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

Tuesday, May 20, 2025

- ✓ **Skitnet Malware Powers Ransomware Campaigns**
- ✓ **A new malware strain named *Skitnet* is being deployed by ransomware groups to exfiltrate sensitive data and establish remote access on compromised systems. First observed in April 2024, Skitnet is now a key post-exploitation tool in underground cybercriminal forums. The Hacker News**
- ✓ **Critical WordPress Plugin Vulnerability**
- ✓ **A severe flaw (CVE-2025-4389) in the Crawlomatic WordPress plugin allows unauthenticated attackers to upload arbitrary files, potentially leading to remote code execution. Thousands of sites are at risk, underscoring the importance of timely patching. Cyware Labs**
- ✓ **O2 UK Location Leak**
- ✓ **A vulnerability in O2 UK's implementation of VoLTE and WiFi Calling services exposed sensitive user metadata, including location, IMSI, and IMEI, through overly verbose SIP headers. Cyware Labs+1SecurityWeek+1**
- ✓ ---
- ✓ 🧠 **Strategic & Policy Developments**
- ✓ **Biden Administration's Sweeping Cybersecurity Executive Order**
- ✓ **The U.S. government has issued a comprehensive executive order mandating 52 actions across federal agencies to bolster cyber defenses. This includes new plans to address spiraling cyber threats and enhance national cybersecurity posture. CSO Online**
- ✓ **Salt Typhoon Campaign Exposes Telecom Vulnerabilities**
- ✓ **The Salt Typhoon cyberattack campaign has been described as one of the most consequential against the U.S., exploiting vulnerabilities in the telecommunications**

sector and highlighting the need for improved coordination between federal agencies and industry. CyberScoop+2Cybersecurity Dive+2Cybersecurity Dive+2

- ✓ ---
- ✓ 🧪 **Innovations & Tools**
- ✓ **Google Unveils Sec-Gemini v1 for Cybersecurity**
- ✓ **Google has introduced *Sec-Gemini v1*, an experimental AI model designed to revolutionize cybersecurity by enhancing threat detection and response capabilities. Cyber Security News**
- ✓ **GPOHound: New Tool for Active Directory Analysis**
- ✓ **The open-source tool *GPOHound* has been released to analyze Group Policy Objects in Active Directory environments, helping identify potential privilege escalation paths and strengthen internal security. Cyber Security News**
- ✓ ---
- ✓ 📈 **Industry & Market Trends**
- ✓ **Cybersecurity Stocks to Watch Amid Earnings Reports**
- ✓ **Investors are eyeing cybersecurity firms like Palo Alto Networks, Zscaler, CrowdStrike, Check Point, and CyberArk as they prepare to release earnings reports and 2025 guidance, indicating potential shifts in the cybersecurity market landscape. Investor's Business Daily**
- ✓ 🧠 **AI & Cybersecurity: Emerging Concerns**
- ✓ **AI Surpasses Ransomware as Top Security Concern**
- ✓ **According to Arctic Wolf's 2025 Trends Report, artificial intelligence has overtaken ransomware as the primary concern for security and IT leaders. Organizations are grappling with the dual nature of AI—balancing its innovative potential against the risks it introduces .GlobeNewswire**
- ✓ **Hospitals Vulnerable to AI-Powered Intrusions**
- ✓ **A Black Book survey reveals that 82% of hospitals have not audited physical risks associated with deepfakes, synthetic IDs, and AI-enabled breaches, despite expressing confidence in their cybersecurity measures .Newswire**
- ✓ ---
- ✓ 🛡️ **Critical Vulnerabilities & Exploits**
- ✓ **SAP Zero-Day Exploited Weeks Before Disclosure**
- ✓ **Cybersecurity experts have identified that CVE-2025-31324, a critical zero-day vulnerability in SAP NetWeaver, was actively exploited nearly three weeks prior to its public disclosure. The flaw allows unauthenticated attackers to upload malicious files, leading to potential remote code execution .GBHackers**
- ✓ **Firefox Zero-Day Vulnerabilities Patched**

- ✓ **Mozilla has patched two critical zero-day vulnerabilities in Firefox that were exploited during the Pwn2Own Berlin competition. Hackers earned $100,000 in bounties for these discoveries .Medium+1Wikipedia+1**
- ✓ ---
- ✓ **IN India's Cybersecurity Readiness**
- ✓ **Only 7% of Indian Organizations Prepared for Cyber Threats**
- ✓ **Cisco's 2025 Cybersecurity Readiness Index indicates that merely 7% of organizations in India are well-prepared to face AI-driven cybersecurity threats. This highlights a significant vulnerability and underscores the urgent need for enhanced cybersecurity measures .@EconomicTimes**
- ✓ ---
- ✓ 🏛️ **Legal and Policy Developments**
- ✓ **Delta Air Lines Lawsuit Against CrowdStrike Proceeds**
- ✓ **A Georgia state judge has ruled that Delta Air Lines can proceed with most of its lawsuit against cybersecurity company CrowdStrike. The case pertains to a July 2024 computer outage, allegedly caused by a defective update to CrowdStrike's software, which led to the cancellation of 7,000 flights and significant financial losses for Delta .Reuters**
- ✓ **U.S. Congress Plans Cybersecurity Hearing in Silicon Valley**
- ✓ **The House Homeland Security Committee is organizing a field hearing on cybersecurity in Silicon Valley during the upcoming congressional recess. Scheduled at Stanford University, the hearing aims to address the state of U.S. cybersecurity and foster dialogue between government officials and key stakeholders in the technology sector .Axios**
- ✓ ---
- ✓ 🌐 **Industry Reports & Trends**
- ✓ **Global State of Security Report Highlights Operational Challenges**
- ✓ **Splunk's "State of Security 2025" report reveals that 46% of organizations spend more time maintaining tools than defending against threats. Additionally, only 11% fully trust AI for mission-critical tasks, emphasizing the need for connected security operations .Cisco Investor Relations+1Quantisnow+1**
- ✓ **Pentera's 2025 State of Pentesting Report Released**
- ✓ **Pentera's latest report indicates that while companies continue to invest in security measures, breaches remain widespread. The findings suggest a shift towards automated, ongoing penetration testing as a critical component of modern cyber resilience .World Economic Forum+1The Hacker News+1**
- ✓ ---

- ✓ 🚨 **Sector-Specific Alerts**
- ✓ **Travel Industry Faces Persistent Cybersecurity Challenges**
- ✓ **Rapid advances in travel technology are leading to more sophisticated cyberattacks. The travel sector must address these persistent cybersecurity problems to protect customer data and maintain trust .PhocusWire**
- ✓ **Shipping Industry Urged to Enhance Cybersecurity Measures**
- ✓ **Recent cyberattacks have exposed vulnerabilities in the shipping industry, prompting calls for immediate action to strengthen cybersecurity protocols and protect critical infrastructure .Splash247**