomware attack. That temporary injunction has now been made permanent by the Australian New South Wales Supreme Court. The court order prevents third parties from publishing, viewing, or accessing the data if it is released by the attackers. The Qantas Airlines' accounts of 5.7 million customers were compromised in a data breach which hit one of the airline's call centers. The data stolen included the business and residential addresses attached to 1.3 million accounts, the phone numbers of 900,000 customers, and the dates of birth of a further 1.1 million. So it's a mess. The ruling justice in the case also agreed to impose a 6-month non-publication order over the names of the solicitors and counsel acting for Qantas in the matter. The attorneys insisted that their identities not be published in any press coverage for fear of retaliation from the attackers.

This whole thing seems really bizarre. I'm pretty certain that the attackers could not care less who Qantas hired to obtain an order blocking the publication of their stolen data, any more than they could care about some Australian court order blocking the data's publication. It's not as if anyone who might use the stolen data would be law abiding and would feel the least bit constrained by some court in another country. The data would be released onto the Dark Web, perhaps be merged into larger aggregate databases, or who knows what. And no reputable law abiding entity that might manage to obtain the data would be re-publishing it with or without a supreme court order.

The only thing that makes sense is that this is a CYA move by the Qantas CEO to appear to be doing the responsible thing after one of their own call centers was breached. One hopes they're spending equal or more time and money shoring up the security of their systems to prevent more trouble in the future.

Brave Browser passes 100 million users

Last Wednesday, October 1st, Brave posted the news that the use of the Brave Browser had surpassed 100 million monthly active users.

> *Over the past two years, the Brave browser has seen an average of about 2.5 million net new users each month. This September, we officially surpassed 100 million monthly active users (MAU) worldwide. At the same time, we surpassed 42 million daily active users (DAU), for a DAU-to-MAU ratio of 0.42, underlining the high engagement that users have with Brave.*
>
> *This growth has been fueled by a global awareness that Brave is an alternative to Big Tech and that users benefit greatly from a browser that preserves their privacy and is up to 3 times faster than competitors. Also, when users are given a choice, users exercise that choice and switch to new browsers. For example, daily installs for Brave on iOS in the EU went up 50% with the new browser choice panel, following the implementation of the DMA and release of iOS 17.4 in 2024.*

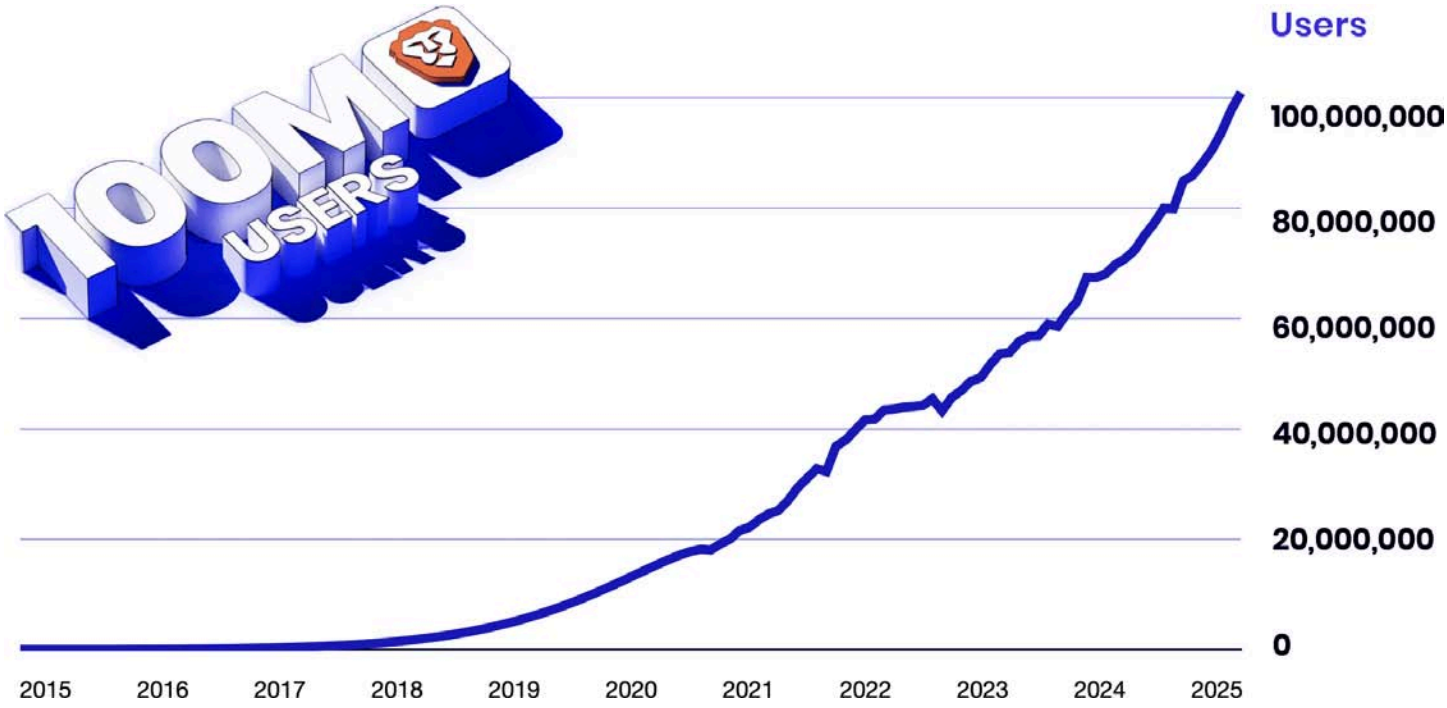
Their usage numbers are nice and they have an impressive upward-pointing graph, but what really annoyed me was their utterly bogus claim of being up to 3 times faster than competitors. What a load of nonsense. Brave is based upon the same Chromium engine as Chrome, Edge, Vivaldi, and Opera. And believe me, if it was possible for any of those browsers to go any faster they already would be. It's not as if the Brave folks have some magic pixie dust they're keeping

to themselves which magically triples the speed of their browser. Brave is no faster than any of those others when it's doing the same job. It can't be. The only possible way for any browser that's using the same underlying engine code to render pages any faster would be for it to be rendering less of those pages – and that must be what's going on with Brave. But 300%? Give me a break.

If you managed to find a web page that's massively loaded down with large advertisements bringing massive JavaScript blobs and tracking code and heavy scripting all being served by slow servers a long ways away, so that the page's fully burdened completion takes an inordinately long time, then sure, okay. If Brave's privacy enhancing policies block some of that crap from being loaded at all, it gets to declare "done" faster than its sibling competitors, but only because they are choosing to render the page's entire burden.

This claim drove me to poke around the Net to see what I could find. There are some useful head-to-head benchmark comparisons on the Android platform where, when Brave is loading a heavily privacy-disrespecting page, it manages to perform around 21% better than browsers that are rendering the entire page. So that's useful. It means that sometimes Brave will, indeed, be a little bit faster than other browsers. But these guys should really be ashamed of themselves for claiming that Brave users will, in any meaningful way, actually ever experience Brave running three times faster than its competitors. As I noted, they're all actually the same browser. They differ only in UI and feature policies, not in their underlying page rendering technologies.

