CyAN Cybersecurity Advisors Network

Cyber (In)Securities

Issue #131

NEWS:

EU looks to tech sovereignty with EuroStack amid trade war

Original Source: Biometric Update by Masha Borak

The European Union is making significant strides towards tech sovereignty with the development of EuroStack, a comprehensive technology initiative aimed at reducing dependence on foreign tech giants amid ongoing trade tensions.

This ambitious project seeks to bolster the EU's capabilities in digital services and infrastructure, promoting a self-reliant approach to technology that aligns with its strategic economic and security interests.

EuroStack is poised to enhance data protection, cloud computing, and overall digital autonomy for the EU, marking a pivotal shift in the global tech landscape as Europe navigates the complexities of international trade and tech dominance.

CyberSecurity Advisors Network

NEWS:

2. Trump Coins Used as Lure in Malware Campaign

Original Source: SecurityWeek by Kevin Townsend

In a novel cyberattack, malicious actors are exploiting the popularity of Trump-themed commemorative coins to distribute malware.

This campaign targets supporters through phishing emails that offer a chance to purchase these coins, only to infect their systems with malicious software when they attempt to engage.

The deceptive emails are crafted with convincing details and a call to action that redirects users to compromised websites. This strategy highlights a growing trend of using political memorabilia and current events as bait, reflecting an evolution in social engineering tactics aimed at specific demographic groups.

CyberSecurity Advisors Network

NEWS:

3. Experts Warn of Mass Exploitation of Critical PHP Flaw CVE-2024-4577

Original Source: Security Affairs by Pierluigi Paganini

Cybersecurity experts are raising alarms about a critical vulnerability in PHP, identified as CVE-2024-4577, which is being exploited on a massive scale.

This severe flaw allows attackers to execute arbitrary code on servers running vulnerable versions of PHP, potentially compromising millions of websites and web applications.

The widespread use of PHP in server-side scripting for web development makes this vulnerability particularly dangerous.

Security professionals urge immediate patching and updates, as exploiting this flaw can give attackers control over web servers, leading to data theft, site defacement, and further network compromise.

CyberSecurity Advisors Network

NEWS:

4. SideWinder' Intensifies Attacks on Maritime Sector

Original Source: Dark Reading by Jai Vijayan

The cyber threat group known as SideWinder is intensifying its targeted attacks on the maritime sector, deploying sophisticated tactics to infiltrate networks and steal sensitive information.

This group's activities have raised significant security concerns within the maritime industry, which is crucial for global trade and logistics.

SideWinder’s methods include using advanced malware and phishing attacks to gain access to ship management systems and port authority databases, aiming to disrupt operations and gather strategic data.

The escalation of these attacks underscores the need for enhanced cybersecurity measures in critical infrastructure sectors to protect against increasingly adept and persistent threat actors.

CyberSecurity Advisors Network

NEWS:

5. X outages reportedly caused by massive cyberattack

Original Source: ZDNet by Lance Whitney

A significant cyberattack is reported to be the cause behind recent widespread outages of the social media platform X.

This attack highlights the vulnerabilities in digital platforms that are increasingly becoming targets for sophisticated cyber threats.

The cyberattack not only disrupted service for millions of users worldwide but also raised concerns about data security and the robustness of infrastructure against such incursions.

The incident has prompted urgent calls for stronger cybersecurity protocols and resilience strategies to shield against future disruptions and potential data breaches.

CyberSecurity Advisors Network

NEWS:

6. Multiple vulnerabilities found in ICONICS industrial SCADA software

Original Source: Cyberscoop by Derek B. Johnson

Recent findings have revealed multiple vulnerabilities in ICONICS industrial SCADA software, posing significant risks to critical infrastructure systems that depend on this technology for operational control and monitoring.

These vulnerabilities could allow cyber attackers to manipulate controls, alter configurations, or even shut down operations, potentially leading to severe consequences in sectors like energy, manufacturing, and water treatment.

The discovery underscores the critical need for continuous vulnerability assessments and prompt patching within industrial systems to safeguard them from potential cyber threats and ensure the continuity of essential services.

