CyAN Cybersecurity Advisors Network

Cyber (In)Securities

Issue #141

NEWS:

1. Former cyber official targeted by Trump quits company over move

Original Source: NBC News by Kevin Collier

Chris Krebs, former Director of the Cybersecurity and Infrastructure Security Agency (CISA), has resigned from his role at cybersecurity firm SentinelOne. This move follows actions by former President Donald Trump, who revoked Krebs' security clearance and initiated a Department of Justice investigation into his tenure at CISA.

Krebs stated that his departure aims to shield SentinelOne from political fallout, emphasising, "This is my fight, not the company's."

The cybersecurity community has largely remained silent, with only one of 33 firms contacted by Reuters offering public support. This situation underscores concerns about the politicisation of cybersecurity roles and the potential chilling effect on professionals in the field.

CyberSecurity Advisors Network

NEWS:

2. MITRE's CVE program given last-minute reprieve

Original Source: itNews by Raphael Satter

CISA has granted an 11-month funding extension to MITRE's Common Vulnerabilities and Exposures (CVE) program, averting a shutdown that had alarmed the global cybersecurity community.

The move preserves a critical resource used worldwide to identify and catalog software vulnerabilities.

In response to sustainability concerns, CVE Board members are launching the nonprofit CVE Foundation to reduce reliance on U.S. government funding.

The reprieve highlights the need for a more resilient, community-led approach to supporting vital cybersecurity infrastructure

For more information on this subject see article number 48, '*No Time for Antics with Semantics: Why CVEs Are Cybersecurity's Lifeline*' by Kim Chandler McDonald

NEWS:

3. Whistle Blower: Russian Breach of US Data Through DOGE Was Carried Out Over Starlink "Directly to Russia”

Original Source: Narativ by Zev Shalev

A whistleblower has alleged that systems used by the Department of Government Efficiency (DOGE) were linked to Starlink and exposed to the open internet, potentially granting Russian adversaries access to critical U.S. infrastructure—including nuclear oversight agencies.

DOGE engineers are accused of unlawfully accessing government systems and creating credentials later used by Russian IPs.

The whistleblower has since been threatened and surveilled, raising fears of retaliation while highlighting urgent questions about national security, tech accountability, and civilian-military data separation.

For more on this topic see article number 43, *‘DOGE’s tech takeover threatens the safety and stability of our critical data ’*

NEWS:

4. Midnight Blizzard deploys new GrapeLoader malware in embassy phishing

Original Source: BleepingComputer by Bill Toulas

Russia-linked APT group Midnight Blizzard is using a new malware loader, dubbed GrapeLoader, in targeted phishing attacks against diplomatic entities.

The campaign impersonates embassies in Central Asia and delivers malware via weaponised PDFs, allowing stealthy execution of additional payloads.

GrapeLoader’s minimalist design helps it evade detection, highlighting the group’s evolving toolkit.

This operation reinforces the growing sophistication of state-backed phishing campaigns and their reliance on socially engineered lures crafted to exploit trust in official institutions and international diplomacy.

CyberSecurity Advisors Network

NEWS:

5. Infamous message board 4chan taken down following major hack

Original Source: BleepingComputer by Sergiu Gatlan

4chan, the notorious message board often associated with far-right extremism, harassment campaigns, and conspiracy theories, was forced offline after hackers breached its infrastructure.

The attackers reportedly accessed administrator credentials, backend tools, and IP address logs—offering unprecedented visibility into the site's inner workings.

While 4chan denies any user data was compromised, the takedown marks a rare and significant disruption to one of the internet's most persistent hubs of online radicalisation. For a platform that thrives on chaos, being silenced—even briefly—landed like a gut punch.

CyberSecurity Advisors Network

NEWS:

6. Chinese law enforcement places NSA operatives on wanted list over alleged cyberattacks

Original Source: Cyberscoop by Tim Starks

In a provocative move, China has issued arrest warrants for several U.S. NSA operatives, accusing them of launching cyberattacks on Chinese institutions.

The wanted list includes both named and unnamed officials linked to Tailored Access Operations (TAO), the NSA's elite hacking unit.

While largely symbolic, the announcement signals escalating cyber posturing between the two powers, China's decision to publicly name American cyber operators mirrors tactics used by the U.S. against Chinese APT actors and adds a new layer of diplomatic friction to an already tense cybersecurity landscape. The move also reflects growing efforts by China to shape the narrative around global cyber norms.

CyberSecurity Advisors Network

NEWS:

7. RansomHouse Ransomware: What You Need To Know

Original Source: Fortra by Graham Cluley

RansomHouse is a financially motivated ransomware group that distinguishes itself by prioritising data theft over encryption.

Active since at least 2022, the group targets poorly secured networks—often exploiting weak credentials or outdated software—and pressures victims by threatening public exposure.

Their branding as “negotiators” rather than hackers reflects a growing trend of cybercriminal PR spin, where extortion is framed as a business transaction.

Recent attacks show they favour agility and psychological pressure over brute-force disruption. Their methods serve as a warning that data exposure alone can now cripple an organisation's operations and reputation.

CyberSecurity Advisors Network

NEWS:

8. Wave of Wine-Inspired Phishing Attacks Targets EU Diplomats

Original Source: Dark Reading by Elizabeth Montalbano

A phishing campaign dubbed “VinoPhish” is targeting EU diplomats with wine-themed emails crafted to appear personal and culturally relevant.

The lures include malicious Word attachments that deploy malware designed to steal credentials and sensitive data.

The campaign demonstrates the increasing precision of social engineering, where attackers exploit not only institutional trust but regional familiarity and lifestyle cues.

By blending charm with compromise, these phishing tactics highlight how even sophisticated targets can be caught off guard when threats arrive in elegant disguise. The campaign is also notable for its creative use of familiar imagery to reduce suspicion.