People do appear to be switching to Brave in significant numbers, as their chart shows. But I hope it's for the browser's privacy respecting features and not because they buy into that three times faster nonsense.



https://brave.com/blog/100m-mau/ I've dropped the link to Brave's October 1st posting into the show notes. There's much more to be said and Brave does appear to be assembling an entire privacy-respecting ecosystem. They have their own search engine index of which they wrote: *"Unlike Alphabet's Google or Microsoft's Bing, or supposedly independent providers like DuckDuckGo (which relies on Bing for its results), Brave doesn't bias or censor results, or manipulate its search algorithm."*

So, by all means, adopt Brave for privacy if you wish. Just don't hold your breath waiting for it to be three times faster than others.

Next Tuesday, October 14th: The EU member countries vote on "Chat Control"
Some news coverage from last Wednesday, which I had Firefox translate from German, reads:

> *The head of the messenger app Signal – who we know is Signal's president Meredith Whittaker – threatens to withdraw from the European market. The reason is the EU's plan to install backdoors in apps that allow automatic search for criminal content.*
>
> *The head of the Signal app has criticized plans in the EU, according to which Signal Messenger should have backdoors to enable the automatic search for criminal content. Meredith Whittaker told the DPA news agency: "If we were faced with the choice of either undermining the integrity of our encryption and our privacy safeguards or leaving Europe, we would unfortunately make the decision to leave the market."*
>
> *The European Union has been deliberating for three years on a law to re-regulate the fight against depictions of child sexual abuse. The proposal of the corresponding regulation stipulates that messengers such as WhatsApp, Signal, Telegram or Threema should enable the content to be checked before encryption.*

This is not the first time we've seen this new language talking about checking the content before its encryption. If this were going to be done, that's the way to do it. You have an image that's essentially in plaintext before it's pushed through the encrypted tunnel. So don't screw with the encryption. If you insist upon breaching the user's privacy, don't also weaken the integrity of their communications at the same time. Simply check the image before it's sent.

But here's where I hope someone with some technical chops is paying attention. No application running on iOS or Android has any contact whatsoever with the underlying imaging hardware, either its capture or its display. All of the messaging and communications apps are application programs, so they are accessing an application program interface – an API – which is published by the underlying operation system to give its client applications access to camera and stored images and to the device's screen. The API deliberately divorces all of the hundreds of thousands of platform applications from the underlying hardware. This allows the manufacturer the freedom to change their smartphone hardware at will. It explains why the same app can run on wildly differing smartphones without trouble.

And, of course, all of this is Computer Operating Systems 101. During the first year of my life, 70 years ago between 1955 and 1956, General Motors Research working with IBM, developed the GM-NAA I/O system for the IBM model 704 mainframe computer. That work, for the first time in human history, used an I/O abstraction layer between the programs running on the machine and its underlying hardware. Needless to say, the idea was a good one and it's been evolving ever since.

So here's my point: It is completely wrong-headed for any legislation to be aimed at any communicating platform application, whether encrypted or not. That's the wrong target. And if that's the target then we're playing an endless game of whack-a-mole. The legislation should be directed at the underlying operating system. It's the OS that runs the camera, the screen, and the storage. It's not any messenger app's fault if it's given an abusive image to send, it's the operating system that gave that image to the messenger app. The operating system always sees the image first and, if the EU insists upon some behavior based upon the detected content of

that image, then the operating system is the proper place for that to happen. If this is not done then every application that communicates, whether encrypted or not, will need to be doing this, including iOS's and Android's own built-in encrypted Messenger apps. We have printer drivers today so that every application doesn't need to bring along its own collection of printer drivers.

Filtering messaging content is exactly the same. Rather than expecting every application to do this separately – especially since iOS and Android will also be needing to have this technology to support their own legally compliant messaging apps.

We don't know what's going to happen one week from today, but we'll know soon. 12 of the EU bloc's 27 members are publicly backing the proposal, with eight against, and the rest undecided. The proposal will pass if the Council is able to obtain a "qualified majority". In this case that means at least 55% of the 27 member states, so 15 of 27, and the majority must also represent at least 65% of the EU population. The measure could also be blocked by at least 4 countries which represent more than 35% of the EU population.

In any event, stay tuned! If this legislation should pass things are going to get exciting.

Microsoft Security Store: https://securitystore.microsoft.com/
Anyone going to the URL: securitystore.microsoft.com will find themselves looking at Microsoft's just-launched Security Store from which Microsoft is literally selling Azure solution solutions. So just to be clear, this is not for end users.

Last Tuesday, the Microsoft Security Community Blog posting was titled *"Introducing Microsoft Security Store"*, which starts out:

> *Security is being reengineered for the AI era—moving beyond static, rulebound controls and after-the-fact response toward platform-led, machine-speed defense. We recognize that defending against modern threats requires the full strength of an ecosystem, combining our unique expertise and shared threat intelligence. But with so many options out there, it's tough for security professionals to cut through the noise, and even tougher to navigate long procurement cycles and stitch together tools and data before seeing meaningful improvements.*
>
> *That's why we built **Microsoft Security Store** - a storefront designed for security professionals to discover, buy, and deploy security SaaS solutions and AI agents from our ecosystem partners such as Darktrace, Illumio, and BlueVoyant. Security SaaS solutions and AI agents on Security Store integrate with Microsoft Security products, including Sentinel platform, to enhance end-to-end protection. These integrated solutions and agents collaborate intelligently, sharing insights and leveraging AI to enhance critical security tasks like triage, threat hunting, and access management.*

The page continues at some length describing how the Security Store essentially allows security professionals to browse, point, click, purchase, deploy and manage their cloud security more easily than ever before. No more waiting for those pesky purchasing cycles and authorizations. Just get what you need and start using Microsoft's new "Security Copilot" solutions in minutes.

I have no doubt that we have many listeners who will find this new Microsoft packaging and deployment to be very useful, so I wanted to make sure that those listeners were aware of this new facility.

Outlook to block inline Scalable Vector Graphics (SVG's)
There's welcome news on the Scalable Vector Graphics security front. Earlier this year the world saw a dramatic rise in the abuse of SVG-format image files. To many people's surprise and frank astonishment, SVG image files, being formally defined as XML, are allowed to contain JavaScript which is faithfully executed whenever the image is rendered. This capability sat idle for most of that image format's life until it was rediscovered by malefactors and starting being abused with increasing frequency.

Various product vendors changed the behavior of their SVG rendering code, such as stripping out <script> tags and code before rendering the described images. And Microsoft just announced:

> *Starting September 2025, Outlook for Web and new Outlook for Windows will stop displaying inline SVG images, showing blank spaces instead. This affects under 0.1% of images, improves security, and requires no user action. SVG attachments remain supported. Organizations should update documentation and inform users.*

So, images embedded in Outlook email so that they would normally be displayed, will no longer be. This of course only applies to SVG images which, as Microsoft correctly notes accounts for a miniscule percentage of all email images. GIFs, JPEGs and PNGs account for all typical images. So anyone who needs to email an SVG can still do so as a non-rendered file attachment. Sorry, bad guys!

