CyAN Cybersecurity Advisors Network

Cyber (In)Securities

Issue #107

NEWS:

1. Black Friday turning into Black Fraud Day, says UK cybersecurity chief

Original Source: The Guardian by Zoe Wood

The UK’s cybersecurity chief has sounded an alarm over the growing risks of Black Friday, warning that cybercriminals are exploiting the shopping frenzy to conduct widespread online fraud. Tactics like phishing emails, counterfeit websites, and fraudulent ads are being used to harvest payment details and personal data.

Shoppers are urged to verify links, use secure payment methods, and scrutinise deals that seem too good to be true. Businesses, meanwhile, must strengthen their cybersecurity protocols to guard against increasingly sophisticated threats.

With online shopping surging, this stark warning highlights the need for heightened vigilance and proactive defences to protect consumers and commerce alike.

CyberSecurity Advisors Network

NEWS:

2. US space tech giant Maxar discloses employee data breach

Original Source: BleepingComputer by Bill Toulas

Maxar, a leading US space technology company, has disclosed a breach affecting employee data, caused by a third-party vendor compromise. Exposed information includes Social Security numbers, personal contact details, and other sensitive data.

Maxar has responded with mitigation measures, including identity theft protection services for affected individuals. This breach underscores the escalating risks posed by supply chain vulnerabilities, where external partnerships become critical points of failure.

As cyber threats grow, the incident serves as a reminder of the importance of robust vendor security and proactive risk management.

CyberSecurity Advisors Network

NEWS:

3. Jen Easterly, CISA Director, to Step Down on Inauguration Day

Original Source: Dark Reading

Jen Easterly, the highly regarded Director of the US Cybersecurity and Infrastructure Security Agency (CISA), has announced her resignation, effective on Inauguration Day.

During her tenure, Easterly spearheaded efforts to enhance critical infrastructure protections and build strong public-private cybersecurity partnerships. Her departure comes at a pivotal time, as CISA faces growing threats from ransomware, nation-state actors, and emerging vulnerabilities.

This leadership transition raises concerns about the agency's ability to maintain its momentum and adapt to evolving challenges. With cyber risks escalating, Easterly’s successor will inherit significant responsibility in securing the nation’s digital landscape.

CyberSecurity Advisors Network

NEWS:

4. US charges Phobos ransomware admin after South Korea extradition

Original Source: BleepingComputer by Sergiu Gatlan

US prosecutors have charged an alleged administrator of the Phobos ransomware group following their extradition from South Korea. The individual is accused of orchestrating ransomware attacks that encrypted victims' data and demanded cryptocurrency payments for decryption keys.

This case highlights the success of international cooperation in combating ransomware and bringing cybercriminals to justice. It also underscores the growing need for coordinated global action against threat actors targeting organisations worldwide.

The indictment sends a strong message to ransomware operators, reinforcing the importance of holding perpetrators accountable.

CyberSecurity Advisors Network

NEWS:

5. Palo Alto Networks Patches Critical Zero-Day Firewall Bug

Original Source: Dark Reading by Becky Bracken

Palo Alto Networks has patched a critical zero-day vulnerability in its firewalls that was being actively exploited by attackers. The flaw allowed threat actors to bypass security measures and gain unauthorised access to networks, posing significant risks to organisations relying on these devices.

The incident highlights the urgency of applying security updates promptly to address vulnerabilities before they are exploited. Organisations are urged to patch their systems immediately to mitigate exposure. Additionally, it underscores the vital role of vendor responsiveness and proactive cybersecurity measures in safeguarding enterprise networks.

CyberSecurity Advisors Network

NEWS:

6. New Stealthy BabbleLoader Malware Spotted Delivering WhiteSnake and Meduza Stealers

Original Source: The Hacker News by Ravie Lakshmanan

BabbleLoader, a newly identified malware variant, has been observed delivering WhiteSnake and Meduza stealers, which target credentials, financial data, and other sensitive information.

This malware employs advanced evasion techniques to bypass detection, making it a formidable threat. Researchers warn that BabbleLoader's stealth capabilities highlight the increasing sophistication of modern malware campaigns.

Organisations are advised to enhance endpoint security, deploy layered defences, and monitor systems proactively to mitigate risks posed by this emerging threat.

CyberSecurity Advisors Network

NEWS:

7. Fake Bitwarden ads on Facebook push info-stealing Chrome extension

Original Source: BleepingComputer by Bill Toulas

Cybercriminals are exploiting fake Bitwarden ads on Facebook to distribute malicious Chrome extensions that steal sensitive credentials and personal data.