CyberSecurity Advisors Network

NEWS:

9. Chinese espionage group leans on open-source tools to mask intrusions

Original Source: Cyberscoop by Derek B. Johnson

A Chinese-linked threat actor has been observed using legitimate open-source tools, such as SoftEther VPN and Cobalt Strike, to conduct cyber espionage while evading detection.

By blending into normal network traffic and avoiding custom malware, the group minimises its forensic footprint and complicates attribution.

This strategy reflects a broader shift among APTs favouring low-profile, modular operations over flashy exploits.

Security teams are being urged to monitor behavioural anomalies, not just indicators of compromise, as open-source misuse becomes a common cloak for advanced threat campaigns.

CyberSecurity Advisors Network

NEWS:

10. Critical Apache Roller Flaw Allows to Retain Unauthorised Access Even After a Password Change

Original Source: Security Affairs Pierluigi Paganini

A critical vulnerability in Apache Roller allows attackers to maintain unauthorised access to user accounts even after a password has been changed.

The flaw stems from insecure session handling and token management, enabling persistent access through session fixation or hijacking techniques.

This issue highlights the risks posed by poor session invalidation and the importance of revoking all active sessions following credential updates. If exploited, the flaw could enable long-term account compromise despite user attempts to secure their profiles—raising broader concerns about web application hygiene and design assumptions.

CyberSecurity Advisors Network

NEWS:

11. Chinese Hackers Target Linux Systems Using SNOWLIGHT Malware and VShell Tool

Original Source: The Hacker News by Ravie Lakshmanan

A Chinese APT group is deploying a custom Linux malware called SNOWLIGHT in espionage campaigns targeting government and defence sectors.

The group pairs SNOWLIGHT with VShell, a legitimate remote access tool, to establish stealthy backdoors into Linux systems.

This combination allows attackers to avoid detection by blending malicious payloads with trusted software.

The campaign reflects a growing trend of targeting Linux environments with tailored implants and dual-use tools—highlighting how enterprise defenders must expand visibility beyond Windows-based threats to secure increasingly heterogeneous infrastructure.

CyberSecurity Advisors Network

NEWS:

12. 2.6 Million Impacted by Landmark Admin, Young Consulting Data Breaches

Original Source: SecurityWeek by Ionut Arghire

Two third-party benefits administrators, Landmark Admin and Young Consulting, have disclosed separate data breaches affecting a combined 2.6 million individuals.

The exposed data includes US Social Security numbers, health insurance information, and other personally identifiable details.

The breaches, both linked to external file transfer vulnerabilities, underline the risks posed by supply chain dependencies in sectors handling sensitive data.

As benefit platforms become lucrative targets, the incidents highlight the urgent need for stronger vendor oversight and improved security around data-sharing tools used by service providers.

CyberSecurity Advisors Network

NEWS:

13. China-Backed Threat Actor 'UNC5174' Using Open Source Tools in Stealthy Attacks

Original Source: Dark Reading by Alexander Culafi

UNC5174, a suspected Chinese state-sponsored threat actor, has been leveraging open-source tools like MeshAgent and SoftEther VPN to conduct covert cyber operations.

These tools allow the group to blend into normal network activity, reducing the chances of detection and complicating attribution.

The campaigns have targeted organisations across Asia and Europe, focusing on telecom and government sectors.

This approach reflects a growing preference among APTs for publicly available tools to maintain stealth and persistence, making threat detection increasingly dependent on behavioural analysis rather than signatures.

CyberSecurity Advisors Network

NEWS:

14. A whistleblower's disclosure details how DOGE may have taken sensitive labor data

Original Source: NPR by Jenna McLaughlin

A critical zero-day vulnerability in Fortinet's FortiOS SSL-VPN (CVE-2024-21762) has led to widespread exploitation, with over 14,000 devices compromised globally.

Despite patches, Fortinet has warned that attackers may retain access post-update through a symlink exploit that bypasses standard defences.

This chain of exploitation reveals both the severity of the initial flaw and the sophistication of access persistence techniques.

The incident underscores the importance of thorough post-patch auditing, comprehensive configuration reviews, and the need for greater transparency in disclosing real-world attack behaviour.

CyberSecurity Advisors Network

NEWS:

15. Govtech giant Conduent confirms client data stolen in January cyberattack

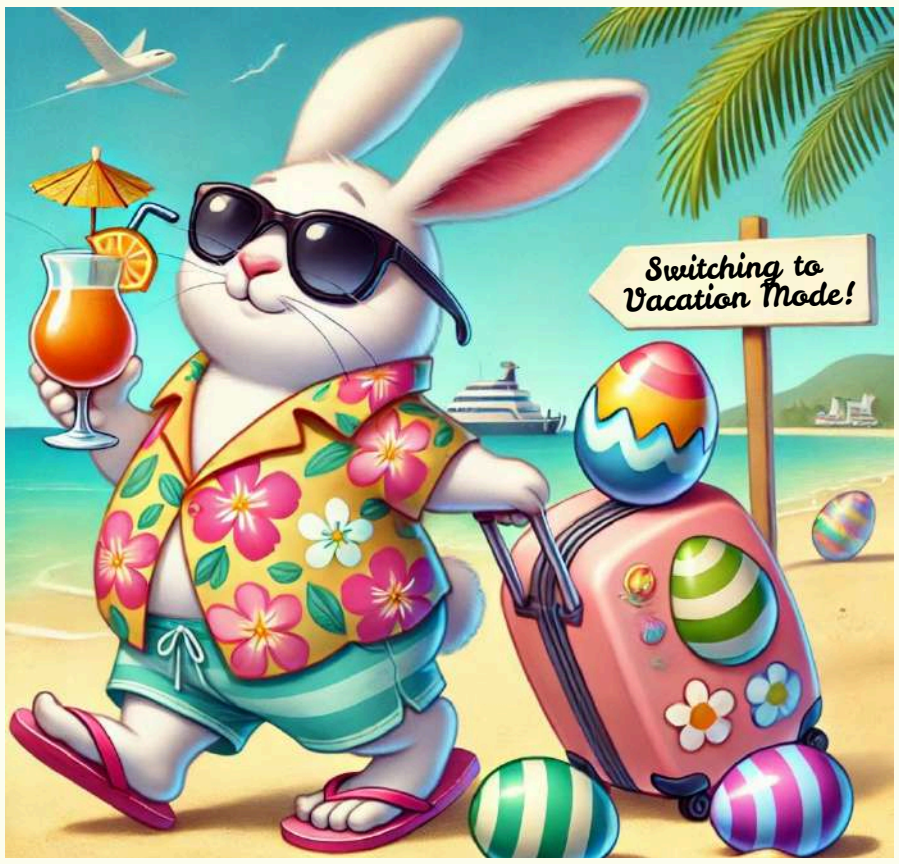
Original Source: BleepingComputer by Lawrence Abrams