Chrome 141
Chrome advanced to version 141. The Web functions moved forward and two high priority vulnerabilities were patched. The most severe of the two, a heap buffer overflow in WebGPU, earned discoverer and reporter $25K. The second was another heap buffer overflow in the browser's Video code which earned its reporter $4K. There was also a $5K bounty paid for a side-channel information leakage in Storage. Overall, 21 security problems were fixed with Google paying out $49K to external security researchers.

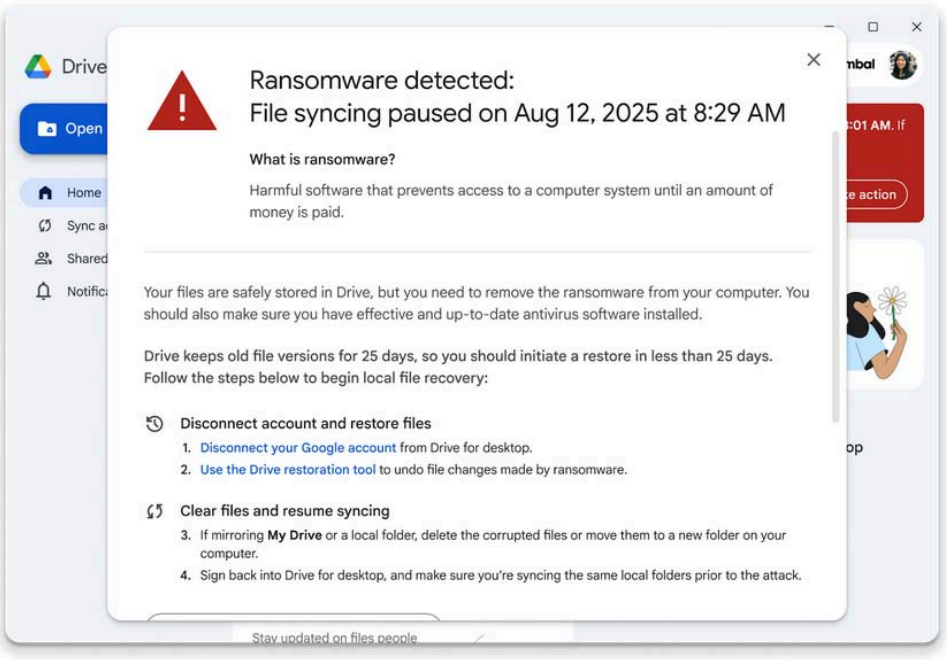
It's clear that the concept of paying researchers bounties for their responsible reporting of bugs they discover is a winning strategy.

Gmail: No more POP pulling
Just one more note from Google. Not security related but perhaps affecting some of our listeners: Starting in January of next year, Google will be eliminating gmail's "POP Fetching" feature which pulls email from other external accounts via POP, the original Post Office Protocol. Google recommends that users who wish to have their other account email sent to their Gmail inboxes have that mail forwarded there. So instead of Google pulling via POP, the other end needs to push.

Google Drive blocking Ransomware
In a move that I expect we're going to be seeing everyone adopt, Google announced that their Drive product for Windows and MacOS has been enhanced to detect and block ransomware. And, of course, they couldn't resist tossing in the fact that it's enhanced with "AI". They announced:

> *While native Google Workspace documents (e.g., Google Docs, Sheets) are not impacted by ransomware and ChromeOS has never had a ransomware attack, ransomware is a persistent*

threat for other file formats (e.g., PDF, Microsoft Office) and desktop operating systems (e.g., Microsoft Windows). That's why we're enhancing ***Google Drive for desktop*** *with AI-powered ransomware detection to automatically stop file syncing and allow users to easily restore files with a few clicks.*



In addition, the built-in virus detection in Drive, as well as in Gmail and Chrome, helps to prevent ransomware from spreading to other devices with the aim of taking over an entire network. As a result, these defenses can help organizations in industries such as healthcare, retail, education, manufacturing, and government from being disrupted by the types of ransomware attacks that have been so destructive up to this point.

Drive for desktop, available on Windows and macOS, is used to efficiently and securely sync user files and documents to the cloud. It can be also used as a critical line of defense against malware and ransomware attacks. With that in mind, we've built a specialized AI model, trained on millions of real-world ransomware samples, to look for signals that a file has been maliciously modified. The detection engine adapts to novel ransomware by continuously analyzing file changes and incorporating new threat intelligence from VirusTotal. When Drive detects unusual activity that suggests a ransomware attack, it automatically pauses syncing of affected files, helping to prevent widespread data corruption across an organization's Drive and the disruption of work.

Users then receive an alert on their desktop and via email, guiding them to restore their files. Unlike traditional solutions that require complex re-imaging or costly third-party tools, the intuitive web interface in Drive allows users to easily restore multiple files to a previous, healthy state with just a few clicks. This rapid recovery capability helps to minimize user interruption and data loss, even when using traditional software such as Microsoft Windows and Office.

Bravo Google. Other well known cloud-based file backup provides such as Dropbox, Backblaze, Veeam, FileCloud and Scality have been marketing similar ransomware protections for their backup solutions. Pretty much anytime you have file versioning and file deletion protection, you're going to be able to recover from anything that attempts to encrypt storage in bulk. But

it’s nice that Google Drive will detect and disconnect to minimize the impact.

UK gives it another shot with Apple’s cloud data

“If at first you don’t succeed...” Last Wednesday, Reuters headline was *“UK makes new attempt to access Apple cloud data”* Reuters re-reported a Financial Times article which was also published last Wednesday, which mostly recounted everything we already know. What’s new is that according to the Financial Times report, the UK has now reissued a new order to Apple requiring them to provide access to the iCloud data of any UK citizen. This amended their previous “we demand access to anyone’s data anywhere”. And once again, Apple was reportedly not impressed.

