Security Now! #1038 - 08-12-25

Perplexity's Duplicity

This week on Security Now!

• CISA's Emergency Directive to ALL Federal agencies re: SharePoint. • NVIDIA firmly says "no" to any embedded chip gimmicks. • Dashlane is terminating its (totally unusable) free tier. • Malicious repository libraries are becoming even more hostile. • The best web filter (uBlock Origin) comes to Safari. • The very popular SonicWall firewall is being compromised. • More than 100 models of Dell Latitude and Precision laptops are in danger. • The significant challenge of patching SharePoint (for example). • A quick look at my DNS Benchmark progress. • Does InControl prevent an important update? • A venerable Sci-Fi franchise may be getting a great new series! • What to do about the problem of AI "website sucking"?

The latest solution for controlling the high cost of healthcare:

(Sometimes the best solutions are the most obvious.)

Security News

CISA *"ED 25-02: Mitigate Microsoft Exchange Vulnerability"*

Last Thursday the 7th CISA issued a rare emergency directive ordering all federal agencies to patch a new attack vector in Microsoft Exchange email servers — and giving them just four days (which included the two days of this past weekend) in which to do so.

So let's first step back for a moment and examine CISA's authority to compel the actions of federal agencies. That authority does exist and it comes from section 3553(h) of title 44 of the U.S. Code, which <quote>:

> *Authorizes the Secretary of Homeland Security, in response to a known or reasonably suspected information security threat, vulnerability, or incident that represents a substantial threat to the information security of an agency, to "issue an emergency directive to the head of an agency to take any lawful action with respect to the operation of the information system, including such systems used or operated by another entity on behalf of an agency, that collects, processes, stores, transmits, disseminates, or otherwise maintains agency information, for the purpose of protecting the information system from, or mitigating, an information security threat."*

The CISA emergency directive explains what's going on, writing:

> *CISA is aware of a post-authentication vulnerability (CVE-2025-53786) in Microsoft Exchange hybrid-joined configurations that allows an attacker to move laterally from on-premises Exchange to the M365 cloud environment.* ***This vulnerability poses grave risk to all organizations operating Microsoft Exchange hybrid-joined configurations that have not yet followed the April 2025 patch guidance and immediate mitigation is critical.*** *Although exploitation of this vulnerability is only possible after an attacker establishes administrative access on the on-premises Exchange server, CISA is deeply concerned at the ease with which a threat actor could escalate privileges and gain significant control of a victim's M365 Exchange Online environment.*

The emergency directive issued last Thursday then begins with *"By 9:00 AM EDT on Monday, August 11, 2025,* ***ALL*** *agencies must:"* And then it proceeds to enumerate a rather long list of steps that must be taken and reported back to CISA upon their completion.

This all surrounds an Exchange Server design flaw which affects hybrid on-prem/cloud environments where Exchange on-premise servers sync data to an Exchange Online instance. Microsoft explained that in old default setups, on-prem servers share the authentication service (known as the Service Principal) with the synced online instance. When deployed for the first time, default hybrid installations will upload the on-prem authentication certificates to this Service Principal to allow local instances to authenticate on the Exchange Online server and sync data. The problem arises when attackers compromise an on-prem Exchange server because they can abuse their control over the system to hijack, create, or alter authentication tokens that grant intruders access further up the cloud environment. And, what's more, Microsoft says that this attack scenario does not leave an *"easily detectable and auditable trace"* meaning that this could all be invisible to compromised companies.

Owners of on-prem servers must install the April hotfix that converts the connection between on-prem and online environments into a standalone Entra app. It's then necessary to follow setup instructions that include steps to clean older hybrid auth certs and upload new ones to the

separate Entra hybrid app exclusively, where an attacker's access will be severely limited.

Because this hybrid on-prem-to-online attack is essentially a design flaw, it not only works on Exchange 2016 and Exchange 2019, but also on the latest pay-as-you-go Exchange Server Subscription Edition. Customers of all three versions will have to follow the steps if using a hybrid configuration.

What this means for any of our listeners who may not be within federal agencies but may still be responsible for their enterprise's hybrid on-premises / cloud Exchange Server setup, is that all of this must be done to be secure. For anyone needing more information, I have links to CISA's directive and to Microsoft's disclosure in the show notes:

(https://www.cisa.gov/news-events/directives/ed-25-02-mitigate-microsoft-exchange-vulnerability) (https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53786)

NVIDIA firmly says "no" to any embedded chip gimmicks

Various news outlets have reported that US officials have been exploring the idea of mandating that Nvidia include killswitches, backdoors, and location-tracking tech in its chips to prevent products from reaching adversaries like China. This pushing and its rumors – which would clearly have a negative impact upon Nvidia's sales – led Nvidia to make the following formal statement for the record. Last week they posted under the title *"No Backdoors. No Kill Switches. No Spyware."* the following:

NVIDIA GPUs are at the heart of modern computing. They're used across industries — from healthcare and finance to scientific research, autonomous systems and AI infrastructure. NVIDIA GPUs are embedded into CT scanners and MRI machines, DNA sequencers, air-traffic radar tracking systems, city traffic-management systems, self-driving cars, supercomputers, TV broadcasting systems, casino machines and game consoles.

To mitigate the risk of misuse, some pundits and policymakers propose requiring hardware "kill switches" or built-in controls that can remotely disable GPUs without user knowledge and consent. Some suspect they might already exist.

NVIDIA GPUs do not and should not have kill switches and backdoors. Hard-Coded, Single-Point Controls Are Always a Bad Idea

NVIDIA has been designing processors for over 30 years. Embedding backdoors and kill switches into chips would be a gift to hackers and hostile actors. It would undermine global digital infrastructure and fracture trust in U.S. technology. Established law wisely requires companies to fix vulnerabilities — not create them.

Until recently, that policy was universally held and beyond question. When security researchers discovered vulnerabilities such as "Spectre" and "Meltdown" for CPUs, governments and industry responded with speed and unity to eliminate the risk.

That principle still holds. There is no such thing as a "good" secret backdoor — only dangerous vulnerabilities that need to be eliminated. Product security must always be done the right way: through rigorous internal testing, independent validation and full compliance with global cybersecurity standards. Robust security is built on the principle of "defense in depth": layering multiple safeguards so that no single-point vulnerability can compromise or shut down a system. For decades, that's how NVIDIA and American industry have promoted innovation

while protecting users and growing the economy. This is no time to depart from that winning formula.

The Clipper Chip was a Debacle, a Policy and Technical Failure: The cybersecurity community learned these lessons the hard way during the 1990s with the NSA's Clipper Chip initiative. Introduced in 1993, the Clipper Chip was designed to provide strong encryption while maintaining government backdoor access through a key escrow system.

The Clipper Chip represented everything wrong with built-in backdoors. Security researchers discovered fundamental flaws in the system that could allow malicious parties to tamper with the software. It created centralized vulnerabilities that could be exploited by adversaries. The mere existence of government backdoors undermined user confidence in the security of systems.

Kill switches and built-in backdoors create single points of failure and violate the fundamental principles of cybersecurity. We must promote smart software tools, not dangerous hardware traps. Some point to smartphone features like "find my phone" or "remote wipe" as models for a GPU kill switch. That comparison doesn't hold water — optional software features, controlled by the user, are not hardware backdoors.

