26 for 26 - Potential topics

1. AWS Buckets
2. Ransomware as a Company
3. North Korean: Remote Workers
4. Arizona Laptop
5. No more buffer overflows
6. Learn Buffer Overflows through gaming
7. USBIP
8. Signal pulling out of Sweden
9. GPL might fall
10. China on small power utility's network
11. How NixOS could have detected xz attack with reproducible builds
12. Oxidier - Ubuntu 25.10 using rust uutils instead of coreutils
13. Cloud Security Explained: what's left
14. Russians lure European diplomats into malware trap with wine-tasting invite
15. AI LLm craft exploit from patches
16. Protecting yourself from North Korean hackers with one question
17. AI Slop Bug reports in Curl
18. Coinbase extorted for $20M, interesting case
19. Cybercrime is "orders of magnitude" larger than state-backed ops, says ex-white house adviser
20. AI Finds 0-day in Linux Kernel - ksmbd
21. TrueNAS uses "AI" for customer support, and it goes horribly wrong
22. Psylo browser - every tab different IP address
23. 23andMe bankruptcy - data up for grabs
24. Asterinas: a new Linux-compatible kernel project
25. Vet - tool for analyzing SBOM
26. https://cybercanon.org/ - Essential Cybersecurity Reads
27. Ghost/Stealth Laptop
28. Rayhunter
29. Azure to turn off default outbound access for VMs in Azure
30. Microsoft moving a/v providers out of the windows kernel
31. Libxml2's no security embargo
32. How to Hack Windows 11 to fix some of its issues
33. Dave's Garage - WIndows Sandboxing
34. Windows 11 Hacks - Turn off Second Chance Notification and Others
35. Your CV is not fit for the 21st Century
36. The biggest challenges in software supply chains in 2025
37. Are you willing to pay $100k a year per developer on AI?
38. Magical Jelly Bean - Product KeyFinder
39. Village AI Powered Pentesting Tool
40. Three Alternative Kernels to Linux
41. AI Coding Hyper Overblown, Bain Shrugs

42. Silent Courier - New MI6 system for anonymous contribs
43. Chinese gang used ArcGIS as a backdoor for a year – and no one noticed
44. Nosey Parker - command line tool finding information - digital ocean/aws/azure etc
45. A simple AI prompt saved a developer from this job interview scam
46. Shadow AI tools - people bringing their AI tools from home into work
47. Ironclad OS project popping out Unix-like kernel in a unique mix of languages
48. AI companies keep publishing private API keys to GitHub
49. AppAnyRun - run software
50. Chinese spies told Claude to break into about 30 critical orgs. Some attacks succeeded
51. Rust developer writing new language Rue with Claude
52. IBM Bob AI agent will do bad things - prompt overflow
53. Just the Browser - remove the AI, telemetry and product sponsorships
54. Vibe coding a few Security issues
55. Future phones to have less memory

AWS Buckets

https://www.theregister.com/2025/02/04/abandoned_aws_s3/

Abandoned S3 buckets are being registered and potentially having information being pulled from them

Ransomware as a Company

https://www.theregister.com/2025/02/07/ransomware_costs_analysis/

Ransomware as a company was not very successful as a company in 2024. Interesting approach to how to measure company's success

North Korean: Remote Workers

https://www.theregister.com/2025/02/11/it_worker_scam/

Follow up to 25 in 25 article about North Korean workers trying to get jobs via AI, etc. Security expert almost falls for it.

Arizona Laptop Sentencing

https://www.theregister.com/2025/02/12/arizona_woman_laptop_farm_guilty/

Lady sentenced for 8-10 years for helping setup fake laptops for North Korean hackers. Helped create false identities etc, so a lot more egregious than most.

No more buffer Overflows

https://www.theregister.com/2025/02/13/fbi_cisa_unforgivable_buffer_overflow/

Lays out more info about how we need to make transition to safer languages. Identifies a bunch of issues in the process.

Learn Buffer Overflows Through Gaming

https://overthewire.org/wargames/behemoth/

it will teach you how to exploit several of the most common coding mistakes including buffer overflows, race conditions and privilege escalation.