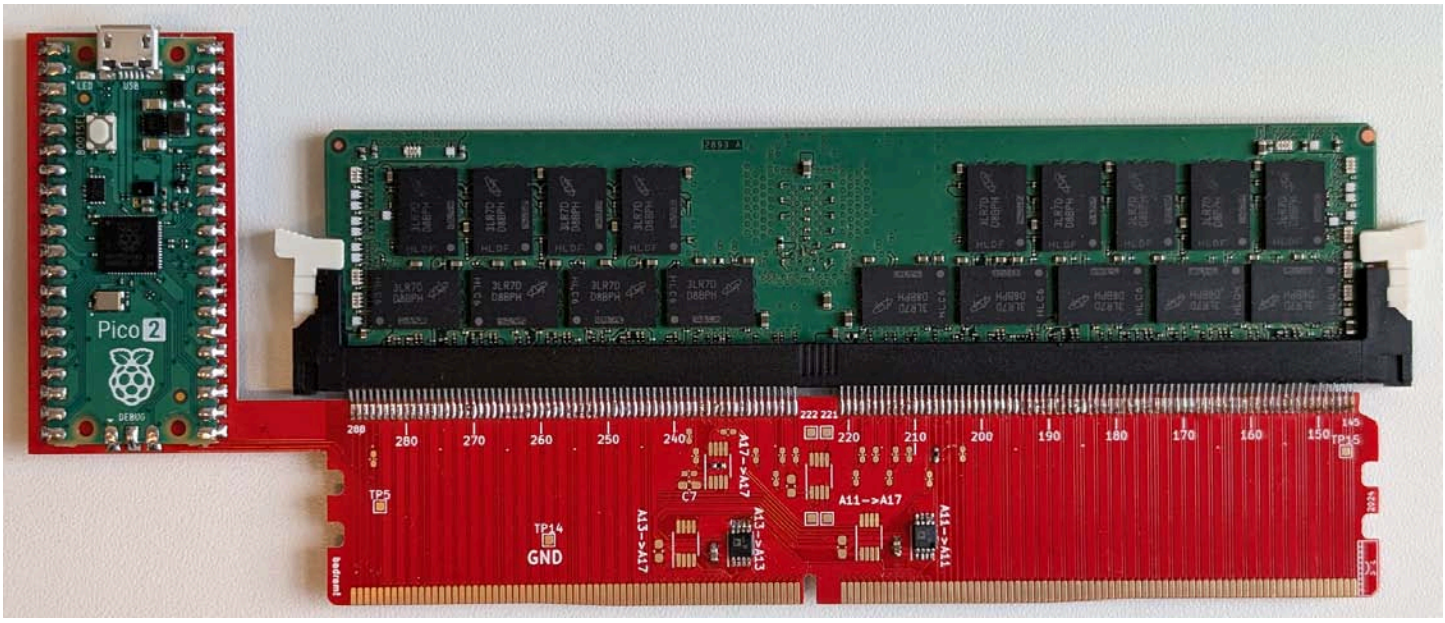
As before, all we have is off-the-record hearsay and speculation. But it seems clear that this newer order won’t go any further with Apple than the last one did. This revised UK order appears to be responsive to the U.S. administration which stepped into the fray, objecting to a foreign government demanding access to the private data of U.S. citizens. So the U.S. likely has no such worries over what the UK does with its own citizens’ data. But we know that Apple does.

We also know that the UK’s Investigatory Powers Tribunal (IPT) confirmed last April that Apple had appealed the UK’s earlier order. So it’s going to be interesting so see what happens next.

The “Battering RAM” attack

A team of Belgian academics built a malicious memory module that can be used to break the confidentiality of modern clouds. The module, which they call Battering RAM, must be deployed by rogue data center employees. It sits between the RAM and motherboard and can allow attackers to break the security features of Intel and AMD processors powering cloud servers. According to the research team, the entire module only costs around $50.

I knew that some of our listeners would enjoy seeing this bit of hardware. Here’s what its developers explained:



With Battering RAM, we show that even the latest defenses on Intel and AMD cloud processors can be bypassed. We built a simple, $50 interposer that sits quietly in the memory path, behaving transparently during startup and passing all trust checks. Later, with just a flip of a software switch, our interposer turns malicious and silently redirects protected addresses to attacker-controlled locations, allowing corruption or replay of encrypted memory.

Battering RAM fully breaks cutting-edge Intel SGX and AMD SEV-SNP confidential computing processor security technologies designed to protect sensitive workloads from compromised hosts, malicious cloud providers, or rogue employees. Our stealthy interposer bypasses both memory encryption and state-of-the-art boot-time defenses, invisible to the operating system. It enables arbitrary plaintext access to SGX-protected memory, and breaks SEV's attestation feature on fully patched systems. Ultimately, Battering RAM exposes the limits of today's scalable memory encryption. Intel and AMD have acknowledged our findings, but defending against Battering RAM would require a fundamental redesign of memory encryption itself.

Unlike commercial passive interposers, which are exceedingly expensive and commonly cost over $100,000, we developed a custom-built interposer that uses simple analog switches to actively manipulate signals between the processor and memory, and can be built for less than $50.

This is just a proof of concept device – but it did thoroughly prove its concept. And this demonstrates why Apple has been so ruthlessly rigorous with the physical security of the server in their iCloud data centers. They fully realize that physical access to a server means that all bets are off.

For those who do not have access to the photo in the show notes, the device looks like what we would have once referred to as a RAM extender. It plugs into a standard DRAM socket and it contains its own DRAM socket into which the original RAM plugs. So this device interposes itself between the system's motherboard and a DRAM chip. Off the the side, attached to one edge of this RAM extended, we see a little Raspberry Pi Pico 2 which provides the intelligence for the assembly.

The device is likely not practical as is, since the DRAM is elevated an inch and a half away from its socket where it would be likely to not fit within a close server chassis. But the point was to create a proof of concept device rather than a practical attack platform. The practical part is that the attacks work.

HackerOne year in review

The HackerOne bug bounty platform paid $81 million to security researchers in the past year. The company received almost 85,000 valid reports and paid out an average of $1,090 per award. Vulnerabilities in AI products were a rising category this year, with more than $2.1 million paid to researchers. Most of the reports covered prompt injection attacks.

Imgur goes dark across the UK

The extremely popular online image hosting site, Imgur felt the need to remove its service from the UK. The first I heard of this was when the people I interact with in the UK, testing the DNS Benchmark, reported that they were unable to use their preferred image posting and hosting site, Imgur.com.

https://help.imgur.com/hc/en-us/articles/41592665292443-Imgur-access-in-the-United-Kingdom

Imgur has posted a page titled: *"Imgur access in the United Kingdom"* which says: *"From September 30, 2025, access to Imgur from the United Kingdom is no longer available. UK users will not be able to log in, view content, or upload images. Imgur content embedded on third-party sites will not display for UK users."* Wow. What we've been anticipating is happening. This is what that looks like.

Here's what the BBC's reporting explained under their headline *"Imgur blocks access to UK users after regulator warned of fine"*:

> *Image-hosting platform Imgur has blocked people in the UK from accessing its content. Imgur is used by millions to make and share images such as memes across the web, particularly on Reddit and in online forums. [Yeah, like in GRC's newsgroups which are deliberately text-only.]*
>
> *But UK users trying to access Imgur on Tuesday were met with an error message saying "content not available in your region" - with Imgur content shared on other websites also no longer showing. The UK's data watchdog, the Information Commissioner's Office (ICO), said it recently notified the platform's parent company, MediaLab AI, of plans to fine Imgur after probing its approach to age checks and use of children's personal data.*
>
> *A help article on Imgur's US website, seen by the BBC, states that "from September 30, 2025, access to Imgur from the United Kingdom is no longer available. UK users will not be able to log in, view content, or upload images. Imgur content embedded on third-party sites will not display for UK users."*
>
> *The ICO launched its investigation into Imgur in March - saying it would probe whether the companies were complying with both the UK's data protection laws, and the children's code. These require platforms to take steps to protect children using online services in the UK, including minimising the amount of the data they collect from them. A document published by the ICO alongside the launch of its investigation stated that Imgur did not ask visitors to declare their age when setting up an account. It said on Tuesday it had reached initial findings in its investigation and, on 10 September, issued MediaLab with a notice of intent to impose a fine.*
>
> *Tim Capel, an interim executive director at the ICO said "Our findings are provisional and the ICO will carefully consider any representations from MediaLab before taking a final decision whether to issue a monetary penalty. We have been clear that exiting the UK does not allow an organisation to avoid responsibility for any prior infringement of data protection law, and our investigation remains ongoing."*

Yikes. That seems rather harsh. But I suppose that retroactive responsibility is necessary, otherwise the law will just be ignored until notice is given. The BBC wrote:

> *The watchdog would not elaborate on what its findings were, nor the details of the potential fine, when asked by the BBC. Tim Capel said: "This update has been provided to give clarity on our investigation, and we will not be providing any further detail at this time."*
>
> *Some Imgur users and reports speculated as to whether Imgur moved to block UK users from its services, rather than comply with child safety duties recently imposed on some platforms under the Online Safety Act.*

Among these are requirements for sites allowing pornography or content promoting suicide and self-harm to use technology to check whether visitors are over 18. But both the ICO and Ofcom - the media regulator enforcing the Online Safety Act - said Imgur suspending access for UK users had been its own "commercial decision." An Ofcom spokesperson told the BBC: "Imgur's decision to restrict access in the UK is a commercial decision taken by the company and not a result of any action taken by Ofcom. Other services run by MediaLab remain available in the UK – such as Kik messenger, which has implemented age assurance to comply with the Online Safety Act."