These fraudulent extensions mimic legitimate Bitwarden software, tricking users into downloading compromised versions that expose their information to attackers. Researchers warn that this is a sophisticated social engineering tactic, targeting unsuspecting users by exploiting trust in reputable brands.

Facebook is under scrutiny for inadequate ad vetting, highlighting the need for stronger platform security. Users are advised to verify software sources and use official sites to ensure their safety from deceptive campaigns.

CyberSecurity Advisors Network

NEWS:

8. Warning: DEEPDATA Malware Exploiting Unpatched Fortinet Flaw to Steal VPN Credentials

Original Source: The hacker News by Ravie Lakshmanan

The DEEPDATA malware is actively targeting an unpatched vulnerability in Fortinet VPN appliances to steal sensitive credentials, creating a significant threat to organisations reliant on these devices. By exploiting this flaw, attackers can infiltrate networks, access critical systems, and potentially exfiltrate valuable data.

Fortinet has urged users to update their systems, but reports indicate many devices remain vulnerable, leaving networks exposed to exploitation. This incident highlights the escalating risks posed by unpatched software, as threat actors increasingly focus on widely used solutions to maximise their impact. Proactive patching and effective vulnerability management are critical in addressing these evolving threats.

CyberSecurity Advisors Network

NEWS:

9. NSO group used WhatsApp exploits even after Meta-owned company sued it

Original Source: Security Affairs by Pierluigi Paganini

New evidence reveals that the NSO Group continued deploying Pegasus spyware using WhatsApp exploits even after being sued by Meta. These exploits targeted journalists, activists, and political figures, reinforcing concerns over Pegasus's role in global surveillance.

Despite WhatsApp's efforts to secure its platform and ongoing litigation, NSO's persistence highlights the challenges of combating sophisticated spyware developers. This case raises critical questions about tech accountability, privacy protections, and the effectiveness of existing legal frameworks to deter unethical surveillance practices. The revelations also underscore the need for stronger international cooperation to address the misuse of powerful surveillance tools in a rapidly evolving digital landscape.

CyberSecurity Advisors Network

NEWS:

10. Phishing emails increasingly use SVG attachments to evade detection

Original Source: BleepingComputer by Lawrence Abrams

Phishing campaigns are increasingly leveraging SVG attachments to evade email security filters, embedding malicious links or scripts that redirect recipients to phishing sites. These seemingly harmless files exploit weaknesses in traditional detection methods, making it difficult for automated defences to identify and block the threats.

The tactic is particularly effective at stealing credentials or delivering malware. Security researchers stress the importance of adapting email security protocols and educating employees about recognising suspicious attachments. This evolution in phishing highlights the adaptability of attackers as they continuously innovate to bypass protective measures and exploit unsuspecting users.

CyberSecurity Advisors Network

NEWS:

11. Cybersecurity dominates concerns among the C-suite, small businesses and the nation

Original Source: Security Intelligence by Jonathan Reed

Cybersecurity has emerged as a top priority for leaders at all levels, from C-suite executives to small business owners, as increasingly frequent and costly cyberattacks reshape the threat landscape. This shift underscores cyber's critical role as both an operational safeguard and a strategic imperative.

Small businesses, often lacking resources and expertise, are especially vulnerable to attacks, while larger organisations focus on resilience and regulatory compliance. The report highlights the need for cybersecurity to transcend IT departments, becoming a collaborative, organisation-wide effort.

By integrating cybersecurity into every layer of decision-making, leaders can ensure greater economic and operational stability while addressing the ever-evolving risks of a digital-first world.

CyberSecurity Advisors Network

NEWS:

12. Security plugin flaw in millions of WordPress sites gives admin access

Original Source: BleepingComputer by Bill Toulas

A critical flaw in a widely used WordPress security plugin has exposed millions of websites to potential takeover by unauthorised users, granting admin-level access. Exploiting this vulnerability allows attackers to deface sites, steal sensitive data, or inject malicious code, significantly compromising website functionality and user trust.

Administrators are strongly urged to update affected plugins immediately to reduce risks and prevent exploitation. This incident underscores the persistent dangers posed by vulnerabilities in third-party plugins, which remain a common entry point for attackers. It also highlights the need for proactive monitoring, regular updates, and stringent security practices to defend against increasingly sophisticated threats targeting popular website platforms.