NVIDIA has always supported open, transparent software that helps customers get the most from their GPU-powered systems — diagnostics, performance monitoring, bug reporting and timely patching — with the user's knowledge and consent. That's responsible, secure computing. It helps our customers excel, and our industry to stay ahead.

Hardwiring a kill switch into a chip is something entirely different: a permanent flaw beyond user control, and an open invitation for disaster. It's like buying a car where the dealership keeps a remote control for the parking brake — just in case they decide you shouldn't be driving. That's not sound policy. It's an overreaction that would irreparably harm America's economic and national security interests.

Hardware integrity must be nonpartisan and nonnegotiable: For decades, policymakers have championed industry's efforts to create secure, trustworthy hardware. Governments have many tools to protect nations, consumers and the economy. Deliberately weakening critical infrastructure should never be one of them.

There are no back doors in NVIDIA chips. No kill switches. No spyware. That's not how trustworthy systems are built — and never will be.

I'm certain there's no foolproof way to keep politician's hands off of technology. We're seeing this, without any apparent end in sight, in the never ending smartphone encryption battle.

Dashlane terminating its free plan

I was going to mention to our listeners that the Dashlane password manager would be ending their free-tier service, effective September 16th. I figured I'd aim anyone who might be using Dashlane over at either of this network's password manager sponsors, 1Password or Bitwarden.

But then I saw Dashlane boasting that their paid Premium plan would allow for unlimited passwords and passkeys. Which of course caused me to wonder if unlimited passwords and passkeys is the big selling point of Dashlane's Premium plan, what could possibly be the limit they had imposed for their free plan?

Believe it or not, you get all of 25 passwords for free with Dashlane. 25! In the year of our lord 2025 it's not possible to meaningfully use any password manager that imposes any limit – well, okay, unless it's 1,000 – on the number of passwords it will store. Under their "Why upgrade to Premium?" explanation, Dashlane actually says:

- Unlimited passwords and passkeys: Say goodbye to the 25-password limit and start saving ***every*** password and passkey in your encrypted vault. *(How convenient not to need to decide which precious 25 passwords you'll choose to save, and no more needing to delete those lesser-needed passwords out to make room for newer more important ones.)*

- Access to your logins on ***any*** device: Move beyond single-device access and seamlessly sync and access your vault on any device, browser, or operating system. *(More than one device is reserved for premium users? Again, what year do these people think it is?)*

- Real-time phishing protection: Step up your security and stay ahead of AI-powered phishing with real-time alerts that warn you before you autofill your info on a suspicious site. *(Wait, but auto-fill won't work at all on a phishing site. Everyone has that for free.)*

As a consequence of what I have learned, I no longer imagine that any of our users could possibly be using the free Dashlane product, so I see no need to warn of the impending end of their free tier. The other thing I've learned is what a great deal 1Password and Bitwarden offer. Why would anyone be struggling to accommodate a single device with a 25-password limit?

Developers beware (and maintain running versioning backups)
Last Wednesday, Socket Security detailed two particularly nefarious NPM packages they discovered in the NPM repository. They article was titled *"Malicious npm Packages Target WhatsApp Developers with Remote Kill Switch"* with the teaser *"Two npm packages masquerading as WhatsApp developer libraries include a kill switch that deletes all files if the phone number isn't whitelisted."* Here's the top of their posting:

> *Socket's Threat Research Team discovered two malicious npm packages specifically targeting developers building WhatsApp API integrations with a remote-controlled destruction mechanism. Published by npm user nayflore using email idzzcch@gmail.com, both naya-flore and nvlore-hsc masquerade as WhatsApp socket libraries while implementing a phone number-based kill switch that can remotely wipe developers' systems. The packages have accumulated over 1,110 downloads in a month and remain active on the npm registry. We have submitted takedown requests to the npm security team and petitioned for the suspension of the associated account.*
>
> *WhatsApp Business API adoption has surged, with over 200 million businesses now using the platform globally. This growth has created a thriving ecosystem of third-party libraries and tools for WhatsApp automation. Developers regularly install packages like whatsapp-web.js, baileys, and similar libraries to build chatbots, customer service automation, and messaging integrations. The packages published by nayflore exploit this trust by positioning themselves as alternative WhatsApp socket implementations.*
>
> *The malicious packages first retrieve a remote database of phone numbers from a GitHub repository. Both packages use Base64 encoding to obfuscate the endpoint URL:* https://raw[.]githubusercontent[.]com/navaLinh/database/main/seska.json

The Base64 encoding conceals the GitHub endpoint from casual inspection. The database is hosted on GitHub Pages, making it appear legitimate while providing the threat actor with remote control over which phone numbers trigger destruction.

*The malicious kill switch logic is embedded within the **requestPairingCode** function, which developers would naturally call when setting up WhatsApp bot authentication. This function appears legitimate and necessary for WhatsApp integration. When **requestPairingCode** executes, it immediately begins the kill switch process.*

The logic is simple: if the phone number exists in the remote database, the package continues normal operation. If not found, the function sets getsNumberCode to "0000" and executes: `rm -rf *` *, which recursively deletes all files in the current directory. This approach allows the threat actor to maintain a whitelist of "safe" phone numbers while destroying systems for any unlisted numbers.*

The pairKey parameter is particularly clever - it makes the function signature look more authentic for WhatsApp development while having no impact on whether your system gets destroyed. It's a clever social engineering touch to make developers think this is a legitimate WhatsApp pairing function.

*Both packages contain identical **generateCreds** functions capable of exfiltrating device information to https://api[.]verylinh[.]my[.]id/running, but the calls to this function are commented out in both packages. This suggests the threat actor initially planned data collection but simplified the attack to focus purely on destruction. And since the kill switch executes* `rm -rf *` *immediately when a phone number isn't whitelisted, any subsequent exfiltration attempt would fail on the destroyed system. For whitelisted numbers that continue normally, there's no valuable data to steal anyway.*

The presence of complete, functional exfiltration code indicates the threat actor has the infrastructure ready and could easily reactivate data collection in future versions by simply uncommenting the function calls.

Our takeaway here is for all developers to be deadly serious about maintaining some sort of versioning incremental backup system which will not delete any previously backed-up files even in the event that a file is deleted from the backup source.

For many years I was using and loving the free Sync.com encrypted file backup and cross-machine synchronization service. Then they went through a service outage rough patch a couple of years ago. The inconvenience of that was enough to kick me back over to SyncThing. SyncThing is truly terrific, but I haven't been as big a fan of its versioning, whereas Sync.com really has that nailed. Being something of a belt and suspenders guys I'm now using both.

If anyone's interested in looking at Sync.com, you can use my referral code and we each get an extra Gigabyte of storage. That means that you'll start out with 6 gigabytes to play with rather than their 5 gig free plan. The referral code is a GRC shortcut. It's grc.sc/sync.

But in any event, it's very clearly a jungle out there. So if you're a developer who occasionally grabs pre-packaged solution libraries from repositories, do yourself the favor of arranging some bulletproof backup archive. Sync's free 30-day deep complete file versioning has saved my butt a few times. Not because I was infected by anything, but because for one reason or another I needed some from the past.