It feels as though we're going to be passing through a period of turmoil and confusion until the technology has the chance to catch up to the legislation, which is barreling along without much apparent concern for the feasibility of implementing the controls that are being mandated.

And I should note that Imgur is not alone. Last Friday, March 3rd, ICO, the UK's regulator posted under their headline: *"Investigations announced into how social media and video sharing platforms use UK children's personal information"*:

We are today announcing three investigations looking into how TikTok, Reddit and Imgur protect the privacy of their child users in the UK.

Our investigation into TikTok is considering how the platform uses personal information of 13–17-year-olds in the UK to make recommendations to them and deliver suggested content to their feeds. This is in light of growing concerns about social media and video sharing platforms using data generated by children's online activity in their recommender systems, which could lead to young people being served inappropriate or harmful content.

Our investigations into Imgur and Reddit are considering how the platforms use UK children's personal information and their use of age assurance measures. Age assurance plays an important role in keeping children, and their personal information, safe online. There are tools or approaches that can help estimate or verify a child's age, which then allow services to be tailored to their needs or access to be restricted.

The investigations are part of our efforts to ensure companies are designing digital services that protect children. At this stage, we are investigating whether there have been any infringements of data protection legislation. If we find there is sufficient evidence that any of these companies have broken the law, we will put this to them and obtain their representations before reaching a final conclusion.

It should be abundantly clear by now that regardless of how anyone feels about it, the accurate determination of the age of anyone using a social media or content-sharing service will be part of the cost of doing business. It may only be in the UK and a few states in the U.S. today, but the entire European Union doesn't feel far off, and many other U.S. states have their own legislation working its way through their legislatures. And this feels like something which will accelerate as more and more regions are seen to be successfully adopting these new laws.

The Netherlands is "NO" on "Chat Control"

In other late breaking news regarding the embattled EU "Chat Control" legislation, the Dutch government of The Netherlands has stated that it plans to vote "No" on "Chat Control" when that measure comes up for a vote next Tuesday. Minister Van Oosten's letter to Parliament states that

the Netherlands cannot support the proposal in its present form, citing privacy concerns, encryption risks, and proportionality issues. The ministry emphasizes that combating child sexual abuse remains vital, but insists on "legally sound, effective, and privacy-respecting" measures.

To which I say, these politicians want the impossible, which is why this is a supremely difficult problem. On the one hand they say that they want a privacy-respecting solution, but if the goal is to combat the sharing of illegal content, and the only way it's possible to know whether content is illegal is for some**one** or some**thing** to look at it, then that, by definition, requires that everyone's privacy be compromised. You literally can't have it both ways. And, as has been pointed out, breaching everyone's privacy is a direct contravention of the EU's existing and well established privacy protections.

Meanwhile we last reported that Germany was planning to vote "No", but it's since been reported that they are apparently succumbing to pressure and may be voting in favor. All of the independent messaging platforms have said they would leave any jurisdiction that compels them to break their promises of absolute privacy. But iOS and Android both have their own native securely encrypted messaging platforms. iMessage is famously secure. So what will Apple and Google do? Very interesting times we're living through.

A Discord breach

Reading about a breach that Discord just revealed, one of the factoids there caught my eye. As usual, hackers made off with sensitive user data. The breach occurred at a third-party company that handles Discord's customer support. The stolen data includes names, emails, payment details, and customer support tickets. But guess what the breached and stolen data also contained? The scanned images of government IDs that Discord had been compelled to collect for age verification. Yep. We don't yet have the infrastructure in place for securely allowing for the assertion of users' ages online. So we've dropped to the lowest common denominator, which is to present some of our most private information. I certainly don't want criminals to have front and back scans of my driver's license or other similar clearly identifying document. And while I'm sure that the 3rd-party that was breached is not a criminal organization, they've just demonstrated that they are unable to protect our private data from disclosure.

The question we should ask is why they had retained that identifying data at all. Once an age verification has been made, the data required to do that can and should have been erased. But people like to collect data and we have no way to force its deletion after it's served its purpose. So the only way to prevent the inadvertent disclosure of our personally identifying data is to never provide it in the first place, which is why we need technology that we do not have in place.