A whistleblower claims that DOGE, a lesser-known tech vendor contracted by the U.S. Department of Labor, may have inappropriately accessed sensitive worker data through its role in a major government modernisation project.

The allegations include insecure systems, poor oversight, and potential mishandling of personally identifiable information.

Though the full extent is unclear, the claims have prompted investigations and concern over the vetting of contractors in federal IT projects. The case highlights growing unease around vendor accountability and the risks of outsourcing critical infrastructure.

CyberSecurity Advisors Network



🌴 Holiday Schedule for (In)Securities!

Hop into the holiday spirit! Due to this weekend's Easter celebrations and next week's ANZAC Day commemorations, during the weeks of Monday, April 14th and 21st, we're taking a small breather just like our beach-loving bunny here.

We'll be publishing only one edition each week, on the Thursdays (April 17th and 24th).

So, while our newsletter takes a mini-holiday, we hope you enjoy your festivities too! Look out for the Easter edition dropping into your inboxes with just as much zest as a bunny on a beach vacation!

Thank you for being such fabulous readers. Stay safe, have fun, and let's keep cracking on those cyber eggs together!

🐰✉️ Catch you on the sunny side of Cyberspace!

NEWS:

16. Cybersecurity firm buying hacker forum accounts to spy on cybercriminals

Original Source: BleepingComputer by Bill Toulas

Conduent, a major provider of tech services to government and business clients, has confirmed that sensitive data was stolen during a January 2024 cyberattack.

The breach affected file transfer systems and led to the exposure of personally identifiable information across multiple clients.

While Conduent has not disclosed the total number of impacted individuals, it has begun notifying affected parties and working with forensic investigators.

The breach underscores ongoing concerns about the security of file exchange tools, especially in high-trust environments like healthcare and government contracts.

CyberSecurity Advisors Network

NEWS:

17. Cyber congressman demands answers before CISA gets cut down to size

Original Source: The Register by Jessica Lyons

A cybersecurity firm has admitted to purchasing accounts on underground hacker forums to monitor cybercriminal activity from within.

By gaining access to internal discussions, leaked databases, and illicit marketplace chatter, the company claims it can better anticipate emerging threats.

While controversial, the tactic highlights the blurry ethical line between intelligence gathering and infiltration.

Critics warn that such actions could compromise investigations or unintentionally fund illegal platforms.

The move raises important questions about what responsible threat intelligence operations should look like in today's threat landscape.

CyberSecurity Advisors Network

NEWS:

18. Huntress Documents In-The-Wild Exploitation of Critical Gladinet Vulnerabilities

Original Source: SecurityWeek by Ryan Naraine

Cybersecurity firm Huntress has observed active exploitation of multiple critical vulnerabilities in Gladinet's CentreStack cloud file-sharing platform.

Attackers are using these flaws to gain unauthorised access, exfiltrate sensitive data, and potentially deploy ransomware.

The vulnerabilities, which affect both cloud and on-premise deployments, were disclosed alongside proof-of-concept exploits. Huntress warns that thousands of instances may still be exposed.

The incident highlights the urgent need for patching overlooked enterprise software and reinforces the risks posed by seemingly niche but widely deployed tools.

CyberSecurity Advisors Network

NEWS:

19. Chinese APTs Exploit EDR 'Visibility Gap' for Cyber Espionage

Original Source: Dark Reading by Becky Bracken

Chinese state-backed threat actors are taking advantage of a visibility gap in many Endpoint Detection and Response (EDR) systems, using advanced tactics to bypass monitoring tools and avoid detection.

These groups are reportedly exploiting design limitations in how EDR products log and track activity, particularly in virtualised environments.

The campaigns target government, telecom, and critical infrastructure organisations.

As adversaries grow more adept at evading automated defences, the incident underscores the need for enhanced telemetry, behavioural analysis, and closer scrutiny of endpoint blind spots.

CyberSecurity Advisors Network

NEWS:

20. Aviation sector faces heightened cyber risks due to vulnerable software, aging tech

Original Source: Cybersecurity Dive by David Jones

The aviation sector is facing growing cybersecurity challenges driven by legacy systems, outdated software, and fragmented digital infrastructure.

Experts warn that flight operations, maintenance systems, and passenger data platforms are increasingly vulnerable to exploitation.

Recent incidents and red-team assessments reveal how attackers could disrupt critical operations or gain access to sensitive data through overlooked vectors.

The sector's slow pace of digital modernisation, combined with increasing connectivity, makes it a prime target for both criminal and nation-state actors seeking high-impact outcomes.

