CyAN Cybersecurity Advisors Network

Cyber (In)Securities

Issue #116

NEWS:

1. Microsoft Cracks Down on Malicious Copilot AI Use

Original Source: Dark Reading by Kristina Beek

Microsoft has announced stricter measures to address the misuse of its AI-powered Copilot tool, following reports of malicious applications.

The crackdown includes enhanced safeguards to prevent the tool from being exploited for phishing, malware creation, and other cyber threats. This move highlights the double-edged nature of generative AI, which offers innovation while introducing new risks.

Microsoft's stance demonstrates the importance of balancing technological advancement with ethical considerations.

CyberSecurity Advisors Network

NEWS:

2. Cryptojacking, backdoors abound as fiends abuse Aviatrix Controller bug

Original Source: The Register by Connor Jones

A critical vulnerability in the Aviatrix Controller is being actively exploited by attackers for cryptojacking and backdoor installation.

The flaw allows cybercriminals to hijack computing resources, often going undetected. Experts warn that the exploitation could escalate, urging affected organisations to patch systems immediately.

This incident underscores the importance of rigorous vulnerability management and proactive monitoring to counter evolving cyber threats.

CyberSecurity Advisors Network

NEWS:

3. Cyberattackers Hide Infostealers in YouTube Comments, Google Search Results

Original Source: Dark Reading by Elizabeth Montalbano

Cybercriminals are embedding infostealing malware in seemingly harmless YouTube comments and Google search results, leveraging trusted platforms to distribute malicious links. These tactics exploit user trust and familiarity, increasing their success rate.

Security experts recommend heightened vigilance when interacting with online content and emphasise the need for advanced threat detection technologies to combat such creative distribution methods.

CyberSecurity Advisors Network

NEWS:

4. Ransomware crew abuses AWS native encryption, sets data-destruct timer for 7 days

Original Source: iThe Register by Jessica Lyons

A ransomware group is weaponising AWS's native encryption capabilities, locking victim data and setting a seven-day destruction timer.

By using legitimate cloud features maliciously, attackers make detection and recovery challenging. Security analysts warn this approach may inspire similar tactics across cloud platforms.

Organisations are urged to tighten access controls and implement robust backup strategies to mitigate potential fallout.

CyberSecurity Advisors Network

NEWS:

5. Europe coughs up €400 to punter after breaking its own GDPR data protection rules

Original Source: The Register by Brandon Vigliarolo

In a notable GDPR enforcement case, Europe has paid €400 to an individual after admitting a breach of its own data protection rules.

The incident has reignited debates on accountability, showcasing that even regulatory bodies must adhere to compliance.

Critics argue the payout is symbolic but insufficient to address broader systemic issues.

The case underscores the necessity of stringent self-regulation to maintain public trust in GDPR's legitimacy.

CyberSecurity Advisors Network

NEWS:

6. Emerging FunkSec Ransomware Developed Using AI

Original Source: Security Week by Ionut Arghire

A new ransomware variant, FunkSec, is gaining attention for its use of AI in development, allowing for advanced evasion and rapid adaptation.

The malware targets enterprise networks, encrypting data while bypassing traditional defences. This evolution highlights the growing intersection of artificial intelligence and cybercrime.

Experts stress the importance of advanced detection solutions and cross-industry collaboration to counter this new wave of AI-powered threats.

CyberSecurity Advisors Network

NEWS:

7. Expired Domains Allowed Control Over 4,000 Backdoors on Compromised Systems

Original Source: The Hacker News Ravie Lakshmanan

Researchers discovered that expired domains were being exploited to control over 4,000 backdoors on compromised systems.

Cybercriminals used these domains to maintain access and exfiltrate data, demonstrating the risks of poor domain management.

Organisations are urged to monitor and secure unused or expired domains to prevent their exploitation.

The incident reinforces the importance of holistic cybersecurity strategies that include asset management.

CyberSecurity Advisors Network

NEWS:

8. Credit card skimmer campaign targets Wordpress via Database Injection

Original Source: Security Affairs by Pierluigi Paganini

A new credit card skimming campaign is targeting WordPress sites through database injection attacks.

Cybercriminals exploit vulnerabilities to insert malicious code, capturing payment data directly from e-commerce platforms.

Security experts emphasise the importance of patching WordPress plugins, securing databases, and monitoring for unauthorised changes.

