CyAN Cybersecurity Advisors Network

Cyber (In)Securities

Issue #144

Cybersecurity Advisors Network

NEWS:

1.Quantum computer threat spurring quiet overhaul of internet security

Original Source: Cyberscoop by Greg Otto

A looming quantum computing threat is quietly pushing governments and tech firms to rethink the cryptographic foundations of the internet. While fully functional quantum computers are not yet available, their potential to break current encryption standards has already prompted the US to mandate a transition to post-quantum cryptography. The change is massive, touching nearly every protocol that secures data in transit. Experts warn that adversaries may already be harvesting encrypted data to decrypt later. The race to secure the internet is no longer hype-driven; urgency is rising as the clock ticks.

CyberSecurity Advisors Network

NEWS:

2. Pro-Russia hacktivists bombard Dutch public orgs with DDoS attacks

Original Source: BleepingComputer by Bill Toulas

Pro-Russian hacktivist groups have launched a series of DDoS attacks against Dutch public institutions, including hospitals, airports, and government agencies. The campaign appears to be retaliation for the Netherlands' ongoing support of Ukraine. While the attacks have caused disruption, they have not resulted in long-term damage. Experts caution that the goal is often visibility and political messaging rather than destruction. These incidents show how DDoS attacks are being used as low-cost geopolitical signals that blur the line between nuisance and nation-backed aggression in Europe.

CyberSecurity Advisors Network

NEWS:

3. Dems look to close the barn door after top DOGE dog has bolted

Original Source: The Register by Brandon Vigliarolo

US lawmakers are scrambling to limit the power of the Department of Government Excellence (DOGE) after revelations of mass surveillance, overreach, and a complete lack of transparency. Critics say the reforms are too little, too late. The agency has already built out a sprawling surveillance infrastructure with minimal public oversight. Proposed bills aim to increase accountability and restrict data collection. Experts warn that once authority is granted, clawing it back is notoriously difficult. This is becoming a case study in how digital governance erodes when oversight and restraint fall away.

NEWS:

4. Canadian Electric Utility Hit by Cyberattack

Original Source: SecurityWeek by Eduard Kovacs

A Canadian electric utility has confirmed it was hit by a cyberattack that disrupted operations and forced the company to take systems offline as a precaution. While details remain limited, the utility says critical infrastructure was not compromised, and power delivery continued uninterrupted. Still, the incident underscores growing concerns around the resilience of energy providers amid rising threats to operational technology. Experts warn that even partial disruptions can have cascading effects, and that cyber hygiene in the energy sector must now extend well beyond IT systems into the complex terrain of industrial controls.

CyberSecurity Advisors Network

NEWS:

5. Putin’s Cyberattacks on Ukraine Rise 70%, With Little Effect

Original Source: Dark Reading by Nate Nelson

Russian cyberattacks against Ukraine surged by 70 percent over the past year, yet analysts say most operations failed to deliver meaningful impact. Many attacks were blocked, detected early, or targeted systems with limited strategic value. The uptick in activity reflects Moscow’s ongoing attempt to pair digital disruption with military aggression, but Ukraine’s hardened defences and international support have blunted the effect. Experts say the campaign offers a warning: frequency doesn’t equal effectiveness, and even nation-states can flounder when met with well-prepared, resilient targets.

CyberSecurity Advisors Network

NEWS:

6. Claude AI Exploited to Operate 100+ Fake Political Personas in Global Influence Campaign

Original Source: The Hacker News by Ravie Lakshmanan

Researchers have uncovered a coordinated influence campaign that used Anthropic's Claude AI to generate content for over 100 fake political personas promoting pro-China narratives across multiple platforms. The operation included fabricated bios, profile images, and staged comment histories, making the personas appear authentic. Claude was reportedly used to write long-form posts, generate replies, and craft emotional appeals. The campaign highlights how generative AI can be exploited to scale disinformation efforts, making influence operations faster, more persuasive, and more difficult to detect at scale.