CyberSecurity Advisors Network

NEWS:

21. Phishing Campaigns Use Real-Time Checks to Validate Victim Emails Before Credential Theft

Original Source: The Hacker News by Ravie Lakshmanan

A new wave of phishing campaigns is using real-time email validation to confirm whether a target address is active before launching credential theft attacks.

The technique involves embedding scripts that ping the email provider for verification, improving attacker efficiency and helping bypass spam filters.

Once validated, victims are redirected to tailored phishing pages that mimic trusted login portals.

This tactic marks a shift toward more calculated, adaptive phishing operations and highlights the urgent need for stronger email authentication, layered defences, and user awareness training.

CyberSecurity Advisors Network

NEWS:

22. SSL/TLS certificate lifespans reduced to 47 days by 2029

Original Source: BleepingComputer by Bill Toulas

A new wave of phishing campaigns is using real-time email validation to confirm whether a target address is active before launching credential theft attacks.

The technique involves embedding scripts that ping the email provider for verification, improving attacker efficiency and helping bypass spam filters. Once validated, victims are redirected to tailored phishing pages that mimic trusted login portals.

This marks a shift toward more calculated, adaptive phishing operations. The added precision allows attackers to focus resources on live targets and increases the likelihood of successful compromise with less noise.

CyberSecurity Advisors Network

NEWS:

23. Malicious NPM Packages Target PAYPAL Users

Original Source: Security Affairs Pierluigi Paganini

Browser vendors including Google, Mozilla, and Apple plan to reduce the maximum validity of SSL/TLS certificates to 90 days by 2024, with a longer-term goal of just 47 days by 2029.

The shift aims to improve security by limiting the window of exposure in case of certificate compromise or mis-issuance.

While automation via ACME protocols will ease renewal burdens, the change may strain organisations relying on manual processes.

Shorter lifespans also push the industry toward more agile, machine-driven trust models. Experts suggest the move will require widespread operational changes in both infrastructure and compliance strategies.

CyberSecurity Advisors Network

NEWS:

24. Risks to children playing Roblox ‘deeply disturbing’, say researchers

Original Source: The Guardian by Libby Brooks & Jedidajah Otte

A new study has found that children using the gaming platform Roblox are being exposed to grooming, harassment, and disturbing content via in-game chat and social features.

Researchers warn that moderation is inconsistent and easy to bypass, creating an environment where predatory behaviour can flourish undetected.

Despite Roblox’s popularity among younger audiences, the platform’s safety mechanisms are struggling to keep pace with evolving threats.

The report urges urgent intervention by regulators and calls for stronger accountability in child-facing digital spaces to protect young users from online harm.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

CyAN

NEWS:

25. Fortinet Zero-Day Bug May Lead to Arbitrary Code Execution (Dark Reading by Kristina Beek); Over 14K Fortinet devices compromised via new attack method (Cybersecurity Dive by Rob Wright) & Fortinet Warns Attackers Retain FortiGate Access Post-Patching via SSL-VPN Symlink Exploit (The Hacker News by Ravie Lakshmanan)

A critical zero-day vulnerability (CVE-2024-21762) in Fortinet's FortiOS SSL-VPN has led to the compromise of more than 14,000 devices, with attackers maintaining access even after patches are applied.

The flaw, actively exploited in the wild, enables remote code execution and is part of a broader campaign exploiting symlink techniques to bypass remediation efforts.

Fortinet's warning that systems remain compromised post-update underscores the growing sophistication of persistence methods.

The incident also raises urgent concerns around patch efficacy, vendor communication, and the need for deeper post-incident validation to ensure environments are truly clean.

CyberSecurity Advisors Network

NEWS:

26. Hertz confirms exposure in file transfer platform incident

Original Source: itNews

Hertz has confirmed that a breach of a third-party file transfer platform led to the unauthorised exposure of sensitive customer and employee data.

The incident, part of a broader wave of supply chain vulnerabilities, affected files containing names, contact details, and possibly financial information.

Regulators have been notified and impacted individuals are being contacted.

Hertz says it has strengthened security measures, but the breach underscores how widely-used data exchange tools remain high-risk targets.

It also illustrates the ongoing challenge of enforcing secure practices across increasingly outsourced digital infrastructure.

CyberSecurity Advisors Network

NEWS:

27. NIST Updates Privacy Framework, Tying It to Recent Cybersecurity Guidelines

Original Source: NIST

NIST has released an update to its Privacy Framework, aligning it with Cybersecurity Framework 2.0 to promote integrated, risk-based approaches to privacy and data protection.

The revision includes clearer guidance on data minimisation, cross-border data flow management, and accountability measures, helping organisations strengthen governance across evolving regulatory environments.

New mappings to international standards aim to support interoperability for global operations. The update reinforces the message that privacy and security cannot operate in silos—they are foundational, co-dependent pillars of digital trust.

CyberSecurity Advisors Network

NEWS:

28. China accuses US of launching 'advanced' cyberattacks

Original Source: itNews by Laurie Chen

China has publicly accused the United States of conducting advanced cyberattacks against Chinese institutions, claiming that American agencies exploited zero-day vulnerabilities and leveraged anonymising tools to avoid attribution.

The allegations were presented in a report by China's National Computer Virus Emergency Response Center and appear to be part of a broader geopolitical strategy to counter U.S. criticism of Chinese hacking activity.

The report coincides with rising tensions and mirrors tactics often used by Western governments. It also signals a continued escalation in the blame game over state-sponsored cyber operations.

CyberSecurity Advisors Network

NEWS:

29. Invasion’ barges, subsea cable cutters and surprise naval drills: how China is testing Donald Trump

Original Source: The Guardian by Angela Dewan

China is escalating its grey-zone tactics by deploying civilian vessels equipped to damage subsea internet cables—vital infrastructure responsible for carrying more than 95% of the world’s digital traffic.

These provocations, alongside naval drills and surveillance incursions, appear carefully timed to test U.S. responses under shifting political conditions.