This campaign serves as a reminder of the persistent threat to online payment systems.

CyberSecurity Advisors Network

NEWS:

9. Australian Cyber Security Centre names its next head

Original Source: itNews by Ry Crozier

The Australian Cyber Security Centre (ACSC) has named its new head, signalling a strategic shift in leadership to bolster the nation’s defences. With a robust background in intelligence and cybersecurity, the appointee is tasked with addressing escalating cyber threats.

The announcement underscores the government’s focus on collaboration between the public and private sectors, ensuring Australia's readiness to respond to complex cyber challenges.

Industry observers view this leadership change as pivotal to advancing resilience in a rapidly evolving threat landscape.

CyberSecurity Advisors Network

NEWS:

10. Phishing texts trick Apple iMessage users into disabling protection

Original Source: Bleeping Computer by Lawrence Abrams

A sophisticated phishing campaign is targeting Apple users via iMessage, tricking them into disabling critical security protections.

By masquerading as legitimate alerts, the attackers lure users into clicking malicious links, opening the door to device compromise. This tactic exposes the risks of social engineering and the importance of vigilance.

Apple users are reminded to scrutinise unexpected messages and avoid links, even those that appear trustworthy. With phishing tactics becoming increasingly advanced, education remains key to mitigating these attacks.

CyberSecurity Advisors Network

NEWS:

11. Tech giants told UK online safety laws ‘not up for negotiation’

Original Source: The Observer by Michael Savage

The UK government has taken a firm stance with tech giants over its Online Safety Bill, making it clear that compliance is non-negotiable.

Designed to tackle harmful online content and enhance user protection, the law introduces stringent penalties for noncompliance. Critics argue the measures could undermine encryption standards, while supporters emphasise the urgent need for accountability in digital spaces.

The debate highlights tensions between privacy advocates and regulatory bodies as the UK aims to set global standards for online safety.

CyberSecurity Advisors Network

NEWS:

12. Fake LDAPNightmware exploit on GitHub spreads infostealer malware

Original Source: Bleeping Computer by Bill Toulas

Cybercriminals are exploiting GitHub to distribute a fake LDAPNightmare exploit, which deploys infostealer malware onto unsuspecting systems.

By masquerading as a tool for addressing known vulnerabilities, the malicious software infiltrates networks to steal sensitive data. This campaign highlights the persistent dangers of downloading unverified tools, even from trusted platforms.

Security experts urge vigilance, emphasising the need for proper vetting and monitoring to counter the growing use of trusted ecosystems for malicious purposes.

CyberSecurity Advisors Network

NEWS:

13. Microsoft MFA outage blocking access to Microsoft 365 apps

Original Source: Bleeping Computer by Sergiu Gatlan

A Microsoft multi-factor authentication (MFA) outage left users unable to access Microsoft 365 apps, disrupting business operations worldwide.

The issue highlighted the reliance on cloud services and the potential impact of downtime.

While Microsoft worked to resolve the problem, experts underscored the importance of having contingency plans for critical systems to minimise disruption during service outages.

CyberSecurity Advisors Network

NEWS:

14. Microsoft DRM Hacking Raises Questions on Vulnerability Disclosures

Original Source: Security Week by Eduard Kovacs

A recent vulnerability in Microsoft's DRM system, exploited to bypass content restrictions, has sparked debate over responsible disclosure.

Researchers argue that such vulnerabilities could serve as a blueprint for malicious actors if mishandled. While Microsoft moves to patch the issue, critics emphasise the delicate balance between transparency and security.

The case reignites discussions around the ethics of vulnerability research and how companies respond to public disclosures.

CyberSecurity Advisors Network

NEWS:

15. Russian ISP confirms Ukrainian hackers "destroyed" its network

Original Source: Bleeping Computer by Sergiu Gatlan

A Russian ISP has publicly acknowledged that Ukrainian hackers caused significant disruptions to its network, describing the attack as destructive.

This incident underscores the escalating role of cyber warfare in geopolitical conflicts. With critical infrastructure often the target, the attack highlights vulnerabilities and the increasing sophistication of cyber adversaries.

The broader implications of these attacks extend beyond regional disputes, emphasising the need for global readiness.