Salesforce back in the news... and not in the way they would choose

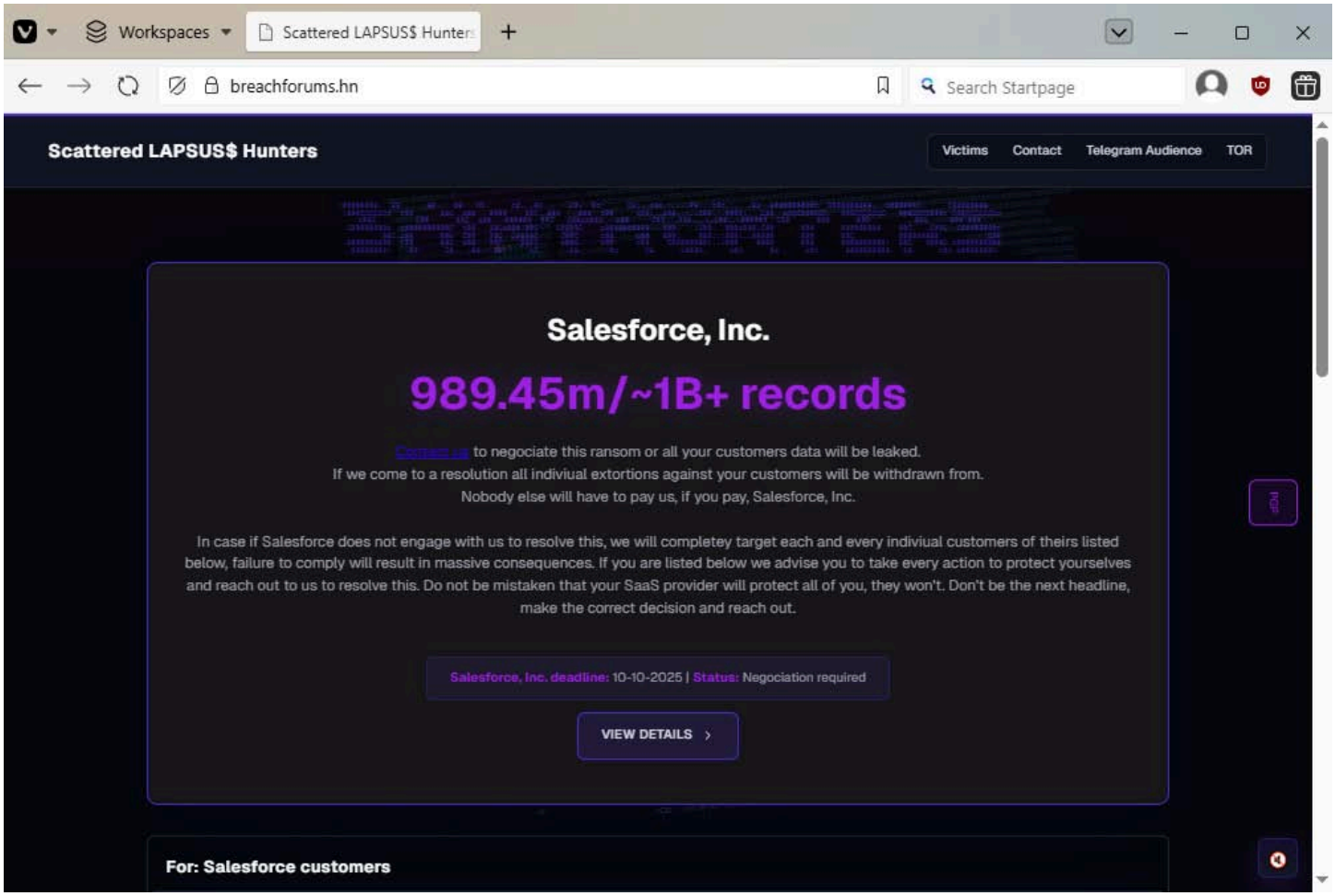
Last Thursday Salesforce explained that the new extortion attempts their customers have been receiving are ***not*** the result of ***another*** hack. Their headline was *"Security Advisory: Ongoing Response to Social Engineering Threats"* where they explained:

> *We are aware of recent extortion attempts by threat actors, which we have investigated in partnership with external experts and authorities. Our findings indicate these attempts relate to past or unsubstantiated incidents, and we remain engaged with affected customers to provide support. At this time, there is no indication that the Salesforce platform has been compromised, nor is this activity related to any known vulnerability in our technology.*
> *We understand how concerning these situations can be. Protecting customer environments and data remains our top priority, and our security teams are fully engaged to provide guidance*

and support. As we continue to monitor the situation, we encourage customers to remain vigilant against phishing and social engineering attempts, which remain common tactics for threat actors.

Brought to you by the "Salesforce Public Relations Department" which has been working overtime pretty much all year. I tracked down the posting that the group calling themselves "Scattered LAPSUS$ Hunters" posted over in "BreachForums", but I could not determine its posting date. What the posting does make very clear is the Salesforce deadline, which is 10-10-2025, which is this coming Friday.

The BreachedForums posting cites 989.45 million (approximately 1 BILLION records) and it reads:



So there may be another shoe dropping by this time next week.

Signal's Sparse Post Quantum Ratchet (SPQR)

The Signal messenger system was just further enhanced by the addition of what they are calling a "Sparse Post-Quantum Ratchet (SPQR)." As we have covered previously, Signal already incorporated post-quantum encryption protection. But these guys are seriously never satisfied. We also previously covered the operation of their double ratchet technology.

They have added another ratchet to create a triple ratchet, and this one is quantum computing safe. The details are interesting and plenty, so I'm thinking that it might be time for a deep dive next week into the operation of Signal's new triple ratchet, one of which is quantum safe.

SpinRite

Goran Jordanov

Hello Steve, I'm a long time fan of the podcast and recently decided to try SpinRite and try to revive some old drives from a TrueNAS system. SpinRite did a phenomenal job of repairing a few HDs, speeding up some SSDs and detected a bad, out of the box Inland NVMe! A bootable SpinRite on a USB stick will now be part of my "must carry" collection of USBs. Thank you!

Sci-Fi

Steve Penfold

I've just spotted the (supposed!) release date on Amazon here in the UK for book 2 in Peter F. Hamilton's latest 2-book Exodus series. I thought that you, Leo and the Security Now audience might like to know how long we all have left to wait! (I assume that the release date will be fairly consistent across countries.) Regards, Steve Penfold.

Title: *"Exodus: The Helium Sea"* with a release date of June 16th, 2026. I was working on the DNS Benchmark when Steve's email arrived and eM Client popped up a notification of email from a Security Now! listener. So I quickly thanked Steve for his note and he replied:

I thought you might like that - I'm holding out before reading the first book, until they're both available!

Amen to that. I now regret that I already read the first half. The problem was, the plot was so convoluted with behind the scenes machinations and subtle long-range manipulations – a reader really needed to be taking notes along the way. But I didn't know that when I started and since then I've pretty much forgotten everything I knew about who, what, where, when and why. And, frankly, I didn't feel that the book was really all that good in the first place.

I'm sorry to report that this beloved author's works seem to be on a steady decline. I loved Fallen Dragon, Pandora's Star and Judas Unchained. I think those were Peter's pinnacle works. And before those, everyone went nuts over his Reality Dysfunction Night's Dawn trilogy series, which was what first put him on the map for those who hadn't discovered him after his earlier Greg Mandel series. I've read and enjoyed them all. But Peter's later works have demanded more and more from his readers and, for me at leave, they haven't been returning as much as they once did.

So I'm not even sure that I have the energy to re-read the first book again once the story's conclusion is available. I suppose I will, because at least the writing is good. But he's beginning to lose me.

Listener Feedback

Mike Lendvay

Hi Steve, In the past few episodes you've mentioned that your iPhone 12 doesn't support Liquid Glass. However, nothing online from Apple or anywhere else indicates that a subset of iPhones that support iOS 26 don't support the new design. Is it possible that you have accessibility settings enabled that tone down the new visual effects, such as Reduce Transparency or Reduce Motion (in Settings > Accessibility > Display & Text Size and Settings > Accessibility > Motion respectively)? This is a small and perhaps unimportant clarification, but it's been bugging me since I can't confirm this piece of information anywhere else! Much thanks to you and Leo for the show, I look forward to it every Tuesday :)

Thank you for challenging me on that, Mike. And I CAN confirm that you are 100% correct. After reading Mike's note I checked the settings on my older iPhone 12 and, sure enough, I had previously disabled all of the previous nonsense. So when I upgraded that phone to iOS 26, Apple continued to honor those settings, so all I saw was relatively minor changes to the UI.

Curious to see what iOS 26 looks like for everyone else, I flipped those switches back to their normal defaults and... wow! (And not in a good way.) My most honest impression is that this is a demonstration of Apple having run out of anything useful to do. The phone has become cartoony. You know how, when the Wiley Coyote is about to take off chasing the Road Runner, in true cartoon fashion Wiley will first pull back a bit, as if to compress some invisible spring to help him then launch out after the Road Runner? When unrestrained, iOS 26's various elements give extra little hops and giggles and splurts just because it can and because, apparently, it's not actually the content in the phone that we want to focus on. We want to have our attention called to admire Apple's amazing animated user interface.