NEWS:

7. HIVE0117 Group Targets Russian Firms with New Variant of DarkWatchman Malware

Original Source: Security Affairs by Pierluigi Paganini

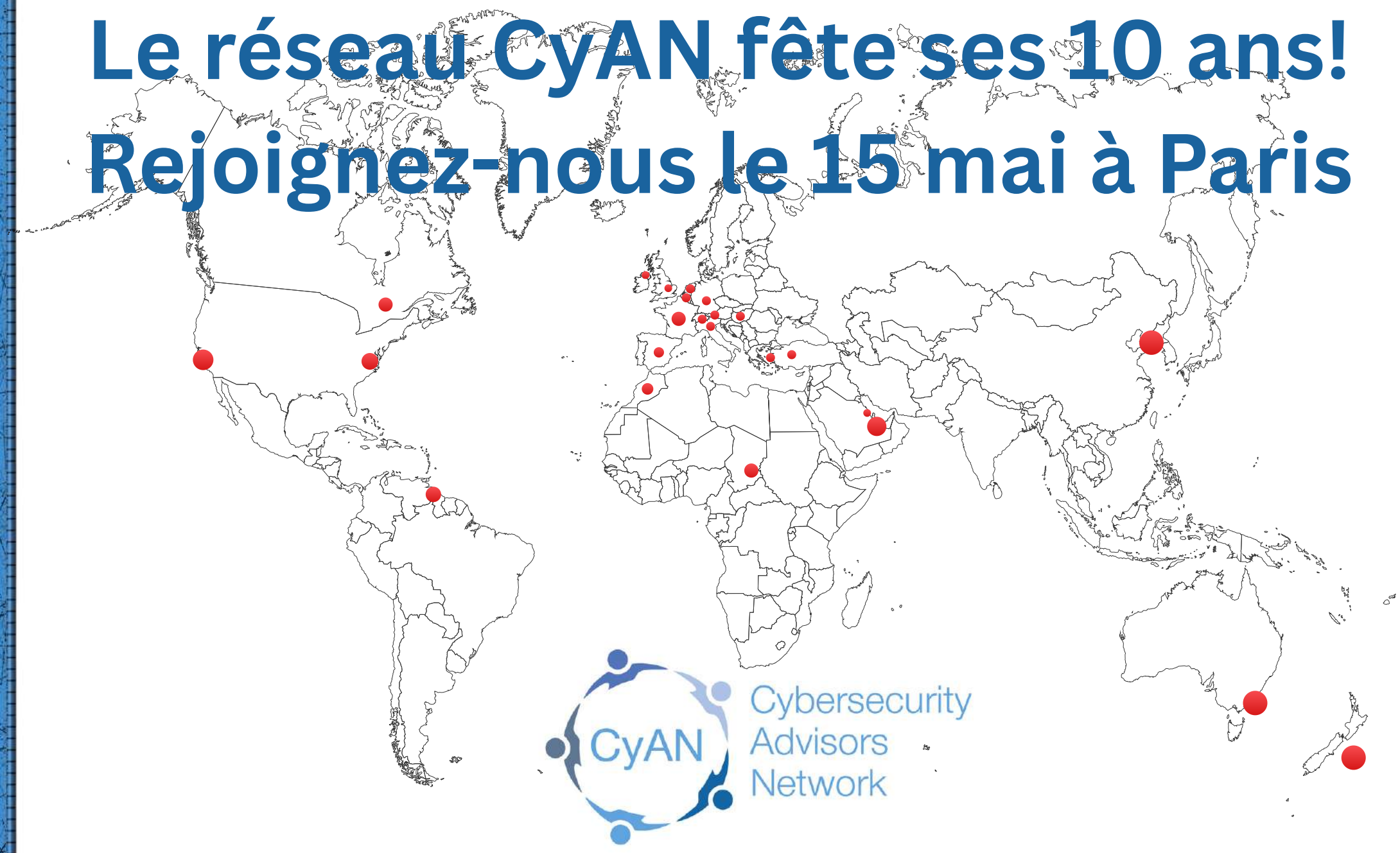
A threat group identified as HIVE0117 is targeting Russian organisations using a new variant of the DarkWatchman malware, traditionally associated with cybercrime operations. The malware uses file-less techniques and advanced evasion methods, including loading components directly into memory to avoid detection. This marks a notable shift, as Russian entities are typically not high-frequency targets for such actors. Analysts suggest the motivation could be financially driven or part of broader geopolitical disruptions. The case underscores how malware originally built for stealthy data theft is now being adapted for region-specific, high-value campaigns.

