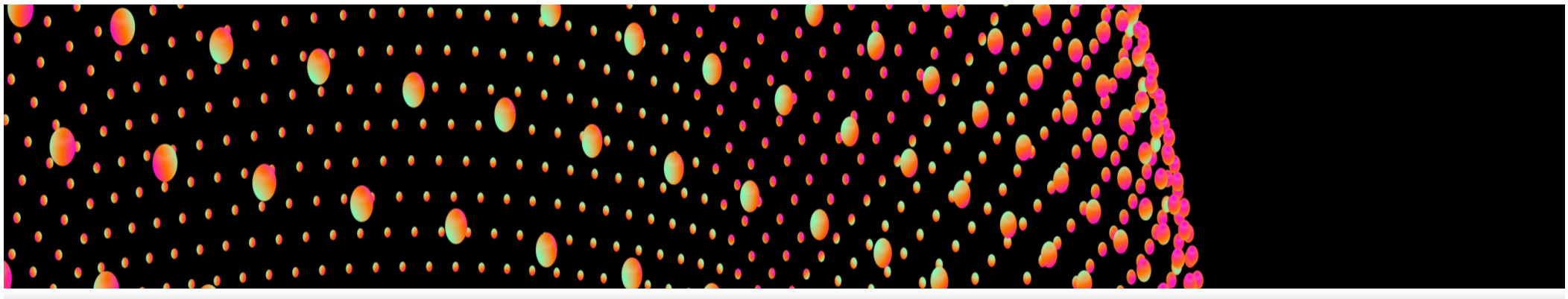


Week of September 29, 2025

Cybersecurity Headlines

Digital Threat Landscape

Cybercrimes, Scams, Threats, Vulnerabilities and Incidents

Weekly Recap: Cisco 0-Day, Record DDoS, LockBit 5.0, BMC Bugs, ShadowV2 Botnet & More

thehackernews.com

From hidden software bugs to massive DDoS attacks and new ransomware tricks, this week's roundup gives you the biggest security moves to know. Whether you're protecting key systems or locking down cloud apps, these are the updates you need before making your next security decision.

UK government to be guarantor for Jaguar Land Rover loan as it recovers from cyberattack

therecord.media

The British government announced it is underwriting a loan for auto manufacturer Jaguar Land Rover (JLR) as the company and its supply chain attempt to recover from the disruption caused by a cyberattack earlier this month.

First Malicious MCP Server Found Stealing Emails in Rogue Postmark-MCP Package

thehackernews.com

Cybersecurity researchers have discovered what has been described as the first-ever instance of a malicious Model Context Protocol (MCP) server spotted in the wild, raising software supply chain risks...

Industry Updates

Legislation, Business, Privacy, Updates, Related Technologies

Law enforcement is using AI to synthesize evidence. Is the justice system ready for it?

therecord.media

In an effort to process the vast amount of data his agency is collecting and save investigators time, Dorsey has turned to TimePilot, software produced by the startup Tranquility AI. The platform is now being used by at least a dozen law enforcement agencies nationwide...

Cyber information-sharing law and state grants set to go dark as Congress stalls over funding

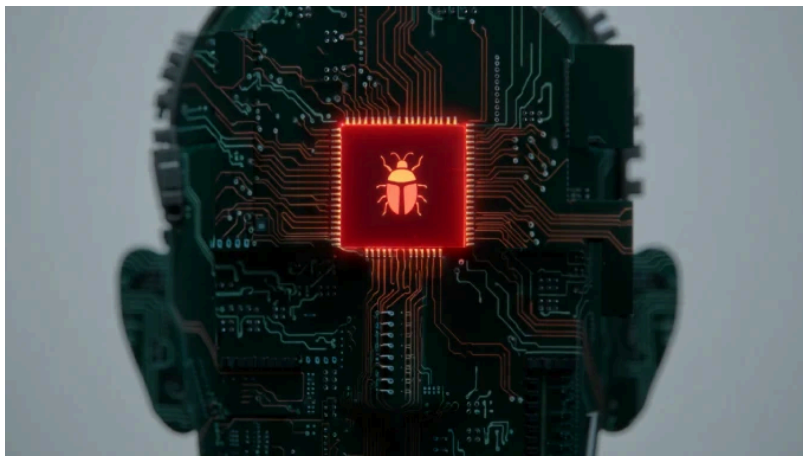
therecord.media

Congress is unlikely to move this week to renew two key cybersecurity efforts that were expected to hitch a ride on legislation to keep the government running.

