

Cybersecurity Weekly Digest



What's New

Apple Faces Zero-Day Exploit in Safari WebKit – CVE-2025-3469

Apple has released urgent security updates for iOS, iPadOS, and macOS after the discovery of a critical zero-day vulnerability tracked as CVE-2025-3469 in its WebKit engine. The flaw allows remote code execution through malicious web content, effectively letting attackers take control of vulnerable devices. According to researchers, the exploit has been actively used in targeted spyware campaigns, specifically aimed at journalists and human rights activists. The attack involves tricking victims into visiting compromised websites, delivering spyware without their knowledge. Apple confirmed the issue affects multiple devices and is already being exploited in the wild. This marks the third WebKit zero-day patched in 2025, indicating ongoing exploitation by advanced threat actors. The company has credited independent researchers for uncovering the flaw and acted swiftly with patches. Users are advised to immediately update to the latest OS versions and enable Lockdown Mode if at high risk. The situation underscores the importance of regular software updates and stronger browser engine defenses.

[🔗 Read the full report - The Hacker News – Apple Patches WebKit Zero-Day Used in Spyware Attacks \(3 min\).](#)

Europol Dismantles World's Largest Phishing-as-a-Service Platform – LabHost

In a major international sting, Europol and law enforcement from 19 countries have dismantled LabHost, a notorious phishing-as-a-service (PhaaS) platform. Since 2021, LabHost had empowered over 10,000 cybercriminals to create phishing pages impersonating global banks, telecom providers, and e-commerce platforms. The platform hosted more than 40,000 phishing sites, stealing credentials from tens of thousands of victims worldwide. Authorities revealed LabHost's premium tool, LabRat, enabled real-time credential harvesting, including two-factor authentication codes. During the takedown, 37 suspects were arrested and 70 properties raided, including the arrest of the platform's alleged creator. Investigators reported the service collected over 1 million passwords and 480,000 card numbers, monetizing stolen data and subscriptions worth over £1 million. UK police confirmed at least 70,000 local victims, highlighting the platform's widespread reach. Law enforcement also seized and shut down 207 servers, dealing a critical blow to the PhaaS ecosystem. Europol emphasized this operation as a model of global cooperation against cybercrime, targeting not just users, but the infrastructure that fuels mass phishing.

[🔗 Read the full report - Europol News – LabHost Phishing Platform Dismantled \(4 min\).](#)

North Korean Hackers Breach U.S. Health Sector, CISA Confirms

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has issued a formal advisory revealing that the North Korea-linked APT group "Kimsuky" has breached multiple U.S. healthcare and public health (HPH) organizations. The threat actors reportedly stole sensitive patient data and medical research intellectual property, posing a serious threat to national healthcare infrastructure. The attacks involved the use of custom malware loaders specifically designed to evade standard detection tools used in healthcare environments. To remain undetected, the group used DNS tunneling to disguise command-and-control (C2) traffic within normal network activity. According to the advisory, access was most likely gained via phishing emails, targeting personnel with lures tied to healthcare operations and research. Once inside, Kimsuky actors deployed backdoors and executed script-based malware to escalate privileges and extract sensitive information. CISA has urged all HPH organizations to review indicators of compromise (IOCs) and enhance email security protocols and monitoring capabilities. This campaign forms part of a broader trend in which state-sponsored groups target the health sector for both espionage and financial gain. The advisory serves as a warning that critical infrastructure remains highly vulnerable to nation-state cyber operations.

 **Read the full report** - [CISA Security Alert on Kimsuky Targeting Healthcare \(AA24-207A\) \(4 min\)](#)

Cloudflare Mitigates Record-Breaking HTTP/2 DDoS Attack Targeting Financial and Crypto Sectors

Cloudflare has disclosed details of a massive DDoS campaign that exploited a vulnerability in the HTTP/2 protocol, known as "Rapid Reset", to launch one of the largest denial-of-service attacks ever recorded. At its peak, the botnet reached over 250 million requests per second (RPS), targeting high-value sectors including financial institutions and cryptocurrency exchanges. The attackers abused HTTP/2's stream cancellation feature to rapidly open and reset thousands of streams, overwhelming server infrastructure. The botnet behind the attack was composed of roughly 20,000 compromised IoT devices, showing that scale can be achieved without traditional large botnets. Cloudflare, along with Google and AWS, confirmed they were all affected by the zero-day vulnerability, which has been tracked as CVE-2023-44487. The attack was mitigated with minimal impact, but the company warns that the attack vector is now publicly known, making future exploitation likely. Vendors have since patched the protocol-level flaw, and organizations are urged to apply updates and implement robust DDoS protection. Cloudflare highlighted the growing risk of application-layer attacks that abuse protocol features rather than sheer volume. This incident marks a turning point in DDoS evolution, leveraging software logic over bandwidth brute-force.