Long ago, it was observed that the best user interfaces were those that went unnoticed and which did not call attention to themselves. The example of this I've always loved was the telephone handset. When you're using it, you don't think in terms of talking into a mouthpiece and microphone. No. Your attention extends past the phone all the way to the person to whom you are talking at the other end. The phone disappears, as it should. But here we have Apple's new user interface jumping up and down like a spoiled infant, going out of its way to constantly call attention to itself and to make everything about it. It's really over the top. But the good news is, it's possible to tone that way, way down, so that the only thing you see is some improved visibility enhancements. And those I very much like.

Eric Perry

Hi Steve, I really enjoyed your show #1045. I've been listening since my career change about 5 years ago. I'm an admin of an m365 tenant, and your read of the passkey authentication for Microsoft accounts felt all too familiar. I wanted to share some additional knowledge that I've found is unique with Microsoft over other passkey accounts I've worked with.

There are several issues I've run into with Microsoft passkey configuration. If you attempt to use passkeys with LastPass, the setup fails when registering with a Microsoft account. I don't know if the same goes for bitwarden or not. I personally use a Yubikey registered as a passkey, and the experience is great! Although we have users testing the Microsoft

Authenticator method, and it's exactly as that listener described. It's clunky, far too many steps, and defeats the point of making login easier and more secure. If Microsoft fixed the LastPass or any third party storage of passkeys, this would have really great adoption in my opinion, especially if the password managers are managed and compliant with company policies.

Love the show, I look forward to it every week! Thanks, Eric

So that's really interesting. As Leo noted last week, his experience with Passkeys is entirely different because he's able to store his Passkeys in Bitwarden that's able to perform the required cryptographic operations on behalf of its user – so the entire process is smooth and seamless.

But our listener Eric notes that Microsoft refuses to work with password managers, at least with LastPass. One of the things we learned way back at the dawn of all this, was that the FIDO2 specification for Passkeys allowed sites to determine the nature of the authenticator being used and could refuse to accept what they might feel is insufficiently secure. And that appears to be what's going on with Eric's observation. At this time, Entra ID and Azure ID do not accept browser-based Passkeys authentication.

Andrew Ayre in Perth, Western Australia raises a very interesting question:

Hi Steve, I thought you and your listeners might find the following helpful...

My son has a PC which is (only) 3 years old running Windows 10. Windows 10 said that the PC does not meet the minimum hardware requirements. After a bit of digging it appears that the reason was that TMP 2.0 could not be found.

I used ChatGPT to find the Windows command to identify the motherboard. Then I asked ChatGPT if that motherboard did have a TPM 2.0. Which it replied "Yes". After more ChatGPT'ing and frowning, to my relief, I was able to discover that a BIOS update would likely make TMP 2.0 appear to Windows. I asked ChaGPT how to upgrade the BIOS (upgrading the BIOS on some gaming machines is not that simple), and it diligently provided all the steps for the motherboard in question.

The PC then qualified for a Windows 11 upgrade and was upgraded successfully.

This begs the question, how many PCs around the world are perfectly good and will end up as e-waste and will never be upgraded to Windows 11 simply because of an older BIOS, or an incorrect BIOS setting?

ChatGPT saved me hours. I thought other listeners may find this experience useful.

Andrew's observation is extremely useful. TPM provisioning can be through either a discrete chip on the motherboard or via the motherboard's own firmware. In the case that Andrew cited, his son's relatively new (only 3-year old) gaming PC was using a firmware based TPM... and since its initial release when that motherboard's firmware was set, newer firmware was released which happily included the TPM 2.0 API. So this is a **very** important observation. Thank you Andrew!

Google's Developer Registration Decree

I encountered a posting over at F-Droid.org that I wanted to share because I thought it was so well conceived and heartfelt. It was written by a well-known developer of a system called "SkipTools" which enables the creation of native SwiftUI apps for iOS and Android. Here's what Marc wrote:

For the past 15 years, F-Droid has provided a safe and secure haven for Android users around the world to find and install free and open source apps. When contrasted with the commercial app stores — of which the Google Play store is the most prominent — the differences are stark: they are hotbeds of spyware and scams, blatantly promoting apps that prey on their users through attempts to monetize their attention and mine their intimate information through any means necessary, including trickery and dark patterns.

F-Droid is different. It distributes apps that have been validated to work for the user's interests, rather than for the interests of the app's distributors. The way F-Droid works is simple: when a developer creates an app and hosts the source code publicly somewhere, the F-Droid team reviews it, inspecting it to ensure that it is completely open source and contains no undocumented anti-features such as advertisements or trackers. Once it passes inspection, the F-Droid build service compiles and packages the app to make it ready for distribution. The package is then signed either with F-Droid's cryptographic key, or, if the build is reproducible, enables distribution using the original developer's private key. In this way, users can trust that any app distributed through F-Droid is the one that was built from the specified source code and has not been tampered with.

Do you want a weather app that doesn't transmit your every movement to a shadowy data broker? Or a scheduling assistant that doesn't siphon your intimate details into an advertisement network? F-Droid has your back. Just as sunlight is the best disinfectant against corruption, open source is the best defense against software acting against the interests of the user.

The future of this elegant and proven system was put in jeopardy last month, when Google unilaterally decreed that Android developers everywhere in the world are going to be required to register centrally with Google. In addition to demanding payment of a registration fee and agreement to their (non-negotiable and ever-changing) terms and conditions, Google will also require the uploading of personally identifying documents, including government ID, by the authors of the software, as well as enumerating all the unique "application identifiers" for every app that is to be distributed by the registered developer.

The F-Droid project cannot require that developers register their apps through Google, but at the same time, we cannot "take over" the application identifiers for the open-source apps we distribute, as that would effectively seize exclusive distribution rights to those applications.

If it were to be put into effect, the developer registration decree will end the F-Droid project and other free/open-source app distribution sources as we know them today, and the world will be deprived of the safety and security of the catalog of thousands of apps that can be trusted and verified by any and all. F-Droid's myriad users will be left adrift, with no means to install — or even update their existing installed — applications.

(How many F-Droid users are there, exactly? We don't know, because we don't track users or have any registration: "No user accounts, by design")

While directly installing — or "sideloading" — software can be construed as carrying some inherent risk, it is false to claim that centralized app stores are the only safe option for software distribution. Google Play itself has repeatedly hosted malware, proving that corporate gatekeeping doesn't guarantee user protection. By contrast, F-Droid offers a trustworthy and transparent alternative approach to security: every app is free and open source, the code can be audited by anyone, the build process and logs are public, and reproducible builds ensure that what is published matches the source code exactly. This transparency and accountability provides a stronger basis for trust than closed platforms, while still giving users freedom to choose. Restricting direct app installation not only undermines that choice, it also erodes the diversity and resilience of the open-source ecosystem by consolidating control in the hands of a few corporate players.

Furthermore, Google's framing that they need to mandate developer registration in order to defend against malware is disingenuous because they already have a remediation mechanism for malware they identify on a device: the Play Protect service that is enabled on all Android Certified devices already scans and disables apps that have been identified as malware, regardless of their provenience. Any perceived risks associated with direct app installation can be mitigated through user education, open-source transparency, and existing security measures without imposing exclusionary registration requirements.

