CyAN Cybersecurity Advisors Network

Cyber (In)Securities

Issue #103

NEWS:

1. DocuSign's Envelopes API abused to send realistic fake invoices

Original Source: BleepingComputer by Bill Toulas

Cybercriminals are exploiting DocuSign’s Envelopes API to deliver highly convincing fake invoices, tricking recipients into clicking on malicious links. By abusing this legitimate API, attackers are able to create phishing emails that appear authentic, bypassing traditional security filters and making detection challenging for both users and security teams.

DocuSign, aware of the issue, has advised customers to remain vigilant and verify invoice details before interacting. This incident underscores the risks posed by phishing schemes that misuse trusted services, pushing organisations to enhance security measures and user awareness around potential threats.

CyberSecurity Advisors Network

NEWS:

2. Regulator's Call to Breached Organiations: 'Be Human’

Original Source: ISMG Data Breach Today by Mathew Schwartz

In light of increasing data breaches, regulators are calling for a more human-centred approach from affected organisations, urging them to prioritise empathy and transparency in their communications with customers.

Traditionally, responses to breaches have often been impersonal and overly technical, which can erode trust and lead to further reputational damage. The new guidance emphasises clear, compassionate communication that addresses customers' concerns directly, ensuring they understand the incident’s impact and the measures taken to protect them. This shift aims to improve customer relationships and trust as organisations navigate breach responses more thoughtfully.

CyberSecurity Advisors Network

NEWS:

3. Gmail 2FA Cyber Attacks—Open Another Account Before It’s Too Late

Original Source: Forbes by Davey Winder

Cybercriminals are exploiting vulnerabilities in Gmail’s two-factor authentication (2FA) system through sophisticated phishing and man-in-the-middle techniques, which allow attackers to capture both user credentials and 2FA codes in real time.

By setting up fake login portals that mimic Google’s login page, they can bypass Gmail’s protections, leaving even vigilant users exposed.

Security experts recommend Gmail users consider moving beyond SMS-based 2FA to app-based or hardware 2FA options, especially for high-value accounts, while also setting up backup accounts to reduce the risk of total account compromise.

CyberSecurity Advisors Network

NEWS:

4. ChatGPT-4o can be used for autonomous voice-based scams

Original Source: BleepingComputer by Bill Toulas

ChatGPT-4o's voice generation capabilities are now being exploited for highly realistic, autonomous voice phishing scams, enabling scammers to create interactive calls that convincingly mimic voices of trusted contacts.

With minimal input, attackers can generate dialogues that sound credible and manipulate victims into revealing sensitive information or transferring funds. This AI-powered approach bypasses traditional trust-based security measures like voice recognition, as it closely replicates human speech.

Experts stress the urgent need for new regulatory frameworks and user awareness to counter the growing threat posed by AI-driven scams.

CyberSecurity Advisors Network

NEWS:

5. LastPass Warns of Hackers Misusing Reviews for Fake Support Numbers

Original Source: Cyber Security News by Guru Baran

LastPass has issued a warning after discovering that hackers are posting fake customer support numbers in online review sections, tricking users into calling these numbers and connecting with fake “support agents.”

Once connected, the attackers impersonate LastPass representatives, manipulating victims into disclosing account information or credentials. This indirect phishing method bypasses traditional detection systems by exploiting trusted review platforms.

LastPass is urging users to verify support numbers from official channels only and avoid using search engines or third-party sources, as these scams continue to evolve in sophistication.

CyberSecurity Advisors Network

NEWS:

6. Synology hurries out patches for zero-days exploited at Pwn2Own

Original Source: BleepingComputer by Sergiu Gatlan

Synology released urgent patches after two zero-day vulnerabilities were exploited at the Pwn2Own competition, where researchers showed how attackers could gain unauthorised access to Synology's network-attached storage (NAS) systems.

These zero-days, if left unpatched, could allow cybercriminals to manipulate or steal data stored on Synology devices. Synology's quick response illustrates the importance of prompt security patches, especially for devices storing critical information. Users are advised to apply the updates immediately, underscoring how events like Pwn2Own play a crucial role in identifying and remediating vulnerabilities before they're widely exploited.