 **Read the full report** - [Cloudflare Blog – HTTP/2 Rapid Reset DDoS Attack \(2 min\)](#)

Microsoft AI Research Portal Leaks 38TB of Internal Data Due to Misconfigured Cloud Token

In a major cloud security lapse, researchers from Wiz discovered that Microsoft had accidentally exposed 38 terabytes of internal sensitive data through a publicly accessible GitHub repository used

by its AI research team. The leak was caused by an improperly configured Azure Shared Access Signature (SAS) token, which granted full control access to a cloud storage container intended only for open-source AI training data. Instead, it exposed disk backups containing passwords, secret keys, internal Teams messages, and credentials belonging to Microsoft employees. The token remained active for nearly three years, with no expiration and excessive permissions. Security experts warned that attackers could have modified or replaced AI model files using this access, especially due to the insecure use of pickle files in the repository. Microsoft was alerted in June 2023 and revoked the token immediately, confirming that no customer data was compromised. The company has since implemented tighter controls around SAS token usage and automated secret scanning in public code repositories. This incident highlights the growing risks associated with cloud misconfigurations and the importance of access control in AI model development and sharing.

 **Read the full report -** [Microsoft AI Team Accidentally Leaks 38TB \(5 min\)](#)

In-Depth Insights

AI-Generated Spam Emails Surge

A June 24, 2025, ET CISO study found that 51% of spam emails are AI-generated, with 14% linked to business email compromise (BEC) attacks, up 20% since January 2025. Advanced language models create hyper-realistic phishing emails, targeting finance and healthcare with \$1.8M average losses per BEC incident. These emails evade traditional filters by mimicking legitimate communication patterns. AI-driven email analysis and behavioral detection are critical to identify anomalies. Regular employee training on phishing recognition is essential. The study predicts a 30% rise in AI-based attacks by 2026. Organizations must adopt adaptive AI defenses and conduct frequent phishing simulations to build resilience.

 **Read the full report -** [ET CISO, June 24, 2025 \(3 min\)](#)

FileFix Malware Targets Developer Toolchains via Build Scripts


On June 22, 2025, security researcher mr.d0x uncovered FileFix, a stealthy ClickFix variant that embeds backdoors into Visual Studio PreBuild events, as well as Python and JavaScript scripts. It delivers AsyncRAT and Lumma Stealer, enabling theft of credentials and financial data from development environments. FileFix evaded detection by blending into normal build processes, raising serious concerns about software supply chain security. Experts recommend disabling unverified scripts, sandboxing builds, and integrating automated scanning tools to mitigate risk.

 **Read the full report -** [mr.d0x Blog \(2 min\)](#)

AI in Cybersecurity

Microsoft Repositions Cybersecurity Leadership Under AI Focus

In a significant internal shift, Microsoft has reassigned its Chief Information Security Officer (CISO), Igor Tsyganskiy, from the security group to its Cloud + AI division. The move signals Microsoft's growing focus on aligning cybersecurity architecture with AI-driven infrastructure and services. This change comes amid escalating AI-powered threats and a need to secure large-scale AI deployments like Copilot and Azure OpenAI.

 **Read the full report** - [Business Insider \(3 min\)](#)

AI Agents Are Getting Better at Hacking Code

A new study from UC Berkeley demonstrates that large language model agents are becoming capable of discovering and exploiting software vulnerabilities. Using a framework called CyberGym, researchers tested multiple AI models across open-source repositories and found 17 bugs, including 15 zero-day vulnerabilities. Though early-stage, the research points to a future where AI tools can independently conduct offensive and defensive cyber tasks.

 **Read the full report** - [WIRED \(3 min\)](#)

Google India Launches AI Safety Charter to Counter Cybercrime

In response to a growing surge in AI-driven fraud, Google has launched its AI Safety Charter in India to prevent an estimated ₹20,000 crore in cyber losses this year. The initiative includes AI-powered fraud detection tools, real-time abuse monitoring, and partnerships with law enforcement to enhance public awareness. Google says this effort will bolster national resilience against increasingly automated scam campaigns.

 **Read the full report** - [Times of India \(5 min\)](#)

Actionable Insights

“EvilPackage” Malware Campaign Still Active on GitHub

Despite takedown efforts, the “EvilPackage” campaign continues to spread malicious dependency confusion attacks through Python and JavaScript packages on GitHub. Attackers are injecting harmful payloads into open-source projects by mimicking legitimate libraries. Developers should audit dependencies and block unknown package sources immediately.

 [Read Details – Cyfirma \(3 min\)](#)

U2F Security Keys Urged for Finance Teams

Security experts are urging organizations to enforce Universal 2nd Factor (U2F) security keys for employees accessing financial systems and admin dashboards. U2F offers strong phishing resistance and protects against session hijack attacks better than OTPs or SMS.

 [Guide – Passkey Central \(4 min\)](#)

Miscellaneous Links

- [Iran-Linked Phishing Uses AI Voice Calls](#)
- [FBI Warns of Scattered Spider's Expanding Attacks on Airlines Using Social Engineering](#)
- [Zero Trust Architecture Mandate for US Contractors](#)

Published By - Deeptansh Nagar

Team 2 - (Deeptansh Nagar & Keshav Goyal)

Week - 4