CyAN Cybersecurity Advisors Network

Cyber (In)Securities

Issue #106

NEWS:

1. NSO – not government clients – operates its spyware, legal documents

Original Source: The Guardian by Stephanie Kirchgaessner

New legal documents suggest that NSO Group, not its government clients, operates the Pegasus spyware used to hack into devices. This claim contradicts NSO's public stance that only authorised government entities handle its software, sparking fresh controversy over the company's practices.

Filed as part of an ongoing lawsuit, these revelations may lead to intensified scrutiny from international regulators, especially given allegations of human rights abuses tied to Pegasus.

If NSO is proven to be in control, it could face legal and diplomatic consequences, as Pegasus has been used against journalists, activists, and political dissidents worldwide.

CyberSecurity Advisors Network

NEWS:

2. “FYI. A Warrant Isn’t Needed': Secret Service Says You Agreed To Be Tracked With Location Data

Original Source: 404 Media by Joseph Cox

Documents obtained by 404 Media reveal the US Secret Service’s claim that individuals implicitly consent to location tracking simply by using apps or services that gather location data. As a result, the agency asserts it does not need a warrant to access this information, sparking debates about consent and privacy.

Privacy advocates argue that this broad interpretation infringes on citizens’ rights and lacks transparency, especially since many users may not be fully aware of how their data is accessed. The stance raises questions about data collection practices, privacy boundaries, and the balance between surveillance and individual rights.

CyberSecurity Advisors Network

NEWS:

3. More Spyware, Fewer Rules: What Trump's Return Means for US Cybersecurity

Original Source: Wired by Eric Geller

Donald Trump's returns to the US presidency, could mean sweeping changes to cybersecurity policy, including fewer restrictions on government spyware use.

During his previous term, Trump's administration took a lenient approach toward surveillance, potentially allowing law enforcement agencies broader powers. Experts warn that a similar policy shift could prioritise surveillance capabilities at the expense of privacy protections, impacting both domestic and international cybersecurity practices.

Such changes could lead to increased use of cyber tools for intelligence gathering, intensifying the privacy-security debate and raising concerns among rights advocates and tech industry leaders alike.

CyberSecurity Advisors Network

NEWS:

4. Idaho Man Gets 10 Years for Hacking, Cyber Extortion

Original Source: Dark Reading

An Idaho man has been sentenced to a decade in prison for hacking into private data and extorting victims for financial gain, a significant penalty that reflects the seriousness of cyber extortion.

The convicted hacker used illegal access to extract sensitive information, demanding money to avoid data leaks. The case is part of a growing trend of law enforcement clamping down on cyber extortionists, as courts recognise the damaging impacts these crimes have on individuals and businesses.

This sentence sends a strong message to others involved in cybercrime: exploiting cyber vulnerabilities for personal gain will have serious legal consequences.

CyberSecurity Advisors Network

NEWS:

5. Global cybersecurity alert reveals surge in zero-day exploits targeting high-priority networks in 2023

Original Source: Industrial Cyber News by Anna Ribeiro

A global alert has been issued in response to a sharp rise in zero-day exploits in 2023, particularly targeting high-priority networks and critical infrastructure. These exploits, often orchestrated by state-sponsored groups and sophisticated cybercriminals, are challenging traditional defences as they exploit undisclosed vulnerabilities.

Experts warn that this surge calls for proactive detection and stronger international collaboration, as unpatched systems in sectors like energy, finance, and healthcare are at high risk. The alert emphasises the urgent need for organisations to improve patch management, threat intelligence, and cross-border security cooperation to combat these rapidly evolving threats.

CyberSecurity Advisors Network

NEWS:

6. Coalition demands split of privacy package

Original Source: InnovationAus by Brandon How

Australia’s Coalition has called for the privacy reform package to be split into separate bills, arguing that the current omnibus proposal is too complex for effective debate and passage.

The proposed reforms aim to modernise Australia’s data protection laws, including stronger data handling standards and enhanced transparency requirements. Splitting the bill could delay the reforms, a concern for privacy advocates who see urgent need for updates in a data-driven world.

The move has sparked debate in parliament, with the Coalition arguing for careful consideration of each component, while others urge swift action to protect Australians’ personal data.

CyberSecurity Advisors Network

NEWS:

7. China-Linked Threat Actors Compromised Multiple Telcos and Spied on a Limited Number of U.S. Government Officials

Original Source: Security Affairs by Pierluigi Paganini

China-linked threat actors have reportedly compromised several telecommunications providers, using access to spy on a limited number of US government officials. The breach highlights the ongoing cybersecurity risks from state-sponsored groups targeting critical infrastructure.

The targeted espionage underscores how valuable telecommunications data is for intelligence operations, particularly data linked to government communications.

