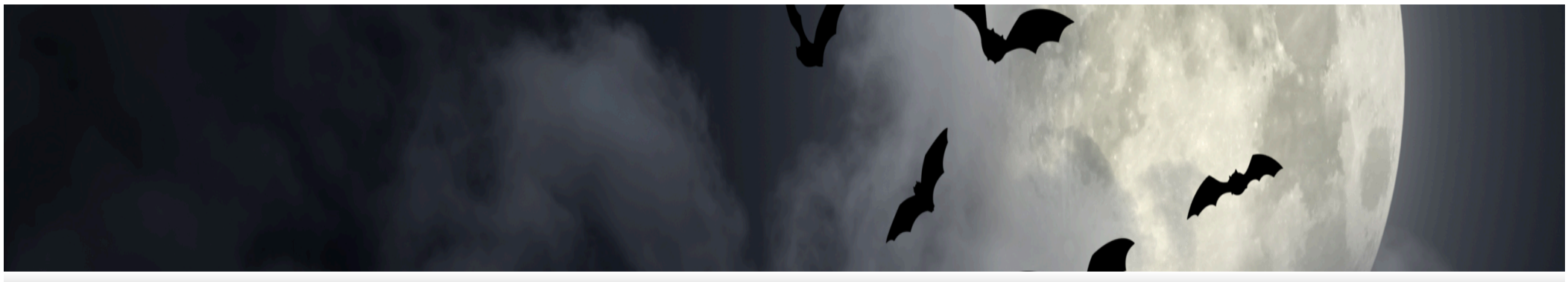
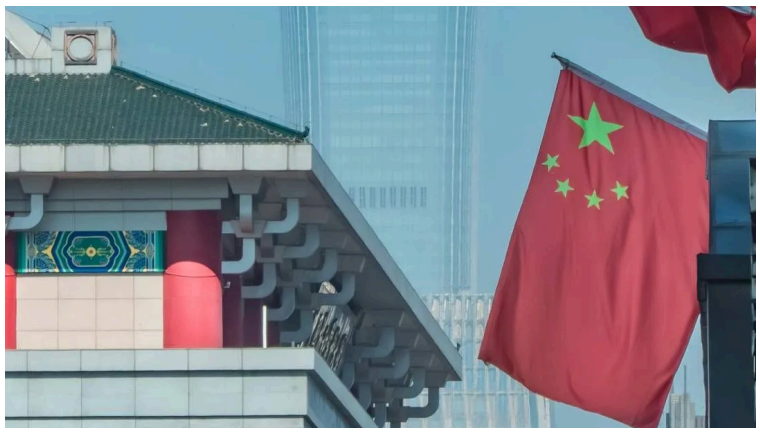


Week of October 20, 2025

Cybersecurity Headlines

Digital Threat Landscape

Cybercrimes, Scams, Threats, Vulnerabilities and Incidents



China claims it caught US attempting cyberattack on national time center

therecord.media

Chinese authorities accused the U.S. on Sunday of compromising the National Time Service Center (NTSC), a research institute responsible for providing timekeeping services in China for national security applications.

Jaguar Land Rover cyberattack cost $2.5 billion, says monitoring group

therecord.media

The nonprofit Cyber Monitoring Centre says the cyberattack on Jaguar Land Rover is “the most economically damaging cyber event” to ever impact the United Kingdom.

Cyber incidents in Texas, Tennessee and Indiana impacting critical government services

therecord.media

A large suburb outside of Dallas was one of multiple municipalities across the U.S. this week to report cyber incidents affecting public services.

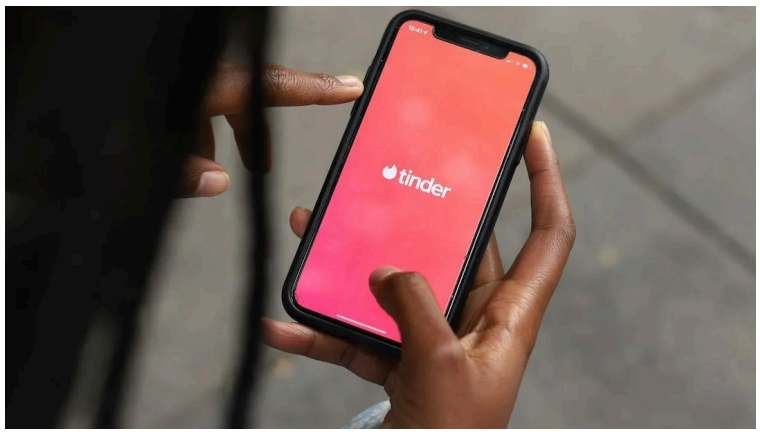
Industry Updates

Legislation, Business, Privacy, Updates, Related Technologies

Judge bars NSO from targeting WhatsApp users with spyware, reduces damages in landmark case

therecord.media

A federal judge on Friday ordered a major commercial spyware company to not target Meta’s WhatsApp messaging platform, which the firm had previously told the court could force it to shut down operations.



Tinder to expand face verification tech to more states

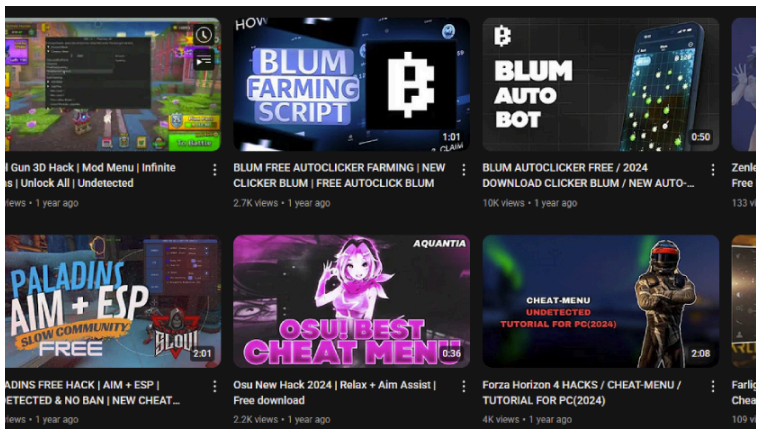
therecord.media

Technology that uses video selfies to verify Tinder users will be expanding soon beyond California, the dating app's parent company says.

Trump pardons former Binance CEO after guilty plea in letting cybercrime proceeds flow through platform

therecord.media

The Wall Street Journal first reported that Trump was pardoning Zhao, who had pleaded guilty to several criminal charges in 2023 related to his role in Binance’s failure to report cryptocurrency circulating on the platform that had come from ransomware attacks, large-scale hacks, account takeovers, and darknet markets dealing in illegal narcotics, counterfeit and fraud-related goods and services,



3,000 YouTube Videos Exposed as Malware Traps in Massive Ghost Network Operation

thehackernews.com

A malicious network of YouTube accounts has been observed publishing and promoting videos that lead to malware downloads, essentially abusing the popularity and trust associated with the video hosting platform for propagating malicious payloads.

Counter Ransomware Initiative stresses importance of supply-chain security

therecord.media

Companies should improve the resilience of their software supply chains against ransomware, according to guidance the International Counter Ransomware Initiative (CRI) published on Friday after its fifth annual summit in Singapore.

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