Security Now! #1000 - 11-12-24

1000!

This week on Security Now!

Did Bitwarden go closed-source? The rights of German security researchers are clarified. Australia to impose age limits on social media. Free Windows Server 2025 anyone? UAC wasn't in the way enough, so they're fixing that! "From Russia with fines" -- obey or else. South Korea fines Meta over serious user privacy violations. Synology's (very) critical zero-click RCE flaw. Malicious Python packages invoked by typos. Google to enforce full MFA for all cloud service users. Mozilla Foundation lays off 30%? Is Firefox safe? Some feedback from Dave's Garage (https://grc.sc/dave) And thought provoking "Closing The Loop" feedback from our terrific listeners.

What they intended was not what happened

Security News

Is Bitwarden going closed?

For the past few weeks our listeners have been sending me notes regarding their concern that Bitwarden's licensing might be changing to make it less open. It turned out that it was good that I hadn't found the chance to dig into whatever that was about since it appears to have resolved itself. The Register weighed in with an explanation, which I've edited for podcast clarity:

Fear not, FOSS fans. Bitwarden is not going proprietary after all. The company has changed its license terms once again – but this time, it has switched the license of its SDK from its own homegrown license to v3 of the GPL. The move comes just weeks after we reported that it wasn't strictly FOSS any more. At the time, the company claimed this was just a mistake in how it packaged its software, writing on Twitter:

> *It seems that a packaging bug was misunderstood as something more, and the team plans to resolve it. Bitwarden remains committed to the open source licensing model in place for years, along with retaining a fully featured free version for individual users.*

Now it's followed through on this. A GitHub commit entitled "Improve licensing language" changes the licensing on the company's SDK from its own license to the unmodified GPL3.

Previously, if you removed the internal SDK, it was no longer possible to build the publicly available source code without errors. Now the publicly available SDK is GPL3 and you can get and build the whole thing. Chief Technology Officer Kyle Spearrin added a new comment to the discussion on bug #11611 on GitHub, where that Bug was titled: "Desktop version 2024.10.0 is no longer free software." Kyle wrote:

> *We have made some adjustments to how the SDK code is organized and packaged to allow you to build and run the app with only GPL/OSI licenses included. The sdk-internal package references in the clients now come from a new sdk-internal repository, which follows the licensing model we have historically used for all of our clients (see LICENSE_FAQ.md for more info). The sdk-internal reference only uses GPL licenses at this time. If the reference were to include Bitwarden License code in the future, we will provide a way to produce multiple build variants of the client, similar to what we do with web vault client builds.*
>
> *The original SDK repository will be renamed to sdk-secrets, and retains its existing Bitwarden SDK License structure for our Secrets Manager business products. The sdk-secrets repository and packages will no longer be referenced from the client apps, since that code is not used there.*

This is genuinely good news for the program's more fervently FOSS-focused fans. It's all open source, and it's possible to build the whole thing, including the SDK, from freely available code.

It seems to us that Bitwarden has responded to its users' unhappiness with the changes to the licensing around its password manager and has not merely undone the changes but gone further towards making it all Free Software – even if it continues to maintain that it was all just an error. The change is commendable, and we're glad to see it. It does, however, look as if the company is leaving itself room to build more non-FOSS tools in the future.

I think this is a terrific example of community action which helped to bring some clarification to some initial confusion over Bitwarden's licensing terms. And to their credit, as the Register

reported, Bitwarden really stepped up and did the right thing.

Germany clarifies the rights of researchers:
In some good news for German security researchers, the German government has drafted legislation to protect security researchers who discover and report vulnerabilities. The proposed law would eliminate the risk of criminal liability from cybersecurity research as long as bugs are responsibly disclosed to vendors. At the same time, the law does also introduce harsh prison sentences – ranging from 3 months to 5 years – for any researchers who abuse the process of vulnerability research for criminal acts. These include incidents when researchers cause substantial financial damage during their research, extortions, or acts that damage critical infrastructure. In other words, if you're a true researcher in Germany, any previous gray area has been eliminated. But if you're hoping to abuse the "but I'm a security researcher" claim, your inability to get away with that has also been clarified, too.

Australia moves to impose social media lower age limits:
The Australian government is preparing legislation that would introduce a minimum age of 16 years for social media accounts. Under this new legislation – not yet law, just to be clear – access to social media platforms in Australia would be legally restricted to only those 16 years of age or older, and this legislation would hold online platforms accountable for enforcing the ban. Presumably it would also incur meaningful fines for failure to do so under this law. Australia's government plans to introduce the bill in Parliament next week. Government officials explained that they're introducing the bill due to the harm social media is causing for Australian children.

We've talked a lot in the past about the technological challenges associated with filtering access to online services by their accessor's age. How is that done, exactly? And will the legislation somehow put parents in charge? Can parents choose to opt their children out of such filtering? If so, that creates another slippery slope since then one's kids will be saying: "But Mom and Dad! All the other kids' parents let them watch TikTok!" – regardless of the degree of its truth.

But regardless of the legal and social side of this, it seems to me that if we're going to start legislating age-based filtering for Internet services of any kind, the underlying platform itself should be robustly providing this information to any application through a platform-specific API.

At this time, for example, iOS allows granular restrictions of age 4 and above, 9 and above, 12 and above or 17 and above. But there's no 16 and above... so that's kind of a mess. And none of this is automatic. It's up to Mom and Dad to lock down their children's iPhones. Nor does this locked-down setting change automatically. From that point, the device's apps that have previously declared their own appropriate minimum age will be restricted by the phone.

It seems to me that a superior solution would be to allow the parent to set and lock-in the date of birth of the phone's user. Based upon their feelings about the maturity of their child and/or their feelings about the perceived dangers of unrestricted access to social media, they could choose to fudge their child's declared birth year in either direction, as they see fit. So this could be a set-and-forget feature where services would become available on successive birthdays... and at some point it will become accepted that on such-and-such birthday access to this-or-that social media service becomes available.