We do not believe that developer registration is motivated by security. *We believe it is about consolidating power and tightening control over a formerly open ecosystem.*

If you own a computer, you should have the right to run whatever programs you want on it. This is just as true with the apps on your Android or iPhone mobile device as it is with the applications on your Linux/Mac/Windows desktop or server. Forcing software creators into a centralized registration scheme in order to publish and distribute their works is as egregious as forcing writers and artists to register with a central authority in order to be able to distribute their creative works. It is an offense to the core principles of free speech and thought that are central to the workings of democratic societies around the world.

By tying application identifiers to personal ID checks and fees, Google is building a choke point that restricts competition and limits user freedom. We must find a solution which preserves user rights, freedom of choice, and a healthy, competitive ecosystem. What do we propose?

Regulatory and competition authorities should look carefully at Google's proposed activities, and ensure that policies designed to improve security are not abused to consolidate monopoly control. We urge regulators to safeguard the ability of alternative app stores and open-source projects to operate freely, and to protect developers who cannot or will not comply with exclusionary registration schemes and demands for personal information.

If you are a developer or user who values digital freedom, you can help. Write to your Member of Parliament, Congressperson or other representative, sign petitions in defense of sideloading and software freedom, and contact the European Commission's Digital Markets Act (DMA) team to express why preserving open distribution matters. By making your voice heard, you help defend not only F-Droid, but the principle that software should remain a commons, accessible and free from unnecessary corporate gatekeeping.

As with any high-quality dispute where both sides are engaged in a good faith, it's possible to empathize with each side of the argument. We absolutely know that malware is a problem on the Android platform. We also know that Google's Play Store is a sewer of shenanigans. We've covered many of them in the past. So it's understandable for Google to wish to somehow get a handle on the mess that has evolved from their original good intentions. And I would bet that there are those inside Google who are no more happy with this decision than the author of this F-Droid piece.

For one thing, Google is dramatically changing the game in what amounts to a bait-and-switch tactic. The requirement to completely deanonymize all Android developers is doubtless a big deal. But so much real damage is done through the abuse of the absolute freedom of anonymity that holding developers accountable for the actions of their code would likely go a long way toward cleaning up the mess that the Play Store has become.

And then there's the requirement of a developer fee to register. I suppose I can understand Google feeling that they have the right to cover their registration costs – although Google doesn't need the money. But obtaining payment from someone creates another barrier to malicious registrations.

It's also worth noting that Google's Play store is currently home to over 2 million apps. Let me say that again: 2 MILLION APPS. I have no right to judge. But does anyone really believe that more than a tiny fraction of those 2 million apps could possibly be useful? One thing seems sure, which is that this move by Google will change the nature of the Play Store. And it sounds as though it may spell the end of F-Droid unless they're able to work around the limitations.

Marc wrote:

> *The F-Droid project cannot require that developers register their apps through Google, but at the same time, we cannot "take over" the application identifiers for the open-source apps we distribute, as that would effectively seize exclusive distribution rights to those applications.*

I certainly get it that F-Droid would not choose or wish to "take over" the application identifiers for the open-source apps they distribute, but that may be the solution assuming that Google allows them to do that. Given what Marc wrote, F-Droid is already fully, deeply and thoroughly inspecting and vetting any app that they distribute. So they should not have any trouble signing the result with their developer ID.

And if F-Droid became the sanctuary for all those legitimate Play Store developers who do not wish to reveal themselves to Google, then that could be good for F-Droid, too. Though the tsunami of developer submissions might be a lot to handle.

I wanted to finish with a pair of posts I found over on YCombinator. The first is in reply to Marc's F-Droid post:

> *I contacted the European Commission DMA team on this gross abuse of power (Google just followed Apple in this regard, who reacted to the DMA by coming out with this notarization of developers), here is their flacky answer:*

Dear citizen,

Thank you for contacting us and sharing your concerns regarding the impact of Google's plans to introduce a developer verification process on Android. We appreciate that you have chosen to contact us, as we welcome feedback from interested parties.

As you may be aware, the Digital Markets Act ('DMA') obliges gatekeepers like Google to effectively allow the distribution of apps on their operating system through third party app stores or the web. At the same time, the DMA also permits Google to introduce strictly necessary and proportionate measures to ensure that third-party software apps or app stores do not endanger the integrity of the hardware or operating system or to enable end users to effectively protect security.

We have taken note of your concerns and, while we cannot comment on ongoing dialogue with gatekeepers, these considerations will form part of our assessment going forward.

Kind regards, The DMA Team.

The DMA is in fact cementing their duopoly power, the opposite of the objective of the law.

In reply to this, Marc wrote:

Post author here. I've also been in various DMA enforcement workshops and consulted with EU regulators on the topic of app distribution. The "strictly necessary and proportionate measures to … not endanger the integrity of the hardware or operating system" defense comes up time and time again, and is clearly a primary talking point for those lobbying against effective enforcement.

From a developer's perspective, this stipulation is obviously intended to ensure that the existing on-device protections (sandboxing, entitlement enforcement, signature checks, etc) are not permitted to be circumvented by third-party app stores. But the anti-DMA brigades have twisted their interpretation to imply that gatekeepers are permitted to ... keep on gatekeeping.

Apple still requires that all software be funneled through its app review (they call it "notarization", but it is the exact same thing as review: developer fees, terms and conditions, arbitrary review delays, blocking apps based on policy, etc.) before it is signed, encrypted, and re-distributed to third party marketplaces like AltStore. And now Google is going to introduce its own new gatekeeping for all software on Android-certified devices, which covers 95%+ of all Android devices outside of China.

The lack of alarm has been, for me, quite alarming. Every piece of software installed on billions of mobile devices around the world is going to be gate-kept by two US companies headquartered 10 miles away from each other and with increasingly authoritarian-friendly leadership.

If you have an Android device, install F-Droid today and let it be known that you won't give up your right to free software without a fight.

I completely understand where Marc is coming from. But the scourge of Internet malware and Internet malconduct is changing the nature of computing. Windows developers need to sign their code to have it pass Windows Defender's "guilty until proven innocent" deletion. The author of Notepad++ discovered this when he attempted to push an unsigned update. It did not go well. And code signing certificates do not come cheap. Fortunately, Microsoft no longer gives EV code signing certs any extra beneficial treatment so my next certificate will be much less expensive. But "not free" means that it's becoming much more difficult for freeware authors who just want to contribute to the community to do so.

Unfortunately, to me all of this change, which is taking us in the direction of having less freedom, feels inevitable. I feel as though the handwriting has been on the wall for some time. I believe that big tech is going to continue exerting its influence toward its own ends and that governments are going to inevitably regulate more and more what can be done on the Internet.

Are these actions by the powerful being taken in response to crime? Or is crime just their excuse? No one will argue against protecting children. But whatever the reason, the outcome is the same. New gates are being erected and with those gates come gatekeepers.

The truth is, the Internet remains an incredible place. It is an incredibly rich asset for anyone who wishes to plumb its depths. And we'll be back here next week to do some more plumbing and discuss what's going on!