CyberSecurity Advisors Network

NEWS:

7. German police arrest two for alleged ties to DDoS-for-hire platform

Original Source: The Record by James Reddick

German police arrested two individuals allegedly connected to a Distributed Denial-of-Service (DDoS)-for-hire platform that rented out attack power to disrupt online services for paying clients. DDoS-for-hire services allow anyone to conduct damaging attacks with minimal technical skill, often targeting businesses or public institutions.

This crackdown marks a win for international cybersecurity, as DDoS-for-hire remains a significant and ongoing threat. The incident emphasises the importance of cross-border cooperation in combating cybercrime and highlights the need for organisations to implement robust DDoS defences to mitigate these types of attacks.

CyberSecurity Advisors Network

NEWS:

8. Chinese Hackers Use Quad7 Botnet for Credential Theft

Original Source: ISMG Bank Info Security by Akshaya Asokan

Chinese threat actors are deploying the Quad7 botnet to conduct credential theft attacks, primarily targeting government agencies and financial institutions.

The botnet infects devices and captures login credentials, sending them back to attacker-controlled servers for later use in unauthorized access or data exfiltration. By focusing on credential theft, hackers can infiltrate systems more stealthily, often bypassing traditional security alerts.

Experts recommend multi-factor authentication and vigilant botnet monitoring as essential defences to counteract these evolving botnet-based credential theft methods and protect sensitive organisational data.

CyberSecurity Advisors Network

ANALYSIS:

9. National Cyber Threat Assessment

Original Source: Canadian Centre for Cyber Security

Canada’s Communications Security Establishment (CSE) identifies China’s extensive and assertive cyber activities as the leading internet-based threat to the nation, highlighting concerns over data theft, surveillance, and espionage. The report warns that state adversaries, including China and Russia, are actively targeting Canada’s digital infrastructure with the aim of sowing division within Canadian society.

Additionally, ransomware is pinpointed as the most significant cybercrime threat, particularly impacting Canada’s critical infrastructure sectors such as energy, healthcare, and transportation. With these escalating risks, Canada has committed close to a billion dollars over the next five years to bolster intelligence operations and cybersecurity programs, a strategic investment aimed at fortifying national resilience against both cybercriminal and state-sponsored threats.

CyberSecurity Advisors Network

ANALYSIS:

10. 2024 ISC2 Cybersecurity Workforce Study

Original Source: ISC2

The 2024 ISC2 Cybersecurity Workforce Study reveals that approximately 50% of cybersecurity practitioners and decision-makers anticipate that generative artificial intelligence (GenAI) will render certain technical skills and roles obsolete within the field.

This perspective underscores a significant shift in the cybersecurity landscape, where AI-driven tools are expected to automate routine tasks such as threat detection and incident response. Consequently, the demand for professionals with advanced technical expertise may diminish, while the need for skills in AI oversight, strategic decision-making, and ethical considerations is likely to increase. Organisations must adapt by redefining job roles and investing in training programs that equip their workforce with competencies aligned with an AI-integrated cybersecurity environment.

CyberSecurity Advisors Network

ANALYSIS:

11. CISO Top 10 Priorities for Q3 2024: Navigating Cybersecurity's Evolving Challenges

Original Source: SC Media by Bill Brenner & Dustin Sachs

The "CISO Top 10 Priorities for Q3 2024" report highlights the evolving challenges in the cybersecurity landscape, emphasising the need for a strategic approach to risk, compliance, and technology. Governance, Risk, and Compliance (GRC) remain at the forefront, underscoring the importance of aligning operations with regulations and internal policies.

The integration of emerging technologies is crucial for enhancing threat detection and response capabilities. Additionally, Cloud Security and Identity and Access Management (IAM) are critical areas of focus, reflecting the widespread adoption of cloud services and the necessity of controlling access to sensitive data. The report underscores the need for CISOs to act as both security leaders and strategic advisors, navigating the balance between innovation and risk.

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!