CyAN Cybersecurity Advisors Network

Cyber (In)Securities

Issue #100

CELEBRATING A CENTURY!

NEWS:

1. Apple launches eSafety feature ahead of regulation

Original Source: InnovationAus by Brandon How

Apple has introduced a new eSafety feature in Australia to protect users from online abuse and harmful content. This launch comes ahead of regulations requiring tech companies to implement stronger safeguards, particularly for child safety. The feature includes enhanced parental controls and tools to block inappropriate content and interactions across Apple devices.

By proactively rolling out this feature, Apple aims to align with Australia's regulatory expectations and strengthen its commitment to user privacy and security. The move signals a broader shift within the tech industry as companies anticipate tighter governmental oversight of online safety standards.

CyberSecurity Advisors Network

NEWS:

2. Lazarus Group Exploits Chrome Zero-Day in Latest Campaign

Original Source: Dark Reading by Jai Vijayan

The Lazarus Group, a North Korean state-sponsored hacking group, has launched a new campaign exploiting a recently discovered Chrome zero-day vulnerability.

The group is using this flaw to target cryptocurrency and financial services sectors, aiming to steal sensitive data and funds. The vulnerability allows attackers to gain remote access to compromised systems, posing a significant threat to organisations relying on Chrome for their operations.

Security experts urge immediate updates to Chrome and heightened vigilance, as this campaign underscores the growing sophistication of nation-state cyberattacks and the importance of patching zero-day vulnerabilities quickly.

CyberSecurity Advisors Network

NEWS:

3. Threat Spotlight: The evolving use of QR codes in phishing attacks

Original Source: Barracuda by Kyle Blanker

Barracuda researchers have highlighted a rise in phishing attacks that exploit QR codes to bypass traditional security measures. These attacks trick users into scanning malicious QR codes, which then direct them to fraudulent websites designed to steal credentials or deliver malware.

The evolving nature of these attacks makes them particularly dangerous, as they can often evade detection by security filters that focus on email links and attachments.

The report urges organisations to educate employees on the risks associated with QR codes and to implement enhanced security measures to detect and block these emerging threats.

CyberSecurity Advisors Network

NEWS:

4. Think You're Secure? 49% of Enterprises Underestimate SaaS Risks

Original Source: The Hacker News

A new report reveals that nearly half of enterprises are failing to implement fundamental cybersecurity practices, despite rising threats.

The study highlights gaps in areas like patch management, access control, and incident response, leaving organisations vulnerable to attacks. This widespread lack of basic security measures is alarming, given the increasing frequency and sophistication of cyber threats.

The report urges companies to prioritise strengthening their cybersecurity foundations, emphasising that even advanced security solutions are ineffective without solid baseline protections in place.

CyberSecurity Advisors Network

NEWS:

5. Inside the U.S. Government-Bought Tool That Can Track Phones at Abortion Clinics

Original Source: Wired by Joseph Cox

A new investigation reveals that U.S. government agencies have purchased a cyber tool capable of tracking mobile phones at sensitive locations, including abortion clinics.

The tool, sold by a data broker, collects geolocation data from mobile devices, raising significant cybersecurity and privacy concerns. The potential misuse of this data by law enforcement or other government bodies has sparked fears over surveillance and the ethical implications of tracking individuals in healthcare-related contexts.

This case highlights the growing intersection of cybersecurity, privacy, and surveillance, and the dangers of commercially available data being weaponised for monitoring sensitive activities.

CyberSecurity Advisors Network

NEWS:

6. VMware Releases vCenter Server Update to Fix Critical RCE Vulnerability

Original Source: The Hacker News by Ravie Lakshmanan

VMware has released an important update for vCenter Server, addressing multiple critical vulnerabilities that could allow attackers to execute arbitrary code or escalate privileges. The flaws, affecting versions prior to the update, pose a significant risk to organisations using vCenter for managing virtualised environments.

Admins are urged to apply the patch immediately to mitigate the risk of exploitation, as attackers are increasingly targeting such vulnerabilities in enterprise environments. This update underscores the need for regular security maintenance in virtual infrastructure to safeguard against evolving threats.

CyberSecurity Advisors Network

NEWS:

7. Encrypted Chat App ‘Session’ Leaves Australia After Visit From Police

Original Source: 404 Media by Joseph Cox

Session, an encrypted chat app known for its privacy-focused approach, has moved its operations out of Australia after a visit from police raised concerns about user privacy. The app’s creators cited increasing pressure from Australian authorities, who they feared might compel them to weaken encryption or introduce backdoors.

This decision highlights the challenges privacy-centric apps face in jurisdictions with stringent surveillance laws and the potential conflicts between privacy rights and law enforcement demands.

Session’s departure from Australia underscores the growing global debate over the balance between cybersecurity, privacy, and government oversight.

CyberSecurity Advisors Network

NEWS:

8. The billionaire behind Trump's 'unhackable' phone is on a mission to fight Tesla's FSD

Original Source: The Register by Iain Thomson

Dan O’Dowd, CEO of Green Hills Software, has taken aim at Tesla’s Full Self-Driving (FSD) technology, calling it unsafe and a risk to public safety. O’Dowd claims the company is prioritising profits over safety, pushing out underdeveloped technology that endangers drivers and pedestrians. He also criticised former President Trump’s cybersecurity policies, arguing they failed to protect the U.S. from digital threats.

O’Dowd’s critique underscores broader concerns about the rapid development of autonomous driving technologies and the need for stronger cybersecurity measures.

[CyberSecurity Advisors Network]

ANALYSIS:

9. Over 6,000 WordPress hacked to install plugins pushing infostealers

Original Source: Bleeping Computer by Lawrence Abrams

More than 6,000 WordPress websites have been compromised, with hackers installing malicious plugins that push infostealer malware. The attackers are using these plugins to harvest sensitive data from site visitors, including login credentials and other personal information. This large-scale campaign exploits vulnerabilities in outdated or poorly secured WordPress installations, targeting both individual websites and larger platforms.

Website owners are urged to update their WordPress installations, review security settings, and remove any suspicious plugins to prevent further compromise. The attack highlights the ongoing risk of running outdated software and the importance of maintaining robust security measures.

CyberSecurity Advisors Network

We are thrilled to announce that Kim Chandler McDonald, our APAC Director of Operations and Policy Development, has been appointed Global VP of the Cybersecurity Advisors Network (CyAN)!

Kim is a dedicated champion of CyAN's mission to foster a safer, more resilient digital world. Her commitment to cybersecurity excellence makes her the perfect choice to take on this global role. We're excited to see the impact she will have in this new role on a global level.

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!