CyberSecurity Advisors Network

NEWS:

16. Microsoft moves to disrupt hacking-as-a-service scheme that’s bypassing AI safety measures

Original Source: Cyberscoop by Derek B. Johnson

Microsoft has disrupted a hacking-as-a-service operation that leveraged AI to bypass safety protocols, demonstrating the growing sophistication of cybercriminals.

The service targeted enterprises by automating attacks, emphasising the intersection of AI and cyber threats. While Microsoft’s intervention highlights the power of collaboration, the incident raises concerns about future AI misuse.

The tech community is increasingly focused on balancing innovation with safeguarding against exploitation.

CyberSecurity Advisors Network

NEWS:

17. PayPal Phishing Campaign Employs Genuine Links to Take Over Accounts

Original Source: Security Week by Ionut Arghire

Cybercriminals are exploiting PayPal accounts with a phishing campaign that cleverly embeds legitimate links alongside malicious ones, tricking users into sharing credentials. This tactic preys on trust, exploiting familiarity with real PayPal URLs to bypass suspicion.

Once credentials are captured, attackers gain full control of user accounts. Experts warn this approach is increasingly common and urge users to verify all emails, avoid clicking unsolicited links, and activate multi-factor authentication to reduce risk.

CyberSecurity Advisors Network

NEWS:

18. Google Project Zero Researcher Uncovers Zero-Click Exploit Targeting Samsung Devices

Original Source: The Hacker News by Ravie Lakshmanan

A zero-click exploit targeting Samsung devices has been exposed by a Google Project Zero researcher, revealing vulnerabilities that allow attackers to execute remote code without user interaction.

The exploit, aimed at Samsung's Exynos chipsets, poses a significant threat to user security, particularly for high-value targets.

Samsung has responded with security updates, but the incident underscores the urgency of maintaining updated devices and highlights the role of proactive vulnerability research in defending against emerging threats.

CyberSecurity Advisors Network

NEWS:

19. Telegram Shared Data of Thousands of Users After CEO’s Arrest

Original Source: Security Week by Eduard Kovacs

Telegram faces backlash after it shared data on thousands of users, reportedly under legal pressure following its CEO's arrest.

Known for its encryption and privacy-first approach, this revelation challenges the platform’s credibility. Critics warn this sets a dangerous precedent for user trust and data protection.

While Telegram defends its actions as compliance, the incident fuels debates over the balance between legal obligations and user privacy, especially in jurisdictions with authoritarian leanings.

CyberSecurity Advisors Network

NEWS:

20. FCC Launches 'Cyber Trust Mark' for IoT Devices to Certify Security Compliance

Original Source: The Hacker News by Ravie Lakshmanan

The FCC has introduced a new 'Cyber Trust Mark' program to certify IoT devices that meet stringent security standards.

This initiative aims to improve consumer confidence and address vulnerabilities in smart home devices, a known weak link in cybersecurity. By setting clear compliance benchmarks, the program encourages manufacturers to prioritise security.

Experts applaud the move but caution that enforcement and keeping pace with evolving threats will be critical for its success.

CyberSecurity Advisors Network

ANALYSIS:

21. Will the EU fight for the truth on Facebook and Instagram?

Original Source: The Guardian by Lucas Graves

The EU faces mounting pressure to hold Meta accountable for misinformation on Facebook and Instagram.

Critics argue that Meta's policies favor profit over truth, undermining democratic values. As elections approach, the EU must decide whether to enforce stricter regulations or risk the spread of harmful content.

This debate highlights the growing role of regulatory bodies in shaping the digital information landscape and ensuring platforms prioritise societal responsibility.

CyberSecurity Advisors Network

ANALYSIS:

22. Best Practices & Risks Considerations in LCNC and RPA Automation

Original Source: Dark Reading by Jordan Bonagura

Low-code/no-code (LCNC) and robotic process automation (RPA) tools are transforming efficiency but introducing unique security risks.

As businesses adopt these platforms to streamline operations, experts warn of potential vulnerabilities, including misconfigurations and inadequate oversight.

Organisations are encouraged to implement strict governance, conduct thorough risk assessments, and train users to mitigate security gaps. While LCNC and RPA offer immense benefits, ensuring security must remain a top priority.

CyberSecurity Advisors Network

ANALYSIS:

23. Innovation, Automation, And The Cybersecurity Challenges Ahead

Original Source: Forbes by Tony Bradley

The rapid integration of automation and innovative technologies is reshaping cybersecurity, offering both opportunities and challenges.