Malicious Packages:
While we're on the subject, Socket also found 11 malicious Go libraries that download and run malware on infected systems, and GitLab's security team found five malicious PyPI packages targeting the dev ecosystem of the Bittensor cryptowallet.

uBlock Origin Lite – Now available for Safari
I have some happy news, at last, uBlock Origin's stalwart developer, Raymond Hill has just released uBlock Origin Lite for Safari: https://apps.apple.com/us/app/ublock-origin-lite/id6745342698 for the iPad, iPhone and Mac. Since finding things within the Apple App Store has always been mysteriously difficult, I have a link in the show notes for anyone who would like to add what many feel is the best web filtering technology to their Apple Safari browser. The App just appeared in the store, so it only has 84 ratings at the moment, but it's holding a 4.8 out of 5.

SonicWall trouble.
I encountered the following brief news blurb about SonicWall. The news was: *"SonicWall has told owners of Gen 7 firewalls to disable the device's SSLVPN feature due to a security risk. The company says it received reports of attacks against the devices over the past three days from at least three security firms. According to Arctic Wolf, Google Mandiant, and Huntress Labs, attackers hacked SonicWall systems and then deployed ransomware. SonicWall says it's investigating to see if the attacks used older bugs or a new zero-day exploit."*

So first of all, this would/should be terrifying to anyone whose enterprise is behind any late-model SonicWall firewall which offers remote SSLVPN access. Not just one, but three, major high-reputation security firms independently determined that ransomware was being deployed within enterprise networks via an unknown penetration vulnerability in SonicWall's firewall. It doesn't get much worse than that. And, as we know, the idea of a remotely exploitable 0-day vulnerability in an SSL VPN would, sadly, not itself be very surprising since we've seen this many times before. So I went looking for SonicWall's statement about this. Here the clarification they provided:

> *Following our earlier communication, we want to share an important update on our ongoing investigation into the recent cyber activity involving Gen 7 and newer firewalls with SSLVPN enabled.*
>
> *We now have high confidence that the recent SSLVPN activity is not connected to a zero-day vulnerability. Instead, there is a significant correlation with threat activity related to CVE-2024-40766, which was previously disclosed and documented in our public advisory SNWLID-2024- 0015.*
>
> *We are currently investigating fewer than 40 incidents related to this cyber activity. Many of the incidents relate to migrations from Gen 6 to Gen 7 firewalls, where local user passwords were carried over during the migration and not reset. Resetting passwords was a critical step outlined in the original advisory.*
>
> *SonicOS 7.3 has additional protection against brute-force password and MFA attacks. Without these additional protections, password and MFA brute force attacks are more feasible.*

They followed that with their updated guidance, and something there stood out:

To ensure full protection, we strongly urge all customers who have imported configurations from Gen 6 to newer firewalls to take the following steps immediately:

- *Update firmware to version 7.3.0, which includes enhanced protections against brute force attacks and additional MFA controls.*
- *Reset all local user account passwords for any accounts with SSLVPN access, especially if they were carried over during migration from Gen 6 to Gen 7.*
- *Continue applying the previously recommended best practices:*
- *Enable Botnet Protection and Geo-IP Filtering.*
- *Remove unused or inactive user accounts.*
- *Enforce MFA and strong password policies.*

If any local administrator accounts have been compromised through CVE-2024-40766, attackers may exploit administrative features such as packet capture, debugging, logging, configuration backup, or MFA control to obtain additional credentials, monitor traffic, or weaken the overall security posture. It is advisable to review any packet captures, logs, MFA settings, and recent configuration changes for unusual activity, and rotate any credentials that may have been exposed.

We appreciate the continued support from third-party researchers that have helped us throughout this process, including Arctic Wolf, Google Mandiant, Huntress, and Field Effect.

Those of you who have been following along at home may have noticed something in their list of remediation and prevention measures that I don't think we've seen before. Their 4th bullet point was: "*Enable Botnet Protection and Geo-IP Filtering*". And the Geo-IP Filtering phrase is a link. It links to a page describing what they mean by the term. It reads:

Geo-IP Filter allows administrators to block connections coming to or from a geographic location by resolving the Public IP address to a particular country. This feature is usable in two modes, blanket blocking or blocking through firewall access rules.

Blocking through firewall access rules gives a network administrator greater control over what traffic is and isn't scanned by the Geo-IP Filter. This is useful for deployments in which Outbound Traffic may want to be uninhibited but Inbound traffic should be subject to scanning. Typical deployments of Geo-IP Filter with firewall access rules include DDoS and other network attack mitigation as well as anti-spoofing.

This is great to see. Naturally, everything we've seen and learned informs us that any and all such SSLVPN's, public-facing web management portals, and anything similar should be locked down out of the box with the engineer who is configuring it forced to ***selectively enable*** only the country or countries from which valid remote access is expected to originate. Alas, the industry is not there yet, but at least we're seeing progress. Having SonicWall offering such a feature right there in its UI at least means there's a chance that a security-oriented engineer who is offered the option may take the hint.

And note that the beauty of an IP-based filter is that no one scanning the Internet from Russia or China or anywhere else outside of the allowed jurisdiction will detect that anything at all is there. Their scanning packets will simply be dropped and the scanner will move on.

"ReVault" — Bad news for Dell

Cisco's Talos security group headlined last week's disclosure: *"ReVault! When your SoC turns against you…"* SoC stands for "System on a Chip" and the *"Vault"* in the name stems from a subsystem on Dell laptop PCs called *"ControlVault3"*. The short news blurb that caused me to look deeper said: *"A set of vulnerabilities can allow threat actors to take control of tens of millions of Dell laptops. The bugs impact the ControlVault3 firmware that is used to safely store passwords and biometric data inside a secure chip on Dell Windows laptops. The five bugs, codenamed ReVault, impact more than 100 Dell laptop models. The bugs can be exploited via a Windows API and don't require elevated privileges. Dell has released firmware updates."*

By far the most worrisome part of that entire statement is: "*The bugs can be exploited via a Windows API and don't require elevated privileges.*" This is truly horrific. Most flaws in security device firmware are actually quite obscure, requiring things like boot-time access or access to the system motherboard management interface or ... something. But here we have a flaw that literally ANY Windows app running on anyone's Dell laptop under their non-UAC minimal user privilege account could exploit. Wow.

As I mentioned, Cisco's Talos security group discovered and publicly disclosed this last week. I'm sure their discovery was much earlier, since they waited until Dell had created and tested the required firmware updates. The good news is that those updates exist. The bad news is that they need to be installed before any of those more than 100 Dell laptop models will be safe. So let's see what Cisco's Talos group disclosed last week. Their report leads with 4 bullet points:

- *Talos reported 5 vulnerabilities to Broadcom and Dell affecting both the ControlVault3 Firmware and its associated Windows APIs that we are calling "ReVault".*
- *100+ models of Dell Laptops are affected by this vulnerability if left unpatched.*
- *The ReVault attack can be used as a post-compromise persistence technique that can remain even across Windows reinstalls.*
- *The ReVault attack can also be used as a physical compromise to bypass Windows Login and/or for any local user to gain Admin/System privileges.*

Wow. They continued:

Dell ControlVault is "a hardware-based security solution that provides a secure bank that stores your passwords, biometric templates, and security codes within the firmware." A daughter board provides this functionality and performs these security features in firmware. Dell refers to the daughter board as a Unified Security Hub (USH), as it is used as a hub to run ControlVault (CV), connecting various security peripherals such as a fingerprint reader, smart card reader and NFC reader.

Okay. So that seems like good design.

