CyAN Cybersecurity Advisors Network

Cyber (In)Securities

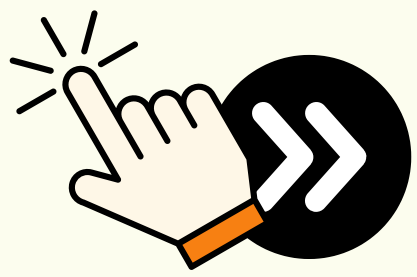
Issue #98

NEWS:

1. Iranian hackers act as brokers selling critical infrastructure access

Source: Bleeping Computer by Ionut Ilascu

Iranian hacking groups are now acting as brokers, selling access to critical infrastructure networks. These state-sponsored actors target sectors like energy and healthcare, using brute force attacks to gain access. Once inside, they sell this access to other malicious actors, raising the stakes for organisations worldwide. The increased sophistication of these operations is alarming, as it allows multiple groups to exploit the same compromised infrastructure. The growing market for selling compromised access underscores the need for stronger defences and proactive threat monitoring. For more on how to protect your organisation, visit Australian Signals Directorate.



Swipe for more

CyAN Cybersecurity Advisors Network

NEWS:

2. Anthropic flags AI's potential to 'automate sophisticated destructive cyber attacks

Source: ZDNET by Tiernan Ray

Anthropic, a leading AI research lab, has raised alarms about the potential for AI to automate and escalate destructive cyberattacks. By leveraging advanced AI systems, cybercriminals could significantly increase the frequency, complexity, and impact of attacks with less human involvement, potentially overwhelming traditional defences. This emerging threat has prompted calls for stricter regulations on AI development and deployment, as well as a rethinking of cybersecurity strategies to address AI-powered threats. With AI's capabilities advancing rapidly, there is a growing fear that bad actors could weaponize it to exploit vulnerabilities on an unprecedented scale. As these risks evolve, organisations must bolster their defences to mitigate the looming threats of AI-driven cyber warfare.

Swipe for more

CyAN Cybersecurity Advisors Network

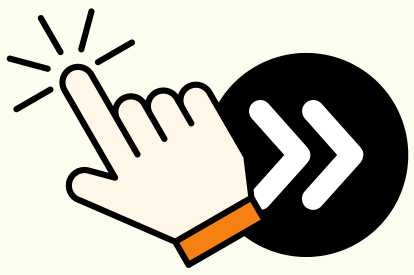
NEWS:

3. This AI Tool Helped Convict People of Murder. Then Someone Took a Closer Look

Source: Wired by Todd Feathers

The rise of Cybercheck, a tool used by law enforcement to automate digital evidence reviews, is sparking concern. While it promises to speed up cybercrime investigations, critics argue that the tool may be leading to rushed prosecutions, incomplete investigations, and potential miscarriages of justice. By relying heavily on automated processes, police risk missing key nuances in cases and undermining trust in the system. Cybercheck's rapid adoption highlights a tension between technological efficiency and the potential for serious legal consequences if human oversight is sidelined. As the tool becomes more widespread, questions remain about its long-term impact on the justice system.

Swipe for more



CyAN Cybersecurity Advisors Network

NEWS:

4. Election Day is Close, the Threat of Cyber Disruption is Real

Source: Security Week by Kevin Townsend

With the US Election Day looming, cybersecurity experts are warning of increased risks of cyber disruptions, including potential attacks on voting infrastructure and disinformation campaigns. Hackers, possibly linked to nation-states, could seek to undermine the integrity of the electoral process through denial-of-service attacks, data breaches, or targeted misinformation. This heightened threat landscape is a stark reminder for election officials and organisations to bolster their defences and ensure that robust safeguards are in place to maintain public trust. As the election draws near, the emphasis on securing both physical and digital infrastructure has never been more critical.