This incident adds to growing tensions over cyber-espionage and emphasises the need for stronger international cyber defences, as telecom networks remain prime targets for nation-state actors seeking strategic intelligence advantages.

CyberSecurity Advisors Network

NEWS:

8. New Glove infostealer malware bypasses Chrome’s cookie encryption

Original Source: BleepingComputer by Sergiu Gatlan

A new malware known as Glove has emerged, capable of bypassing Google Chrome’s cookie encryption to access stored user data, including login information. This infostealer is particularly dangerous, as it allows attackers to hijack user sessions and potentially take over accounts without direct access to login credentials.

Security researchers warn that Glove represents a sophisticated threat in the landscape of browser-based attacks, as traditional encryption measures prove ineffective.

Chrome users are advised to stay vigilant, as this malware’s capabilities show the evolving tactics of cybercriminals targeting sensitive information via commonly used browsers.

CyberSecurity Advisors Network

NEWS:

9. White House Slams Russia Over Ransomware's Healthcare Hits

Original Source: ISMG Data Breach today by Mathew Schwartz

The White House has issued a strong condemnation of Russia-linked ransomware groups for targeting US healthcare providers, citing the significant risks these attacks pose to patient care and safety.

The attacks have disrupted hospital operations, endangering lives and raising ethical concerns. The US government is urging Russia to address ransomware activity originating from within its borders, as healthcare systems remain vulnerable.

This statement reflects the geopolitical tensions surrounding ransomware and the White House’s emphasis on protecting critical infrastructure from cyber threats that have human costs, especially in vital sectors like healthcare.

CyberSecurity Advisors Network

NEWS:

10. Pregnancy Tracking App ‘What to Expect’ Refuses to Fix Issue that Allows Full Account Takeover

Original Source: 404 Media by Joseph Cox

The What to Expect pregnancy tracking app is under fire for refusing to fix a security vulnerability that enables full account takeover, putting users’ sensitive data at risk. Despite reports of this flaw, the app’s developers have yet to implement a solution, raising concerns over the protection of users’ personal and health information.

Privacy advocates argue that this inaction reflects a disregard for user safety and responsibility, especially given the sensitive nature of health-related apps.

The incident underscores the broader risks associated with health apps that fail to prioritise adequate security measures, leaving users vulnerable to potential data breaches.

CyberSecurity Advisors Network

NEWS:

11. Nearly 40% of Aussie kids aged between 16 and 18 use ChatGPT

Original Source: Cyberdaily.au by David Hollingworth

A recent study highlights that nearly 40% of Australian teenagers aged 16-18 are actively using ChatGPT, primarily for academic support. While AI tools like ChatGPT can aid in learning, the findings raise concerns regarding privacy, data security, and the potential impact on students' independent thinking.

Experts worry about AI dependency among teens and call for stricter privacy guidelines to safeguard underage users' data. This report underscores the importance of developing responsible AI policies to address both the benefits and risks of widespread AI usage in educational contexts, especially among younger users who may not fully grasp data privacy implications.

CyberSecurity Advisors Network

NEWS:

12. A new iOS 18 security feature makes it harder for police to unlock iPhones

Original Source: The Verge by Wes Davis

With iOS 18, Apple introduces a security feature that requires iPhones to reboot after extended inactivity, complicating law enforcement's ability to unlock devices without user cooperation.

This update, which aims to protect user privacy, is seen by privacy advocates as a positive step in securing personal data against unauthorised access. However, some law enforcement agencies argue it impedes investigations, sparking debate over balancing privacy rights with investigative needs.

Apple's approach reaffirms its dedication to user privacy, marking another milestone in its stance on protecting data against potential overreach by government authorities while preserving consumer trust.

CyberSecurity Advisors Network

NEWS:

13. New Ymir ransomware partners with RustyStealer in attacks

Original Source: BleepingComputer by Sergiu Gatlan

The newly surfaced Ymir ransomware strain has teamed up with RustyStealer malware, merging ransomware capabilities with credential theft for a more potent attack. By stealing user credentials and deploying ransomware simultaneously, Ymir increases its financial and operational impact on targeted organisations.

Cybersecurity experts highlight that such partnerships between malware strains reflect a concerning trend in the cybercrime ecosystem, with criminals pooling resources for devastating attacks. Organisations are urged to adopt multi-layered defences and remain vigilant, as this dual-pronged threat underscores the need for comprehensive protection against sophisticated, multi-vector cyber threats.

CyberSecurity Advisors Network

NEWS:

14. Amazon Discloses Employee Data Breach Aft4er May 2023 MovelT Attacks

Original Source: Security Affairs by Pierluigi Paganini

Amazon has revealed a data breach involving employee information following the MOVEit vulnerability exploitation in May 2023. The attack exposed sensitive data, underscoring the significant risks associated with third-party software vulnerabilities in widely used platforms.

