CyAN Cybersecurity Advisors Network

Cyber (In)Securities

Issue #113

NEWS:

1. How Chinese insiders are stealing data scooped up by President Xi's national surveillance system

Original Source: The Register by Jessica Lyons

Chinese insiders have reportedly leaked data from President Xi Jinping’s national surveillance system, exposing significant vulnerabilities within the massive monitoring network.

These breaches, involving sensitive personal and governmental information, were motivated by financial gain and dissatisfaction among employees. The incident underscores the paradox of surveillance programs—designed to monitor others but susceptible to insider threats.

Experts emphasise the importance of implementing robust internal security measures, including strict access controls, encrypted storage, regular audits, and insider threat detection systems, to safeguard critical data from unauthorised access and internal sabotage.

CyberSecurity Advisors Network

NEWS:

2. Ultralytics AI Library Compromised: Cryptocurrency Miner Found in PyPI Version

Original Source: The Hacker News by Ravie Lakshmanan

The popular Ultralytics AI library was recently compromised on the Python Package Index (PyPI), with malicious versions containing cryptocurrency mining malware.

Attackers inserted the miner into the package, exploiting its widespread use among developers in AI and machine learning projects. The breach highlights ongoing risks in the software supply chain, as open-source repositories remain prime targets for cybercriminals.

Experts urge developers to verify package integrity, review dependencies, and use automated tools to detect compromised libraries. The incident underscores the need for enhanced security in managing open-source ecosystems.

CyberSecurity Advisors Network

NEWS:

3. Anna Jaques Hospital ransomware breach exposed data of 300K patients

Original Source: Bleeping Computer by Bill Toulas

Anna Jaques Hospital has confirmed a ransomware breach that compromised the personal data of over 300,000 patients. The attackers accessed sensitive information, including medical records and Social Security numbers, raising concerns about identity theft and patient privacy.

The breach highlights the growing vulnerability of healthcare institutions, which often lack sufficient cybersecurity defences to combat increasingly sophisticated ransomware tactics. Experts emphasise the urgent need for robust encryption, proactive threat detection, and incident response plans in the healthcare sector. This incident also underscores the importance of educating staff on cyber hygiene and investing in comprehensive data security to prevent future attacks targeting critical patient data.

CyberSecurity Advisors Network

NEWS:

4. 8Base Ransomware Group Hacked Croatia’s Port of Rijeka

Original Source: Security Affairs by Pierluigi Paganini

The 8Base ransomware group has claimed responsibility for a cyberattack on Croatia's Port of Rijeka, disrupting operations and exposing sensitive data.

This breach underscores the growing risks ransomware poses to critical infrastructure, particularly ports that are vital to global supply chains. Experts warn that the group’s tactics include encrypting systems and threatening data leaks to pressure victims into paying.

The attack highlights the urgent need for maritime and logistics sectors to strengthen cybersecurity measures, such as real-time monitoring, zero-trust architectures, and incident response protocols. As ransomware groups increasingly target critical infrastructure, international collaboration and regulatory frameworks are essential to mitigate these escalating threats

CyberSecurity Advisors Network

NEWS:

5. FBI Says Everyone Should Use Encryption Apps for Their Calls and Texts After China Hack: ‘Encryption Is Your Friend’

Original Source: People by Toria Sheffield

The FBI is urging Americans to adopt end-to-end encryption for calls and texts following a massive China-linked hack.

Encryption, the agency says, is a vital tool for safeguarding personal and sensitive communications from advanced cyber threats. This advice comes amid increasing attacks on private and public systems, with state-sponsored groups exploiting unencrypted communications to gather intelligence and compromise security.

The call to action underscores the importance of digital literacy, encouraging individuals and businesses to prioritise secure communication tools. As cyber espionage threats escalate globally, encryption remains a critical line of defence against unauthorised access and data breaches.

CyberSecurity Advisors Network

NEWS:

6. Romania’s Election System Hit by 85,000 Attacks Ahead of Presidential Vote

Original Source: Security Affairs by Pierluigi Paganini

Romania’s election system endured 85,000 cyberattacks in the lead-up to its presidential vote, highlighting vulnerabilities in democratic processes. The attacks, ranging from DDoS to phishing, aimed to destabilise operations and sow distrust.

Analysts suggest state-sponsored actors may have been involved, leveraging the chaos to influence outcomes or disrupt electoral confidence. Romania’s cybersecurity agencies responded with defensive measures, but the scale and intensity of the threats underscore the global risk to electoral integrity.