CyberSecurity Advisors Network

NEWS:

7. Details Disclosed for SCADA Flaws That Could Facilitate Industrial Attacks

Original Source: SecurityWeek by Eduard Kovacs

Recent disclosures have shed light on several critical flaws within SCADA systems that could potentially facilitate industrial cyberattacks.

These vulnerabilities, if exploited, could allow attackers to gain unauthorised access and control over industrial control systems, posing severe risks to sectors heavily reliant on automation, such as utilities, manufacturing, and energy.

The detailed report emphasises the urgency of addressing these security gaps through comprehensive system audits, timely updates, and the implementation of layered security measures. It also highlights the importance of collaboration between industry stakeholders to develop robust defences against increasingly sophisticated cyber threats targeting industrial environments.

CyberSecurity Advisors Network

NEWS:

8. Swiss critical sector faces new 24-hour cyberattack reporting rule

Original Source: BleepingComputer by Bill Toulas

Switzerland has introduced a stringent new regulation requiring critical sector organizations to report cyberattacks within 24 hours of detection.

This rule aims to enhance national cybersecurity resilience by ensuring swift and coordinated response efforts to digital threats.

The legislation covers entities in essential services such as healthcare, transportation, finance, and utilities, emphasising the importance of transparency and prompt communication in mitigating the impacts of cyber incidents.

The move reflects a growing global trend toward tighter cyber regulations as governments seek to fortify defences against the increasing frequency and sophistication of cyberattacks.

CyberSecurity Advisors Network

NEWS:

9. Researchers Expose New Polymorphic Attack That Clones Browser Extensions to Steal Credentials

Original Source: The Hacker News by Ravie Lakshmanan

Security researchers have uncovered a new polymorphic attack technique that clones legitimate browser extensions to stealthily steal user credentials.

This sophisticated method involves altering the code of popular extensions, turning them into trojans that can capture sensitive information such as passwords and banking details without alerting users or security systems.

The findings highlight a significant escalation in browser-based threats, emphasising the need for users to verify the authenticity of extensions and maintain updated anti-malware solutions.

The report calls for heightened awareness and stricter security practices to counteract these deceptive strategies that exploit the trust in commonly used digital tools.

CyberSecurity Advisors Network

NEWS:

10. Rhysida pwns two US healthcare orgs, extracts over 300K patients' data

Original Source: The Register by Connor Jones

The cyber threat group Rhysida has successfully breached two US healthcare organizations, compromising the personal and medical information of over 300,000 patients.

This sophisticated attack highlights the increasing vulnerability of the healthcare sector to cyber incursions, which can have devastating consequences for patient privacy and institutional integrity.

The hackers utilized advanced tactics to infiltrate network defences and exfiltrate a significant amount of sensitive data, underscoring the critical need for healthcare entities to enhance their cybersecurity measures.

This incident serves as a stark reminder of the importance of robust security protocols and continuous monitoring to protect patient information against such malicious activities.

CyberSecurity Advisors Network

CYAN APAC EVENT IN SYDNEY!

Mark your calendars—this is one event you won't want to miss!

In a world where cyber threats are reshaping global power dynamics, understanding their geopolitical implications has never been more critical. This event will provide unique insights into how the evolving cyber landscape impacts nations, organisations, and individuals, offering strategies to navigate these challenges with clarity and resilience.

We'll begin with a keynote from acclaimed cybersecurity advisor Dan Elliott, followed by a panel discussion moderated by Dr. Saba Bagheri, Cyber Threat Intelligence Manager at BUPA, featuring

- **Peter Evans, CISO at NSW Police Force**
- **Robbie Abraham, Head of Cyber Threat Intelligence at Newfold Digital**

NEWS:

11. Former NSA cyber director warns drastic job cuts threaten national security

Original Source: Cybersecurity Dive by David Jones

The former director of NSA's cyber division has issued a stark warning that significant job cuts within the agency pose a serious threat to national security.

These reductions in cybersecurity personnel come at a time when cyber threats are becoming more frequent and sophisticated.

