CyAN Cybersecurity Advisors Network

Cyber (In)Securities

Issue #101

NEWS:

1. Cybercriminals Pose a Greater Threat of Disruptive US Election Hacks Than Russia or China

Original Source: Wired by Lily Hay Newman & Dell Cameron

As the 2024 U.S. election season unfolds, the Department of Homeland Security highlights that cybercriminals, motivated by financial or ideological aims, pose a more direct risk to election infrastructure than state-backed actors.

While nation-states focus on espionage, cybercriminals target local governments with ransomware and DDoS attacks, risking election disruption without directly impacting vote counts. Recent incidents underline how minor breaches can delay operations, heightening the urgency for robust defences. Cyber experts stress the importance of collaboration between local and federal authorities to reduce vulnerabilities.

CyberSecurity Advisors Network

NEWS:

2. Free, France’s second largest ISP, confirms data breach after leak

Original Source: BleepingComputer by Sergiu Gatlan

Free, France's second-largest ISP, has confirmed a data breach following the appearance of customer data on a hacker forum. The leak exposes sensitive information, including email addresses and customer IDs, highlighting risks around ISP security practices.

Free’s response includes assurances of additional protections, but experts warn that such breaches expose serious vulnerabilities within essential service providers. This incident raises concerns for internet users and regulators alike, fueling ongoing discussions around data privacy standards and the need for stricter ISP security measures.

CyberSecurity Advisors Network

NEWS:

3. Russia targets Ukrainian conscripts with Windows, Android malware

Original Source: BleepingComputer by Bill Toulas

Russia has reportedly launched a new cyber campaign targeting Ukrainian military conscripts using malware that infects both Windows and Android devices.

The campaign appears to use phishing emails that trick recipients into downloading malicious attachments. Once downloaded, these attachments deploy two types of malware: one for Windows, designed to steal information and monitor activity, and one for Android, focusing on exfiltrating sensitive data and tracking the conscript's movements.

The dual-platform approach highlights a growing sophistication in Russian cyber capabilities, targeting a broader range of operating systems to maximise reach and impact.

CyberSecurity Advisors Network

NEWS:

4. Over 70 zero-day flaws get hackers $1 million at Pwn2Own Ireland

Original Source: BleepingComputer by Bill Toulas

At the latest Pwn2Own Ireland event, hackers exploited over 70 zero-day vulnerabilities, collectively winning $1 million in prizes for their discoveries. Devices from major brands, including Samsung, QNAP, and Synology, were successfully breached, revealing security weaknesses even in fully patched products.

Many attacks used new techniques, reflecting the rapid evolution of threat vectors in consumer technology. This year’s event underscores the pressing need for stronger, real-time vulnerability defences across IoT and mobile devices. Vendors now have 120 days to patch the vulnerabilities before public disclosure, a tight window to safeguard users and prevent future exploits.

CyberSecurity Advisors Network

NEWS:

5. Black Basta ransomware poses as IT support on Microsoft Teams to breach networks

Original Source: BleepingComputer Lawrence Abrams

The Black Basta ransomware group has been using a new tactic to infiltrate corporate networks by posing as IT support staff on Microsoft Teams. By impersonating legitimate IT personnel, the attackers gain trust and trick employees into granting access, ultimately deploying ransomware on company systems.

This method highlights the growing sophistication of social engineering tactics in ransomware campaigns and underscores the need for organisations to train employees on verifying identities and being cautious with unsolicited support interactions. Experts warn that this approach bypasses traditional security measures, making user education a critical line of defense against similar attacks.

CyberSecurity Advisors Network

NEWS:

6. Apple will pay you up to $1 million if you can hack into Apple Intelligence servers

Original Source: ZD Net Lance Whitney

Apple has raised the stakes on its bug bounty program, offering up to $1 million for security researchers who can identify vulnerabilities within its Apple Intelligence servers. This bounty underscores Apple’s commitment to strengthening its cybersecurity defences by incentivising ethical hacking.

The initiative aims to uncover potential security gaps that could otherwise be exploited by malicious actors. With cyber threats becoming more complex, Apple’s move reflects a proactive stance in engaging the security community to help safeguard its infrastructure and user data, reinforcing its dedication to user privacy and system integrity.

CyberSecurity Advisors Network

NEWS:

7. 'Consent' LinkedIn used for data processing was not freely given, says Ireland

Original Source: The Register by Jude Karabus

Ireland’s data protection authority has ruled that LinkedIn’s consent for data processing does not meet the standard of being “freely given.” The decision questions LinkedIn's methods of obtaining user consent and may have implications for other companies operating under GDPR guidelines.

With the ruling, LinkedIn could face penalties or be required to adjust its data policies to comply with European standards. This finding emphasises the importance of transparent data practices and could lead to broader scrutiny of how consent is gathered across social media and tech platforms, impacting privacy practices industry-wide.

CyberSecurity Advisors Network

ANALYSIS:

8. Regulatory Index: Comparing international approaches and perspectives to online safety regulation

Original Source: Global Online Safety Regulators Network

The Global Online Safety Regulators Network Regulatory Index provides an international framework for online safety regulation, setting a collaborative standard for digital protection. Each jurisdiction's approach—whether content-based, systems-based, or hybrid—reflects diverse regulatory goals that share the common ground of mitigating cyber risks and online harm. This document highlights the increasing regulatory convergence aimed at countering threats such as child exploitation, disinformation, and extremism across platforms.

From a cybersecurity standpoint, the Index's focus on information gathering, proactive content scanning, and service blocking shows a shift toward enforcing safer digital environments. This harmonisation effort also emphasises robust mechanisms like data transparency, blocking orders, and encryption standards, creating a broader toolkit for digital resilience. The Network's Index ultimately underscores the need for both regulatory alignment and adaptable enforcement tactics as cyber threats evolve globally.

ANALYSIS:

9. Cybersecurity Priority Recommendations for the Next President

Original Source: Lohrmann on Cybersecurity by Dan Lohrmann

As the next U.S. administration prepares for office, cybersecurity experts underscore key priorities to bolster national cyber resilience. High among the recommendations is the urgent need for federal leadership to build a cohesive, long-term national cybersecurity strategy. Experts advise leveraging frameworks like the NIST Cybersecurity Framework to enhance public-private sector coordination, which can strengthen response capabilities against large-scale cyber threats.

Another critical recommendation focuses on securing both physical and digital assets across sectors, from government agencies to energy and healthcare. Additionally, funding cyber education is essential to develop the workforce needed to maintain the nation’s digital defences. Lastly, international cooperation is emphasised to combat cross-border cyber threats, where combined efforts are most effective.

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!