This case reinforces the urgency of fortifying election systems against evolving cyber threats.

CyberSecurity Advisors Network

NEWS:

7. Micropatchers share 1-instruction fix for NTLM hash leak flaw in Windows 7+

Original Source: The Register by Iain Thomson

A critical NTLM hash leak vulnerability in Windows 7 and newer systems has prompted the micropatching community to deliver a one-instruction fix, providing temporary protection for users.

Exploited by attackers to harvest credentials, the flaw highlights ongoing risks in both legacy and modern Windows systems. While Microsoft has yet to release an official patch, this micropatch exemplifies the importance of community-driven initiatives to address urgent security gaps.

The incident reinforces the need for organisations to adopt rigorous patching protocols, robust endpoint monitoring, and a proactive approach to safeguarding sensitive data.

CyberSecurity Advisors Network

NEWS:

8. Solana blockchain's popular web3.js npm package backdoored to steal keys, funds

Original Source: The Register by Thomas Claburn

The popular web3.js npm package, integral to Solana blockchain development, has been compromised with a backdoor, enabling attackers to steal private keys and funds.

This alarming breach highlights the vulnerabilities of open-source ecosystems, where malicious actors exploit the trust developers place in widely used libraries. The incident underscores the need for robust vetting processes, dependency audits, and real-time monitoring of software supply chains.

Solana developers are urged to update affected packages immediately to mitigate risks and safeguard assets, as this breach could have far-reaching implications for the broader web3 and crypto communities.

CyberSecurity Advisors Network

NEWS:

9. No one is safe from Pegasus: spyware detected on ordinary people's phone

Original Source: CyberNews by Ernestas Naprys

Pegasus spyware, infamous for targeting high-profile individuals, has now been found on the phones of ordinary citizens, raising fresh alarms about privacy and surveillance.

This development highlights the evolving threat posed by sophisticated spyware, which can compromise devices without user interaction. Experts warn that Pegasus's widespread availability underscores the need for stronger global regulation and advanced security measures to protect vulnerable users. T

he case demonstrates that no one is immune from such invasive tools, urging individuals and organisations to prioritise device security and vigilance against emerging threats.

CyberSecurity Advisors Network

NEWS:

10. Texas Teen Arrested for Scattered Spider Telecom Hacks

Original Source: Dark Reading by Becky Bracken

A Texas teenager has been arrested for their alleged involvement in the Scattered Spider group, linked to high-profile telecom hacks.

This group has been accused of breaching multiple companies, using advanced social engineering techniques to gain access to sensitive systems. The arrest highlights the growing participation of young hackers in sophisticated cybercriminal operations.

Experts stress the importance of proactive threat detection and employee training to prevent such breaches. The incident also raises questions about how easily determined attackers can exploit human factors, underscoring the need for organisations to bolster both technological and behavioural defences.

CyberSecurity Advisors Network

NEWS:

11. Ransomware Gangs' Merciless Attacks Bleed Small Companies Dry

Original Source: Insurance Journal by Ryan Gallagher

Ransomware gangs are increasingly targeting small businesses, leaving them struggling with financial losses and operational chaos. These attacks exploit weaker defences, encrypting critical data and demanding exorbitant ransoms.

Many businesses face closure, as recovery costs often exceed available resources. Cybersecurity experts stress the need for robust backups, employee training, and incident response plans to mitigate risks.

As ransomware tactics grow more aggressive, small businesses must prioritise cybersecurity as an essential component of survival in an increasingly hostile digital environment.

CyberSecurity Advisors Network

NEWS:

12. Senate Passes TAKE IT DOWN Act to Combat Image-Based Sexual Abuse

Original Source: Levin Law

The U.S. Senate has passed the TAKE IT DOWN Act, a landmark bill aimed at combating image-based sexual abuse (IBSA), such as revenge porn and non-consensual deepfakes.

The legislation empowers victims to request the removal of abusive content from online platforms and imposes stricter obligations on tech companies to address such violations.

Advocates praise the act as a step toward protecting vulnerable populations, particularly women and minors, from exploitation. Critics, however, highlight enforcement challenges and potential loopholes. The Act reflects growing recognition of the need for stronger safeguards against digital abuse, setting a precedent for international action on this issue.