This is certainly another interesting aspect of today's Internet, the ubiquity of smartphones among minors, and of the platform's willingness to treat them like everyone else.

Free Windows Server upgrade, anyone?
Last Wednesday, The Register posted an interesting piece that I don't recall seeing anywhere else. Their headline was *"Sysadmin shock as Windows Server 2025 installs itself after update labeling error."* And then, being The Register, their tagline on the article was *"Screens sprayed with coffee after techies find Microsoft's latest OS in unexpected places."* With that tease, we need to find out what happened. So, The Register writes:

> *Administrators are reporting unexpected appearances of Windows Server 2025 after what was published as a security update turned out to be a complete operating system upgrade.*

Whoopsie!

> *The problem was flagged by a customer of the web app security company, Heimdal. Arriving at the office on the morning of November 5, they found, to their horror, that every Windows Server 2022 system had either upgraded itself to Windows Server 2025 or was about to.*
>
> *Sysadmins are cautious by nature, so an unplanned operating system upgrade could easily result in morning coffee being sprayed over a keyboard. Heimdal's services include patch management, and it relies on Microsoft to label patches accurately to ensure the correct update is applied to the correct software at the correct time. In this instance, what should have been a security update turned out to be Windows Server 2025.*
>
> *It took Heimdal a while to trace the problem. According to a post on Reddit: "Due to the limited initial footprint, identifying the root cause took some time. By 18:05 UTC, we traced the issue to the Windows Update API, where Microsoft had mistakenly labeled the Windows Server 2025 upgrade as KB5044284. Our team discovered this discrepancy in our patching repository, as the GUID for the Windows Server 2025 upgrade does not match the usual entries for KB5044284 associated with Windows 11. This appears to be an error on Microsoft's side, affecting both the speed of release and the classification of the update. After cross-checking with Microsoft's KnowledgeBase repository, we confirmed that the Knowledge Base number indeed references Windows 11, not Windows Server 2025."*
>
> *The Register has contacted Heimdal for more information and will update this piece should the security organization respond. We also asked Microsoft to comment almost 24 hours ago. Since then? Crickets.*
>
> *As of last night, Heimdal estimated that the unexpected upgrade had affected 7 percent of customers – it said it had blocked KB5044284 across all server group policies. However, this is of little comfort to administrators finding themselves receiving an unexpected upgrade.*
>
> *Since rolling back to the previous configuration will present a challenge, affected users will be faced with finding out just how effective their backup strategy is or paying for the required license and dealing with all the changes that come with Windows Server 2025.*

Yikes! What a mess. I cannot speak for other other admins, but I would be desperately checking that everything was still working after such a jump. If it were, I'd probably choose to remain on that platform after the jump had been made since Microsoft would eventually be forcing that move anyway. But I can definitely empathize with the panic that would ensue.

And in other Windows news...

UAC in Windows 11 gets stronger protection:
We've all come to know UAC – User Account Control. This is Windows' clever and workable solution to the age-old dilemma of users running full "root" privileges on a system just so they are not constantly being told they can't do what they want to do with their own system. The problem with doing this, with running as "root", is that it's their logon account that has the "root" privileges. This means that anything they might inadvertently do, like innocently run some malicious software, inherits their account's root privileges and allows their system to be easily and potentially irreversibly compromised.

So the solution Microsoft evolved was to create split credentials where an administrative user effectively logs on with both standard user and elevated credentials, while always running as a standard user with reduced privileges. This way they're protected from anything that might inadvertently happen. Then, when they try to do something that their lesser privileges doesn't permit, such as installing a new application into the system or disabling some system protections, Windows will pop-up the User Account Control "UAC" prompt which essentially serves as an "Are you sure you want to do this?" confirmation. And when the user sighs and clicks the "Yes, I'm sure I want to do what I just asked for", Windows briefly switches over to their elevated permissions credentials to allow that requested action to be performed.

Okay. So that's the way it's been for many years. But we learned last week that it will be possible to optionally add another layer of security to this existing mechanism. Microsoft wrote:

> *Administrator protection is an upcoming platform security feature in Windows 11, which aims to protect free floating admin rights for administrator users allowing them to still perform all admin functions with just-in-time admin privileges. This feature is off by default and needs to be enabled via group policy. We plan to share more details about this feature at Microsoft Ignite*

The Hacker News further elaborated, and I've edited a bit for the podcast:

> *Microsoft will add a new security system to Windows 11 that will protect admin accounts when they perform highly privileged and sensitive actions. Named "Admin Protection," the system is currently being tested in Windows 11 canary builds. The new feature works by taking all the elevated privileges an admin needs and putting them into a separate super admin account that's—most of the time—disabled and locked away inside the core of the operating system.*
>
> *When users select the "Run as Administrator" option, they will receive a prompt from the Admin Protection feature. The difference from a classic UAC prompt that features "Yes" and "No" buttons is that the Admin Protection features will ask the user to authenticate with a password, PIN, or other form of authentication to continue.*
>
> *But a change in prompting authentication is not the only major change. According to technical and non-technical write-ups from Microsoft MVP Rudy Ooms, who first spotted the feature, Admin Protection is a lot more powerful and innovative than you might expect. It changes how the entire Windows OS assigns admin privileges. In past versions, Windows created two tokens for an admin account, one to use for normal operations and one for when the admin needed to do admin things, with the user switching between the two.*

Unfortunately, this allowed threat actors to develop UAC bypass techniques and abuse admin accounts for malicious purposes.