Swipe for more

Cybersecurity Advisors Network

CyAN

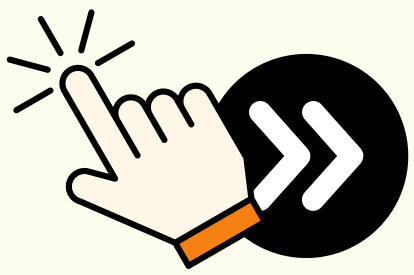
NEWS:

5. New Linux Variant of FASTCash Malware Targets Payment Switches in ATM Heists

Source: The Hacker News by Ravie Lakshmanan

A new Linux variant of the notorious FASTCash malware is posing a serious threat to financial institutions, enabling attackers to withdraw large sums of cash by manipulating bank transaction systems. This malware, long associated with North Korean state-sponsored hackers, has been upgraded to exploit vulnerabilities in Linux servers. The emergence of this new variant signals an elevated risk for banks that rely on outdated or unpatched systems. Institutions are urged to strengthen their security measures to prevent exploitation, as the malware's sophistication grows and attackers continue to target financial networks globally.

Swipe for more



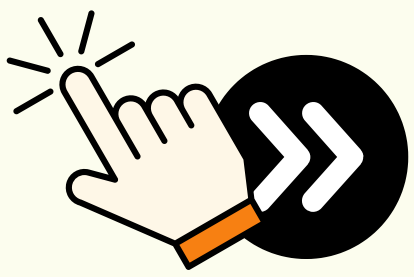
NEWS:

6. National Public Data, the hacked data broker that lost millions of Social Security numbers and more, files for bankruptcy

Source: Tech Crunch by Zack Whittaker

National Public Data, a U.S. data broker, has filed for bankruptcy following a massive breach that exposed millions of Social Security numbers and other sensitive personal information. The breach, which has sent shockwaves through the data brokerage industry, involved hackers exploiting vulnerabilities in the company's systems. This incident highlights the growing risks posed by companies that handle vast amounts of personal data without adequate security measures. For organisations dependent on data brokers, this serves as a critical reminder to reassess third-party risks and ensure robust protections are in place to guard against breaches that could have devastating consequences.

Swipe for more



CyAN Cybersecurity Advisors Network

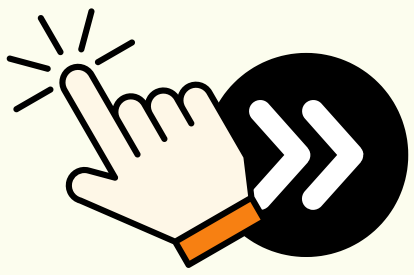
NEWS:

7. Millions of People Are Using Abusive AI ‘Nudify’ Bots on Telegram

Source: Wired by Matt Burgess

Telegram's 'nudify' bots are using AI to create non-consensual deepfake nudes of unsuspecting women, raising alarm bells across the digital rights community. These bots, which strip clothing from images and generate realistic deepfakes, are causing irreparable harm by targeting victims and spreading the doctored images across private and public channels. While Telegram has seen increased scrutiny over its lax content moderation, the rise of AI-powered abuse tools has intensified calls for stronger regulations and platform accountability. This growing threat underscores the dangerous intersection of AI and digital exploitation, demanding urgent attention from lawmakers and tech companies alike to curb the abuse.

Swipe for more



NEWS:

8. Lots of PCs are poised to fall off the Windows 10 update cliff one year from today

Source: Ars Technica by Andrew Cunningham

In a year’s time, a significant number of PCs will no longer receive updates for Windows 10, potentially leaving millions of devices vulnerable to security risks. With Microsoft ending support for older systems, users will face a difficult choice between upgrading their hardware or running outdated, unsupported software. As the deadline approaches, the tech world is bracing for a wave of devices left exposed to cyber threats. This situation underscores the importance of forward planning for organisations reliant on legacy systems, ensuring that upgrades or mitigation strategies are in place to avoid the growing risks of running unpatched, outdated software.

Swipe for more

UPCOMING CyAN EVENTS

Dubai: October 14th - 18th
CyAN Partners with GITEX 1

Sydney: November 27th
Women (and their allies!) in Cyber

Swipe for more

CyberSecurity Advisors Network

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

#ReallyInterestingCyberStuff!