CyberSecurity Advisors Network

NEWS:

13. EDR and cyber logging: Preparing for the next big cybersecurity guidance

Original Source: NexGov by Patti Chanthaphone

Endpoint detection and response (EDR) and advanced cyber logging are becoming increasingly critical as cybersecurity regulations evolve, offering improved visibility into network activity and enabling faster threat detection and response. These technologies are vital for meeting anticipated regulatory shifts that prioritise detailed data logging and operational security.

Proactively adopting EDR and logging solutions strengthens organisational defences, reduces downtime, and ensures compliance with emerging standards. As cyber threats grow more sophisticated, integrating advanced monitoring is essential for maintaining resilience, enhancing compliance, and mitigating risks in an evolving threat landscape.

CyberSecurity Advisors Network

NEWS:

14. US Prosecutors Charge Hackers in Snowflake Data Theft

Original Source: ISMG Data Breach Today by Chris Riotta

Hackers involved in a significant data theft targeting Snowflake's cloud platform have been charged by US prosecutors, spotlighting the rising risks of cybercrime in cloud environments. The attackers allegedly exploited vulnerabilities to access sensitive customer data, emphasising the critical importance of implementing robust defences in cloud systems.

Snowflake has since enhanced its security measures, but the case underscores the persistent threats targeting cloud infrastructure. This legal action sends a strong message to cybercriminals while highlighting the need for proactive security practices.

As reliance on cloud services grows, addressing vulnerabilities and improving defences is vital to safeguarding data and maintaining customer trust.

CyberSecurity Advisors Network

NEWS:

15. National cyber director calls for streamlined security regulations

Original Source: Cybersecurity Dive by David Jones

The US National Cyber Director has urged for streamlined cybersecurity regulations to reduce complexity and foster greater compliance across industries.

Current frameworks, fragmented across jurisdictions, often lead to confusion and inefficiencies, hampering organisational efforts to implement robust defences. Simplifying these policies would allow businesses to allocate resources more effectively and improve national resilience against evolving threats.

This initiative reflects growing recognition that disjointed regulations hinder progress. A unified, well-coordinated strategy is critical to addressing increasingly sophisticated cyber challenges while supporting economic and operational security.

CyberSecurity Advisors Network

ANALYSIS:

16. The cybersecurity provider’s next opportunity: Making AI safer

1. **Original Source: McKinsey by by Justin Greis and Marc Sorel with Julian Fuchs-Souchon and Soumya Banerjee**

AI’s rapid adoption has introduced new vulnerabilities, making cybersecurity vital for protecting AI systems against threats like adversarial attacks and data poisoning. This McKinsey analysis examines how providers can address these risks to position themselves as leaders in AI security.

Developing robust tools and frameworks to safeguard AI represents both a technical challenge and a lucrative market opportunity. By prioritising AI security, organisations can build trust, foster innovation, and ensure AI’s potential is leveraged safely.

The article underscores the importance of balancing progress with ethical standards, enabling an AI-driven future that prioritises safety and resilience in increasingly complex threat landscapes.

CyberSecurity Advisors Network

ANALYSIS:

17. How Generative AI Will Change Jobs In Cybersecurity

Original Source: Forbes by Bernard Marr

Generative AI is transforming cybersecurity roles by automating tasks like threat detection and incident analysis, allowing professionals to focus on strategic challenges and creative problem-solving.

This article explores how AI tools enable cybersecurity teams to address complex threats more effectively while leveraging advanced technologies to streamline operations. However, the shift demands significant reskilling, as understanding and integrating AI tools becomes essential for success.

The evolution signals a future where adaptability, technical fluency, and innovation define cybersecurity roles, with AI acting as a powerful ally in combating sophisticated cyber threats and improving resilience.

CyberSecurity Advisors Network

ANALYSIS:

18. Washington's Cybersecurity Storm of Complacency

Original Source: Dark Reading by Jeffrey Wells

Washington faces growing criticism for its fragmented and complacent approach to cybersecurity, leaving critical systems exposed to escalating threats. Insufficient regulatory coordination and enforcement have created gaps that adversaries exploit, endangering vital infrastructure.

This article urges policymakers to address systemic weaknesses by adopting unified strategies that prioritise national security and strengthen defences. Without decisive action, the US risks falling behind in countering cyber threats, jeopardising both economic stability and global competitiveness.

Comprehensive reforms are essential to secure critical systems and maintain resilience in a rapidly evolving threat landscape.

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!