In other words, UAC – even as intrusive and potentially annoying as it was – was still too easy to use, so it has been abused, too. So Microsoft is going to give it another go and even more robustly lock-up these privileges which are too powerful to allow bad guys and bad'ware to get their hands on. The Hacker News explains:

The new Admin Protection basically locks away all those highly privileged actions into a separate, system-managed account. A threat actor would not be able to switch to that super admin account unless they could now bypass the extra authentication options.

The way this will exactly work in detail is still unknown. Microsoft is set to provide more details about the new Admin Protection feature at its Ignite developer conference later this month, and we hope [writes The Hacker News] that these extra authentication prompts will be able to support some sort of MFA. If they do, threat actors that compromise admin accounts will have a much harder time exploiting those accounts for high-privileged actions.

I suspect that the operational profile of a developer – such as myself – is probably very different from the typical office worker. Even having UAC constantly popping up drives me nuts since I am extremely careful with what I do with my system and I maintain somewhat obsessive management over my machines. So I really don't need Microsoft to protect me from myself.

At the other end of the Windows user spectrum we have someone sitting behind a desk at a large enterprise. They are probably running a fixed set of pre-approved software and logging into a "standard" rather than "admin" account. So they would already need to provide complete administrative credentials if they wanted to change anything in their system.

That suggests that this forthcoming Windows 11 "Admin Protection" feature is intended to better protect everyone else – all of those who have been logging in with admin accounts but for whom the "Are you sure? Yes/No" UAC pop-up has not been providing sufficient protection.

I suppose this is a good thing, at least to offer as an option. But I worry about it being far too obnoxious for those who are "messing around" with their systems. If it could be tied to a quick biometric authentication such as a fingerprint reader to facilitate quick multi-factor authentication then it might be tolerable.

Under the category of "who cares?" ...
Last week we noted that fine-happy Russian courts had levied such insanely large fines against Google, for refusing to allow YouTube to spew Russian media anti-Ukraine propaganda, that not only did their own spokespeople have no idea how to pronounce the number of Russian rubles levied, but the fine far exceeds the total amount of money in the known universe. Moreover, Google Russia, the local Google entity Russia has fined, went belly-up and bankrupt about a year and a half ago. So no assets there, either.

It seems that Russia has not been deterred in the fining department, but they apparently decided that levying a reasonable fine against a going concern might actually produce some cash, if not any change in that entity's behavior.

A Moscow court has fined Apple, Mozilla, and TikTok for failing to remove content the Russian government deems "illegal." Apple was fined for not removing two podcasts, Mozilla for failing to remove some add-ons from its store, and TikTok for failing to remove videos related to the war in Ukraine. The fines range from $35,000 USD to $40,000 USD in Russian rubles. Since fines on that scale fall into the "petty cash" category for those three companies, at least there's something to discuss.

South Korea fines Meta $15.67 million

While we're on the topic of fines, South Korea has fined Meta 21.62 billion won. Although it takes around 1,400 Won to equal one US dollar, when the fine is 21.62 Billion won, that still equals around $15.67 million US dollars. So that's an attention-getting fine that, unlike Russia's fine for Google, South Korea actually expects Meta to pay.

So, what did Meta do to upset South Korea's data privacy watchdog? The fine is for illegally collecting sensitive personal information from Facebook users, including data about their political views and sexual orientation, and ... wait for it ... sharing it with Meta's advertisers without their users' consent.

The country's Personal Information Protection Commission (PIPC) says that Meta gathered information such as religious affiliations, political views, and same-sex marital status of about 980,000 domestic South Korean Facebook users – so just shy of a million – and then shared it with 4,000 advertisers.

The PIPC said in a press statement: *"Specifically, it was found that behavioral information, such as the pages that users 'liked' on Facebook and the ads they clicked on, was analyzed to create and operate advertising topics related to sensitive information."*

The PIPC added that these topics categorized users as following a certain religion, identifying them as a gay or transgender person, or being a defector from North Korea. The agency accused Meta of processing such sensitive information without a proper legal basis, and that it did not seek users' consent before doing so. It also called out the tech giant for failing to enact safety measures to secure inactive accounts, thereby allowing malicious actors to request password resets for those accounts by submitting fake identification information. Meta approved such requests without sufficient verification of the fake IDs, resulting in the leak of the personal information of 10 South Korean users.

PIPC said: *"Going forward, the Personal Information Protection Commission will continue to monitor whether Meta is complying with its corrective order, and will do its best to protect the personal information of our citizens by applying the protection law without discrimination to global companies that provide services to domestic users."*

For their part, in a statement shared with the Associated Press, Meta said that it will "carefully review" the commission's decision... after which it will probably get out its checkbook to pay the fine.

Everywhere we turn it appears that the early freewheeling behavior of unaccountable Internet services is being increasingly brought to heel. If user profiling has been as valuable as advertisers claim, and if this profiling is gradually being squeezed and reduced, that suggests that the economics of online advertising will eventually be changing, too.

Synology's Critical Zero-Click RCE Flaw
My favorite NAS supplier, Synology just patched a critical zero-click zero-authentication flaw that would have created chaos had it been discovered first by bad guys. The flaw affected Synology DiskStation and BeePhotos and could be used for full remote code execution.

It's being tracked as CVE-2024-10443 and has been dubbed "RISK:STATION" by security researcher Rick de Jager of Midnight Blue who successfully demonstrated and exploited the vulnerability at the recent Pwn2Own Ireland 2024 hacking contest. And this one is as bad as they get. "RISK:STATION" is an *"unauthenticated zero-click vulnerability allowing attackers to obtain root-level code execution on the Synology DiskStation and BeeStation NAS devices which would affect millions of devices."* As we know, "zero-click" means full remote takeover without any action needed. We also know that the only way this would be possible would be if Synology Photos for DiskStation or BeePhotos for BeeStation have open and exposed ports to the Internet.