The current iterations of the product are called ControlVault3 and ControlVault3+ and can be found in more than 100 different models of actively-supported Dell laptops (see DSA-2025-053), mostly from the business-centric Latitude and Precision series. These laptop models are widely used in the cybersecurity industry, government settings and challenging environments in their Rugged version. Sensitive industries that require heightened security when logging in (via smartcard or NFC) are more likely to find ControlVault devices in their environment, as they are necessary to enable these security features.

Oh that's just great. So it's the machines that are most in need of security, and would therefore likely most be targets, that have had their security dramatically impacted. That's a big whoops!

> *Today, Talos is publishing five CVEs and their associated reports. The vulnerabilities include multiple out-of-bounds vulnerabilities* [in other words "buffer overflows"] *(CVE-2025-24311, CVE-2025-25050) an arbitrary free (CVE-2025-25215) and a stack-overflow (CVE-2025-24922), all affecting the CV firmware. We also reported an unsafe-deserialization (CVE-2025-24919) that affects ControlVault's Windows APIs.*

To do this, Talos would have had to extract and reverse-engineer the firmware. Dell certainly didn't say "Hey, please check the firmware we wrote for our core security chip which provides all of the most critical physical and biometric security for our most secure laptops. My point is, it's really a shame that this sort of symbiotic relationship doesn't exist between manufacturers and security researchers. How many times have we looked at all the extra and unnecessary effort security researchers have had to go through, just to reverse engineer and obtain the same information that the manufacturer has sitting in a file somewhere? And after all that work, which might also all come to nothing, the security researchers say to the manufacturer: "Hey, we just worked our butts off, thanklessly for several months, to discover a set of five really horrendous security vulnerabilities that affect tens of millions of your most security-essential laptops."

There's something very wrong with the way we're doing all of this, today. The economics are all wrong. Cisco's Talos group continued:

> *With a lack of common security mitigations and the combination of some of the vulnerabilities mentioned above, the impact of these findings is significant. Let's highlight two of the most critical attack scenarios we have uncovered.*
>
> ***1. The post-compromise pivot:***
> *On the Windows side, a non-administrative user can interact with the ControlVault firmware using its associated APIs and trigger an Arbitrary Code Execution on the CV firmware.* [Given what we know, it's likely possible for the user to load a large buffer of executable code into the ControlVault's RAM and then cause that buffer to be executed.] *From this vantage point, it becomes possible to leak key material essential to the security of the device, thus gaining the ability to permanently modify its firmware. This creates the risk of a so-called implant that could stay unnoticed in a laptop's CV firmware and eventually be used as a pivot back onto the system in the case of a Threat Actor's post-compromise strategy. We show how a tampered CV firmware can be used to "hack Windows" by leveraging the unsafe deserialization bug mentioned previously.*
>
> ***2. The Physical attack***
> *A local attacker with physical access to a user's laptop can pry it open and directly access the USH board over USB with a custom connector. From there, all the vulnerabilities described previously become in-scope for the attacker without requiring the ability to log-in into the system or knowing a full-disk encryption password. While chassis-intrusion can be detected, this is a feature that needs to be enabled beforehand to be effective at warning of a potential tampering.*
>
> *Another interesting consequence of this scenario is that if a system is configured to be unlocked with the user's fingerprint, it is also possible to tamper with the CV firmware to accept any fingerprint rather than only allowing a legitimate user's.*

When you think about that, the "any fingerprint" attack is sort of diabolical. How often does anyone go around asking random people to verify that their fingerprint does NOT unlock their laptop? Probably not often and perhaps never. The affected user would simply notice that their fingerprint reader had apparently suddenly become much better at accepting their fingerprint than previously. Cisco says:

To mitigate these attacks, Talos recommends the following:

- *Keep your system up to date to ensure the latest firmware is installed. CV firmware can be automatically deployed via Windows Update, but new firmware usually gets released on the Dell website a few weeks prior.*
- *If not using any of the security peripherals (fingerprint reader, smart card reader and NFC reader) it is possible to disable the CV services (using the Service Manager) and/or the CV device (via the Device Manager).*
- *It is also worth considering disabling fingerprint login when risks are heightened (e.g., leaving one's laptop unattended in a hotel room). Windows also provides Enhanced Sign-in Security (ESS), which may help mitigate some of the physical attacks and detect inappropriate CV firmware.*

To detect an attack, consider the following:

- *Depending on your laptop model, chassis intrusion detection can be enabled in the computer's BIOS. This would flag physical tampering and may require entering a password to clear the alert and restart the computer.*
- *In the Windows logs, unexpected crashes of the Windows Biometric Service or the various Credential Vault services could be a sign of compromise.*
- *Cisco customers using Cisco Secure Endpoint can be made aware of potential risks with the signature definition "bcmbipdll.dll Loaded by Abnormal Process".*

And their report concludes:

These findings highlight the importance of evaluating the security posture of all hardware components within your devices, not just the operating system or software. As Talos demonstrated, vulnerabilities in widely-used firmware such as Dell ControlVault can have far-reaching implications, potentially compromising even advanced security features like biometric authentication. Staying vigilant, patching your systems and proactively assessing risk are essential to safeguard your systems against evolving threats.

Dell's own pages label this CRITICAL and they provide a 36 megabyte download to patch this. For any Dell Latitude or Precision laptop owners who would like to be proactive and get this patched, I have the links to Dell's support and download pages at the bottom of page 11 of today's (episode 1038) show notes:

https://www.dell.com/support/kbdoc/en-us/000276106/dsa-2025-053
https://www.dell.com/support/home/en-us/drivers/driversdetails?driverid=g7k77

The firmware and Windows patch download itself:
https://dl.dell.com/FOLDER12702584M/3/Dell-ControlVault3-Driver-and-Firmware_G7K77_WIN64_5.15.10.14_A31_01.EXE

Listener Feedback

Rosco

Hi Steve, WRT the Sharepoint on-prem patching issue, it's important to understand that the ecosystem can be highly complex and patching can be more difficult than it seems. Office 365 might seem to be an obvious way to resolve all of these issues, but that can be problematic, too.

The Enterprise office suite has many components, which form an extensive requirements matrix and consists of:

- *Windows server version*
- *Active Directory version*
- *Exchange Server version*
- *Dynamics CRM Server version*
- *Sharepoint Server ('SP') version*
- *MS-Project Server version*
- *Dynamics Great Plains ('GP') accounting*
- *Dynamics Human Resources*

...to name some of the commonly-deployed solutions, although some have been withdrawn as on-prem installable components.

The versions of all of these components need to be harmonised in order to have a viable, working installation. As a result, in order to update / patch to the latest Sharepoint on-prem version, the trickle-down requirements might extend to updating / patching any of all of the other components in the service stack.

In extreme situations, this can result in days or even weeks of applying patches, backing out, applying in patches in version order or to different services first (eg. applying a patch to AD first, then CRM, then finally to Sharepoint, rather than to Sharepoint first). The result can be almost-unmaintainable, especially for a Small-to-Medium-Enterprise with limited IT resources.

