Issue #117

1. **Biden administration rolls out wide-reaching cybersecurity executive order | Cybersecurity Dive by David Jones** https://tinyurl.com/5hb7e9ek | The Biden administration has unveiled a comprehensive cybersecurity executive order aimed at enhancing national security. Key measures include mandatory zero-trust adoption across federal agencies, rigorous supply chain risk management, and improved threat intelligence sharing with private entities. The order emphasises collaboration between public and private sectors to counter advanced threats targeting critical infrastructure. While experts applaud the initiative, they caution that effective implementation will demand significant resources, accountability, and coordination.
2. **Millions of Internet Hosts Vulnerable to Attacks Due to Tunneling Protocol Flaws | SecurityWeek by Eduard Kovacs** https://tinyurl.com/mvz2f8mz | Researchers have identified critical flaws in tunnelling protocols, leaving millions of internet hosts vulnerable to cyberattacks. Exploiting these weaknesses, attackers can intercept traffic, execute malicious commands, or extract sensitive data. The vulnerabilities are tied to outdated configurations and weak encryption practices. Security experts urge organisations to upgrade protocols, enforce stronger authentication, and conduct regular network audits. This discovery underscores the ongoing risks associated with improperly secured network infrastructure.
3. **New UEFI Secure Boot flaw exposes systems to bootkits, patch now | BleepingComputer by Bill Toulas** https://tinyurl.com/3kcftddc | A critical flaw in UEFI Secure Boot has been uncovered, enabling attackers to bypass protections and deploy bootkits that compromise systems at the firmware level. Such attacks grant persistent access, making malware detection and removal challenging. This vulnerability impacts millions of devices globally, prompting urgent patches from vendors, including Microsoft. Security experts emphasise the need for timely updates, regular firmware audits, and robust hardware security measures to safeguard against these advanced threats.
4. **Microsoft catches Russian state-sponsored hackers shifting tactics to WhatsApp | Cyberscoop by Greg Otto** https://tinyurl.com/4r6pwbd4 | Microsoft has detected Russian state-backed hackers adapting their tactics by using WhatsApp to distribute malware. Posing as legitimate profiles, they exploit the platform to manipulate conversations and deliver infected files. This shift highlights the evolving strategies of cyber adversaries targeting both public and private sectors. Experts recommend heightened vigilance when engaging on messaging platforms, implementing robust endpoint protection, and raising awareness about phishing tactics to mitigate risks.
5. **Wolf Haldenstein law firm says 3.5 million impacted by data breach | BleepingComputer by Bill Toulas** https://tinyurl.com/4aprukx7 | Wolf Haldenstein, a prominent U.S. law firm, has disclosed a significant data breach affecting 3.5 million individuals. Exposed information includes sensitive client and employee data, raising concerns about cybersecurity practices within the legal industry. The firm has enlisted forensic experts to investigate and mitigate the incident. This breach serves as a stark reminder for legal organisations to prioritise robust security measures to protect confidential information in the face of rising cyber threats.
6. **FTC sues GoDaddy for years of poor hosting security practices | BleepingComputer by Sergiu Gatlan** https://tinyurl.com/45nvwj3h | The FTC has filed a lawsuit against GoDaddy, accusing the company of neglecting cybersecurity for

years. Allegations include failure to address known vulnerabilities, inadequate incident response protocols, and insufficient customer protections. This case marks a significant push to hold service providers accountable for poor security practices. Experts warn that such negligence can erode trust and emphasise the need for transparent, robust security measures to protect users and sensitive data. The lawsuit may serve as a wake-up call for the industry to improve its standards.