So I'll say it again: It doesn't matter how tempting and cool it might be to have roaming access to your photos and other such features, available to one and all on the Internet. It doesn't matter that it's necessary to login and authenticate to use such a service. Everything we see reinforces the truism that there is no safe way to do that using today's technology no matter how much we wish it were otherwise.

The good news is, this was disclosed during a Pwn2Own competition, so the bad guys have no idea how it was done. And in keeping with the responsible disclosure that's inherent in Pwn2Own, no technical details about the vulnerability have been released. They are currently being withheld to give Synology's customers sufficient time to apply the patches. Midnight Blue said there are between one and two million Synology devices that are currently simultaneously affected and exposed to the Internet.

I just updated my two Synology NASs, which presumably included fixes for this and other lesser problems. But because I would never expose my NAS to the Internet – it's sitting behind the NAT services of a pfSense firewall with UPnP disabled – my NASs were never in danger and I hope and trust that's true for all of our listeners.

It's DEFINITELY far more hassle not to simply be able to open ports and expose services to the Internet ... which is exactly what between one and two million Synology NAS users have apparently done. There **are** ways to safely obtain remote access – for example, I'm a huge fan of port knocking – but such truly secure mechanisms are still not being built into our devices due to programmer hubris which continues to imagine, despite all evidence to the contrary, that the last horrific bug that was just found and fixed will be the last one ever. This all needs to change.

Malicious PyPI package 'Fabrice' found to be stealing AWS keys
Over on the supply-side of attacks, we learn that cybersecurity researchers discovered a nefarious malicious package in the Python Package Index (PyPI) code repository. And get this... This particular Python package called "Fabrice" has been downloaded tens of thousands of times over the past three years of its availability while going undetected as it stealthily exfiltrated developers' Amazon Web Services (AWS) credentials.

The package's name "Fabrice", which sounds like it would be a believable package name on its own, is actually derived from a "typo" of a very popular Python library known as "Fabric." The legitimate Python "Fabric" library is used to execute shell commands remotely over SSH. But any developer who too hastily types "Fabric" into their code might, instead, wind up with "Fabrice" and that's where things will begin to go wrong for them.
Whereas the legitimate "Fabric" package has over 202 million downloads, its malicious typo-

squatting counterpart has been downloaded more than 37,100 times. Since developers trust the well deserved reputation of the "Fabric" library, that's what they assume they're getting, even when they mistype the name and enter "Farbice." Unfortunately, "Fabrice" is then able to exploit the trust that's associated with "Fabric" to incorporate payloads that steal credentials, create backdoors, and execute platform-specific scripts.

"Fabrice" carries out various malicious actions depending upon which operating system it finds itself running in. If it is executed on a Linux machine it will download, decode, and execute four different shell scripts from an external server located at the IP address: 89:44:9:227.

When the same script runs on Windows, two different payloads – a Visual Basic Script named "p.vbs" and a Python script "d.py" will be extracted and executed. The p.vbs script runs the hidden Python script "d.py" which resides in the Downloads folder. This d.py script downloads another malicious executable which it saves as "chome.exe" then sets up a scheduled task to run the EXE every 15 minutes. Once that's been done, the d.py file is deleted.

In any case, regardless of the operating system and the path taken, the common goal is credential theft. AWS access and secret keys are gathered and exfiltrated to the server. By collecting these AWS access keys the opportunistic attacker gains access to potentially sensitive cloud resources. Who knows what developer will run this and what resources might be obtained? Since 2021, when this malicious "Fabrice" library was first dropped into the PyPi repository, 37,100 developers have downloaded it by mistake, thinking they were getting "Fabric". The first time they ran it, their machines were compromised. When they later corrected their typo it was too late. Their development systems were already infected with a Trojan designed to seek out and send out any AWS credentials they might have.

So at this point, from time to time, the attacker's server at 89:44:9:227 simply receives unsolicited AWS credentials. Every time some new one's show up the attackers probably head over to AWS to see what their trap might have snared.

So we have a sophisticated typosquatting attack, crafted to impersonate a trusted library which exploits unsuspecting developers who enter the wrong library name just once. This thing sat undetected for three years and more than 37 thousand downloads before it was finally spotted and removed. Who knows what other similar typo traps are still out there, salted among the thousands of legitimate repository packages?

Google to begin requiring MFA

We've seen this coming for a while, and we're nearing the year 2025, which is the year during which Google has said they are going to be **requiring** all of their cloud services users – which includes all Gmail users – to be authenticating with some form of multi-factor authentication. So more than just their username and password – that will no longer cut it. Google still hasn't provided explicit deadlines, but anyone who doesn't already have MFA setup can expect to start being pushed to do so near the beginning of next year.

And what of Mozilla?

I don't know how to read between the lines of some recent worrying news from The Mozilla Foundation which is the nonprofit arm of Mozilla. The Foundation has just laid off 30% of its employees. This is not Mozilla, but it still makes me nervous since I depend upon Firefox for the web and Thunderbird for email.

The official statements from The Foundation sound like gobbledygook. Get a load of this:

> *<quote> "The Mozilla Foundation is reorganizing teams to increase agility and impact as we accelerate our work to ensure a more open and equitable technical future for us all. That unfortunately means ending some of the work we have historically pursued and eliminating associated roles to bring more focus going forward. Our mission at Mozilla is more high-stakes than ever. We find ourselves in a relentless onslaught of change in the technology (and broader) world, and the idea of putting people before profit feels increasingly radical. Navigating this topsy-turvy, distracting time requires laser focus — and sometimes saying goodbye to the excellent work that has gotten us this far because it won't get us to the next peak. Lofty goals demand hard choices."*

What a bunch of utter nonsense! I fear for our browser. A modern web browser has become a high-security operating system in its own right. It requires a lot of resources to keep it afloat. My machines run much cooler and quieter when I'm not running Chrome.

