Week of December 1, 2025

Cybersecurity Headlines

Digital Threat Landscape

Cybercrimes, Scams, Threats, Vulnerabilities and Incidents

Chinese hackers exploiting React2Shell bug impacting countless websites, Amazon researchers say

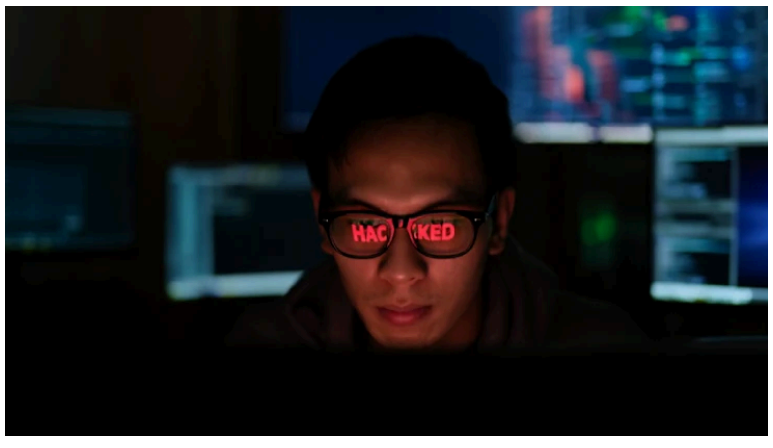
therecord.media

The bug, tagged as CVE-2025-55182 and referred to colloquially as React2Shell, was reported to Meta by researcher Lachlan Davidson on November 29 and publicly disclosed on Wednesday, when a fix was rolled out.

ShadyPanda Turns Popular Browser Extensions with 4.3 Million Installs Into Spyware - The Hacker News

thehackernews.com

ShadyPanda abused browser extensions for seven years, turning 4.3M installs into a multi-phase surveillance and hijacking campaign.



GlassWorm Returns with 24 Malicious Extensions Impersonating Popular Developer Tools - The Hacker News

thehackernews.com

GlassWorm spreads again using 24 fake extensions across Visual Studio Marketplace and Open VSX, hiding Rust implants & Solana-based C2 to target devs.

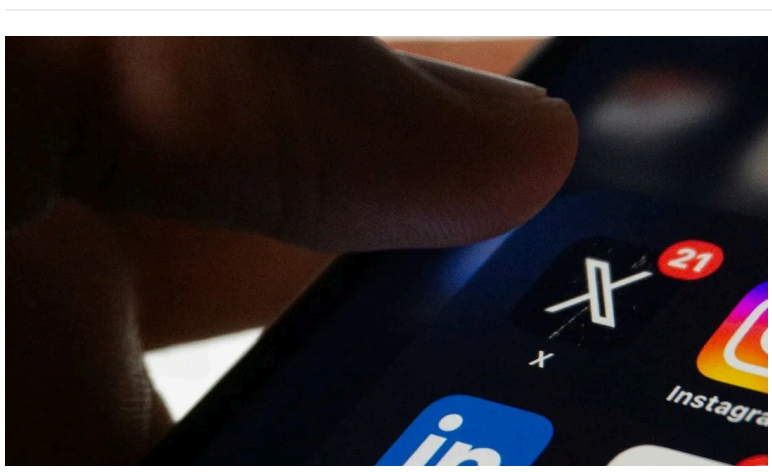
Industry Updates

Legislation, Business, Privacy, Updates, Related Technologies

CISA, NSA warn of China's BRICKSTORM malware after incident response efforts

therecord.media

The Cybersecurity and Infrastructure Security Agency (CISA), NSA and Canadian Centre for Cyber Security published an advisory on Thursday outlining the BRICKSTORM malware based off an analysis of eight samples taken from victim organizations.



EU issues €120 million fine to Elon Musk's X under rules to tackle disinformation

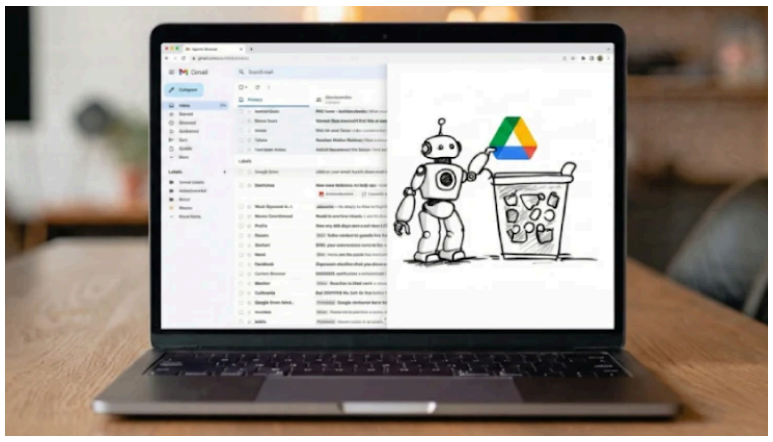
therecord.media

X's paid "blue checkmark" system for verifying users and other aspects of the platform violate the EU's Digital Services Act, the European Commission said in fining the company €120 million ($139 million).

Disinformation and Cyber-Threats Top Global Exec Concerns

www.infosecurity-magazine.com

A new WEF report reveals that AI-powered threats like disinformation are among executives' biggest concerns



Zero-Click Agentic Browser Attack Can Delete Entire Google Drive Using Crafted Emails - The Hacker News

thehackernews.com

A zero-click browser attack uses polite email instructions to trigger agents that delete real files from Google Drive.

New Jersey Launches Civilian Cyber Resilience Corps

www.govtech.com

The cyber corps is mobilizing volunteers as the state continues to fortify its overall cybersecurity posture and work toward filling its coverage gaps, officials have announced.

SMS Phishers Pivot to Points, Taxes, Fake Retailers

krebsonsecurity.com

An instant message spoofing T-Mobile says the recipient is eligible to claim thousands of rewards points.

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