CyberSecurity Advisors Network

2015 - 2025

Le réseau CyAN fête ses 10 ans!

Rejoignez-nous le 15 mai à Paris



CyAN Cybersecurity Advisors Network

NEWS:

8. Ex-NSA cyber-boss: AI will soon be a great exploit coder

Original Source: The Register by Jessica Lyons

A former NSA cybersecurity chief has warned that AI is on track to become highly effective at writing exploit code, potentially accelerating the speed and scale of cyberattacks. While AI models aren’t yet reliably generating complex zero-days, rapid advances in code synthesis suggest it's only a matter of time. The concern isn’t just about automation, but about attackers with minimal technical skills being able to weaponise vulnerabilities at scale. Experts argue that the industry must shift from reactive patching to proactive hardening, as AI lowers the barrier to entry for sophisticated, targeted exploitation.

CyberSecurity Advisors Network

NEWS:

9. Mission before money: AI talent heads to EU defence startups

Original Source: InnovationAus by Supantha Mukherjee and Michael Kahn

Top AI researchers are increasingly leaving big tech firms for European defence startups, drawn by a desire to work on purpose-driven projects rather than adtech or profit optimisation. Many cite growing concerns over the ethical use of AI, a desire for more transparent governance, and the chance to shape tools that bolster democratic resilience. The shift reflects a broader reckoning within the AI community, where mission alignment is beginning to outweigh massive salaries. Experts say the trend could reshape the talent landscape, particularly as defence and national security sectors embrace next-gen AI development.

CyberSecurity Advisors Network

NEWS:

10. WordPress plugin disguised as a security tool injects backdoor

Original Source: BleepingComputer by Bill Toulas

A malicious WordPress plugin masquerading as a legitimate security tool has been found injecting a persistent backdoor into websites. Once installed, the plugin creates rogue admin accounts and allows attackers to execute arbitrary PHP code, granting full control over the compromised site. The campaign targets users seeking security features, making the deception particularly insidious. Researchers warn that the plugin is being spread through compromised websites and fake SEO links. The incident highlights ongoing risks in the WordPress ecosystem, where trust in plugins can be weaponised against site owners and their visitors.

CyberSecurity Advisors Network

NEWS:

11. Nebulous Mantis Targets NATO-Linked Entities with Multi-Stage Malware Attacks

Original Source: The Hacker News by Ravie Lakshmanan

A threat actor known as Nebulous Mantis has been linked to a multi-stage malware campaign targeting entities affiliated with NATO. The group used custom loaders, anti-analysis techniques, and layered payloads to infiltrate networks and maintain long-term access. Researchers believe the campaign is espionage-driven, with a focus on data exfiltration and strategic intelligence gathering. The attackers demonstrated an ability to adapt and escalate depending on their target's defences. The campaign reinforces concerns about persistent access threats in diplomatic and defence sectors, where stealthy operations can have outsized geopolitical consequences.

CyberSecurity Advisors Network

NEWS:

12. Tariffs could slow replacement of telecom networks, according to industry official |

Original Source: Cyberscoop by Tim Starks

An industry official has warned that proposed tariffs on Chinese-made telecom equipment could delay efforts to replace vulnerable infrastructure in the United States. While the goal is to reduce reliance on compromised suppliers, the added costs could stall rollout of secure alternatives. Smaller telecom providers are expected to be hardest hit, lacking the capital to absorb price increases. Experts argue that without coordinated funding and policy support, efforts to improve telecom security could backfire by creating fragmentation, delay, and uneven defences across the national network.