> **Okay...** That covers the most interesting news of the week. Today is Patch Tuesday so we'll have our typical brief retrospective on that next week. And I was glad that there was not a torrent of news for this ONE THOUSANDTH episode of Security Now! since there's been so much news recently that I've been unable to share the truly great listener feedback we've been receiving. Today we have some time.

SpinRite

Dave's Garage

Dave Plummer was an early Microsoft engineer. Among other things, Dave is credited with creating the original Task Manager for Windows and the Space Cadet Pinball ports for WinNT. He was also the developer who added native ZIP file support to Windows. Today, Dave is best known for his two very popular YouTube channels: "Dave's Garage" and "Dave's Attic". I'm mentioning this today first because Dave puts a lot of effort and energy into the videos he posts to his channel and our listeners might find much there to enjoy. So I created one of GRC's shortcut link to make finding Dave's Garage easy: https://grc.sc/dave

But the main reason I'm mentioning this is that one week ago today, Dave posted his look at SpinRite v6.1. His sub-head was: *"Optimize Your Hard Drive and Extend Data Life - Including SSDs - with SpinRite!"* and his review of SpinRite was so positive that in the metadata info about this video he made his motivation clear by explicitly stating: *"By the way, this is NOT a sponsored episode. I'm just a 30+ year customer and fan of the app!"*

Now, everyone who's been following this podcast already knows everything Dave talks about. We all now know that SSDs are prone to slowing down over time when their data is only ever read and never rewritten, such as the file system's metadata and most of the operating system files, drivers, etc. And early in the work on SpinRite 6.1 we discovered that running a SpinRite Level 3

pass over SSDs that had slowed down over time would restore their original factory performance. So I'm mentioning this due to two viewer comments that were posted to Dave's SpinRite video last week:

@BrentSmithline

> *Have used SpinRite since the early 80's after talking with the head of support at Compaq. He stated that they used SpinRite to test hard drives before they were installed in Compaq devices. The bad ones were weeded out and sent back to the manufacturer so they did not become a support issue at the very start for Compaq.*

I've mentioned this several times through the years, but it was fun to see it independently restated. And it brought to mind a strategy that may still be useful today: One of the things I've noticed while running drives on SpinRite is that the drive's self-reported SMART health parameters will often be pushed downward while SpinRite is running. This is one of the biggest mistakes made by all of the various SMART drive health reporting tools. A drive that's just sitting there idle and doing nothing is always going to be relatively happy because it is not being asked to do any work. And it's not the drive's fault for not reporting anything since it has nothing to report. It's only when the drive is under load – by being asked to read or write data – that it's able to gauge its own ability to actually do so. For the past 35 years this has been one of the fundamental tenets of SpinRite's value: A drive can only determine that it has a problem when it's asked to go out into its media and attempt to read or write those regions. The fact that in a sense it "owns" that media doesn't automatically mean that it knows everything about what's going on out there. It needs to be asked to go take a look. And it turns out, today's SpinRite can still be used much the way COMPAQ once used it, to help qualify the relative integrity of spinning hard drives.

Another interesting comment that was posted there (among 756 other since last Tuesday) was by Seagate's ex Chief Technologist, Robert Thibadeau (@rhtcmu) In addition to being Chief Technologist at Seagate for years, Robert is also one of the six founding directors of Carnegie Mellon University's Robotics Institute from which he resigned in order to guide Seagate's development of, among other things, self-encrypting drives. In response to Dave's SpinRite video Robert posted:

> *As a Chief Technologist for Seagate for years, SpinRite is generally done right. There are some errors in Dave's presentation but they are minor.*
>
> *The biggest thing that needs to be said is that if you wish to retain digital data, plan to keep essential data on multiple drives that do not depend on each other (RAID is not a solution except for transactional data management or in disk duplication mode), and always keep a full dated copy or two air gapped — meaning not connected to anything electrical. Safe deposit boxes are useful for this. And plan to make new copies on new drives every few years.*
>
> *Digital storage devices can fail in more ways than you can count, and the ones that can preserve data for decades are really not commercially available and often give a false sense of security leading to catastrophic data losses. The design life of storage devices is generally 5 years, although it is not unexpected that a given device will preserve storage for 10 plus a few years.*

Knowing what I know, I buy new drives every year or so and make new full copies as well as keeping at least a couple of copies air gapped all the time. Lightning can, and does, strike. Fire (heat) demagnetizes. It is not true that solid state drives are not magnetic and susceptible to failures associated with magnetic field losses.

I appreciated Robert's reminder about the inherent volatility of mass storage. Back when I first designed and wrote SpinRite, 10, 20 or 30 **mega**bytes of spinning hard drive storage cost thousands of dollars. That price dropped rapidly, but it was still uncommon for anyone to own more than their system's single primary mass storage drive. That's why SpinRite's data recovery was designed to work "in place" – because back then, there was nowhere else for recovered data to go. That's one of the many things I'm very excited to be changing as SpinRite continues to evolve in the future. And thanks to the ongoing support from this podcast's listeners, the greater SpinRite community, and independent influencers and reviews like Dave Plummer, it appears that SpinRite will have a bright future. Nothing could make me happier because there's truly nothing I will enjoy more than continuing to work on SpinRite to move its code forward.

But I just wanted to mention that I'm always nervous when I get the sense that people are carrying around single copies of important data on today's thumb drives or external drives, in their laptops or desktops where there may not be any other copy of that data. Drives are certainly getting more reliable as time goes on. But there's also a danger in that since, as Robert reminds us, lightning does still strike. So the fact that drives are generally **not** dying left and right can lull us into the false sense of security of believing they never will. With today's data storage being **so** economical, it might pay off to take some time to make backups automatic and transparent.