Here's an entirely plausible cascade that demonstrates the deep interconnectedness:

- *The sun is shining, the birds are singing, the grass is green, systems are stable and everything is beautiful in the world*
- *A critical vulnerability is discovered in Sharepoint with CVSS of 9.8 and a patch is available*
- *The installed SP version is two patch rollups behind, so SP has to be brought up-to date*
- *The second SP rollup will not run on the currently-installed AD, so an AD upgrade is required*
- *The AD upgrade implies a Windows server upgrade*
- *The new AD version no longer supports the installed Exchange version, which must also be upgraded*
- *The new AD version also deprecates NTLM authentication, which M$-SQL was still using(!), so…M$-SQL is also in scope…*
- *The Exchange end of the Dynamics CRM <-> Exchange API deprecates two methods used for email integration for mailouts to customers and reception of replies in order for replies to be tagged to the original outgoing message inside CRM. CRM is now in scope for two rollup installations.*
- *The second of these CRM rollups deprecates an API method being used for integration with the parent company's reporting tools which are required to report the subsidiary's sales*

pipeline prospects to the relevant stock exchange, which is a legislated requirement. The parent company must upgrade their data interchange tooling (alarm bells). The parent company runs Oracle EBS (seasoned operators might guess which freight train is heading down the tracks).

- *Installing the rollups in CRM also breaks three in-house customisations, which must be redesigned and reimplemented*
- *At long last, the full cascading set of upgrades has been deployed and the SP rollups and patch can be installed.*

This is the sort of thing that happens, which can result in weeks of disruption to business activities and manual workarounds. The end effect can be an erosion of trust in the technical solutions provided by O365 and these bolt-on components, hence M$ has pushed clients towards a cloud-based subscription model which provides overall greater stability.

Organisations may choose to wait for patch rollups in order to reduce the inevitable in-depth troubleshooting that can occur if the application of patches results in unexpected behaviours of seemingly-unrelated software components (eg. a patch applied to SP causing unexpected behaviours in CRM).

On-premises Sharepoint offers a broader featureset, however, such as the ability to design and deploy business processes directly into SharePoint, using various 3rd Party Business Process Management add-on tools and database connectivity and functionality required to support business processes. Online SharePoint, however, reduces support for business processes to M$' own development tools, "Logic Apps", Flows, WebJobs and Functions, implying that an organisation's significant investment in 3rd-party tools and business process development and testing becomes redundant and the organisation is forced to either adopt a completely new solution outside of SharePoint or re-engineer all their business processes to confirm to M$' provided frameworks, at possible significant cost and the possibility of losing significant features and functionality.

In corporate environments, such a significant change can mean considerable embarrassment to decision-makers who advocated for the 3rd-party development approach in the first place, which can add to inertia in moving to a cloud-based solution.

I think this broader context might give you a more complete picture of why organisations still run on-prem environments and why they might still be running previous versions of services, including SharePoint. Best Regards, /Rosco

Rosco's perspective leaves me with a much deeper appreciation for the fact that my own world never needed to become embroiled in any of that! What a monumental mess! It feels as though the utter lock-in that has resulted was incremental and more or less inadvertent, but that today's Microsoft is also well aware of the fact that businesses that have gone "all in" no longer have any meaningful freedom or way out. And even if they did have a way out, where would they go? This also suggests that becoming an expert in Microsoft's solutions – just knowing how to keep all of that crap running and mutually synchronized – would be a valid and valuable skill set to have.

Brian Savacool

Steve. Thanks for all that you do. You had recommended a picture tool for Windows that could correct the Keystone or perspective of a picture-of-the-day image was severely skewed. I can't find it in any of the emails or show notes from the past year. Could you please bring it up in the next feedback section? I'm writing some user-documentation and the sample image needs similar correction. Thank you for your weekly breakdowns . It really helps me at the help desk that I work at. /Brian

I've received a number of inquiries about that and I've been remiss in not replying to them all. So I wanted to use Brian's question from last week to get caught up. The tool is free, funky and somewhat finicky. So it's not perfect, polished and proper. But it's the tool I use because the German guy who created it got the basic mechanics exactly right. When I first mentioned this on the podcast, I received a ton of feedback from our listeners about alternative solutions. The one that sticks in my mind was someone commenting that he recalled that my go-to graphic editing tool is PaintShop Pro (he's right) and that PaintShop Pro has built-in perspective correction. And again, he is right, it does. But it's the sort of perspective correction that iOS has, where you have dials for horizontal or vertical distortion. The thing that the Perspective Image Correction app got exactly right is that its operator rubberbands the vertices of a four-sided box whose opposing sides should be parallel in the final image... and it then does that. It's really the correct way to solve the problem. The app lives on SourceForge. I have the link to it in the show notes and I also created a GRC shortcut: grc.sc / perspective.

https://sourceforge.net/projects/perspectiveimg/ — or — https://grc.sc/perspective

This may not be the perfect solution for everyone, but it's the best solution I've found, the price is right (it's free) and it stopped me looking for anything better.

In another note, Brian also asked:

Hi Steve, you had casually mentioned on episode 1035 about running SpinRite on a Kindle device. Can you explain in a future episode how that is accomplished.? Is it done in the native boot environment or does it require VirtualBox and a special device driver? I have a "Black Friday" special Android tablet that has been getting very slow and sludgy, even after multiple factory resets. I would like to run spinrite on it before I give up and toss the thing. Thanks for any tips you may have? I can't wait to try out the DNS Benchmark Pro once it gets released. All the very best, Brian in Schenectady.

Regarding the DNS Benchmark, I'll mention that I'm very nearly finished with all of the new features for the base-model DNS Benchmark v2.0. It is finally working very nicely and through this work I've obtained some clarification about the base model versus the Pro edition:

The new v2.0 non-Pro edition will be full-featured and will be run on demand as a stand-alone app for Windows or WINE. So it does also run under Linux and Mac. Running on demand makes it useful for obtaining an immediate snapshot of any collection of up to 500 remote DNS resolvers over IPv4, IPv6, DoH or DoT from the user's location. What we've seen is that just like the old saying about retail sales, it's "location, location, location". Our testers are spread around the globe, so we've seen how much people's location changes their results.

One of the things we've also seen is that the time of day and the day of week also affects the benchmark's outcomes. If I run the benchmark in the middle of a weekday I consistently see a different result from running in on a weekend morning. The difference may not be significant,

but you won't know until you try it. So if all you had was the interactive edition you might want to run it at the same time as you are using your machine at that location. And running it at differing times can also be useful.

One of the very cool new features is that the benchmark is now aware of whether differences in performance are statistically significant. For example, two different resolvers might have slightly different average performance, but each resolver's individual spread of performance might be wide enough that it's not possible to say with 95% certainty that the differences seen were not just the result of random variations in packet travel times. So the benchmark is now aware of this and it incorporates this awareness into every conclusion that it reaches.

The base model of the benchmark tests each resolver against the Internet's top 50 domains three different ways. So it issues 150 DNS queries to each of the DNS resolvers being benchmarked. This requires about 4 minutes for 120 DNS resolvers, which is about all the time that an interactive benchmark should consume without making its user impatient. During this time, it's measuring the precise time taken for 150 different DNS queries to each of the resolvers being benchmarked. It turns out that statistics are annoying, because even with 150 individual timing samples per resolver, the individual variation among samples means that our ability to draw firm statistically significant conclusions is limited. That's where the Pro edition will come into its own.

Because Pro will operate as a Windows service entirely in the background, its user won't be sitting around impatiently waiting for results. Pro builds and maintains a database which will allow it to measure resolver performance across a continuously broadening time horizon. If the user turns their machine on and off, it will automatically be measuring the times when they use their machine. And if their habit is to leave their machines running, it will be aware of when their machine is unattended and note that while gathering statistics. DNS queries are very small and lightweight, so they will never interfere with the normal foreground operation of the machine. And anytime a Pro owner wishes to see what's up, they simply launch the same Benchmark utility. They can choose to either run an interactive benchmark on the fly if they wish to answer some specific question about DNS, or they can use the same user-interface to display the aggregated results of the entire history that's been collected by the background DNS benchmarking service.