Disrupting these cables could have catastrophic consequences for finance, defence, and emergency coordination. As cyber-physical threats rise, securing digital infrastructure beneath the sea must become a global security priority, not an afterthought.

CyberSecurity Advisors Network

NEWS:

30. Trump crackdown on immigrants aided by largest US private prison operator: Report

Original Source: Middle East Eye

Surveillance technology is playing an increasingly central role in the detention and deportation of both legal and undocumented immigrants in the U.S., with private contractors and data platforms deeply embedded in enforcement workflows.

A new report spotlights how CoreCivic, the nation’s largest private prison operator, profits not only from physical detention but also from digital tracking and biometric monitoring tools.

The findings raise urgent questions about transparency, digital rights, and the ethics of outsourcing surveillance infrastructure to corporations with vested political ties.

CyberSecurity Advisors Network

CyAN Members Only

Are You In the #CyANQuiz?

Hey CyAN Champions,

Have you got what it takes to outsmart your fellow cybersecurity pros?

You've got one more day (till April 18th) to put your skills to the test in our Quarterly #CyANQuiz Challenge!

- 30 Questions. Timed. No second chances.
- Based on Recent Cybersecurity News & Events – Watch out for recent news and Cybersecurity events.

📅 **Check your email on March 31st for the quiz link**; just click, answer, and climb the leaderboard!
💡 Why Play? Compete, have fun, and win awesome prizes (while proving your cybersecurity dominance!

Join the fun—this isn't just a quiz, it's a year-long challenge to **shine in the CyAN community!**

Think you can take the cyber crown? Prove it!

NEWS:

31. ResolverRAT Campaign Targets Healthcare, Pharma via Phishing and DLL Side-Loading

Original Source: The Hacker News by Ravie Lakshmanan

A recent campaign deploying ResolverRAT is targeting healthcare and pharmaceutical organisations using spear-phishing emails and DLL side-loading to deliver remote access trojans.

The malware allows attackers to exfiltrate sensitive data, capture screenshots, and execute commands remotely. By abusing legitimate software to disguise payloads, the campaign increases its chances of bypassing detection.

Security researchers warn that the threat actor appears highly focused on sectors holding valuable medical and intellectual property. The incident highlights the persistent vulnerability of healthcare to sophisticated, data-driven cyber espionage.

CyberSecurity Advisors Network

NEWS:

32. The Most Dangerous Hackers You've Never Heard Of

Original Source: WIRED

A mysterious group known as "Unknown Storm" is gaining notoriety among researchers as one of the most capable yet least publicised threat actors in cyberspace.

Linked to high-impact espionage targeting governments, defence contractors, and infrastructure, they use custom malware and stealthy attack paths to evade detection.

Uninterested in publicity or ransomware headlines, they prioritise quiet infiltration and operational secrecy. Their low profile is deliberate, making attribution difficult and allowing long-term access to sensitive systems without triggering alarms or media attention.

CyberSecurity Advisors Network

NEWS:

33. Hacktivism resurges – but don't be fooled, it's often state-backed goons in masks

Original Source: The Register by Jessica Lyons

While recent headlines suggest a resurgence of grassroots hacktivism, security experts warn that many of these campaigns are covertly orchestrated by state-sponsored actors.

Groups claiming to act in the name of political causes are often proxies used by governments to launch disruptive operations while maintaining plausible deniability.

Targets have included critical infrastructure, media outlets, and government agencies. This blending of activism and espionage muddies attribution and response strategies.

Analysts stress the importance of distinguishing genuine protest from manipulation disguised as cyber civil disobedience.

CyberSecurity Advisors Network

NEWS:

34. AI-hallucinated code dependencies become new supply chain risk

Original Source: BleepingComputer by Bill Toulas

Security researchers are warning that AI-generated code is introducing fictitious software dependencies into projects—posing a novel threat to the software supply chain.

These "hallucinated" packages, suggested by chatbots or coding assistants, often don’t exist or are later created by malicious actors to exploit unsuspecting developers.

Attackers can publish rogue packages under the invented names, delivering malware through what appears to be legitimate code. This risk highlights the need for careful dependency management, human review of AI-generated code, and improved safeguards in development environments.

CyberSecurity Advisors Network

NEWS:

35. Microsoft total recalls Recall totally to Copilot+ PCs

Original Source: The Register by Iain Thomson

Microsoft has pulled its controversial “Recall” feature from general release amid backlash over privacy and security concerns.

Recall, designed for Copilot+ PCs, automatically captured snapshots of user activity to create a searchable timeline—sparking fears of misuse, surveillance, and data exposure.

Critics argued that storing sensitive information locally without clear safeguards introduced unnecessary risk.

Microsoft now says Recall will ship in preview only to Windows Insiders, and with new security measures enabled by default.

The reversal reflects growing pushback against invasive-by-design AI features lacking robust consent and control mechanisms.

CyberSecurity Advisors Network

NEWS:

36. Laboratory Services Cooperative Data Breach Impacts 1.6 Million People

Original Source: Security Affairs Pierluigi Paganini

Laboratory Services Cooperative, a U.S.-based medical lab, has disclosed a data breach affecting approximately 1.6 million individuals.

The incident, traced to a third-party file transfer tool vulnerability, exposed names, Social Security numbers, health data, and insurance information.

The breach underscores ongoing risks tied to insecure third-party systems in healthcare, where sensitive data flows between multiple vendors.

Regulators have been notified, and affected individuals are being contacted. The event highlights the need for stronger contractual controls, continuous vendor assessments, and rapid patch management in high-risk sectors.

CyberSecurity Advisors Network

NEWS:

37. Paper Werewolf Threat Actor Targets Flash Drives With New Malware

Original Source: Dark Reading by Kristina Beek

A newly identified threat actor dubbed "Paper Werewolf" is deploying malware that spreads via infected USB flash drives, targeting air-gapped and offline systems.