The former director emphasises that decreasing the number of skilled cybersecurity professionals undermines the country's ability to defend against and respond to cyber incidents effectively.

This alert calls for urgent reconsideration of budget and staffing decisions to ensure the NSA and other critical security agencies are well-equipped to safeguard national interests in the digital age.

CyberSecurity Advisors Network

NEWS:

12. SilentCryptoMiner Infects 2,000 Russian Users via Fake VPN and DPI Bypass Tools

Original Source: The Hacker News by Ravie Lakshmanan

A new malware known as SilentCryptoMiner is targeting Russian users by masquerading as legitimate VPN and DPI (Deep Packet Inspection) bypass tools.

The malware has already infected approximately 2,000 individuals, covertly mining cryptocurrency using the resources of compromised systems.

This campaign highlights the dangers of downloading software from unverified sources, as attackers capitalise on the demand for privacy tools in regions with strict internet regulations.

The incident underscores the need for heightened vigilance and the importance of using trusted channels for software downloads to prevent such deceptive and harmful intrusions.

CyberSecurity Advisors Network

NEWS:

13. US cities warn of wave of unpaid parking phishing text

Original Source: BleepingComputer by Lawrence Abrams

Several US cities are issuing warnings about a new phishing scam involving unpaid parking tickets.

The scam sends text messages to individuals, falsely claiming they have unpaid parking fines and directing them to a fraudulent website.

Once on the site, victims are prompted to enter personal information, which the scammers can then use for identity theft or financial fraud.

This wave of phishing attacks highlights the increasingly cunning tactics used by cybercriminals to exploit everyday situations.

Authorities are urging the public to verify any such claims through official municipal channels and to be cautious about providing personal information online.

CyberSecurity Advisors Network

NEWS:

14. NCSA ordered to step up preparations against cyber warfare

Original Source: The Nation

The Thai National Cyber Security Authority (NCSA) has been ordered to intensify its preparations against potential cyber warfare threats.

This directive comes in response to escalating global cyber tensions and the increasing sophistication of potential cyber-attacks that could target critical national infrastructure.

The NCSA's enhanced focus aims to bolster the country's defences by developing more advanced cyber response strategies, conducting regular security drills, and strengthening collaborations with international cybersecurity entities.

This proactive approach is designed to ensure the nation remains resilient in the face of growing cyber threats and can effectively mitigate the impact of any cyber-attacks.

CyberSecurity Advisors Network

NEWS:

15. Internet shutdowns at record high in Africa as access ‘weaponised’

Original Source: The Guardian by Eromo Egbejule

Internet shutdowns have reached a record high across Africa, with governments increasingly 'weaponising' access to control information and suppress dissent.

This trend is alarming advocates for freedom of expression and digital rights, as shutdowns not only curtail civil liberties but also impact economies and disrupt everyday life.

The use of internet blackouts as a political tool is particularly prevalent during protests, elections, and civil unrest, raising serious concerns about the erosion of democratic norms.

This pattern underscores the urgent need for international dialogue and policy interventions to protect internet access as a fundamental right and to prevent its use as a tool for political manipulation.

CyberSecurity Advisors Network

NEWS:

16. Stalked: how a relentless campaign of online abuse derailed one woman’s life

Original Source: The Observer by Carole Cadwalladr

This in-depth article chronicles the harrowing experience of a woman whose life was dramatically affected by a relentless campaign of online abuse.

It explores the devastating impact of cyberstalking, which included constant harassment, the spreading of personal information, and threats that extended beyond the digital realm into her physical life.

The case study sheds light on the psychological and social repercussions of such targeted attacks, highlighting the insufficient legal protections and the often inadequate response from law enforcement agencies.

This story calls for stronger regulatory measures and more robust support systems to protect individuals from cyber harassment and to hold perpetrators accountable.

CyberSecurity Advisors Network

NEWS:

17. White House cyber director’s office set for more power under Trump, experts say

Original Source: The Record by Suzanne Smalley

According to experts, the office of the White House cyber director is poised to receive expanded powers under the Trump administration.

This move aims to enhance the national cybersecurity strategy by centralising authority and improving coordination among various federal agencies involved in cyber defence.

