GLOBAL NEXT CONSULTING INDIA PRIVATE LIMITED

GNCIPL

(Leader In Consulting)

www.gncipl.com|www.gncipl.online

Cybersecurity Daily News Analysis(C-DNA) Across the Globe

21 May 2025

Starlink and Resecurity Form Cybersecurity Alliance

At GISEC Global 2025 in Dubai, Resecurity and Starlink announced a strategic partnership to enhance satellite communications security. This collaboration aims to bolster global cybersecurity infrastructure, particularly in space-based networks. Yahoo Finance

---

SANS Institute Releases 2025 Cyber Threat Intelligence Survey

The SANS Institute is presenting its annual Cyber Threat Intelligence (CTI) Survey findings today at 10:30 AM EDT (8:00 PM IST). The survey highlights top use cases and key trends in threat intelligence, providing valuable insights for cybersecurity professionals. GlobeNewswire

---

From Sharpshooter to Cybersecurity Expert: Shahana Fatima's Journey

Shahana Fatima, a former ace shooter from Nagpur, has transitioned into cybersecurity. After earning a master's degree in cyber forensics from the Illinois Institute of Technology, she chose to work in India's cyber defense sector over lucrative U.S. offers. Recently, she was the only Indian selected for a project to build cybersecurity infrastructure in Kosovo. The Times of India+1Australian Cyber Security Magazine+1

TIER IV Partners with PlaxidityX for Autonomous Bus Cybersecurity

Japanese autonomous vehicle company TIER IV has selected PlaxidityX to provide cybersecurity expertise for its airport autonomous bus project. The partnership focuses on aligning vehicle

software with UN-R155 cybersecurity regulations. BleepingComputer+3The Manila Times+3Laotian Times+3Laotian Times+1The Manila Times+1

🧠 SecurityWeek Hosts 2025 Threat Detection & Incident Response Summit

SecurityWeek is hosting its virtual Threat Detection & Incident Response (TDIR) Summit today from 11:00 AM to 4:00 PM ET (8:30 PM to 1:30 AM IST). The event features global cybersecurity leaders discussing advanced threats and incident response strategies. SecurityWeek+1SecurityWeek+1

🔍 Hazy Hawk Exploits DNS Vulnerabilities for Malware Distribution

A threat actor known as Hazy Hawk has been hijacking abandoned cloud resources by exploiting DNS misconfigurations. Targets include high-profile organizations like the U.S. CDC, Deloitte, and PwC, with the hijacked domains used to distribute malware. The Hacker News+1Cyware Labs+1

🧩 Malicious Chrome Extensions Steal Credentials and Inject Ads

Researchers have identified over 100 fake Chrome extensions that hijack user sessions, steal credentials, and inject ads. These extensions masquerade as legitimate tools but contain malicious code for data exfiltration and remote command execution. The Hacker News

---

🧬 Skitnet Malware Used by Ransomware Gangs for Data Theft

Ransomware groups are deploying Skitnet malware to steal sensitive data and establish remote control over compromised systems. Skitnet has been available on underground forums since April 2024 and is now part of sophisticated post-exploitation tactics. The Hacker News

---

👨‍🎓 Massachusetts Student Pleads Guilty to PowerSchool Cyberattack

A 19-year-old college student from Worcester, Massachusetts, has pleaded guilty to a cyberattack on PowerSchool, a widely used educational platform. The attack involved extorting millions of dollars in exchange for not leaking personal data of students and teachers. BleepingComputer+1Cybernews+1

📶 Cellcom Confirms Cyberattack Behind Service Outages

Wisconsin-based mobile carrier Cellcom has confirmed that a cyberattack caused widespread service outages beginning May 14. The company is working to restore services and investigate the breach. BleepingComputer

🧠 AI-Driven Fraud Escalates in Financial Sector

The FS-ISAC's "Navigating Cyber 2025" report highlights a surge in fraud and scams facilitated by generative AI. Threat actors are increasingly targeting supply chains and exploiting geopolitical uncertainties, necessitating enhanced cross-border collaboration and proactive intelligence sharing to safeguard the global financial system. Cyber Security Asean+1@EconomicTimes+1

🛡️ India's Cybersecurity Preparedness Lags

According to Cisco's 2025 Cybersecurity Readiness Index, only 7% of Indian organizations are adequately prepared to defend against modern cyber threats, particularly those driven by artificial intelligence. This low level of preparedness underscores a significant vulnerability in India's cybersecurity landscape amid a rising tide of sophisticated AI-powered cyberattacks. @EconomicTimes

---

🏢 Digital Real Estate Faces Cybersecurity Challenges

As the real estate industry undergoes digital transformation, it faces increasing cybersecurity challenges. The integration of advanced technologies requires meticulous planning to navigate potential cyber threats effectively. Daily Journal

---

👩 BT Initiatives to Increase Female Representation in Cybersecurity

British Telecom (BT) is actively working to increase female participation in the cybersecurity sector. By supporting educational programs and providing career opportunities, BT aims to address the gender gap in the cybersecurity workforce. Australian Cyber Security Magazine

---

🧬 Decent Cybersecurity Showcases Post-Quantum Solutions

Slovak firm Decent Cybersecurity is set to present its post-quantum cryptographic solutions at DSEI Japan 2025. As the only Slovak cybersecurity company at the event, Decent aims to

highlight advancements in securing communications against future quantum computing threats. Business Wire

---

🏛️ Uttar Pradesh Launches AI Pragya Training

The Uttar Pradesh government has initiated the AI Pragya program to train 1 million citizens, including government employees, in artificial intelligence, machine learning, data analytics, and cybersecurity. The initiative aims to enhance digital skills and contribute to the state's economic growth. The Times of India

---

🧑🏫 UCSF Enforces Mandatory Cybersecurity Training

The University of California, San Francisco (UCSF) has mandated annual cybersecurity training for all faculty and staff. Starting May 21, 2025, access to critical systems will be restricted for individuals who have not completed the required training, emphasizing the importance of cybersecurity awareness in academic institutions. Office of the Chancellor

---

🛡️ Microsoft Addresses Actively Exploited Zero-Day Vulnerabilities

In its May 2025 Patch Tuesday update, Microsoft fixed 78 security flaws, including five zero-day vulnerabilities that were actively exploited. The company urges users to apply the updates promptly to protect against potential threats. The Hacker News

---

🐍 Chinese Hackers Deploy MarsSnake Backdoor

A China-aligned threat actor, dubbed UnsolicitedBooker, has been identified deploying a previously undocumented backdoor named MarsSnake in a multi-year cyber-espionage campaign targeting a Saudi organization. The attack underscores the persistent and evolving nature of state-sponsored cyber threats. The Hacker News