7. **A CISA secure-by-design guru makes the case for the future of the initiative | Cyberscoop by Tim Starks** https://tinyurl.com/yc5f4an5 | CISA's Secure-by-Design initiative aims to embed security into software development from the ground up, creating resilient systems less prone to vulnerabilities. A CISA leader has outlined how collaboration between developers, vendors, and regulators is key to this vision. The initiative focuses on fostering a culture of proactive risk management and secure coding practices. Experts believe that adopting this approach industry-wide will help counter evolving threats while building trust in digital ecosystems. This initiative reflects a shift toward long-term cybersecurity solutions.
8. **Russian Cyberspies Caught Spear-Phishing with QR Codes, WhatsApp Groups | SecurityWeek by Ryan Naraine** https://tinyurl.com/bdz7wkaa | Russian cyberspies are deploying creative spear-phishing campaigns using QR codes and WhatsApp groups to bypass traditional defences. These methods exploit trust in widely used platforms, targeting government agencies and private organisations. QR codes are particularly effective at avoiding detection, making them a growing threat. Experts recommend enhanced training to help employees recognise phishing attempts, alongside robust threat detection systems to counter these tactics. The campaign highlights the evolving ingenuity of state-sponsored attackers.
9. **Bipartisan cloud study recommends speeding federal adoption, or remain vulnerable on cyber | Cyberscoop by Tim Starks** https://tinyurl.com/mtrmk79d | A bipartisan study underscores the critical need for federal agencies to accelerate cloud adoption, warning that delays leave systems exposed to cyberattacks. The report highlights cloud platforms' benefits, including improved resilience, scalability, and advanced threat detection capabilities. Policymakers are urged to address regulatory and funding barriers to expedite the transition. Experts see this as a vital step toward modernising national infrastructure and safeguarding critical operations in an increasingly hostile cyber environment.
10. **Threat Actor Leaked Config Files and VPN Passwords for Over Fortinet Fortigate Devices | Security Affairs by Pierluigi Paganini** https://tinyurl.com/4w343zws | A threat actor has leaked configuration files and VPN credentials for over 10,000 Fortinet FortiGate devices, exposing sensitive enterprise data. The breach was tied to systems that failed to patch a known vulnerability from 2022, underscoring the critical need for timely updates. Security experts warn this exposure could enable attackers to infiltrate networks, escalate privileges, or deploy ransomware. Organisations are urged to verify patch statuses and enhance monitoring to prevent similar compromises.
11. **SAP fixes critical vulnerabilities in NetWeaver application servers | BleepingComputer by Bill Toulas** https://tinyurl.com/3r9fbyvk | SAP has patched multiple critical vulnerabilities in its NetWeaver application servers, including flaws that could allow remote code execution. These vulnerabilities posed significant risks, especially in enterprise environments reliant on SAP for core business processes. Security researchers stress the urgency of applying these updates to prevent

exploitation. The incident serves as a reminder for businesses to prioritise patch management for essential systems.

12. **CISA's AI cyber collaboration playbook aims to spur information-sharing | Cyberscoop by Matt Bracken** https://tinyurl.com/yhp5jve7 | CISA has introduced an AI Cyber Collaboration Playbook to enhance information-sharing among public and private sectors. The framework focuses on leveraging AI to identify and mitigate cyber threats faster and more efficiently. By encouraging collaboration, the playbook aims to bridge gaps in threat intelligence and bolster national resilience. Experts see this as a proactive step toward improving cybersecurity coordination across industries and government entities.
13. **Google Ads Users Targeted in Malvertising Scam Stealing Credentials and 2FA Codes | The Hacker News by Ravie Lakshmanan** https://tinyurl.com/dx3mfzhy | A sophisticated malvertising scam is targeting Google Ads users, tricking them into revealing credentials and two-factor authentication (2FA) codes. Cybercriminals lure victims to phishing sites designed to resemble Google's login portals. Once compromised, attackers can gain control of critical accounts. Security experts warn businesses to monitor ad campaigns and educate users about identifying phishing attempts to mitigate this growing threat.
14. **Over 660,000 Rsync servers exposed to code execution attacks | BleepingComputer by Bill Toulas** https://tinyurl.com/3e77ay22 | More than 660,000 Rsync servers have been found exposed online, leaving them vulnerable to code execution attacks. These servers, often used for data backups and transfers, can be exploited by attackers to gain unauthorised access or execute malicious commands. The issue stems from misconfigurations and a lack of proper security measures. Experts urge organisations to secure these servers by enabling authentication, limiting IP access, and keeping software up to date to avoid potential breaches.
15. **Lazarus Group Targets Web3 Developers with Fake LinkedIn Profiles in Operation 99 | The Hacker News by Ravie Lakshmanan** https://tinyurl.com/yww2mrje | The notorious Lazarus Group is targeting Web3 developers through Operation 99, using fake LinkedIn profiles to distribute malware. This state-sponsored campaign aims to infiltrate blockchain-related projects, steal intellectual property, and compromise systems. Experts emphasise the importance of vetting professional connections and implementing endpoint security to counter such sophisticated tactics. The attack highlights the persistent risks faced by the rapidly evolving Web3 sector.
16. **DORA's Deadline Looms: Navigating the EU's Mandate for Threat Led Penetration Testing | SecurityWeek by Trevin Edgeworth** https://tinyurl.com/545zmpm9 | The EU's Digital Operational Resilience Act (DORA) is pushing financial institutions to adopt threat-led penetration testing (TLPT) before its 2025 deadline. This mandate aims to strengthen resilience by simulating real-world attacks to uncover vulnerabilities. While many organisations welcome the move, others are grappling with compliance challenges and resource constraints. Industry leaders highlight the need for collaboration and strategic planning to meet DORA's requirements without disrupting operations.
17. **How scammers are tricking Apple iMessage users into disabling phishing protection | ZDNet by Lance Whitney** https://tinyurl.com/muws2dmf | A new phishing campaign is deceiving Apple iMessage users into disabling their built-in phishing protections. Scammers pose as legitimate Apple support, urging users to click malicious links or adjust security settings. This tactic not only compromises devices but