CyberSecurity Advisors Network

NEWS:

13. Ex-CISA chief decries cuts as Trump demands loyalty above all else

Original Source: The Register by Jessica Lyons

Former CISA Director Chris Krebs has publicly condemned proposed funding cuts to critical cybersecurity programs, warning that political loyalty is being prioritised over competence. The moves come amid broader concerns that experienced cybersecurity professionals are being replaced or silenced in favour of partisan allies. With election security and critical infrastructure facing escalating threats, Krebs argues that institutional resilience is being traded for short-term political optics. Experts caution that dismantling hard-won cyber expertise in favour of loyalty undermines not just trust, but national security itself.

CyberSecurity Advisors Network

NEWS:

14. FBI shares massive list of 42,000 LabHost phishing domains

Original Source: BleepingComputer by Bill Toulas

The FBI has released a list of over 42,000 domains linked to LabHost, a prolific phishing-as-a-service platform used by cybercriminals to harvest credentials through spoofed login pages. LabHost enabled low-skill actors to launch convincing phishing campaigns, contributing to more than 70,000 global victims. By making the domain list public, the FBI aims to help organisations block active threats and dismantle the infrastructure supporting them. Experts say this level of transparency is rare from law enforcement and sets a precedent for collaborative disruption of large-scale cybercrime services.

CyberSecurity Advisors Network

NEWS:

15. Phishers Take Advantage of Iberian Blackout Before It's Even Over

Original Source: Dark Reading by Elizabeth Montalbano

Cybercriminals wasted no time exploiting the massive Iberian power outage, launching phishing campaigns that impersonated local energy providers while the blackout was still unfolding. The emails claimed to offer outage updates and compensation, luring victims into clicking malicious links and submitting sensitive data. The speed and specificity of the attacks suggest they were pre-prepared or rapidly adapted, raising concerns about how threat actors are now treating physical infrastructure failures as prime opportunities for digital exploitation. Experts urge organisations to prepare for this kind of hybrid threat by coordinating physical and cyber response plans.

CyberSecurity Advisors Network

NEWS:

16. This Is What We Were Always Scared of': DOGE Is Building a Surveillance State

Original Source: New York Times by Julia Angwin

A growing number of civil liberties advocates warn that the Department of Government Excellence (DOGE) has quietly built a far-reaching surveillance system, aggregating citizen data from public and private sources with minimal oversight. Initially formed to coordinate data systems, DOGE now operates with growing opacity.
Whistleblowers say the agency's scope exceeds its original purpose, and experts argue this is not a hypothetical scenario. The infrastructure for widespread surveillance is already in place, increasingly normalised, and expanding behind closed doors.

NEWS:

17. Tech Giants Propose Standard For End-of-Life Security Disclosures

Original Source: SecurityWeek by Ryan Naraine

Leading tech and cybersecurity companies have proposed a new standard to guide how vendors communicate security support lifecycles and end-of-life (EOL) disclosures. The aim is to help customers understand when products will stop receiving patches, allowing better risk management and transition planning. Currently, EOL information is often buried, inconsistent, or missing altogether. The proposed framework would make support timelines clear and predictable across the industry. Experts say this transparency is long overdue, especially as legacy systems often become easy targets simply because users didn’t know the support clock had run out.

CyberSecurity Advisors Network

2015 - 2025

10 Year Anniversary Celebrations

15 May 2025 Sydney, Australia

CyAN Cybersecurity Advisors Network

NEWS:

18. DARPA believes AI Cyber Challenge could upend patching as the industry knows it |

Original Source: Cyberscoop by Greg Otto

DARPA’s AI Cyber Challenge is showing promise in reshaping how vulnerabilities are found and patched. AI systems are competing to identify and fix software flaws faster than human teams. The long-term goal is to automate the full vulnerability lifecycle, from discovery to remediation, and reduce reliance on slow, manual processes that leave systems exposed. Early results show autonomous patch generation for previously unknown bugs. If these tools scale, experts believe they could transform defensive operations and redefine how the industry handles software security at speed.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