USBIP

https://hackaday.com/2025/02/27/linux-fu-usb-everywhere/

USB IP allows you to share a usb device between linux computers.

There is also a windows version of this as well, but as it is a driver can be quite a pain

Signal pulling out of Sweden

https://www.theregister.com/2025/02/26/signal_will_withdraw_from_sweden/

Fight over encryption back doors

GPL might fall

https://www.theregister.com/2025/02/27/adverse_appeals_court_ruling_could/?td=rt-3a

If the GPL falls what does that mean for Open Source???

Neo4j is arguing it can add non-removable clauses to the GPL.

China on small power utility's network

https://www.theregister.com/2025/03/12/volt_tyhoon_experience_interview_with_gm/

Small power/water facility having been breached by China.

How NixOS could have detected xz attack with reproducible builds

https://www.osnews.com/story/142000/how-nixos-and-reproducible-builds-could-have-detected-the-xz-backdoor-for-the-benefit-of-all/

Really interesting article about how reproducible builds, might have helped figure out the xz backdoor much earlier in the process.

Oxidier - Ubuntu 25.10 using rust uutils instead of coreutils

https://lwn.net/Articles/1014002/

Ubuntu 25.10 moving to rust based uutils instead of coreutils. Beginning of the end of GNU/Linux? Way you can flip utilities is kind of interesting.

Cloud Security Explained: what's left

https://www.theregister.com/2025/03/31/cloud_security_explained_whats_left/

Explanation of how things like S3 configuration need to be done.

Russians lure European diplomats into malware trap with wine-tasting invite

https://www.theregister.com/2025/04/16/cozy_bear_grapeloader/

Social engineering keeps delivering ☹️

AI LLm craft exploit from patches

https://www.theregister.com/2025/04/21/ai_models_can_generate_exploit/

Using an LLM to generate exploit from CVE and patches different.

Protecting yourself from North Korean hackers with one question

https://www.theregister.com/2025/04/29/north_korea_worker_interview_questions/

The one question that could help you avoid NK hackers. How fat is Kim Jon Un

AI Slop Bug reports in Curl

https://www.theregister.com/2025/05/07/curl_ai_bug_reports/

Objecting to AI generated security reports against Curl and other projects

Coinbase extorted for $20M, interesting case

https://www.theregister.com/2025/05/15/coinbase_extorted_for_20m_support/

Story about extortion of coinbase

Cybercrime is “orders of magnitude” larger than state-backed ops, says ex-white house adviser

https://www.theregister.com/2025/05/24/cyber_crime_bigger_than_nation_state/

Analyst says the true cybercrime is a lot larger than the official estimates

AI Finds 0-day in Linux Kernel - ksmbd

https://www.youtube.com/watch?v=jDimK-89rfw
https://sean.heelan.io/2025/05/22/how-i-used-o3-to-find-cve-2025-37899-a-remote-zeroday-vulnerability-in-the-linux-kernels-smb-implementation/

0-day found in Linux kernel SMBD - CVE-2025-37899

Amazing tech

TrueNAS uses “AI” for customer support, and it goes horribly wrong

https://www.osnews.com/story/142417/truenas-uses-ai-for-customer-support-and-of-course-it-goes-horribly-wrong/
https://aphyr.com/posts/387-the-future-of-customer-support-is-lies-i-guess

Just straight up hallucinations and lies. Very bad potentially. “Why don’t you try rm -rf /?” is only so far away

Psylo browser - every tab different IP address

https://www.theregister.com/2025/06/24/psylo_browser_privacy_tab_silos/

iOS based mobile browser
Implements things like canvas randomization different in each tab

23andMe bankruptcy - data up for grabs

https://www.npr.org/2025/03/24/nx-s1-5338622/23andme-bankruptcy-genetic-data-privacy

With 23andMe all bets are off as to what is going to happen to your personal information. Bankruptcy allows companies to break any contract

Asterinas: a new Linux-compatible kernel project

https://www.osnews.com/story/142631/asterinas-a-new-linux-compatible-kernel-project/
https://asterinas.github.io/

Attempting to write a rust replacement for the linux kernel. This and Redox are both interesting projects about potentially replacing the Linux Kernel

Vet - tool for analyzing SBOM

https://github.com/safedep/vet

Very cool tool for doing SBOM analysis. Supports package managers like PyPi, NPM, Go, Rust, PHP
Container Images, SBOMS: CycloneDX< SPDX, JAR File and others

https://cybercanon.org/ - Essential Cybersecurity Reads

Great resource for vetting Cybersecurity books.