Automated defences like AI-driven threat detection are accelerating responses but also raising concerns about over-reliance.

Experts emphasise balancing innovation with human oversight to address emerging risks. As attackers adapt to these technologies, the cybersecurity industry must prioritise collaboration and adaptability to outpace threats.

CyberSecurity Advisors Network

ANALYSIS:

24. The Path Toward Championing Diversity in Cybersecurity Education

Original Source: Dark Reading by Laurie Salvail

Building diversity in cybersecurity education is vital to addressing talent shortages and fostering innovation.

Experts argue that inclusive programs attract a broader range of perspectives, essential for tackling complex challenges. Initiatives like scholarships, mentorships, and targeted outreach aim to reduce barriers for underrepresented groups.

By embracing diversity, the cybersecurity industry can better prepare for future demands while creating equitable opportunities for all.

CyberSecurity Advisors Network

ANALYSIS:

25. How AI will transform cybersecurity in 2025 - and supercharge cybercrime

Original Source: ZDNet by Dan Patterson

Artificial intelligence is set to revolutionise cybersecurity in 2025, both as a defense tool and a weapon for cybercriminals.

On the defensive side, AI-driven solutions promise faster threat detection and response. However, attackers are also harnessing AI to automate and amplify cybercrime, creating sophisticated malware and bypassing traditional defences.

Experts stress the importance of ethical AI development and robust regulations to mitigate risks while leveraging its potential to bolster cybersecurity frameworks.

CyberSecurity Advisors Network

CyAN Members Op Eds, Articles, etc:

26. The Cybersecurity Landscape in 2025: Top Predictions and Implications for Leaders

Original Source: CyAN Blog by Joe Cozzupoli

The cybersecurity landscape in 2025 is set to evolve dramatically, shaped by advancing technologies and emerging threats.

CyAN member Joe Cozzupoli delivers a thought-provoking analysis in his Op Ed, predicting a rise in supply chain attacks, a rise in supply chain attacks, stricter regulations, and greater reliance on AI-driven defences.

He advises leaders to prioritise risk management, workforce diversity, and public-private collaboration. By anticipating these trends, organisations can navigate challenges and capitalise on opportunities for growth.

CyberSecurity Advisors Network

CyAN Members Op Eds, Articles, etc:

27. Resilience or Regulation? Europe's Digital Transformation at a Crossroads

Original Source: CyAN Blog by Gilles Chevillon

Europe's digital transformation stands at a critical juncture, balancing the need for resilience against the demands of stringent regulations.

In his insightful Op Ed, CyAN member Gilles Chevillon explores the growing tension between fostering innovation and ensuring security in the face of rising cyber threats.

Gilles highlights the central debate: do compliance-heavy frameworks stifle progress or build trust? His analysis underscores the importance of striking the right balance to create a secure, competitive digital ecosystem.

CyberSecurity Advisors Network

CyAN Mentorship Program 2025:

At CyAN, we believe mentorship is a powerful tool to nurture future leaders and strengthen our global community.

Our structured three-month mentorship program offers professional guidance, international networking opportunities, and real-world insights tailored to support graduate students and early-career professionals.

By connecting with experienced CyAN members, mentees gain invaluable skills and perspectives to advance their careers.

If you’re ready to grow, learn, and thrive alongside experts in cybersecurity and trust & safety, we encourage you to join this transformative opportunity.

CyAN Cybersecurity Advisors Network

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!

UPCOMING EVENTS:

- **CyAN AGM 14/15 January**
- **AI Global Everything, Dubai, UAE: 4-6 February**
- **GITEX AFRICA, Marrakesh, Morocco: 14-16 April**
- **GITEX ASIA: Singapore (Marina Bay Sands) 23-25 April**
- **GISEC: Dubai Word Trade Center, Dubai, UAE: 6th to 8th May**
- **The Cyber Outstanding Security Performance Awards (Cyber OSPAs), May 8, London, UK**
- **MaTeCC, Rabat, Morocco: 7-9 June, 2025 (**The third annual North Africa and beyond cybersecurity event, hosted by CyAN partner organisation École High-Tech.)

CyberSecurity Advisors Network

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

#ReallyInterestingCyberStuff!
#SharingIsCaring