NEWS:

19. Indian Court Orders Action to Block Proton Mail Over AI Deepfake Abuse Allegations

Original Source: The Hacker News by Ravie Lakshmanan

1.An Indian court has ordered authorities to block access to Proton Mail following allegations that the encrypted service was used to distribute AI-generated deepfake content. The decision has sparked concern among digital rights advocates, who warn that banning secure communication platforms over user misuse risks setting a dangerous precedent. Proton Mail, known for its end-to-end encryption, argues it cannot access user content even if compelled. Experts warn that while combating AI abuse is urgent, targeting encryption itself undermines privacy and weakens the very tools that protect vulnerable groups and dissidents worldwide.

CyberSecurity Advisors Network

NEWS:

20. Cyber experts, Democrats urge Trump administration not to break up cyber coordination in State reorg

Original Source: Cyberscoop by Derek B. Johnson

Cybersecurity experts and Democratic lawmakers are pushing back on plans to restructure the U.S. State Department in a way that could dismantle key cyber coordination offices. Critics argue the proposed changes would fragment responsibility, dilute expertise, and weaken the nation's diplomatic cyber posture at a time when unified strategy is crucial. With cyber threats increasingly tied to foreign policy, advocates say breaking up coordination teams sends the wrong message to allies and adversaries alike. Experts warn that institutional knowledge is hard to rebuild once scattered, and cyber diplomacy cannot afford to be an afterthought.

CyberSecurity Advisors Network

NEWS:

21. Many Fuel Tank Monitoring Systems Vulnerable to Disruption

Original Source: Dark Reading by Jai Vijayan

Security researchers have found that many fuel tank monitoring systems are exposed to the internet with minimal authentication and outdated software, making them easy targets for disruption. These systems are used to track fuel levels in critical infrastructure, including transportation, logistics, and energy sectors. Attackers could manipulate readings, disable alarms, or cut off monitoring entirely. While no active exploitation has been confirmed, experts warn that the sheer accessibility of these devices makes them low-effort, high-impact targets. The findings highlight how overlooked operational systems can quietly become critical vulnerabilities.

CyberSecurity Advisors Network

NEWS:

22. Hackers ramp up scans for leaked Git tokens and secrets

Original Source: BleepingComputer by Bill Toulas

Threat actors are intensifying efforts to scan public Git repositories for leaked API tokens, credentials, and secrets, often using automated tools to detect exposed data within minutes of a push. The growing reliance on infrastructure-as-code and rapid deployment pipelines means that even brief exposures can lead to significant breaches. GitHub and other platforms offer secret scanning and alerting, but many developers remain unaware or fail to act in time. Experts warn that secure DevOps requires more than automation; it demands consistent security hygiene, training, and careful management of sensitive configuration data.

CyberSecurity Advisors Network

NEWS:

23. France ties Russian APT28 hackers to 12 cyberattacks on French orgs

Original Source: BleepingComputer by Sergiu Gatlan

The French government has formally attributed a series of twelve cyberattacks to APT28, a hacking group linked to Russian military intelligence. The attacks targeted government agencies, universities, and critical infrastructure over the past year, using spear phishing and compromised email servers to gain access. France’s rare public attribution underscores a growing willingness among European governments to call out nation-state threats. Experts say public attribution serves as both a deterrent and a diplomatic signal, but warn it must be followed by tangible consequences if it’s to have any lasting impact on hostile cyber behaviour.

CyberSecurity Advisors Network

NEWS:

24. New Reports Uncover Jailbreaks, Unsafe Code, and Data Theft Risks in Leading AI Systems

Original Source: The Hacker News by Ravie Lakshmanan

A wave of new research reveals that several leading AI models remain vulnerable to prompt injection, code generation flaws, and data leakage. Jailbreak techniques continue to bypass safety filters, while some models output insecure code or inadvertently expose training data. These findings reignite concerns about the speed of AI deployment outpacing risk mitigation. Experts warn that while AI capabilities are advancing rapidly, the basic security hygiene around model development and deployment often lags behind. Without stricter oversight and continuous red-teaming, AI may become more exploitable than empowering in critical domains.