Ghost/Stealth Laptop

https://dicloak.com/video-insights-detail/build-a-ghost-untraceable-laptop-ultimate-guide-to-online-anonymity-and-privacy-diy

https://www.youtube.com/watch?v=lUVKSwO_ZNw

https://www.franksworld.com/2024/12/03/how-to-build-a-ghost-untraceable-laptop-ultimate-guide-to-online-anonymity-and-privacy-diy/

Buying a cheap laptop, removing microphones/cameras/hard drive and setting it up so it is closer to a burner laptop

Rayhunter

https://github.com/EFForg/rayhunter
https://www.eff.org/deeplinks/2025/03/meet-rayhunter-new-open-source-tool-eff-detect-cellular-spying

How to build a rayhunter to detect IMSI Catcher detector

Azure to turn off default outbound access for VMs in Azure

https://www.theregister.com/2025/06/24/outbound_access_vms_azure/

Microsoft is going to turn off default outbound access for Azure VMs
Azure will cost more money as you'll have to setup a NAT gateway on the vnet
Seismic change to Azure

AWS already does this

Microsoft moving a/v providers out of the windows kernel

https://www.osnews.com/story/142647/microsoft-is-moving-antivirus-providers-out-of-the-windows-kernel/

Microsoft is working at moving A/V companies out of the Windows Kernel.
Response to Crowdstrike

Libxml2's no security embargo

https://lwn.net/Articles/1025971/

Interesting writeup about how OSS projects might have to deal with security issues in the future
No money, urgent requests from commercial companies and security vendors

How to Hack Windows 11 to fix some of its issues

https://www.theregister.com/2025/07/21/windows_11_productivity_sink/

Some fixes to Windows 11, turning off notifications and reminders about out of box experience crap.

Dave's Garage - WIndows Sandboxing

https://www.youtube.com/watch?v=1jjGQCGHjuw&pp=ygUNZGF2ZSdzIGdhcmFnZQ%3D%3D

Disposable Windows. Easy Sandboxed Windows VMs - need Windows 11 Enterpise/Pro - works quite well

Windows 11 Hacks - Turn off Second Chance Notification and Others

https://www.theregister.com/2025/07/21/windows_11_productivity_sink/

Bunch of hacks to Make Windows 11 less of a pain in the Butt.

- Turn off Out of the Box Experience - stuff
- Change Taskbar to show apps instead of Windows 11 format
- Tone down the notifications

Your CV is not fit for the 21st Century

https://www.theregister.com/2025/08/11/feature_tech_cv_updates/

Bunch of tips to make your Resume more AI Friendly

- Go long - Configured Fortigate Fortinet firewalls
- Build database with every certification, skill in it
- Exactly copy phrases from job posting - design and implement, not architect and build

The biggest challenges in software supply chains in 2025

https://www.theregister.com/2025/08/11/biggest_challenges_software_supply/

Overview of 2025 software supply chain issues. Written by Canonical, talks about issues with Open Source, fips, supply chain etc.

Are you willing to pay $100k a year per developer on AI?

https://www.theregister.com/2025/08/15/are_you_willing_to_pay/

What happens when you have to start paying the real costs of Vibe coding? Estimates seem high but will be interested to see what happens with this.