The malware uses autorun scripts and malicious executables disguised as legitimate files to gain access, execute payloads, and exfiltrate data once reconnected to the internet.

The campaign appears to focus on espionage rather than financial gain, raising concerns about physical vector attacks in secure environments.

Experts warn that the resurgence of USB-based threats highlights the need for stronger endpoint controls and offline system hygiene.

CyberSecurity Advisors Network

NEWS:

38. Legal Defense Fund exits Meta civil rights advisory group over DEI changes

Original Source: The Guardian by Adria R Walker

The US NAACP Legal Defense Fund has exited Meta's civil rights advisory group, citing the company's dismantling of diversity, equity, and inclusion initiatives.

Meta's recent rollback of DEI programs, fact-checking teams, and moderation policies—reportedly in anticipation of a second Trump term—sparked concern that the platform is abandoning its civil rights commitments.

The Legal Defense Fund warned that these changes could lead to increased harassment, discrimination, and self-censorship.

The departure signals growing tension between civil rights organisations and major tech platforms over accountability.

CyberSecurity Advisors Network

NEWS:

39. Financial Fraud, With a Third-Party Twist, Dominates Cyber Claims

Original Source: Dark Reading by Robert Lemos

New analysis reveals that third-party-related financial fraud now dominates cyber insurance claims, with compromised vendors and service providers emerging as prime points of failure.

The data highlights how attackers exploit weak links in business ecosystems to access financial systems and steal funds.

Claims linked to business email compromise and vendor impersonation are rising sharply, outpacing ransomware in volume.

Insurers are urging companies to tighten third-party risk management and implement more stringent controls over financial authorisations and payment workflows to prevent escalating losses.

CyberSecurity Advisors Network

NEWS:

40. Western Sydney University discloses security breaches, data leak

Original Source: BleepingComputer by Bill Toulas

Western Sydney University has revealed a series of security breaches that exposed personal data, including student and staff information.

The incidents involved unauthorised access via compromised Microsoft 365 accounts over several months, with attackers exfiltrating documents, emails, and identity records.

The university is working with cybersecurity experts and law enforcement, and affected individuals have been notified.

The case highlights the continued targeting of academic institutions and the risks posed by credential-based attacks. It also underscores the need for stronger identity protections in cloud environments.

CyberSecurity Advisors Network

NEWS:

41. Cybersecurity industry silent as Trump turns on SentinelOne

Original Source: InnovationAus by Raphael Satter

Donald Trump has publicly criticised SentinelOne, claiming the cybersecurity firm is part of a so-called “deep state” plot—without offering evidence.

Despite the seriousness of the allegation, the broader cybersecurity industry has remained notably quiet, prompting concern over the chilling effect such rhetoric can have on public trust in cyber professionals.

Analysts warn that politicising cybersecurity firms may endanger efforts to maintain bipartisan cooperation on national defence. The silence also reflects growing unease over how to respond when private companies are dragged into political crossfire.

CyberSecurity Advisors Network

NEWS:

42. China Admitted to Volt Typhoon Cyberattacks on US Critical Infrastructure: Report

Original Source: SecurityWeek by Eduard Kovacs

A leaked U.S. intelligence report suggests that China has privately acknowledged its role in the Volt Typhoon cyber campaign targeting American critical infrastructure.

The group, linked to China's military, reportedly gained long-term access to systems controlling power, water, and transportation.

While Beijing has publicly denied involvement, internal admissions reflect growing confidence in cyber-enabled influence operations.

The disclosure raises concerns over escalation risks and the fragility of essential services. It also highlights the urgency of bolstering critical infrastructure defences against persistent, state-sponsored intrusions.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

CyAN

ANALYSIS:

43. DOGE's tech takeover threatens the safety and stability of our critical data

Original Source: MIT Technology Review

Elon Musk's Department of Government Efficiency (DOGE) is reportedly gaining behind-the-scenes control of major U.S. government IT systems, raising urgent cybersecurity concerns.

Whistleblowers allege unqualified personnel are accessing sensitive infrastructure like Medicare, Social Security, and energy networks.

Lawmakers warn that DOGE's unchecked influence could introduce serious vulnerabilities and reduce transparency. Its use of AI to process government data further complicates oversight.

Critics fear the quiet restructuring of public services without democratic accountability may pose long-term national security risks.

CyberSecurity Advisors Network

ANALYSIS:

44. Are We Prioritizing the Wrong Security Metrics?

Original Source: Dark Reading by Swati Babbar

Security teams are tracking the wrong things, according to growing criticism of how success is measured in cybersecurity.

Standard metrics like incident counts or mean time to detect may look good in boardroom slides but reveal little about actual risk.

Experts advocate for outcome-driven metrics—those that gauge business impact, resilience, and user trust; noting that measuring how quickly operations recover or whether controls reduce real-world harm offers more meaningful insight.

The shift demands closer collaboration between security leaders and executives to align protection efforts with long-term strategic goals.

CyberSecurity Advisors Network

Cybersecurity Advisors Network

CyAN

ANALYSIS:

45. Businesses bleed $100m a year due to cybersecurity failures, study shows

Original Source: IBS Intelligence baby Gloria Methri

A new report reveals that poor cybersecurity practices are costing businesses an average of $100 million annually, with data breaches, system outages, and regulatory fines among the top contributors.

The research highlights widespread underinvestment in preventive controls, inconsistent incident response capabilities, and a lack of board-level engagement.

Analysts warn that as threats become more sophisticated, reactive spending will only widen the damage.

The findings point to an urgent need for proactive strategies, continuous risk assessment, and stronger alignment between cybersecurity and core business objectives.