CyberSecurity Advisors Network

NEWS:

25. Apple 'AirBorne' flaws can lead to zero-click AirPlay RCE

Original Source: BleepingComputer by Sergiu Gatlan

Researchers have uncovered a set of vulnerabilities dubbed "AirBorne" that affect Apple’s AirPlay and Bluetooth Low Energy protocols, enabling zero-click remote code execution attacks. The flaws could allow attackers to compromise nearby devices simply by being within wireless range, with no user interaction required. Apple has issued patches, but experts warn the attack surface is broader than it seems, as similar vulnerabilities could exist across other wireless communication stacks. The findings serve as a reminder that even user-friendly features designed for convenience can quietly introduce high-risk pathways into otherwise secure ecosystems.

CyberSecurity Advisors Network

NEWS:

26. Enterprise tech dominates zero-day exploits with no signs of slowdown

Original Source: The Register by Connor Jones

New data shows that enterprise software and hardware continue to account for the majority of zero-day exploits, with threat actors increasingly targeting widely deployed platforms like VPNs, firewalls, and cloud infrastructure. Attackers are exploiting vulnerabilities faster than ever, often within days of public disclosure or before patches are available. The trend highlights how enterprise systems offer high rewards with relatively low resistance, especially when patching is delayed. Experts warn that defenders must treat zero-day readiness as a strategic priority, not a niche concern, given its growing role in ransomware and espionage campaigns.

CyberSecurity Advisors Network

NEWS:

27. US Critical Infrastructure Still Struggles With OT Security

Original Source: Dark Reading by Becky Bracken

A new report highlights ongoing weaknesses in the cybersecurity of US critical infrastructure, especially in operational technology (OT). Despite repeated warnings, many organisations still rely on outdated hardware, lack proper segmentation, and fail to monitor for OT-specific threats. The convergence of IT and OT has widened the attack surface and allowed lateral movement within networks. Experts stress that compliance alone is no longer enough. Defending infrastructure now requires proactive, risk-based strategies that account for evolving threats and attacker sophistication.

CyberSecurity Advisors Network

NEWS:

28. House passes legislation to criminalize nonconsensual deepfakes

Original Source: Cyberscoop by Derek B. Johnson

The US House has passed a bill that would make the creation and distribution of nonconsensual deepfake content a federal crime. The legislation, prompted by a surge in AI-generated explicit imagery, particularly targeting women and minors, includes provisions for both criminal penalties and civil remedies. While the move has been broadly welcomed, privacy advocates warn that enforcement must be carefully balanced to avoid unintended consequences for end-to-end encryption and secure communications. Experts argue that protecting victims should not come at the cost of undermining the tools that protect journalists, dissidents, and everyday users.

CyberSecurity Advisors Network

NEWS:

29. SentinelOne Uncovers Chinese Espionage Campaign Targeting Its Infrastructure and Clients

Original Source: The Hacker News by Ravie Lakshmanan

SentinelOne has revealed a Chinese state-aligned espionage campaign that targeted its internal infrastructure and several of its clients using advanced malware and stealthy lateral movement techniques. The attackers focused on exfiltrating sensitive data while avoiding detection by exploiting trusted tools and blending into normal activity. This direct targeting of a cybersecurity vendor underscores a growing trend: threat actors are bypassing hardened front doors and heading straight for the security companies themselves. Experts warn that defending against this kind of intrusion requires constant vigilance and deep, real-time telemetry within security supply chains.

CyberSecurity Advisors Network

NEWS:

30. Europol Creates “Violence-as-a-Service” Taskforce

Original Source: Infosecurity Magazine by Phil Muncaster

Europol has launched a new taskforce to investigate the rise of “violence-as-a-service” networks, which offer contract-based physical attacks, assassinations, and harassment coordinated through encrypted platforms. These services are often funded via cryptocurrency and marketed on dark web forums, blurring the lines between cybercrime and real-world violence. The taskforce aims to disrupt these operations by tracing digital footprints, payment flows, and cross-border connections. Experts say the move reflects an urgent need to treat online facilitation of violence as a serious security threat, not just a fringe phenomenon of the cyber underground.