Magical Jelly Bean - Product KeyFinder

https://www.magicaljellybean.com/keyfinder/

Retrieve product keys in windows from your registry. Has a free version which does like 300 program and a commercial program that will do it for 10,000 programs. There is also a similar mac program called Mac Product Key Finder - https://mac-product-key-finder.com/

Village AI Powered Pentesting Tool

https://cybersecuritynews.com/villager-ai-powered-pentesting-tool/amp/

Combines Kali with Deepseek AI models to automate cyber attack workflows

Three Alternative Kernels to Linux

https://www.theregister.com/2025/09/12/three_new_microkernels/

Quick description of three potential alternative kernels to Linux's kernel.

Managram - C++ / Linux compatibility goal
Asterinas - Rust - Linux ABI as well
Xous - another Rust kernel / Own APIs

AI Coding Hyper Overblown, Bain Shrugs

https://www.theregister.com/2025/09/23/developers_genai_little_productivity_gains/

Is AI really the productivity tool they're claiming it is???

Silent Courier - New MI6 system for anonymous contribs

https://www.npr.org/2025/10/14/nx-s1-5564056/security-mi-6-uk-secrets-foreign-intelligence-silent-courier
https://www.nprillinois.org/2025-10-14/new-dark-web-dead-drop-lets-anyone-pass-secrets-to-britains-mi6

Security sharing system to be used for MI6, dangerous?

Chinese gang used ArcGIS as a backdoor for a year – and no one noticed

https://www.theregister.com/2025/10/14/chinese_hackers_arcgis_backdoor/?td=rt-9bs

Mapping software going through the system. Command and Control protected by their signing keys.

Nosey Parker - command line tool finding information - digital ocean/aws/azure etc

https://github.com/praetorian-inc/noseyparker/tree/main/crates/noseyparker/data/default/builtin/rules

System to look for secrets/information. Scan complete history of git repo.

A simple AI prompt saved a developer from this job interview scam

https://www.theregister.com/2025/10/20/ai_prompt_saved_developer/

Guy gets package to do some development against. Asks AI to inspect and finds it has malware in the package

Shadow AI tools - people bringing their AI tools from home into work

https://www.theregister.com/2025/10/14/microsoft_warns_of_the_dangers/

Shadow AI challenges for companies.

Ironclad OS project popping out Unix-like kernel in a unique mix of languages

https://www.theregister.com/2025/11/10/ironclad_os_unix_like_kernel/

Writing an O/S in Ada with Contracts - Ironclad - interesting approach

AI companies keep publishing private API keys to GitHub

https://www.theregister.com/2025/11/10/ai_companies_private_api_keys_github/

AI keep publishing API keys to repos. Bad practice

AppAnyRun

https://app.any.run

https://app.any.run/?utm_source=youtube_pc_security_channel&utm_medium=video&utm_campaign=peazip&utm_content=register&utm_term=181125#register

Very nice system to allow you to run/test unknown software. Works with Windows/LInux/Android

Chinese spies told Claude to break into about 30 critical orgs. Some attacks succeeded

https://www.theregister.com/2025/11/13/chinese_spies_claude_attacks/

Chinese spies told Claude to brak into 30 critical orgs. Still early in the cycle, but this something that is going to get worse and worse in the future.

Rust developer writing new language Rue with Claude

https://www.theregister.com/2026/01/03/claude_copilot_rue_steve_klabnik/

Rust developer writing new language Rue with extensive help in rust. Is this the future. Rue is a systems level memory safe language without garbage collection

IBM Bob AI agent will do bad things - prompt overflow

https://www.theregister.com/2026/01/07/ibm_bob_vulnerability/

IBM AI Bob software dev agent. Can be told to do bad things. Prompt injection can override guard rails

Just the Browser - remove the AI, telemetry and product sponsorships

https://justthebrowser.com/

Just the browser is a set of Open Source scripts to remove telemetry

Vibe coding a few Security issues

https://devclass.com/2026/01/15/vibe-coded-applications-full-of-security-blunders/

Vibe coding full of blunders

Future phones to have less memory

https://www.techradar.com/phones/the-ram-crisis-will-see-smartphone-specs-go-backwards-in-2026-experts-warn-heres-why

Future phones will have less memory to handle dram price crisis