also exposes users to further attacks. Apple users are advised to scrutinise messages carefully, avoid clicking unfamiliar links, and enable multi-factor authentication to add an extra layer of security.

18. **As Tensions Mount With China, Taiwan Sees Surge in Cyberattacks | Dark Reading by Robert Lemos** https://tinyurl.com/mr379cfr | Taiwan is experiencing a surge in cyberattacks as tensions with China escalate. Threat actors are targeting critical infrastructure, government systems, and private enterprises with sophisticated malware and phishing campaigns. Experts link these attacks to China's ongoing geopolitical strategy. The situation underscores the urgent need for Taiwan to bolster its cyber defences and collaborate with international allies to safeguard its digital sovereignty amidst rising threats.
19. **Allstate car insurer sued for tracking drivers without permission | BleepingComputer by Bill Toulas** https://tinyurl.com/mtfesx92 | Allstate is facing a lawsuit over allegations of tracking drivers without their consent. Plaintiffs claim the insurer used telematics systems to collect detailed data, violating privacy laws. The case raises broader concerns about transparency in data collection and the ethical use of telematics technology in the auto insurance industry. Advocates argue for stricter regulations to protect consumer rights and ensure accountability in how sensitive data is handled.
20. **Apple Bug Allows Root Protections Bypass Without Physical Access | Dark Reading by Becky Bracken** https://tinyurl.com/4u4sme3p | A newly discovered Apple bug allows attackers to bypass root-level protections without requiring physical access to devices. This vulnerability poses significant risks to enterprise environments, where attackers could exploit the flaw to install persistent malware or steal sensitive data. Apple has acknowledged the issue and is working on a fix, but security experts stress the importance of regular system updates and endpoint security measures to mitigate potential damage in the meantime.
21. **US govt says North Korea stole over $659 million in crypto last year | BleepingComputer by Sergiu Gatlan** https://tinyurl.com/2xhv5ef3 | The U.S. government has attributed the theft of over $659 million in cryptocurrency last year to North Korean state-backed hackers. The stolen funds are believed to support the regime's weapons programs, highlighting the use of cybercrime as a tool for geopolitical gain. Authorities are calling for increased international collaboration to trace and disrupt these operations. The scale of these heists underscores the critical need for enhanced security across cryptocurrency platforms.
22. **UK Considers Banning Ransomware Payment by Public Sector and CNI | SecurityWeek by Kevin Townsend** https://tinyurl.com/5n7jnw85 | The UK is evaluating a ban on ransomware payments by public sector entities and critical national infrastructure (CNI) operators. The proposed measure aims to reduce the profitability of ransomware attacks and deter cybercriminals. While the initiative has garnered support, critics warn of unintended consequences, such as prolonged disruptions and increased risks for victims. Policymakers must carefully weigh these factors to balance deterrence with resilience in critical sectors.
23. **Google OAuth Vulnerability Exposes Millions via Failed Startup Domains | The Hacker News by Ravie Lakshmanan** https://tinyurl.com/2nj8m6af | A Google OAuth vulnerability has exposed millions of users to potential attacks, with expired startup domains being repurposed for malicious purposes. Threat actors leveraged abandoned domains linked to OAuth to intercept login credentials and access sensitive

