CyAN Cybersecurity Advisors Network

Cyber (In)Securities

Issue #112

NEWS:

1. BT Group confirms attackers tried to break into Conferencing division

Original Source: The Register by Connor Jones

BT Group recently disclosed an attempted cyberattack on its Conferencing division, thwarted before significant damage occurred. The attackers targeted vulnerabilities in communication systems, aiming to disrupt services or access sensitive business data.

BT's swift response underscores the critical need for robust monitoring and rapid incident response capabilities. Communication platforms are increasingly attractive to cybercriminals, given their role in modern business operations.

This incident highlights that even large organisations are not immune to evolving cyber threats, driving home the importance of multi-layered cybersecurity strategies to safeguard critical infrastructure.

CyberSecurity Advisors Network

NEWS:

2. ‘Large number' of Americans' metadata stolen by Salt Typhoon hackers

Original Source: itNews by Raphael Satter

The Salt Typhoon hacking group has reportedly stolen a vast amount of Americans’ metadata in a targeted cyber espionage campaign. The group, believed to be state-sponsored, exploited vulnerabilities to collect sensitive information, raising significant concerns about national security and privacy.

Metadata theft, while often overlooked, provides valuable insights into communication patterns and behaviours, making it a powerful tool for adversaries.

This incident highlights the urgent need for stronger data protection laws and robust defences to counter increasingly sophisticated state-backed cyber threats.

CyberSecurity Advisors Network

NEWS:

3. Eurocops take down 'secure' criminal chat system known as Matrix

Original Source: The Register by Iain Thomso

European law enforcement agencies have dismantled the Matrix, a supposedly secure criminal chat system used by organised crime groups. The operation led to multiple arrests and significant evidence collection, including encrypted messages that were successfully deciphered.

The takedown highlights the growing capability of law enforcement to crack encrypted networks and disrupt illicit activities. This case serves as a stark reminder that even "secure" systems are vulnerable when targeted by determined investigators, underscoring the importance of transparency and compliance for legitimate service providers.

CyberSecurity Advisors Network

NEWS:

4. Police Shutter Largest German-Speaking Criminal Marketplace

Original Source: ISMG Data Breach Today by Akshaya Asokan

Authorities have closed down the largest German-speaking criminal marketplace, seizing servers and arresting key suspects. This platform facilitated the sale of illicit goods and services, including stolen data, counterfeit documents, and hacking tools.

Over 2.3 million messages were intercepted, providing critical insights into criminal operations. The takedown demonstrates the success of international collaboration in combating cybercrime and the growing focus on dismantling dark web marketplaces.

Experts emphasise the need for continuous vigilance to disrupt these evolving criminal ecosystems.

CyberSecurity Advisors Network

NEWS:

5. UK underestimates threat of cyber-attacks from hostile states and gangs, says security chief

Original Source: The Guardian by Dan Milmo

The UK's security chief has issued a stark warning that the nation is underestimating the threat posed by cyberattacks orchestrated by hostile states and organised criminal gangs.

The vulnerabilities in critical infrastructure, financial systems, and public services make the country a prime target. Calls for robust investment in cybersecurity, including enhanced training and threat intelligence sharing, are urgent. Without immediate action, adversaries could exploit these gaps to carry out damaging attacks, potentially impacting national security and economic stability.

The report stresses that a coordinated, proactive approach is vital to strengthen defences against increasingly complex threats.

CyberSecurity Advisors Network

NEWS:

6. Data on 760K workers from Xerox, Nokia, BofA, Morgan Stanley and more dumped online

Original Source: The Register by Jessica Lyons

A significant data breach has exposed sensitive information of 760,000 employees from global corporations including Xerox, Nokia, BofA, and Morgan Stanley.

The leaked data, reportedly stolen during a MOVEit Transfer attack, includes personal and employment details, raising serious concerns about corporate data security and privacy. Experts emphasise the need for robust encryption and secure data transfer practices to mitigate such risks.

This incident highlights the widespread impact of supply chain vulnerabilities, with attackers targeting third-party vendors to infiltrate major organisations. Companies must strengthen oversight of their partners and implement comprehensive incident response strategies.

CyberSecurity Advisors Network

NEWS:

7. CFPB Proposes Rule to Stop Data Brokers from Selling Sensitive Personal Data to Scammers, Stalkers, and Spies

Original Source: Consumer Financial Protection Bureau

The US Consumer Financial Protection Bureau (CFPB) has proposed a new rule targeting data brokers who sell sensitive personal information, aiming to protect consumers from misuse by scammers, stalkers, and spies.

The rule would impose stricter controls on the collection, storage, and sale of data, particularly concerning financial and health-related details.

Advocates praise the move as a step towards greater transparency and consumer rights, though critics warn of potential compliance challenges. If enacted, the rule could reshape data brokerage practices, forcing companies to prioritise security and ethical handling of personal information.