CyberSecurity Advisors Network

ANALYSIS:

46. Cybersecurity in the AI Era: Evolve Faster Than the Threats or Get Left Behind

Original Source: The Hacker News

A new report reveals that poor cybersecurity practices are costing businesses an average of $100 million annually, with data breaches, system outages, and regulatory fines among the top contributors.

The research highlights widespread underinvestment in preventive controls, inconsistent incident response capabilities, and a lack of board-level engagement.

Analysts warn that as threats become more sophisticated, reactive spending will only widen the damage. The findings point to an urgent need for proactive strategies, continuous risk assessment, and stronger alignment between cybersecurity and core business objectives.

CyberSecurity Advisors Network

ANALYSIS:

47. 5 warning signs that your phone's been hacked - and how to fight back

Original Source: ZDNet by Lance Whitney

From sudden battery drain to unusual pop-ups, several common red flags may indicate that your phone has been compromised.

This guide outlines five key symptoms of a potential mobile breach, including performance lags, unexpected data usage, and unfamiliar apps.

It also offers clear, actionable steps for users to regain control—such as checking app permissions, enabling multi-factor authentication, and performing factory resets.

As mobile threats grow more sophisticated, staying alert to subtle behavioural changes is essential. Prevention still starts with awareness and regular security hygiene.

CyberSecurity Advisors Network

ANALYSIS:

48. AI-Driven Disinformation Campaigns: The Digital Fog of War - The Weaponization of AI in Cyber Warfare – Part 3

Original Source: PrivID (Substack)

The third instalment in PrivID's cyber warfare series examines how generative AI is transforming disinformation into a low-cost, high-impact weapon.

From deepfake videos to auto-generated propaganda, AI enables faster, more convincing psychological operations that blur truth and fiction.

State and non-state actors alike can now manipulate narratives at scale, targeting public opinion and destabilising trust.

This article warns that democracies must invest in detection, media literacy, and policy coordination to counter this evolving threat. Left unchecked, AI-fuelled disinformation could outpace our ability to discern reality.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

CyAN CyAN Members Op Eds, Articles, etc

49. No Time for Antics with Semantics: Why CVEs Are Cybersecurity's Lifeline

Original Source: CyAN Global VP Kim Chandler McDonald

In her latest article, Kim underscores the critical role of the (CVE) Common Vulnerabilities and Exposures system in global cybersecurity, likening it to ISBN numbers for vulnerabilities.

The CVE program provides a standardised language that enables swift, coordinated responses to security threats.

This week's funding crisis nearly jeopardised this system, revealing its fragile dependence on U.S. government support.

Kim advocates for a globally sustained model to ensure long-term resilience. Without a stable CVE backbone, we risk a fragmented, slower response to threats in an already overburdened ecosystem.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

CyAN CyAN Members
Op Eds, Articles, etc

50. Vulnerability Scanning Essentials: What Every Cyber Beginner Must Try

Original Source: CyAN General Secretary Fel Gayanilo

In this beginner-friendly guide to vulnerability scanning, Fel shares a clear explanation as to what it is, how it works, and why it matters for anyone entering the cybersecurity field.

From choosing the right tools to interpreting scan results, Fel walks readers through the practical steps needed to identify and address system weaknesses before attackers can exploit them.

With his trademark clarity and no-fuss tone, he demystifies the process and encourages learners to treat scanning as a foundational part of good cyber hygiene.

It’s a must-read starting point for building both confidence and competence.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

CyAN CyAN Members Op Eds, Articles, etc

51. “What happens to Heroes?” EPISODE #4: The Unsung Heroes of the digital world

By CyAN member Didier Annet

In this deeply personal episode, Didier Annet spotlights the unseen labour of cybersecurity defenders who shoulder the emotional burden of protecting digital spaces, often without recognition or support.

Through thoughtful reflection and real-world stories, Didier unpacks the moral weight of being the person relied on to stay calm during chaos—and the personal cost that comes with that role.

This is a call to humanise the profession, acknowledge burnout, and start building cultures that value care as much as competence.

These aren’t just technical experts—they’re the steady hands holding the digital world together.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

CyAN CyAN Members
Op Eds, Articles, etc

52. Information Gathering Tools Explained: From Nmap to Maltego

Original Source: CyAN General Secretary Fel Gayanilo

What looks like curiosity is often the first step in digital defence. In this smart and accessible guide, Fel introduces beginners to key reconnaissance tools like Nmap

and Maltego, showing how they help map networks, uncover relationships, and identify potential weak points.

Fel explains how these tools fit into ethical hacking workflows, highlighting the importance of using them responsibly and legally.

It's a solid primer for understanding where good security starts—by knowing what's visible, what's exposed, and what that visibility reveals.

True security begins with seeing clearly.

CyberSecurity Advisors Network

CyAN Cybersecurity Advisors Network

STATISTICS & INSIGHTS powered by evisec

Highlights from this week's cybersecurity research by evisec - CRD #20

Original Source: CyAN Member and evisec CEO Henry Röigas

Highlights from the latest cybersecurity research sources by evisec:

- The UK Cyber Security Breaches Survey 2025 shows 40% of businesses reported incidents—down from 50%—but board-level prioritisation of cybersecurity has dropped sharply.
- Ransomware insurance claims in the U.S. are back to 2021 levels, with remote access exploited in 80% of successful attacks.
- Analysis of over 46 million devices reveals widespread exploitation of long-known, unpatched vulnerabilities.
- AI is now supercharging phishing attacks by generating convincing messages using stolen personal details.

For more insights, explore the latest Cybersecurity Research Digest.