accounts. Security experts highlight the importance of domain monitoring and timely cleanup of obsolete systems to prevent such risks. This incident underscores the complexities of securing modern authentication ecosystems.

24. **FBI deletes Chinese PlugX malware from thousands of US computers | BleepingComputer by Sergiu Gatlan** https://tinyurl.com/56x77d2a | The FBI has successfully removed PlugX malware, allegedly planted by Chinese-backed hackers, from thousands of U.S. computers. The operation highlights law enforcement's proactive approach to combating state-sponsored cyber threats. PlugX, known for its data exfiltration capabilities, had infiltrated critical systems across multiple sectors. Experts commend the FBI's action but stress the need for global cooperation to address the growing sophistication of nation-state cyber campaigns.
25. **Hackers use FastHTTP in new high-speed Microsoft 365 password attacks | BleepingComputer by Bill Toulas** https://tinyurl.com/y2pzypmw | Cybercriminals are employing FastHTTP tools in a new wave of high-speed attacks targeting Microsoft 365 accounts. These tools enable brute-force password attempts at unprecedented speeds, significantly increasing the risk of account compromises. The attacks are exploiting weak passwords and outdated authentication methods. Security experts recommend implementing multi-factor authentication (MFA), regular password audits, and monitoring for unusual login activity to mitigate these threats effectively.
26. **Russian-Linked Hackers Target Kazakhstan in Espionage Campaign with HATVIBE Malware | The Hacker News by Ravie Lakshmanan** https://tinyurl.com/2tw4z39f | Russian-linked hackers are deploying HATVIBE malware in a targeted espionage campaign against Kazakhstan. The malware is designed to exfiltrate sensitive data from government and private sector entities, further escalating geopolitical tensions in the region. Analysts view this campaign as part of a broader strategy to undermine Kazakhstan's sovereignty. The incident underscores the need for robust cybersecurity defences and regional collaboration to counter state-sponsored threats.
27. **US removes malware allegedly planted on computers by Chinese-backed hackers | itNews by Sarah N. Lynch** https://tinyurl.com/4ubrcyzx | The U.S. government has confirmed the removal of malware allegedly planted by Chinese-backed hackers on thousands of computers across critical infrastructure. This proactive operation highlights the growing threat of nation-state cyber campaigns. The malware, capable of persistent data theft and surveillance, underscores the urgent need for international cooperation and enhanced monitoring. Experts urge organisations to adopt advanced threat detection tools and improve incident response readiness.
28. **Microsoft Cracks Down on Malicious Copilot AI Use | Dark Reading by Kristina Beek** https://tinyurl.com/574726dk | Microsoft is ramping up efforts to address the misuse of its AI-powered Copilot tool after reports of it being exploited for malicious activities, including generating phishing emails and malware code. The company has implemented stricter safeguards to curb abuse, emphasising its commitment to ethical AI use. Security experts applaud the move but caution that generative AI misuse remains a growing challenge. Organisations are encouraged to educate users and adopt AI governance frameworks to prevent similar risks.

Analysis

29. **Cyber Insights 2025: Open Source and Software Supply Chain Security | SecurityWeek by Kevin Townsend** https://tinyurl.com/3fb2zfrh | As open-source adoption grows, so do concerns about supply chain security. A new report highlights

vulnerabilities in the software development pipeline, from dependency risks to insufficient vetting processes. Experts recommend stricter governance, better visibility into open-source components, and widespread adoption of security frameworks like SBOM (Software Bill of Materials). Addressing these challenges is critical to building trust and resilience in modern software ecosystems.