And automatic is the key here and the main point I wanted to make: Everyone is busy. We get distracted. We naturally forget to do things that don't call for our attention. That's why it really makes sense to find some time to arrange to have the data you care about kept safe **for** you without you needing to remember to do anything at all. These days, with storage being so inexpensive that doesn't have to be expensive. The best case is that nothing bad will ever happen and that system will never be needed. But even then, the peace of mind that buys, of knowing that the system you put in place will have your back, is worth the time and trouble.

GRC Email

I mentioned last week that my mailing system's "instant unsubscribe" feature had turned out to be a bit too "instant" since many of our listeners were being repeatedly silently unsubscribed from the Security Now! mailing list. The trouble was caused by some email providers – and this is a known issue I had never encountered – attempt to protect their listeners from malicious links in email by following those links, pulling up the content they point to, and checking them for any sort of malicious content. It's not a bad idea, though it certainly does make email a lot more trackable, since many savvy users will deliberately **not** click anything in spam they receive as a means of remaining invisible. So that must have been a trade-off that these providers decided was worthwhile. In any event, the system I had in place until last week would assume that requesting the content behind the "instant unsubscribe" link was the user clicking it, so it would do as requested and instantly unsubscribe its user.

I want to affirm that I did, in fact, change the way the system functions so that that links now display an unsubscribe confirmation page. That means that one additional click of a "Yes I'm sure" button will be required. But in return everyone should now remain properly subscribed.

So, if you were not among the 12,643 listeners who received today's podcast's topic summary, picture of the week and show notes link in an early morning email, you may now re-subscribe to GRC's Security Now! mailing list by going to https://www.grc.com/mail.htm and subscribing. From now on all subscriptions should be "sticky" and remain in place until and unless you choose to later unsubscribe.

Closing The Loop

Paul Walker asked:

Hi Steve, Just listening to episode 999 and your piece about using AI to find/fix/prevent security vulnerabilities. I'm sure you're right, it'll be a great tool for developers. But I wonder if it'll just become the next arms race in the field? Could bad actors deploy AI similarly to find vulnerabilities, and all we're going to end up doing is raising the bar of complexity, picking off more of the lower hanging fruit as the vulnerabilities just become more obscure and harder to find by humans? Is there even a danger that a bad actor wielding AI might have an advantage for a while as they turn this new generation of powerful bug hunting tools loose on all the old (current) software that's already out there? Don't get me wrong, it should be a good thing (assuming the overall balance of power between good and bad doesn't shift too far the wrong way) but I fear your hope for a world of "no vulnerabilities" still isn't much closer.

Congratulations on reaching 999 and thank you for going past it - here's to the next thousand episodes! Thanks, Paul

Yes. I've had the same thought. I agree that AI could just as easily be used to design exploits for the vulnerabilities that already exist or that will exist. And I also agree that the inertia lag and upgrade friction we see throughout our industry is likely to mean that malicious AI will initially find itself in a target-rich environment.

So, yes, I agree 100% that things may get rough during the phase where AI is newly being deployed by both sides. However, there **is** an important lack of symmetry here. The good guys will have an advantage because no malicious AI, no matter how good it is, will be able to create vulnerabilities out of thin air. All a malicious AI can do is find problems that exist – it cannot create new ones. So once the good guys have their AIs working to starve the bad AIs of any new vulnerabilities to discover and exploit, the game will no longer be an arms race. There **will** be a winner and that winner will be the good guys.

And speaking of AIs...

Mathieu from Montréal, Canada:

Hi Steve, I might not be the first person to share this snippet of code with you, but I thought you'd find it useful!

I asked ChatGPT how to remove YouTube Shorts. Initially, it suggested plugins, but since I

have security concerns about plugins, I asked it again—this time specifying that I wanted a solution using only uBlock Origin. Here's the solution it provided, and it works great:

Steps to Remove YouTube Shorts with uBlock Origin

1. ***Access uBlock Origin's Dashboard**:*
   - *Click on the uBlock Origin icon in your browser's toolbar.*
   - *Click the "Dashboard" (gear icon) to open the settings.*
2. ***Add Custom Filters**:*
   - *Navigate to the "My filters" tab.*
   - *Paste the following filters to hide various instances of YouTube Shorts:*

! Hide Shorts shelf on the homepage
youtube.com##ytd-rich-section-renderer:has(#title-text:has-text(Shorts))

! Hide Shorts from the sidebar menu
youtube.com##ytd-guide-entry-renderer:has-text(Shorts)

! Hide Shorts from the subscriptions feed
youtube.com##ytd-grid-video-renderer:has(a[href^="/shorts/"])

3. ***Apply Changes**:*
   - *Click "Apply changes" to save the filters.*

This approach has worked perfectly for me, and I thought you might find it handy too. Let me know if you try it out! Best regards, Mathieu (from Montréal, Canada)

Mathieu from Montreal found that this worked for him. But a listener named Darrell, a man of few words, just sent a link to a Github page: https://github.com/gijsdev/ublock-hide-yt-shorts So I followed that link and was taken to a page that said:

A uBlock Origin filter list to hide all traces of YouTube shorts videos. This filter list might work with other content blockers, but I haven't looked into that (yet). Copy the link below, go to uBlock Origin > Dashboard > Filters and paste the link underneath the 'Import...' heading:
https://raw.githubusercontent.com/gijsdev/ublock-hide-yt-shorts/master/list.txt

I used WGET to grab the LIST.TXT file referred to in that link. It's an EXTREMELY comprehensive, well-commented, 71-line filter. I'd be quite surprised if anything resembling a YouTube Short was able to squeak though that gauntlet. Then I discovered where Darell found this Github link. He sent me another piece of email with a link to piece on Medium where a software developer explains:

As a software engineer, I typically spend 8 to 10 hours daily on my laptop. Following that, I frequently indulge in YouTube shorts, which, combined with my extensive screen time, has started to negatively impact my eyesight. Despite recognizing this, I found myself too addicted to simply stop.