The bolstering of the cyber director's office reflects an acknowledgment of the growing cyber threats facing the United States and the need for a more unified government response.

Experts suggest that this restructuring will enable more effective policy-making and operational decisions in cybersecurity, potentially leading to stronger protections against cyberattacks on national infrastructure.

CyberSecurity Advisors Network

NEWS:

18. Undocumented commands found in Bluetooth chip used by a billion devices

Original Source: BleepingComputer by Bill Toulas

Recent discoveries have revealed undocumented commands in a widely used Bluetooth chip, present in over a billion devices, raising significant security concerns.

These hidden commands, if exploited, could potentially allow attackers to execute arbitrary actions on affected devices without the user's knowledge.

This vulnerability underscores the critical importance of hardware security and the potential risks associated with overlooked or hidden functionalities in common technology components.

The exposure of such commands highlights the need for manufacturers to conduct thorough security audits and for users to ensure their devices are regularly updated to mitigate any potential threats arising from such vulnerabilities.

CyberSecurity Advisors Network

NEWS:

19. Japanese Telecom Giant NTT Suffered a Data Breach That Impacted 18,000 Companies

Original Source: Security Affairs by Pierluigi Paganini

The Japanese telecommunications giant NTT disclosed a significant data breach impacting approximately 18,000 corporate clients.

This breach involved unauthorised access to a wide range of sensitive data, potentially exposing business secrets and personal information.

The incident highlights vulnerabilities in telecommunications networks that can have far-reaching consequences for both the service provider and its extensive client base.

NTT has initiated a comprehensive security overhaul and is collaborating with law enforcement to investigate the breach.

This event underscores the need for enhanced cybersecurity measures and continuous vigilance to protect against sophisticated cyber threats in an increasingly interconnected world.

CyberSecurity Advisors Network

NEWS:

20. Cyberattacks targeting IT vendors intensify, causing bigger losses

Original Source: Cybersecurity Dive by Alexei Alexis

The frequency and severity of cyberattacks targeting IT vendors have dramatically intensified, resulting in substantial financial and operational losses.

This trend is particularly alarming as IT vendors often serve as gateways to broader networks, making them attractive targets for cybercriminals looking to exploit multiple victims through a single entry point. These attacks not only disrupt IT operations but also compromise the security of their clients' data and systems.

The article highlights the growing need for IT vendors to implement robust cybersecurity strategies, including multi-factor authentication, regular security audits, and employee training, to mitigate the risks and protect both their assets and those of their clients.

CyberSecurity Advisors Network

CyAN Members Only

Are You In the #CyANQuiz?

Hey CyAN Champions,

Have you got what it takes to outsmart your fellow cybersecurity pros? It's time to put your skills to the test in our Quarterly #CyANQuiz Challenge, kicking off on March 31st!

- 🔹 30 Questions. Timed. No second chances.
- 🔹 Based on Recent Cybersecurity News & Events – Watch out for recent news and Cybersecurity events.

📅 **Check your email on March 31st for the quiz link**; just click, answer, and climb the leaderboard!

💡 Why Play? Compete, have fun, and win awesome prizes (while proving your cybersecurity dominance!

Join the fun—this isn't just a quiz, it's a year-long challenge to **shine in the CyAN community!**

Think you can take the cyber crown? Prove it!

NEWS:

21. YouTubers extorted via copyright strikes to spread malware

Original Source: BleepingComputer by Bill Toulas

An emerging cyber threat involves extortion of YouTubers through the manipulation of copyright strike processes to distribute malware.

Cybercriminals are targeting content creators by threatening them with copyright strikes, which can severely impact their channel and revenue, unless they comply with demands that often include downloading malware-laden software. This strategy not only exploits the legal copyright mechanisms but also turns them into a tool for cyber extortion.

The practice highlights a new form of cybercrime that blends traditional copyright abuse with digital extortion, significantly complicating the security landscape for online content creators. It underscores the importance of vigilance and legal awareness among YouTubers to protect against such sophisticated and damaging attacks.