CyberSecurity Advisors Network

NEWS:

13. The number of teenagers who've been deepfaked is seriously worrying

Original Source: Cosmopolitan by Jennifer Savin

A rising wave of deepfake technology is targeting teenagers, sparking significant concerns about digital safety and ethical use. Experts report a disturbing increase in the use of AI-generated content to create fake explicit images of minors, often disseminated without their consent.

This trend highlights the intersection of technological advancement and digital harm, underscoring gaps in regulations and the need for swift intervention. Parents, educators, and policymakers are urged to prioritise education about AI misuse and implement stronger measures to prevent these abuses. As deepfake tools become more accessible, the article stresses the urgency of safeguarding young people in the digital age.

CyberSecurity Advisors Network

NEWS:

14. Russian APT Hackers Co-Opt Pakistani Infrastructure

Original Source: ISMG Data Breach Today by Akshaya Asoka

Russian APT hackers have been found exploiting Pakistani infrastructure to launch cyberattacks, further complicating the global threat landscape.

Using compromised servers and networks, the group has targeted critical industries and government agencies, spreading advanced malware to exfiltrate sensitive data. This tactic not only obscures the attackers' origins but also intensifies geopolitical tensions by implicating third-party nations.

Cybersecurity experts emphasise the need for enhanced threat intelligence sharing and robust defences to detect and thwart such sophisticated attacks, which leverage global infrastructure vulnerabilities.

CyberSecurity Advisors Network

NEWS:

15. 65% of employees bypass cybersecurity policies, driven by hybrid work and flexible access

Original Source: Tech Monitor by Swagath Bandhakavi

A new study reveals that 65% of employees bypass cybersecurity policies, citing hybrid work demands and the need for flexible access.

This widespread non-compliance exposes organisations to significant risks, including data breaches and malware attacks. Employees often prioritise productivity over security, creating a disconnect between user needs and security measures.

Experts recommend cultivating a culture of cybersecurity awareness, using intuitive security tools, and adapting policies to fit hybrid work realities. Addressing this gap is essential for protecting sensitive data and maintaining operational resilience.

CyberSecurity Advisors Network

CyAN Member's Features:

16. The Imperative to Protect End-to-End Encryption in the Face of Rising Cyber Threats

Original Source: Kim Chandler McDonald

In an op-ed, CyAN VP Kim Chandler McDonald highlights the growing importance of protecting end-to-end encryption (E2EE) amidst rising cyber threats.

She argues that E2EE is crucial for safeguarding sensitive communications against escalating risks such as ransomware, espionage, and data breaches. However, calls for backdoors in encryption threaten its integrity, exposing users to vulnerabilities.

The article emphasises that weakening encryption to enable surveillance undermines privacy and security for all. McDonald urges policymakers, tech companies, and citizens to advocate for robust encryption standards, framing it as a cornerstone of digital safety and trust in an increasingly connected world.

CyberSecurity Advisors Network

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!

Entries Open for the 2025 Cyber OSPAs

The Cyber Outstanding Security Performance Awards (OSPAs) are back for 2025, recognising exceptional achievements across the global cybersecurity sector. Entries are open until 4 February 2025, with nominations invited in categories such as:

- Outstanding CISO
- Outstanding Cybersecurity Team
- Outstanding Customer Service Initiative
- Outstanding Young Cybersecurity Professional
- Lifetime Achievement

Winners will be announced during the Big SASIG Conference Dinner on 8 May 2025 in central London.

CyAN is a proud partner of the Cyber OSPAsand we encourage you to nominate the individuals, teams, and initiatives that deserve to be recognised. Whether it's a standout CISO, an innovative product, or an exceptional young professional, this is your opportunity to shine a spotlight on excellence in our industry!

UPCOMING CyAN EVENTS

- **AI Global Everything** will be held from **4th to 6th February 2025** in Dubai, U.A.E.
- **GITEX AFRICA, Marrakesh, Morocco**: **14 - 16 April, 2025**
- **GISEC**: the 14th edition of Middle East & Africa's Cybersecurity Event to be held from **6th to 8th May 2025**, at Dubai Word Trade Center, **Dubai, UAE**
- **MaTeCC, Rabat, Morocco, 7-9 June, 2025**: The third annual North Africa and beyond cybersecurity event, **hosted by CyAN partner organization École High-Tech**

CyberSecurity Advisors Network

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

#ReallyInterestingCyberStuff!
#SharingIsCaring