As usual, I have no idea when all of this will be ready, but I'm becoming excited to get it finished and available for everyone to play with.

As for Brian's question about using SpinRite to revive an Android Tablet: Until we get to SpinRite 7, which will be a pure Windows app, it's necessary to boot any system into DOS where SpinRite is able to run. For people who have never done this, I created the "BootAble" freeware which uses all of the same processes to create and prepare a bootable USB thumb drive. If you're able to boot a PC with BootAble, SpinRite will also work. So the only requirement for restoring the performance of any device's internal FLASH storage is being able to expose it as a drive. That might mean switching its storage mode. Android devices usually have a USB target drive mode. Then attach the tablet or other device to the PC before booting so that the system's BIOS will see its drive at boot time and will assign a BIOS drive number. Then SpinRite will, in turn, see the drive and be able to resuscitate it. A SpinRite level 3 rewrites the drive's entire surface to restore its original factory performance. This will all be much easier once I get SpinRite moved into Windows, but I have a few other things to finish before I can start on that joyous project.

Michael Swanson

Hi Steve, I have had InControl running since shortly after you released it to ensure my laptop is not accidentally updated to Windows 11. However, KB5001716 did NOT install on my laptop until I released control. I believe KB5001716 is the update that provides the free Windows 10 security patch extension, though I still have not seen that offer pop up in the Windows Update dialog. Best regards, Mike

Thanks for this note Michael. It's interesting that InControl appeared to block the installation (or perhaps the re-installation) of KB5001716 since we know that InControl is designed to only block major version changes. Here's what Microsoft tells us about this mysterious update:

After this update is installed, Windows may periodically display a notification informing you of problems that may prevent Windows Update from keeping your device up-to-date and protected against current threats. For example, you may see a notification informing you that your device is currently running a version of Windows that has reached the end of its support lifecycle, or that your device does not meet the minimum hardware requirements for the currently installed version of Windows.

We saw this sort of thing a lot during the forced migration to Windows 10 where Microsoft would be updating their Windows Update system to introduce constantly evolving messages about the coming end of the world. It was almost comical. The dialogs gradually changed from "No thanks" or "Yes please" to would you like to upgrade "now" or "tonight"?

I just checked and my Win10 21H1 is locked with InControl. When I go to Windows Update I see the expected red notification that "Some settings are managed by your organization" and if I click on the "View configured update policies" I see that the policies set on this machine are "Target release version for feature updates" and "Target product version for feature updates".

However, I just tried it and I can confirm that whatever KB5001716 is, briefly releasing InControl and performing a manual Windows Update **DID** install KB5001716 onto my normally InControl-locked Win10 machine.
Another interesting tidbit is that this is not the first time KB5001716 has been offered. More than a year ago back on March 7th of 2024, Ghacks.net's Martin Brinkmann wrote about this under the headline: *"Microsoft's sneaky KB5001716 Windows 10 update pushes Windows 11"* He wrote:

If you run Microsoft's Windows 10 operating system on your devices and want to keep it that way, you may want to check whether the Windows 10 update KB5001716 is installed on the device. The reason for this is that it is designed to push newer versions of Windows, including Windows 11, to the device. Microsoft installs the update automatically on non-managed Windows 10 devices that have automatic updates configured.

"Non-managed" clause would explain why InControl was blocking it, since InControl places a private system under pseudo-organizational management to prevent unwanted messing around. Martin continues:

The installed KB5001716 update is available for all versions of Windows 10 starting with Windows 10 version 1809 and going up to the latest version Windows 10 version 22H2. It introduces two changes to the system when installed:

Once installed, Windows may download and install feature updates to the device. This happens on devices that are "approaching" or have "reached the end of support" according to Microsoft.

Approaching means that this may also happen on devices that are still officially supported. Microsoft does not specify the period in weeks or months. This is a contrast to Microsoft's statement at the top of the page that out of support operating systems are a risk.

Furthermore, Windows may display upgrade prompts to the user periodically after installation of the update. This is not the first Windows update that shows upgrade prompts to the user and it will likely not be the last. This happened for Home devices when Microsoft released KB5020683 in December 2022, and also recently in February 2024. The next update push begins in April 2024 according to Microsoft. The update prompts use a dark pattern to get users to update. Note the tiny "keep Windows 10" option in the lower left corner of the screen. This is your option to keep on using Windows 10.

Given all of the evidence before us, it appears that Michael may be correct about this KB5001716 update being the gateway to Microsoft's forthcoming support extension. I noted that I had not seen it yet. So my use of InControl could be the reason for that. Let's all keep an eye out for these events. If it turns out that InControl's lockdown is preventing Win10 from installing KB5001716 and thus obtaining access to the additional free 6-months of security updates, that would be worth another of the very rare GRC newsletter announcements.

Thanks Michael!

Sci-Fi

I finished Andy Weir's 2nd book, Artemis, more quickly than I expected to. My Kindle showed that I was 90% of the way finished with the book when the plot wrapped up nicely and the story ended. It turned out that the remaining 10% of the book was an interesting Q&A discussion with Andy, and a discussion of the science and underlying economic principles around which he had designed and created the scientifically and economically accurate, but entirely fictional, storyline.

So it was an interesting story to read, but I now also understand why, unlike The Martian and Project Hail Mary, it didn't take the world by storm. I suppose that compared with other material that's available in today's highly competitive Sci-Fi novel world, in the end, Artemis doesn't feel highly memorable.

Shifting gears, I wanted to mention that today, August 12th, 2025, begins the continuation of one of our generation's major Sci-Fi franchises. Exactly two years ***before*** the debut of this franchise's first film, the world was taken by surprise on May 25th, 1977 with the release of a film that, surprisingly in retrospect, many people were unsure of. The movie's title was just "Star Wars" and needless to say the world changed that day. I still recall sitting in a large Theatre in Palo Alto, Northern California, having no idea what to expect and being astonished.

Then, exactly two years later, by coincidence on the same calendar day of May 25th, but this time in 1979, the world was changed again when Ridley Scott directed an horrific alien creature from beyond our imagination to gestate inside an unwitting starship crew member, and to then explosively emerge through his chest.

That scene and others were so over the top with surprise and tension that the movie "Alien" initially received somewhat mixed reviews — reviewers were afraid to like it and weren't sure what to think. But the movie went on to win the Academy Award that year for Best Visual Effects, three Saturn Awards for Best Science Fiction Film, Best Direction by Ridley Scott, and Best Supporting Actress for Veronica Cartwright (she played the role of that wimpy woman who tended to freak out a lot). Sigourney's role didn't win her anything, but it definitely put her on the map. The film also took home a Hugo Award for Best Dramatic Presentation.

Once the world had caught its breath, it was able to look at Alien more objectively. Wikipedia writes: *"In subsequent years, Alien was critically reassessed and is now considered to be* ***one of the greatest and most influential science fiction and horror films of all time.*** *In 2002, Alien was deemed "culturally, historically, or aesthetically significant" by the Library of Congress and was selected for preservation in the United States National Film Registry. In 2008, it was ranked by the American Film Institute as the seventh-best film in the science fiction genre, and as the 33rd-greatest film of all time by Empire."*

James Cameron's sequel "Aliens" is, without any doubt, one of my own personal favorite science fiction films of all time. For those who don't know, "Alien's" original theatrical release was missing some very interesting additional plot development footage that was later included in various Director's Cuts of the movie. They were worth watching if you're interested. I've watched both of those first two movies several times as well as all of the other various Alien follow-on films.