CyberSecurity Advisors Network

NEWS:

22. Developer sabotaged ex-employer with kill switch activated when he was let go

Original Source: The Register by Iain Thomson

A developer orchestrated a sabotage attack against his former employer by implementing a kill switch that activated upon his dismissal.

This deliberate act caused significant disruption to the company's operations, as critical systems were disabled, leading to downtime and financial losses.

The incident underscores the potential risks associated with insider threats and the importance of maintaining stringent security protocols, especially regarding access control and monitoring of sensitive systems.

The company has since taken steps to bolster its security measures and review its policies to prevent such occurrences in the future, highlighting the need for continuous vigilance and robust security practices in the workplace.

CyberSecurity Advisors Network

ANALYSIS:

23. Cybersecurity is a ‘Continual Battle,’ but Industry Can’t Be ‘Complacent,’ Experts Say

Original Source: Security Systems News by Cory Harris

Experts in cybersecurity are emphasising that the fight against cyber threats is an ongoing battle that requires constant vigilance and adaptation.

This article discusses the ever-evolving nature of cyber threats and the critical importance of staying proactive in cybersecurity practices. Industry leaders warn against complacency, highlighting that as technology advances, so do the tactics of cybercriminals.

Harris, editor of Security Systems News, advocates for continuous investment in cybersecurity infrastructure, regular updates to defensive strategies, and ongoing training for all staff. His message is clear: the cybersecurity landscape is dynamic and requires perpetual effort and innovation to keep data and systems safe.

CyberSecurity Advisors Network

ANALYSIS:

24. Rapid7’s Chief Scientist Warns Australian Businesses to Prioritise their Ransomware Policies

Original Source: itWire by Grant Titmus

Rapid7's Chief Scientist, Raj Samani, has issued a stark warning to Australian businesses regarding the escalating threat of ransomware attacks.

Samani, is urging companies to prioritize their ransomware response policies and strengthen their cybersecurity defences to combat this pervasive threat. His call to action comes amid rising incidents of ransomware across Australia, which are increasingly sophisticated and disruptive.

The article highlights the necessity for businesses to implement comprehensive security measures, including regular data backups, employee training on phishing awareness, and robust incident response plans. The emphasis is on preparation and resilience, aiming to mitigate potential impacts and ensure business continuity in the face of these cyber challenges.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

CyAN CyAN Members Op Eds, Articles, etc

25. Copy of FY2024 IT and Cybersecurity Spending Analysis (Selected ASX 200 Companies)

Original Source: CyAN Member Nick Kelly

CyAN Member Nick Kelly provides a detailed analysis of the FY2024 IT and cybersecurity spending across selected ASX 200 companies, revealing significant trends and investment patterns.

The report underscores the growing emphasis on cybersecurity in the corporate sector, reflecting increased allocations towards enhancing digital defences.

Nick’s analysis points out that despite economic pressures, companies are prioritising investments in cybersecurity to address the escalating threat landscape.

The document serves as a crucial resource for understanding how top Australian companies are strategically positioning their resources to combat cyber threats, offering valuable insights into the prioritisation of IT and cybersecurity expenditures in response to evolving challenges.

UPCOMING CyAN and CyAN Partner EVENTS:

- **CyAN APAC: The Geopolitical Impacts of Cyber Threats: From Espionage to Influence keynote by Dan Elliot, March 12, Peoplebank, Sydney**
- **Trust & Safety Forum at Forum INCYBER Europe (FIC), Lille, France: April 1-2**
- **GITEX AFRICA, Marrakesh, Morocco: 14-16 April**
- **GITEX ASIA: Singapore (Marina Bay Sands) 23-25 April**
- **GISEC: Dubai Word Trade Center, Dubai, UAE: 6- 8 May**
- **The Cyber Outstanding Security Performance Awards (Cyber OSPAs), May 8, London, UK**
- **World AI Technology Expo UAE, Dubai, UAE: 14-15 May 2025 https://worldaiexpo.i**
- **MaTeCC, Rabat, Morocco: 7-9 June, 2025**

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!

CyberSecurity Advisors Network

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

#ReallyInterestingCyberStuff!
#SharingIsCaring