CyberSecurity Advisors Network

NEWS:

8. U.S. officials urge Americans to use encrypted apps amid unprecedented cyberattack

Original Source: NBC News by Kevin Collier

As cyberattacks hit unprecedented levels, U.S. officials are urging citizens to adopt encrypted messaging apps to safeguard sensitive communications. These attacks, which target individuals and critical infrastructure alike, underscore the pressing need for personal cybersecurity measures.

End-to-end encrypted platforms offer robust protection, shielding data from interception even by advanced threat actors. This guidance reflects the growing importance of digital literacy, emphasising that secure communication is a vital defense in an era of increasingly sophisticated cybercrime. Public awareness and adoption of these tools are essential to enhancing national resilience against evolving threats.

CyberSecurity Advisors Network

NEWS:

9. 8 Million Android Users Hit by SpyLoan Malware in Loan Apps on Google Play

Original Source: The Hacker News by Ravie Lakshmanan

Over 8 million Android users have fallen victim to SpyLoan malware embedded in loan apps downloaded from Google Play. These apps exploit user data for extortion, demanding payments with threats of sharing private information.

The malware highlights gaps in app store security, as malicious apps evade detection with increasingly sophisticated tactics. Cybersecurity experts stress the need for stricter vetting processes, user vigilance, and enhanced app permissions management.

This incident underscores the risks of trusting unofficial financial apps, emphasising the importance of verifying app legitimacy before installation.

CyberSecurity Advisors Network

NEWS:

10. ‘Russia can turn the lights off’: how the UK is preparing for cyberwar

Original Source: The Guardian by Dan Milmo

The UK is ramping up its defences against potential Russian cyberattacks targeting critical infrastructure, including energy grids and communication networks.

Security experts warn that the scale and sophistication of state-sponsored threats could disrupt essential services and compromise national security. This article highlights ongoing efforts to bolster cybersecurity, such as increased funding, international collaboration, and proactive threat intelligence.

While preparations are underway, officials stress the importance of resilience and public-private partnerships to address emerging challenges. The stakes underscore the urgent need for vigilance in an evolving geopolitical landscape.

CyberSecurity Advisors Network

NEWS:

11. Australia and UK partner to combat scams

Original Source: itWire by Gordon Peters

Australia and the UK have joined forces to tackle the escalating issue of online scams, focusing on disrupting criminal networks and protecting consumers. This partnership enhances data sharing, coordinates enforcement actions, and launches public awareness campaigns aimed at reducing fraud.

Both nations aim to counteract advanced tactics such as AI-driven phishing, social engineering, and identity theft. The collaboration is expected to set new standards for international cooperation, ensuring safer online environments and fostering trust in digital transactions.

With shared expertise and resources, this alliance strengthens efforts to combat evolving cybercrime challenges.

CyberSecurity Advisors Network

ANALYSIS:

12. Bug Bounties: Bringing Hackers and Manufacturers Together

Original Source: ISMG Data Breach Today by Athira Nair

Bug bounty programs are bridging the gap between ethical hackers and manufacturers, fostering collaboration to identify and fix vulnerabilities before they can be exploited. This article highlights the evolution of these initiatives, showcasing how they incentivise hackers to report flaws responsibly, while manufacturers gain critical insights to bolster their defences.

By embracing bug bounties, companies demonstrate a proactive stance on security, addressing risks in real time. As cyber threats grow more sophisticated, such programs offer a win-win, enhancing safety for users and strengthening trust in technology. The approach also sets a precedent for industry-wide adoption, promoting a culture of accountability and innovation in cybersecurity.

CyberSecurity Advisors Network

CyAN Member's Features:

13. Third-Party Risk Management in Formula 1

Original Source: Mohit Makhija

The fast-paced world of Formula 1 isn't just about racing; it's also a lesson in managing third-party risks. This article explores how F1 teams collaborate with numerous suppliers and tech partners, highlighting the crucial role of effective risk management to maintain performance and security.

As teams depend on cutting-edge technology and data sharing, vulnerabilities can arise from third-party integrations. The piece by CyAN Member Mohit Makhija stresses the importance of robust vetting, ongoing monitoring, and clear communication channels to mitigate potential risks.

Drawing parallels to broader industries, it showcases how lessons from Formula 1's meticulous approach can be applied to other sectors, underscoring the need for speed and precision in addressing third-party challenges.

CyberSecurity Advisors Network

CyAN Member's Features:

14. When Networking Turns Toxic: The Dark Side of Industry Events

Original Source: Kim Chandler McDonald

Industry events can be powerful platforms for connection and collaboration, yet they often expose attendees to hidden risks.

This piece by CyAN VP Kim Chandler McDonald highlights how these gatherings can inadvertently enable harmful behaviours, such as harassment, exclusion, or even exploitation, which disproportionately affect underrepresented groups. Tying into the themes of the #16DaysOfActivism, it underscores the need for safer, more inclusive spaces that empower everyone equally.

On the cyber front, the risks are just as pressing—events frequently lack secure digital protocols, making them fertile ground for phishing, data breaches, and malware attacks. By fostering both personal and cyber safety, industries can transform networking into a force for good.

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!

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