So, it is with some anticipation that tonight Lorrie and I will be watching the first two episodes of the Ridley Scott produced, big-budget *"Alien:Earth"* series which will be premiering on FX, FX on Hulu, internationally on Disney+.

The first of tonight's two episodes was pre-released a few weeks ago during San Diego's Comic-

Con which garnered the series a remarkably high IMDB rating of 8.8. Over the years I've found IMDB's ratings to generally be very useful, with 7.0 being my threshold for watchability. So if the series lives up to its early 8.8, we may have another winner.

The first season is eight episodes, so seven weeks from today, on September 23rd, the 8th and final episode will be released and be ready for a full series binge if that's anyone's style.

Perplexity's Duplicity

This is one of those news bits that began in today's show notes as just another piece of news up at the top. But the more I dug into it the more I appreciated its significance. As everyone will see, the deliberate and extensive behavior Cloudflare uncovered and discovered of Perplexity's Internet behavior is significant on many levels and for many reasons.

Controversy emerged right alongside the appearance of the new capabilities of generative AI. The images being generated upon request often bore striking similarity to the known – and copyrighted – work of human artists. Poems and music sounded eerily familiar to those who were familiar with other original works of writers and musicians. Before long we began to realize that when massive large language models are trained on the Internet's content, all of which up to that point had been created solely by the application of human effort and creativity, anything that a generative AI might spit out was inherently a derivative work. Although it wasn't so directly, what we had created carried a whiff of plagiarism. And in many cases it was much more than that. News sites began seeing the recognizable content of their human reporters appearing in the answers being offered by AI chatbots. None of this sat well with the human creators who wished to receive recognition and support in return for their life's work.

The solution was to deploy the Internet's well established automation controls to exclude these web scraping agents from websites that had no interest – thank you very much – in having their content absorbed by and used to train massive AI in the cloud. One of this TWiT Network's sponsors, which catered to programmers of all ilk, advertised their AI bot-blocking as a feature, so that their users could feel confident that their collaborations would remain theirs and not be leaked out into the ether to become the unpaid-for property of this new generation of rapacious AI sponges.

The Internet has a long history of bots. The bots most websites want and even actively invite and solicit are those belonging to search engines. "Search" was the early breakthrough application that entirely transformed the web. What good was it to create a quantity of terrific content of any kind if only your friends and family would ever be aware of its existence? Search changed all that. But the reason "Search" bots were wanted is that search engines would list links back to the sites containing the designed content. So search bots would indirectly drive human traffic to the website where humans would see where that link led to then perhaps poke around and discover other goodies, all the while being presented with advertisements that were producing supporting revenue for the destination website.

By comparison, AI model-building bots are not indexing a site for later discovery and linking, they're proactively scraping up all of the site's content, every juicy little morsel, and then feeding that original content into a massive AI model in the cloud. Effectively, the entire site's content is being incorporated into the AI model so that no one will need to ever visit that site again. They'll simply be able to ask the AI to obtain a homogenized and digested version of that site's once exclusive knowledge and wisdom.

They say that imitation is the sincerest form of flattery. That may be true. But flattery doesn't pay the bills, nor does it give credit to an idea's originator. The consequence was that websites the world over quickly moved to close their doors to content sucking model building AI scraping. Thanks, but no thanks. It quickly became clear that AI bots were the exact antithesis of search bots: Whereas search bots serve to drive future traffic back to a site, as I noted, the effect of an AI bot's visit is to reduce that site's future traffic.

The problem was, for any AI modeler, the entire Internet was the biggest and juiciest source of free ready-to-go machine-readable content imaginable. You couldn't design a better source of training knowledge. Oh, sure, there was that annoyance that the Internet, being a product of humans, also contained a large amount of nonsense and crap and that AI was no more able to tell the difference between truth and fiction than most of the humans who were consuming it. But none of that prevented the AI developers from turning their new scrapers loose on all that material to see what would happen.

And then, of course, AI became totally and utterly dependent upon that big juicy flowing source of ever changing knowledge. The fundamental problem of the entire AI approach is that it operates to model knowledge that it doesn't own and in the process does not again need. So AI inherently takes from the world's websites without ever giving anything back.

So as those website doors began closing to AI, it had a problem. What it needed, what it had selfishly grown utterly dependent upon, was being denied. Increasingly, everywhere its bots turned they were encountering "robots.txt" files sitting passively in the roots of website domains that **were** permitting and welcoming the world's known search engines to enter ... but were also denying entry to anything and everything else – and definitely to anything that hinted at being AI.

"Thanks anyway. Go suck out someone else's brain without even saying thanks."

The problem is, the "robots.txt" file concept was created to help out bots. It's there for their own good. So it inherently depends upon the honor system. It's a file that, by convention, sits in a website's root directory. Shortly after I added the ShieldsUP! facility to GRC I added one to my site. GRC's site contains a bunch of automation that makes no sense to index. The DNS Spoofability pages, the ShieldsUP! service itself, our extensive Internet port references and much more just cause bots to become all tangled up and lost. So GRC's "robots.txt" page lets bots know beyond where dragons lie.

Importantly, the "robots.txt" file is informational only. It is not any sort of enforcement mechanism. If some bot never looks at that file, or chooses to ignore its warnings, it might become tangled up in endless link-chain loops, pulling reams of nonsense data, and wasting a great deal of its own limited time and resources. But if so, so be it. You were warned.

As a consequence, search engines are thankful and appreciative of these "robots.txt" files. They figure that since their presence and services are a benefit to the site's management, anywhere a site doesn't want them to go is fine with them. But as things have evolved with AI, this is not the case. A visit from an AI scraper is not seen as offering the same benefit to a website as a visit from a search engine. Search engines are visiting to find and index. AI is here to steal.

Last week, Cloudflare posted the news under the headline: *"Perplexity is using stealth and undeclared crawlers to evade website no-crawl directives".* Cloudflare wrote:

> *We are observing stealth crawling behavior from Perplexity, an AI-powered answer engine. Although Perplexity initially crawls from their declared user agent, when they are presented with a network block, they appear to obscure their crawling identity in an attempt to circumvent the website's preferences. We see continued evidence that Perplexity is repeatedly modifying their user agent and changing their source addresses to hide their crawling activity, as well as ignoring — or sometimes failing to even fetch — robots.txt files.*

The Internet as we have known it for the past three decades is rapidly changing, but one thing remains constant: it is built on trust. There are clear preferences that crawlers should be transparent, serve a clear purpose, perform a specific activity, and, most importantly, follow website directives and preferences. Based on Perplexity's observed behavior, which is incompatible with those preferences, we have de-listed them as a verified bot and added heuristics to our managed rules that block this stealth crawling.

What happened?

We received complaints from customers who had both disallowed Perplexity crawling activity in their robots.txt files and also created WAF – Web Application Firewall – rules to specifically block both of Perplexity's declared crawlers: PerplexityBot and Perplexity-User. These customers subsequently informed us that Perplexity was still able to access their content even when they saw its bots successfully blocked. We confirmed that Perplexity's crawlers were in fact being blocked on the specific pages in question. We then performed several targeted tests to confirm what exact behavior we could observe.