Hence, I decided it would be better not to see any shorts on YouTube at all. That's when I discovered my savior, uBlock Origin. uBlock Origin is a Chrome extension that not only blocks ads on YouTube but can also stop YouTube shorts, which I hope, in turn, will save me more time. Here are the steps to follow:

https://medium.com/@yaduvanshiharsh15/reclaim-your-time-how-to-stop-youtube-shorts-with-ublock-origin-ed74af6560b1

Well, it turns out that this software engineer is also not the originator of this filter list. At the end of his Medium posting he links to the YouTube video where he presumably learned about uBlock Origin and found this filter.

So we've confirmed my suspicion from last week that uBlock Origin all by itself, which can obviously function as a Swiss Army Knife for web content filtering, could probably nip this YouTube Shorts problem in the bud without the need for any sort of possibly sketchy additional web browser add-on. But I was still unclear about what all of the hullabaloo was over this so-called *"YouTube Shorts **problem**"*. What's the problem exactly? Why are people creating web browser extensions to hide these? So I followed this software engineer's link to the YouTube video where "Chris Titus Tech" tells us how to do this. I did not watch Chris' video, but some of the – I kid you not – 8,423 comments that have been posted to his explainer over the past 10 months since he posted this video (1.6 million views later) were quite illuminating. Here's a sampling: (https://youtu.be/Nfr0uIU2lDI)

- The fact that people want to disable shorts and there are developers that create these amazing tools really goes to show how crap shorts really are.

- What's wrong is YouTube themselves keep pushing shorts on people, it's a form of spam, and should be something you can opt out of. Unfortunately opting out doesn't work within the YouTube platform. I hate shorts and hate the way Youtube is going.

- Thank you for the tip. It is a lifesaver. YouTube shorts are cancer.

- Alternate title: "How to cure YouTube's cancer"

- My child can't stop himself once he starts watching them (I have to step in). He even tells me he wants to stop watching shorts but "can't", which is terrifying. Knowing this will make a huge difference in our lives. Thank you!

- Dude I literally cannot thank you enough for this. I'm currently trying to really focus on my studies but shorts have been my DOWNFALL literally. I just get so addicted to it and I feel like I physically can't stop. Once I realize how much time I wasted doing NOTHING, I feel empty and dumb inside. SO glad this is a thing, and it works great. You're a lifesaver, thank you so much.

- Could you please make a shorter version of your video?

Okay, I confess that I made up that last one asking to have him make a shorter video. But, wow! Whatever this is, it really appears to have people in its grasp. It's somewhat astonishing. But

these reactions to the posting of Chris' extremely comprehensive YouTube Shorts content blocking filter list for uBlock Origin answers the question of why anyone would want to remove these from their browser – and also apparently from their life.

Tom Damon:

> *Steve, I ran into this on Linked in about last week's photo of the week. Just thought I would let you know. "Here's How A Bunch Of Firemen Created A Viral Image That Fooled The Internet" - Business Insider. Thanks, been listening since episode 1 Tom Damon*

Tom's referring to the week before last's photo for episode #998. That was the insane one showing the fire truck's hose crossing the train tracks while being protected by tire protectors, as if that would do what was intended for the wheels of a train.

Tom linked to an article in Business Insider. Unfortunately, it was behind a paywall which placed a firm pop-up in my face and refused to allow me to proceed. But I was quite curious to see what Tom had seen. So, once again, uBlock Origin to the rescue. I simply disabled JavaScript for the site, refreshed the page and no more pop-up blocking the page's content.

Business Insider wrote:

> *If you spent any time on the internet over the last few months, there's a chance you saw a photo of firemen who had found a fool-proof way to lay a hose over train tracks. The photo went viral, being shared all over Twitter and Facebook. Insane, right? Not quite. The photo was actually a joke. Firefighter Tom Bongaerts from Belgium took the photo at the beginning of April, posting it to Facebook: The caption says something like: "Fire early this morning. Our hoses are still protected from the train!"*
>
> *But that track was down that week for repairs. Those in town — presumably Tom's Facebook friends — knew that the photo was created and posted for laughs. There was no chance a train would be coming. But soon, hundreds of people were sharing the photo on Facebook, adding their own commentary. People who didn't know Tom or about the defunct train track began to see the photo, and, in disbelief, share the photo themselves. After his picture was shared hundreds of times, it eventually became separated from its original source and its sarcastic caption.*
>
> *People believed it was real. Stories — like the one about how a train derailed — began going viral as well. Several days later, after tons of tweets, shares, and email forwards in lots of languages, Tom wrote a follow up post explaining what happened:*
>
> *It says: Hey, this past week our funny photo went viral throughout the whole world. Thousands of shares and likes in many different countries! Once and for all: The picture was taken in Belgium, in a small village called Bornem. After a minor intervention, we had some time left near the railway to make this picture. Since there were no trains running at all for a week due to maintenance works, we can state that our joke was a real success!*

So a big "thank you" to our own Tom, our listener Tom Damon, for resolving this mystery for us. It's good to know that those fire fighters were aware that either their scheme would not actually survive a train... or that any passing train might not survive their scheme. (Opinions among our

listeners who sent feedback about that photo differed widely about what might transpire if the integrity of that crossing hose solution were to be tested.)

Paul Northrup:

Dear Steve, In regards to the new DNS Benchmark offering: Will there be versions for other operating systems? Apple, Linux, BSD? Thanks!

15 years ago when I first wrote the DNS Benchmark I took pains to make sure it would run under WINE, and it does, beautifully. So I'll definitely be preserving that and anywhere WINE can be used the DNS Benchmark will run... and as it turns out all three of those non-Windows OSes – Apple, Linux and BSD – are POSIX-compliant and can run WINE. So while it won't run natively, it will be possible to run it on any of those platforms.

