CyAN Cybersecurity Advisors Network

Cyber (In)Securities

Issue #102

NEWS:

1. LottieFiles hacked in supply chain attack to steal users' crypto

Original Source: BleepingComputers by Bill Toulas

LottieFiles, a platform for animated graphics, recently suffered a supply chain attack compromising its 'lottie-player' library versions 2.0.5 to 2.0.7. The attackers injected malicious code designed to steal cryptocurrency by prompting users to connect their wallets, subsequently draining their assets.

Upon discovery, LottieFiles promptly released version 2.0.8, reverting to a secure state and advising users to update immediately. This incident underscores the critical need for vigilance in monitoring third-party dependencies and ensuring the integrity of software supply chains

NEWS:

2. Fired Employee Allegedly Hacked Disney World's Menu System to Alter Peanut Allergy Information

Original Source: 404 Media by Jason Koehler

A former Disney employee is facing accusations of hacking into the company’s menu management system to alter peanut allergy information, allegedly marking certain items as safe for allergy sufferers when they weren’t.

This deliberate change raised serious safety concerns, as it directly impacted allergen disclosures critical to visitor health. After being terminated, the employee reportedly accessed Disney’s systems without permission, leading to an investigation by both Disney and federal authorities. This incident underscores the risks of internal cyber sabotage, especially regarding sensitive health and safety data.

CyberSecurity Advisors Network

NEWS:

3. Interbank confirms data breach following failed extortion, data leak

Original Source: BleepingComputers by Sergiu Gatlan

Interbank finds itself in hot water after a failed ransomware demand led cybercriminals to leak sensitive customer data. The breach has exposed account details, prompting investigations and sparking questions about financial sector cyber resilience.

The bank, previously known as the International Bank of Peru (Banco Internacional del Perú) is currently bolstering its cybersecurity while reassuring clients, but the incident illustrates an alarming trend of hackers turning to public data leaks when extortion efforts falter. This high-profile breach emphasises the need for financial institutions to adopt more stringent protective measures against increasingly aggressive cyber threats.

CyberSecurity Advisors Network

NEWS:

4. Canada spy agency says India is using cyber tech to track Sikh separatists

Original Source: The Guardian and Agence France-Presse

Canada’s spy agency claims that India is using sophisticated cyber tools to monitor Sikh separatists, highlighting a growing international privacy and surveillance issue. The agency reports that Indian authorities are leveraging spyware to track activists globally, which adds another layer to an already tense diplomatic relationship.

These allegations bring renewed scrutiny to the ethics of government surveillance and are likely to prompt calls for stronger international policies against cross-border cyber intrusions. The report fuels a larger debate on the limits of state surveillance in political matters.

CyberSecurity Advisors Network

NEWS:

5. Uncle Sam outs a Russian accused of developing Redline infostealing malware

Original Source: The Register by Jessica Lyons

The U.S. Department of Justice has charged Russian national Maxim Rudometov with developing and administering the RedLine infostealer malware, which has compromised millions of computers globally since 2020. RedLine, sold as malware-as-a-service, enables cybercriminals to steal personal and financial data from victims.

This indictment is part of Operation Magnus, an international effort led by Dutch authorities that recently dismantled servers supporting RedLine and Meta infostealers. The case underscores the persistent threat posed by sophisticated malware and the importance of international collaboration in combating cybercrime

CyberSecurity Advisors Network

NEWS:

6. Massive hack-for-hire scandal rocks Italian political elites

Original Source: Politico by Hannah Roberts and Antoaneta Roussi

(A Free article usually reserved for subscribers)

Italy's political circles are rocked by a sweeping hack-for-hire scandal that's exposed sensitive communications among high-ranking officials. Alleged to have targeted politicians and other public figures, this scandal reveals the depth of cyber espionage risks within European political systems.

As investigations deepen, the incident underscores the vulnerability of public figures to espionage-for-hire and raises ethical questions around the misuse of cyber expertise for political manipulation. This scandal is likely to prompt discussions on better cybersecurity practices and regulations for political entities.

CyberSecurity Advisors Network

NEWS:

7. Chinese hackers targeted Eric Trump's and Jared Kushner's call data, sources say

Original Source: CNN by Sean Lyngaas, Evan Perez and Kara Scannell

The FBI alleges that Chinese hackers breached the mobile devices of Donald Trump's family members in a high-profile cyber espionage incident. Using sophisticated tactics, the attackers reportedly aimed to gather sensitive information, highlighting ongoing concerns about the vulnerability of prominent political figures' digital security.

As state-backed cyber campaigns increasingly target personal devices, this incident underscores the need for secure communication channels and advanced cybersecurity protocols for government officials and their families. The case raises further questions about the reach of foreign surveillance.

CyberSecurity Advisors Network

NEWS:

8. 7 in 10 firms lament workers’ lack of basic cybersecurity sense

Original Source: Frontier Enterprise

A recent survey shows that 70% of companies are struggling with basic cybersecurity awareness among employees, a worrying statistic as cyber threats continue to escalate. Many employees remain unaware of even the most fundamental practices, such as recognising phishing attempts, which makes businesses more susceptible to attacks.

Experts stress the importance of company-wide cybersecurity training as a primary defense against breaches. This report highlights the critical need for organisations to foster a proactive cybersecurity culture, especially in the face of growing digital risks.

CyberSecurity Advisors Network

NEWS:

9. LLM firewalls enter the secure AI debate

Original Source: InnovationAus by Jason Stevens

As AI becomes integral to industry operations, security remains a pressing concern, with LLM firewalls emerging as a new line of defense. These firewalls aim to prevent misuse by intercepting and evaluating prompts before they reach AI models, thereby safeguarding sensitive data.

Security experts suggest that these firewalls could set a new standard for AI safety by acting as a gatekeeper against harmful or unintended outcomes. As AI adoption surges, the addition of LLM firewalls marks a pivotal shift in the ongoing conversation about AI security and responsible tech deployment.

CyberSecurity Advisors Network

NEWS:

10. NSW desktop review finds dearth of data breach policies

Original Source: itNews by Ry Crozier

A NSW review has exposed significant gaps in data breach policies, showing many organisations are unprepared for security incidents. The lack of formal guidelines leaves companies vulnerable and risks non-compliance, particularly with stricter data protection regulations.

Experts are calling for an overhaul of breach response strategies, emphasising the need for structured policies that outline steps for detection, reporting, and remediation. This review highlights a critical weak spot in cybersecurity readiness and signals a need for widespread improvements in data governance.

CyberSecurity Advisors Network

NEWS:

11. Russian court fines Google $20,000,000,000,000,000,000,000,000,000,000,000

Original Source: The Register by Iain Thomson

(*Yep, we had to shrink the font for the thirty-four 0's in that headline...*)

A Russian court has handed Google an astronomical fine, widely seen as a heavy-handed response to the company's modest efforts to curb disinformation and propaganda. The unprecedented penalty underscores a punitive stance toward platforms that attempt even minimal content moderation, illustrating the risks tech companies face in authoritarian settings.

Critics argue that while Google's efforts may be limited, they represent a necessary, if incremental, step in addressing misinformation—a priority in global trust and safety work. This clash highlights the complex and often precarious role of tech platforms navigating content control amid regulatory pressures.

CyberSecurity Advisors Network

We are thrilled to announce that Inssata Ricourt has been appointed the Cybersecurity Advisors Network (CyAN) Representative for Africa!

Inssata’s expertise in cybersecurity and data protection, combined with her leadership and active engagement across the African continent, makes her the perfect choice to lead our expansion efforts in this dynamic region!

CyberSecurity Advisors Network

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!