In response, Amazon is working to bolster its security posture to prevent similar incidents. This breach serves as a critical reminder of the importance of third-party risk management and timely patching, even for large organisations, as vulnerabilities in essential software platforms remain a prevalent attack vector for cybercriminals looking to exploit weak links in corporate digital ecosystems

CyberSecurity Advisors Network

NEWS:

15. Malicious Python Package Exfiltrates AWS Credentials

Original Source: ISMG Data Breach today by Prajeet Nair

A malicious Python package uploaded to the PyPI platform has been found exfiltrating AWS credentials from developers, amplifying concerns over open-source software security.

Disguised as a legitimate tool, the package was widely downloaded, leading to potential data exposure for numerous organisations. This incident highlights the critical importance of vigilance when using third-party code, particularly from open-source repositories, and underlines the rising threat of supply chain attacks in software development.

Security experts advocate for enhanced screening processes within repositories and recommend developers closely monitor dependencies to avoid similar attacks in the future

CyberSecurity Advisors Network

NEWS:

16. 69,000 Bitcoins Are Headed for the US Treasury—While the Agent Who Seized Them Is in Jail

Original Source: Wired by Andy Greenberg

In a bizarre turn of events, the US Treasury is set to acquire 69,000 Bitcoins seized from the notorious Silk Road marketplace, while the federal agent responsible for the initial seizure is serving prison time for embezzling cryptocurrency.

Worth billions, this asset transfer highlights the complex challenges of managing seized digital assets and the ethical dilemmas faced by law enforcement in handling cryptocurrency.

The case draws attention to the regulatory and procedural gaps in handling digital currency within legal frameworks, emphasising the need for clear protocols as cryptocurrency's intersection with criminal activity and asset forfeiture becomes more prominent.

CyberSecurity Advisors Network

NEWS:

17. 2025 Cybersecurity Acronyms with Definitions

Original Source: Cyber Security Tribe by Dorene Rettas

Navigating cybersecurity often means deciphering a multitude of acronyms, and as the field evolves, new terms and abbreviations emerge.

This article provides a comprehensive guide to the most relevant cybersecurity acronyms expected in 2025, helping professionals stay informed and communicate effectively. Covering everything from threat actors to advanced defence mechanisms, the guide is a valuable resource for industry professionals and newcomers alike.

Staying familiar with these terms not only aids understanding of complex topics but also strengthens collaboration and strategic communication, crucial for addressing emerging challenges in the cybersecurity landscape

CyberSecurity Advisors Network

ANALYSIS:

18. The WIRED Guide to Protecting Yourself From Government Surveillance

Original Source: Wired by Andy Greenberg & Lily Hay Newman

WIRED offers a comprehensive guide for individuals concerned about government surveillance, providing actionable strategies to safeguard personal data and maintain privacy.

The guide explores various privacy tools and tactics, including using encrypted messaging apps, VPNs, and privacy-focused browsers to reduce exposure to tracking and data collection.

As government monitoring capabilities continue to evolve, this guide empowers individuals to make informed choices about their digital presence. It underscores the importance of digital literacy in an era where privacy is increasingly threatened, helping readers navigate today's digital landscape with enhanced security and awareness.

ANALYSIS:

19. CISA, FBI, NSA, and International Partners Release Joint Advisory on 2023 Top Routinely Exploited Vulnerabilities

Original Source: cisa.gov

The CISA, in partnership with the FBI, NSA, and international allies, has issued a joint advisory detailing the most frequently exploited vulnerabilities of 2023. Targeting common weaknesses in widely used software, the advisory urges organisations to prioritise patching and proactive cybersecurity measures.

Unpatched systems remain a prime target for both state-sponsored and criminal actors, and these vulnerabilities can lead to significant breaches if ignored.

By addressing these top vulnerabilities, organisations can better protect their data and infrastructure, bolstering resilience against an evolving landscape of cyber threats that exploit unaddressed security gaps.

CyberSecurity Advisors Network

ANALYSIS:

20. Ask a Data Ethicist: What Happens to Your Data When a Company Goes Bankrupt?

Original Source: Dataversity by Katrina Ingram

When companies declare bankruptcy, personal data can be classified as an asset, often sold or transferred to new entities without user consent.

This reality poses privacy and ethical challenges, as users have little control over their data's fate in corporate insolvencies. Data ethicists argue that current regulations lack the protections needed to secure user data in such scenarios, urging legal reforms to ensure individuals retain rights over their data even if a company dissolves.

This situation underscores the importance of user data control, calling for transparent data governance practices, especially during corporate transitions like bankruptcy.

UPCOMING CyAN EVENTS

Dubai: November 20-21
Third Party & Supply Chain Cyber Security Summit
Sydney: November 27
Women (and their allies!) in Cyber

CyberSecurity Advisors Network

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

#ReallyInterestingCyberStuff!