Jim Riley poses an interesting question:

Hi Steve, Thank you for being here for Security Now every week — you and Leo make a great podcast. I have a question about A.I. which is a bit philosophical. A comparison of answers between Gemini, ChatGPT, and Copilot shows the systems can disagree on basic facts such as who won the 2020 presidential election. Gemini refuses to answer the question. This sounds like "Big Brother" and Google has anointed itself the "Ministry of Truth", deciding what facts it will suppress or reveal. Having our access to knowledge regulated by corporate overseers is disturbing. How can A.I. be trusted if it withholds facts? Do you think a control system should be installed in A.I. that will prohibit A.I. from withholding the truth? Regards, Jim

This is an aspect of AI that I suspect is going to be a real issue. My wife and I have grown to know the neighboring couples within our little community enclave quite well. Lorrie enjoys socializing and since she lets me work every other minute of the day, I'm happy to join in. What I know, because I've grown to know our neighbors, is that I could ask each couple the same question and obtain a different answer from each – sometimes radically different answers. And their intelligence is not artificial – though in some cases it may be questionable.

So I suspect we may be asking a lot of AI for it to be some sort of absolute oracle and truth teller. And moreover, the truest answer may not be a simple binary yes or no, true or false. I believe in the fundamental rationality of the universe, so I believe that there is "an absolute truth." But I've also observed that such absolute truth is often extremely complex and colored by subtlety. Many people just want a simple answer, even when no simple answer can also be completely true. In other words, they will choose simplicity over truth.

Having come to know our neighbors I have also come to understand their various perspectives. So when they share what they believe I'm able to filter that through who I know them to be. I know we would like things to be easier and more straightforward with AI, but I see no reason why it might be so. Whether we like it or not, what we've going to get from AI will just be another opinion.

John Torrisi

Hi Steve, As someone who's been in security for over 20 years I have found myself constantly overthinking anything that would result in lowering security which could lead to a breach or

intrusion. As a keen home automation tinkerer I have numerous devices (prob >100) at home for controlling everything from lights to fans to monitoring solar etc etc. (all partitioned off of course with VLANS / multiple firewalls, separate SSID etc.)

One of my biggest conundrums though is how do I expose the controller (for example Home Assistant) to the internet so i can access it when traveling around. I have a fixed IP so that's fine, but I really don't like exposing this type of software directly to the Internet. At the moment I connect in using OpenVPN. That's fine, but this means I need to turn it on and off every time I want to do something, which is a pain. I have also thought about an overlay network but need to research a bit more on data usage as it will be used primarily from a mobile device and hence limited data.

Anyway, going back to the main thread, I know security by obscurity can be somewhat effective in a layered approach, so what are your thoughts on using an IPV6 address rather than IPV4 for inbound traffic in these scenarios as it's much harder to do full network scans across the IPv6, address space compared to IPv4.

Long time listener and Spinrite owner from Australia - keep up all the great work you, Leo and all the team do over there at Twit. Thanks, John

The problem John has is a problem many people are having. This is why those 1 to 2 million Synology Photo sharing services are exposed and vulnerable. No one appears to have created a solid solution for this because developers keep believing that they've just found and fixed the last problem they're ever going to encounter. What we still need is a clean and efficient means for remotely accessing the devices within our networks at home.

So John's wondering about the security of hiding his devices within the larger 128-bit address space afforded by IPv6. He clearly understands that such a solution is only offering obscurity at best. So I suppose I'd say that doing that would be better than doing nothing. But that also requires IPv6 addressing support at both ends. And the trouble is that it's not as if he gets to pick any 128-bit address at random from all possible 128-bit addresses. ISPs are allocated well-known blocks of IPv6 address space and they generously hand out smaller blocks of 64K (16-bits) of IPv6 addresses per subscriber. So it would be possible for bad guys to target any ISP's range of addresses and scan across that space. Given the scanning power of today's botnets, discovering open ports located within an ISP's assigned IPv6 space would not be prohibitively difficult.

John mentioned the use of an overlay network such as TailScale, ZeroTier or Nebula. I think those solutions are about as close to the perfect user-friendly solution as exists today. They all support all major desktop and mobile platforms as well as popular open-source routing software such as pfSense and OPNsense. So an instance could be installed in an edge router to provide extremely secure connectivity to any roaming devices. Or if you prefer, Docker can be used to install, for example, ZeroTier on a Synology NAS. Once you have an instance of one of these terrific solutions running on something at home you can have secure connectivity to that network from any roaming laptop or smartphone. And there's no indication of excess network bandwidth consumption since all of these solutions are economical in their overhead.

Alan:

Steve, Congratulations on 1000 episodes of Security Now.

I listened to the first episode during my first year of college for Computer Science, while donating blood plasma for money to buy a second monitor. Now, I am a Senior Software Engineer at Google where I have been for 9 years. I have listened to every episode within the week it came out. Your podcast was at least as useful to my understanding as my bachelors degree, and in many cases your early podcasts helped me understand that material in my classes much more deeply. Thank you for all your years making Security Now. -Alan

To Alan and to all of our many listeners who have recently written something similar, I wanted to say, as we conclude this 1000th episode of Security Now! that providing this weekly podcast with Leo has been and I'm sure shall continue to be my sincere pleasure. As I've said before, I'm both humbled by and proud of the incredible listenership this podcast has developed over the years. It has been one of the major features of my life and I'm so glad that Leo thought to ask me, 20 years ago, whether I might be interested in spending around 20 minutes a week to discuss various topics of Internet security. Just look what happened!

So thank YOU, Leo, for making this possible!

Let's see where the next 1000 take us!