We created multiple brand-new domains, similar to testexample.com and secretexample.com. These domains were newly purchased and had not yet been indexed by any search engine nor made publicly accessible in any discoverable way. We implemented a robots.txt file with directives to stop any respectful bots from accessing any part of a website:

We conducted an experiment by querying Perplexity AI with questions about these domains, and discovered Perplexity was still providing detailed information regarding the exact content hosted on each of these restricted domains. This response was unexpected, as we had taken all necessary precautions to prevent this data from being retrievable by their crawlers.

Our multiple test domains explicitly prohibited all automated access by specifying in robots.txt and had specific Web Application Firewall rules that blocked crawling from Perplexity's public crawlers. We observed that Perplexity uses not only their declared user-agent, but also a generic browser intended to impersonate Google Chrome on macOS when their declared crawler was blocked.

Perplexity Bot User-Agent Strings:

Declared: Mozilla/5.0 AppleWebKit/537.36 (KHTML, like Gecko; compatible; Perplexity-User/1.0; +https://perplexity.ai/perplexity-user) 20-25m daily requests

Stealth: Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_7) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/124.0.0.0 Safari/537.36 3-6m daily requests

Both their declared and undeclared crawlers were attempting to access the content for scraping contrary to the web crawling norms as outlined in RFC 9309.

This undeclared crawler utilized multiple IPs not listed in Perplexity's official IP range, and would rotate through these IPs in response to the restrictive robots.txt policy and block from Cloudflare. In addition to rotating IPs, we observed requests coming from different ASNs in attempts to further evade website blocks. This activity was observed across tens of thousands of domains and millions of requests per day. We were able to fingerprint this crawler using a combination of machine learning and network signals.

Wow. Given the aggregate number of websites that are now being hosted, protected and proxied by Cloudflare, no one wants to get themselves blacklisted by Cloudflare. Yet Perplexity has done exactly that. As a consequence of their underhanded bot scraping tactics, which were obviously both deliberate ***and*** would have taken quite some doing, Perplexity's shenanigans have been uncovered and are now blocked for all of their customers, both paid and free. No web property served by Cloudflare that wishes to block AI bots will now be visible for Perplexity's trawling. So once again I find myself saying "Bravo!" to Cloudflare and wanting to thank them on behalf of the industry. If nothing else, the lengths Perplexity went to, to so very clearly ignore the explicitly expressed wishes of website property owners should earn them some serious demerits.

Let me explain a little bit more about that since this is more than just changing their bot's User-Agent declaration. Cloudflare mentioned that they caught Perplexity's attempted stealth bots arriving from different ASNs. ASN stands for Autonomous System Number. Any major ISP who obtains a block of IP address allocations from a Regional Internet Registry will have previously obtained an Autonomous System Number. The IPs that GRC uses fall within AS3356 which were historically owned by Level 3. Google is AS15169 and Microsoft is AS8075. As a customer of Level 3, GRC originally received a block of 24 IPs which we make good use of for all of our various services. But because we're a customer of Level 3, regardless of which IP we use, that IP will always fall within one of Level 3's ASN allocations.

The fact that Cloudflare discovered that Perplexity's bots, once they had been thwarted and switched into attempted stealth mode, were originating their queries from different ASNs means that the Perplexity guys realized that just changing IP addresses from within the same ASN might not be sufficiently sneaky and differentiating. And, of course, they were correct since Cloudflare noticed exactly that. So Perplexity went to the significant extra trouble of obtaining and deliberately using IP addresses that had been allocated to other ASNs – thus from other major Internet Service Providers. This allows us to very reasonably infer that the deliberate bypassing of the anti-AI bot wishes of websites was relatively high up in the corporate strategy hierarchy. Perplexity clearly never had any intention of playing by the rules. They went to great lengths to deliberately break those rules and to attempt to never be caught doing so.

Cloudflare took the opportunity to make this a teaching moment for the entire AI bot industry, and a lesson for any others who might be chafing at the welcome mat being pulled up by the many websites that have no interest in having their content for the uncompensated purpose of training others' AI models.

Under the heading: *"How well-meaning bot operators respect website preferences"* Cloudflare explained:

> *In contrast to the behavior described above, the Internet has expressed clear preferences on how good crawlers should behave. All well-intentioned crawlers acting in good faith should:*
>
> - *Be transparent. Identify themselves honestly, using a unique user-agent, a declared list of IP ranges or Web Bot Auth integration, and provide contact information if something goes wrong.*
> - *Be well-behaved netizens. Don't flood sites with excessive traffic, scrape sensitive data, or use stealth tactics to try and dodge detection.*
> - *Serve a clear purpose. Whether it's powering a voice assistant, checking product prices, or making a website more accessible, every bot has a reason to be there. The purpose should be clearly and precisely defined and easy for site owners to look up publicly.*

- *Separate bots for separate activities. Perform each activity from a unique bot. This makes it easy for site owners to decide which activities they want to allow. Don't force site owners to make an all-or-nothing decision.*

- *Follow the rules. That means checking for and respecting website signals like robots.txt, staying within rate limits, and never bypassing security protections.*

More details are outlined in our official Verified Bots Policy Developer Docs.

***OpenAI** is an example of a leading AI company that follows these best practices. They clearly outline their crawlers and give detailed explanations for each crawler's purpose. They respect robots.txt and do not try to evade either a robots.txt directive or a network level block. And ChatGPT Agent is signing http requests using the newly proposed open standard Web Bot Auth.*

When we ran the same test as outlined above with ChatGPT, we found that ChatGPT-User fetched the robots file and stopped crawling when it was disallowed. We did not observe follow-up crawls from any other user agents or third party bots. When we removed the disallow directive from the robots entry, but presented ChatGPT with a block page, they again stopped crawling, and we saw no additional crawl attempts from other user agents. Both of these demonstrate the appropriate response to website owner preferences.

This year, in 2025, Cloudflare represents somewhere around 20% of websites and 20% of all web traffic globally. Thanks to Cloudflare's diligence and technical expertise, all of its sites, both free and paid, are now protected from Perplexity's duplicity. The problem is, what Perplexity has done and is doing would otherwise be highly effective. It takes a host with Cloudflare's technical chops – and Cloudflare's caring – to detect and shutdown anyone who's as serious about bypassing website wishes as Perplexity is now clearly known to be.

My point is that the other 80% of the Internet has no similar comprehensive protection – and providing that protection is not simple. I'm certain that most hosting providers, even gargantuan hosts, could not care less about policing the traffic flowing to their website customers. They just provide power, environment, servers and bandwidth. What flows across that bandwidth, so long as it's not DDoS attacks which inconvenience many other nearby sites, is of little concern to them.

The upshot of all this is that I don't see Perplexity's behavior – and likely other AI scrapers as well, since I'm sure Perplexity is far from alone – changing in the future unless they are required to. This is a perfect place for the application of legislation. Enough attention has by now been brought to this problem for our ever-lovin' politicians will be able to understand what's going on with it. We already have a well established and well understood simple mechanism in the form of the "robots.txt" file. What it lacks is teeth. We need a law that simply requires any form of automated web agent to examine and respect the directives of any "robots.txt" file that any website might present. And there ought to be a few new "generic" labels by category. One for indexing-only search engines and another for any form of content aggregator such as AI.