CyberSecurity Advisors Network

Online Safety for Kids and Teens

Highlights from the latest Vys ‘Online Safety for Kids and Teens’ Biweekly Brief

By CyAN Member and Vyanams Strategies Founder Vaishnavi J

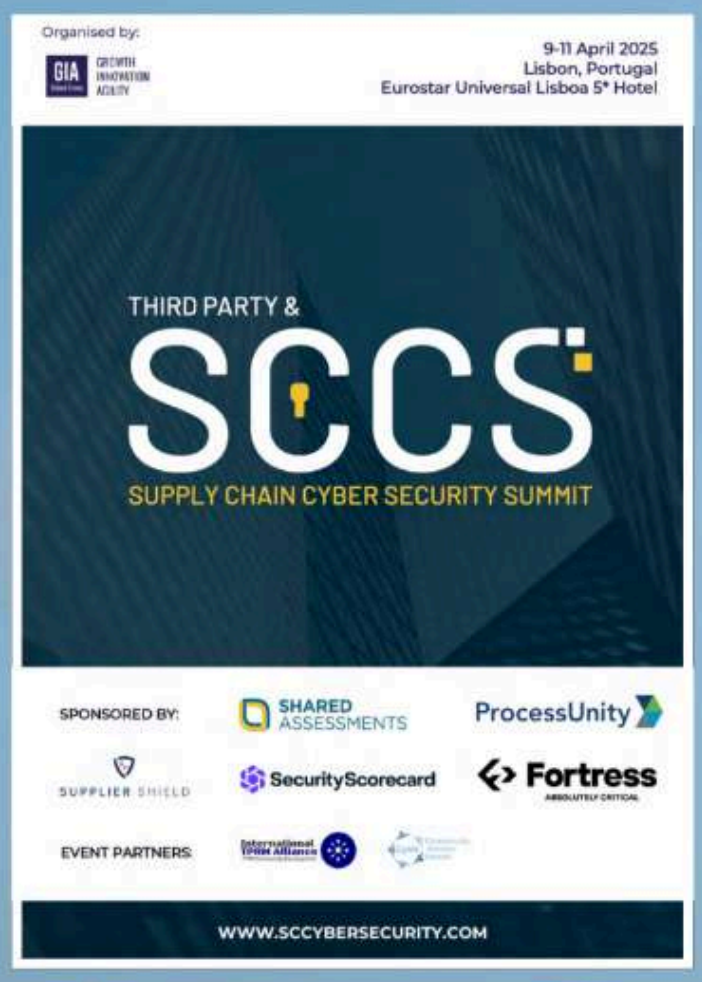
- **A New Jersey teen successfully pushed for legislation criminalising the use of nudify apps, with fines reaching $30,000.** The law sets a powerful precedent for youth-led advocacy against tech-enabled gender-based violence.
- **The EU's CPC Network is cracking down on child safety failures, launching an enforcement action against Star Stable Entertainment.** The move signals a growing willingness to hold gaming companies accountable for age-appropriate design and moderation lapses.
- **Rates of online-facilitated child sexual abuse continue to rise, fuelled by immersive platforms and weak industry safeguards.** Experts are calling for stronger baseline protections across VR, gaming, and messaging environments, where predators often operate unchecked.
- **+ much, much more!**

CyberSecurity Advisors Network

CyAN Member's News:

CyAN thrives because of the incredible talent, leadership, and dedication of our members, and we are proud to see them shaping the future of cybersecurity on a global stage! 🚀💙

Cyan Board Member Bharat Raigangar has been particularly busy recently! April 9th - 11th found him in Lisbon speaking at the Third Party and Supply Chain Cyber Security Summit (SCCS) and this week...



...while in NYC he was able to catch up with fellow CyAN members Vaishnavi J and Gilles Chevillon!

CyAN Member's News:

Congratulations to CyAN member Fatema Fardan, who has spent the past six months as a mentor with the QODWA program, initiated by the CFA Society Bahrain!

Fatema's contribution to the next generation of cybersecurity and finance professionals reflects the heart of what makes our community so special—sharing knowledge, lifting others, and leading by example!

And congrats to CyAN member Will Rivera for representing MyOwn Image at two standout events on public service and responsible tech.

On March 27, Will spoke at Hartwick College's Gender & Public Service event, honouring Judith "Judy" Day's legacy. Then on April 5, he joined All Tech Is Human and NYIT to spotlight MyOwn Image's advocacy against tech-facilitated violence. From campus panels to national policy—Will is leading with purpose!

UPCOMING CyAN and CyAN Partner EVENTS:

- **GITEX ASIA, Singapore (Marina Bay Sands: 23-25 April https://gitexasia.com/**
- **GISEC Global, Dubai World Trade Centre: 6-8 May https://gisec.ae/home**
- **The Cyber Outstanding Security Performance Awards (Cyber OSPAs), London, UK: 8 May https://www.thecyberospas.com/about/**
- **CSG Awards 2025, Dubai: 7 May https://csgawards.com/**
- **World AI Technology Expo, Dubai: 14-15 May https://worldaiexpo.i**
- **CyAN 10th Anniversary Celebrations!**
- **GITEX Europe Messe, Berlin: 21-23 May https://www.gitex-europe.com/**
- **MaTeCC, Rabat, Morocco: 7-9 June https://tinyurl.com/mtecz8vw**
- **CyAN Q2 Community Call (APAC and the Gulf), June 11: 12:00 GST / 16:00 SGT / 18:00 AEST**
- **CyAN Q2 Community Call (EMEA and the Americas), June 11: 20:00 GST / 18:00 CET / 17:00 UTC / 12:00 EDT**

CyAN Cybersecurity Advisors Network

Catch up on Past Issues:

Missed an issue of (In)Securities? No worries! Scan the QR code to explore our archive of past editions—packed with insights, trends, and actionable tips to keep you ahead in the ever-evolving world of cybersecurity. Dive in and catch up today!

CyberSecurity Advisors Network

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

#ReallyInterestingCyberStuff!
#SharingIsCaring