CyberSecurity Advisors Network

NEWS:

31. 76% of Australian orgs experienced at least one high-impact cyber event ‘halting critical business functions’ in past year

Original Source: itWire by Gordon Peters

A new survey reveals that 76 percent of Australian organisations experienced at least one high-impact cyber incident in the past year, with many reporting disruptions to critical business functions. The data points to a growing gap between cyber risk awareness and actual readiness, particularly among mid-sized enterprises. Respondents cited ransomware, third-party breaches, and inadequate incident response as top pain points. Experts warn that without stronger investment in proactive defence, workforce training, and real-time monitoring, the trend will worsen. In an environment of rising threats, hope is not a strategy, and recovery is not resilience.

CyberSecurity Advisors Network

NEWS:

32. France says Russian hackers behind attack on Macron’s 2017 presidential campaign

Original Source: The Guardian by Angelique Chrisafis

The French government has formally accused Russian state-backed hackers of orchestrating the 2017 cyberattack on Emmanuel Macron’s presidential campaign. The operation involved phishing, data leaks, and disinformation designed to disrupt the election and sow distrust. Attribution points to APT28, the same group recently linked to other attacks across Europe. Officials say the announcement is intended to counter ongoing foreign interference ahead of the next election cycle. Experts stress that public attribution is only the first step, and without coordinated deterrence, these long-tail operations will continue to undermine democratic processes.

CyberSecurity Advisors Network

ANALYSIS:

33. A Cybersecurity Paradox: Even Resilient Organizations Are Blind to AI Threats

Original Source: Dark Reading by Arielle Waldman

New research highlights a growing paradox: even organisations with mature cybersecurity programs are largely unprepared for the threats posed by AI. While many have invested in tooling and training, they often lack visibility into how AI systems are built, tested, and deployed. This blind spot leaves them vulnerable to prompt injection, model manipulation, and unsafe code generation. The report calls for tighter collaboration between security and AI teams, alongside new governance models that treat AI as a unique risk class. Experts warn that without this shift, resilience on paper may not translate to real-world protection.

CyberSecurity Advisors Network

ANALYSIS:

34. New Research Reveals: 95% of AppSec Fixes Don't Reduce Risk

Original Source: The Hacker News

New research highlights a growing paradox: even organisations with mature cybersecurity programs are largely unprepared for the threats posed by AI. While many have invested in tooling and training, they often lack visibility into how AI systems are built, tested, and deployed. This blind spot leaves them vulnerable to prompt injection, model manipulation, and unsafe code generation. The report calls for tighter collaboration between security and AI teams, alongside new governance models that treat AI as a unique risk class. Experts warn that without this shift, resilience on paper may not translate to real-world protection.

CyberSecurity Advisors Network

ANALYSIS:

35. Debunking Security 'Myths' to Address Common Gaps

Original Source: Dark Reading by Arielle Waldman

A new report identifies several persistent security myths that are leaving organisations exposed, including the belief that cyber insurance is a fallback for poor defences and that compliance equals security. These misconceptions contribute to misallocated resources and a false sense of protection. The report calls out over-reliance on single tools, underinvestment in basic controls, and the tendency to prioritise convenience over resilience. Experts stress that effective security posture depends on clear-eyed risk assessments, cultural buy-in, and leadership that understands cybersecurity as a business-critical function, not just a checkbox on an audit form.

CyberSecurity Advisors Network

ANALYSIS:

36. World Password Day 2025: Rethinking Security in the Age of MFA and Passkeys

Original Source: It Security Guru by The Gurus

World Password Day 2025 may have passed, but the call to move beyond passwords remains urgent. Experts are encouraging adoption of modern authentication methods like passkeys and multi-factor authentication (MFA), which offer stronger and more user-friendly protection. While awareness is high, adoption remains inconsistent due to poor user experience and fragmented rollout. Passkeys, based on cryptographic standards, offer a promising future but require widespread industry support. Experts argue that the future of identity is password-less, and security must be embedded, not added as an afterthought.