30. **WEF Report Reveals Growing Cyber Resilience Divide Between Public and Private Sectors | SecurityWeek by Kevin Townsend** https://tinyurl.com/33d2vkxu | A World Economic Forum (WEF) report reveals a widening cyber resilience gap between public and private sectors. Private organisations are advancing in adopting AI and automation, while public entities lag behind due to limited resources. This divide leaves critical infrastructure and public services more vulnerable to cyberattacks. The report urges increased collaboration, investment in workforce training, and unified global standards to bridge the gap and enhance overall resilience.
31. **KnowBe4 Research Confirms Effective Security Awareness Training Significantly Reduces Data Breaches | IT Security Guru by the Gurus** https://tinyurl.com/3r6ueyw6 | Research from KnowBe4 shows that effective security awareness training can reduce data breaches by up to 90%. The study highlights how educating employees on phishing, ransomware, and other common threats significantly lowers organisational risk. Security experts emphasise that awareness training should be ongoing and paired with robust technical measures for maximum impact. This research reinforces the value of empowering employees as the first line of defense in cybersecurity.
32. **How to Eliminate “Shadow AI” in Software Development | SecurityWeek by Matias Madou** https://tinyurl.com/22dfpcr4 | The rise of “shadow AI” in software development—unauthorised use of AI tools by developers—poses serious risks, including data breaches, compliance failures, and untracked vulnerabilities. Shadow AI often circumvents governance policies, creating blind spots for security teams. To tackle this, organisations must establish clear AI policies, foster collaboration between IT and development teams, and enforce regular audits. Education on risks and proper AI integration is crucial to ensure innovation aligns with security and regulatory standards.
33. **The Shifting Landscape of Open Source Security | Dark Reading by Christopher Robinson** https://tinyurl.com/4xd2vhjb | Open source security is evolving as organisations increasingly depend on open-source software for innovation. While collaboration accelerates development, it also introduces vulnerabilities, such as dependency attacks and outdated components. Experts stress the need for better visibility into supply chains, automated vulnerability scanning, and widespread adoption of security frameworks like SBOM. As the landscape shifts, proactive measures are key to managing open-source risks effectively.
34. **Console Chaos: A Campaign Targeting Publicly Exposed Management Interfaces on Fortinet FortiGate Firewalls | Arctic Wolf by by Stefan Hostetler, Julian Tuin, Trevor Daher, Jon Grimm, Alyssa Newbury, Joe Wedderspoon & Markus Neis** https://tinyurl.com/mr3yprv2 | A new campaign, dubbed "Console Chaos," is exploiting publicly exposed management interfaces on Fortinet FortiGate firewalls. Threat actors are using brute-force attacks and stolen credentials to gain unauthorised access, potentially allowing them to manipulate configurations, exfiltrate data, and deploy malware. Security researchers warn that the exposed interfaces are a significant attack vector, especially for organisations failing to restrict access. Fortinet has advised

users to disable unnecessary interfaces, enforce multi-factor authentication (MFA), and apply the latest patches to mitigate risks. This campaign highlights the ongoing vulnerabilities in misconfigured devices and the importance of proactive network security.

Upcoming CyAN Global Events:

- AI Global Everything, Dubai, UAE: 4-6 February https://aieverythingglobal.com/
- GITEX AFRICA, Marrakesh, Morocco: 14-16 April https://tinyurl.com/2yhuztwk
- **GITEX ASIA: Singapore (Marina Bay Sands) 23-25 April** https://gitexasia.com/
- GISEC: Dubai Word Trade Center, Dubai, UAE: 6th to 8th May https://gisec.ae/home
- The Cyber Outstanding Security Performance Awards (Cyber OSPAs), May 8, London, UK https://www.thecyberospas.com/about/
- MaTeCC: Rabat, Morocco, 7-9 June, 2025 (The third annual North Africa and beyond cybersecurity event, hosted by CyAN partner organisation École High-Tech.) https://tinyurl.com/mtecz8vw