2025 Cybersecurity Reality Check: Breaches Hidden, Attack Surfaces Growing, and AI Misperceptions Rising

thehackernews.com

The annual research combines insights from over 1,200 IT and security professionals across six countries, along with an analysis of 700,000 cyber incidents by Bitdefender Labs. The results reveal hard truths about how organizations are grappling with threats in an increasingly complex environment.



EvilAI Malware Masquerades as AI Tools to Infiltrate Global Organizations

thehackernews.com

Threat actors have been observed using seemingly legitimate artificial intelligence (AI) tools and software to sneakily slip malware for future attacks on organizations worldwide.

Dutch court rules Meta violated European law by pushing users to profiled feeds

therecord.media

The decision comes in response to a lawsuit filed by the Dutch nonprofit Bits of Freedom, which argued that by controlling users' feeds Meta has been improperly skewing what news consumers receive.

Researchers Warn of Self-Spreading WhatsApp Malware Named SORVEPOTEL

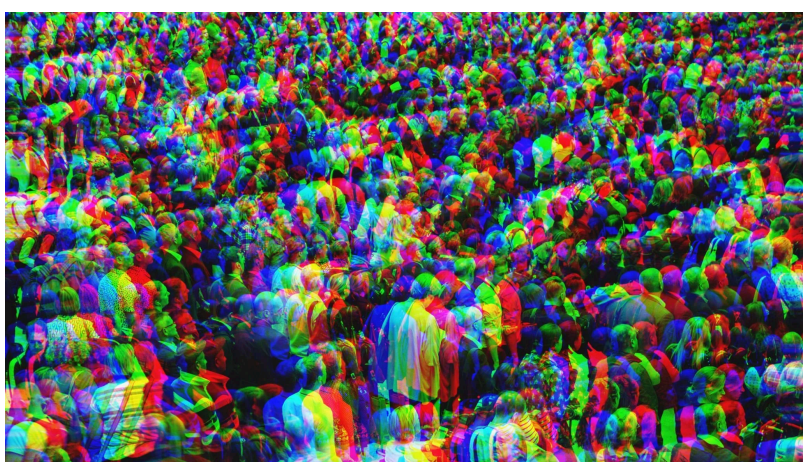
thehackernews.com

The campaign, codenamed SORVEPOTEL by Trend Micro, weaponizes the trust with the platform to extend its reach across Windows systems, adding the attack is "engineered for speed and propagation" rather than data theft or ransomware.

European parliamentarians implore EU leadership to stop funding spyware

therecord.media

Ina letter sent on Tuesday to European Commission officials, the parliamentarians cite recent reporting from the publication Follow the Money documenting how a state-owned Italian bank and the European Union's Defense Fund, among other state entities, are subsidizing spyware companies.



Millions impacted by data breaches at insurance giant, auto dealership software firm

therecord.media

Two companies disclosed new details about data breaches on Wednesday, confirming that millions of people had sensitive information exposed during security incidents this summer.

FTC alleges messaging app violated child privacy law, duped users into subscriptions

therecord.media

A civil complaint filed by the federal government alleges that the Sendit app illegally collected data from users under 13 and tricked people into paying for subscriptions.

External Quick links

- AIScoop
- BleepingComputer
- Cisco Talos Intelligence Group
- CSO Online
- CyberScoop
- Cybersecurity Dive
- Cyware
- CyberWire
- FedScoop
- Government Executive
- Government Technology
- ISACA
- ISSA International
- Krebs on Security
- MITRE ATT&CK®
- NASCIO
- Schneier on Security
- SC Media
- StateScoop
- The Hacker News
- The Record