CyberSecurity Advisors Network

ANALYSIS:

37. Source of data': are electric cars vulnerable to cyber spies and hackers?

Original Source: The Guardian by Dan Milmo

As electric vehicles (EVs) become more connected, cybersecurity experts are warning that they may offer a rich source of data for hackers and nation-state actors. From GPS logs to driver behaviour and communication links with charging infrastructure, EVs generate and transmit vast amounts of sensitive information. Concerns are mounting over data sovereignty, particularly when vehicles are manufactured by companies with ties to authoritarian regimes. Experts say regulatory frameworks have not kept pace with the technology, leaving gaps in how EV data is secured, governed, and protected from potential misuse or espionage.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

STATISTICS & INSIGHTS
powered by evisec

Highlights from this week's cybersecurity research by evisec - CRD #21

Original Source: CyAN Member and evisec CEO Henry Röigas

•Unacknowledged access is a growing blind spot in breach investigations, with too many incidents uncovering long-standing privileges no one thought to revoke.
•Victim shaming remains a problem, especially in complex attack scenarios where detection time is high but defensive posture was solid. Blame doesn't fix blind spots.
•Board-level appetite for action is still being shaped more by regulatory pressure than by a genuine security culture. Henry Röigas suggests that this dynamic is unsustainable in the long run and risks leaving organisations unprepared when external enforcement shifts or fades.
•And yes, AI's risk amplification continues to feature, especially as attackers exploit decision-making dependencies and speed up their own cycles.

For more insights, explore the latest Cybersecurity Research Digest.

CyberSecurity Advisors Network

Online Safety for Kids and Teens

Highlights from the latest Vys ‘Online Safety for Kids and Teens’ Biweekly Brief

By CyAN Member and Vyanams Strategies Founder Vaishnavi J

- UK watchdogs have launched a formal probe into TikTok’s handling of self-harm and suicide content, raising questions about algorithmic amplification and moderation gaps.

- Meta’s announcement of stronger teen protections is being met with scepticism, particularly around real-world enforcement and data use transparency.

- Child sexual abuse material (CSAM) detection proposals in Europe remain deeply polarising, with encryption advocates and child protection campaigners locked in legislative stalemate.

- Meanwhile, a new wave of youth-targeted phishing is exploiting anxiety over school performance, showing how emotional manipulation tactics are evolving in parallel with tech.

CyberSecurity Advisors Network

UPCOMING CyAN and CyAN Partner EVENTS:

- **GISEC Global, Dubai World Trade Centre: 6-8 May https://gisec.ae/home**
- **The Cyber Outstanding Security Performance Awards (Cyber OSPAs), London, UK: 8 May https://www.thecyberospas.com/about/**
- **CSG Awards 2025, Dubai: 7 May https://csgawards.com/**
- **World AI Technology Expo, Dubai: 14-15 May https://worldaiexpo.io**
- **CyAN 10th Anniversary Celebrations!**
- **GITEX Europe Messe, Berlin: 21-23 May https://www.gitex-europe.com/**
- **MaTeCC, Rabat, Morocco: 7-9 June https://tinyurl.com/mtecz8vw**
- **CyAN Q2 Community Call (APAC and the Gulf), June 11: 12:00 GST / 16:00 SGT / 18:00 AEST**
- **CyAN Q2 Community Call (EMEA and the Americas), June 11: 20:00 GST / 18:00 CET / 17:00 UTC / 12:00 EDT**

Catch up on Past Issues:

Missed an issue of (In)Securities? No worries! Scan the QR code to explore our archive of past editions—packed with insights, trends, and actionable tips to keep you ahead in the ever-evolving world of cybersecurity. Dive in and catch up today!

CyberSecurity Advisors Network

If you found this interesting, please like and share it with your friends and colleagues!

#ReallyInterestingCyberStuff!
#SharingIsCaring