



Week of November 3, 2025

Cybersecurity Headlines

Digital Threat Landscape

Cybercrimes, Scams, Threats, Vulnerabilities and Incidents



Microsoft Teams Bugs Let Attackers Impersonate Colleagues and Edit Messages Unnoticed - The Hacker News
thehackernews.com

Cybersecurity researchers have disclosed details of four security flaws in Microsoft Teams that could have exposed users to serious impersonation and social engineering attacks. The vulnerabilities "allowed attackers to manipulate conversations, impe...



Cargo theft gets a boost from hackers using remote monitoring tools
therecord.media

Cybersecurity researchers have been tracking thieves who are using their deep knowledge of trucking and transportation technology to steal cargo.



Hackers are attacking Britain's drinking water suppliers
therecord.media

The U.K.'s water suppliers have reported five cyberattacks since January 2024, according to information reviewed by Recorded Future News. The incidents did not affect the safety of water supplies, but they highlight an increasing threat.

Industry Updates

Legislation, Business, Privacy, Updates, Related Technologies



Health privacy bill seeks protections for data collected by apps, smartwatches
therecord.media

Sen. Bill Cassidy (R-LA) on Tuesday introduced legislation that would add new privacy protections to health data gathered by smartwatches, health apps and other new technologies.

Cloudflare Scrubs Aisuru Botnet from Top Domains List
krebsonsecurity.com

For the past week, domains associated with the massive Aisuru botnet have repeatedly usurped Amazon, Apple, Google and Microsoft in Cloudflare's public ranking of the most frequently requested ...



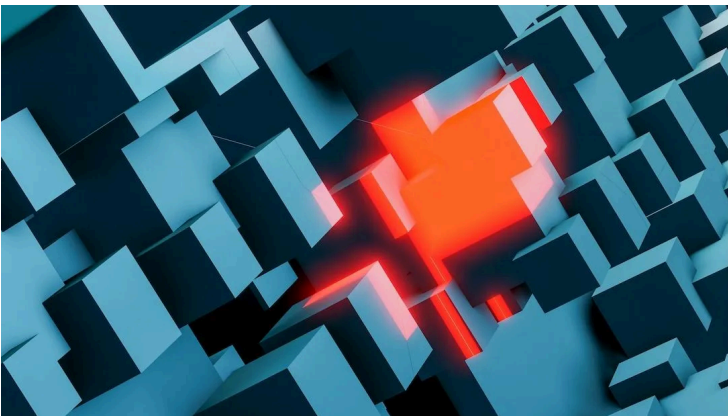
Lawmakers ask FTC to probe Flock Safety's cybersecurity practices
therecord.media

Questioning how Flock Safety protects sensitive user accounts, Sen. Ron Wyden and Rep. Raja Krishnamoorthi want the FTC to investigate the police surveillance tech provider.



Democratic support for surveillance powers will be 'heavier lift' next time, House lawmaker says
therecord.media

Rep. Jim Himes said things have changed for House Democrats when it comes to their potential to back legislation to renew Section 702 of the Foreign Intelligence Surveillance Act.



Russia-linked 'Curly COMrades' turn to malicious virtual machines for digital spy campaigns

therecord.media

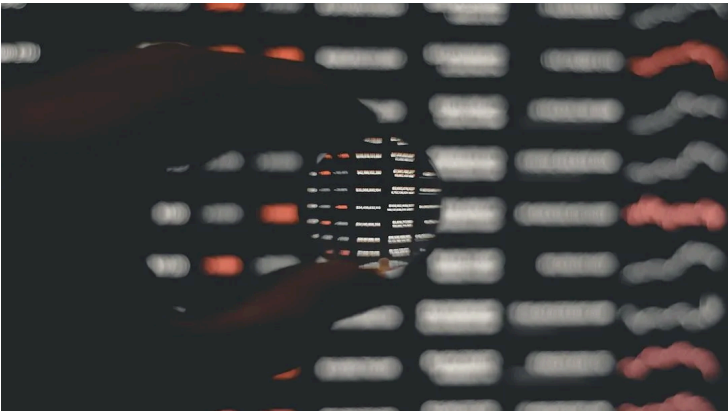
A cyber-espionage operation installed lightweight virtual machines to evade detection, researchers said, in the latest sign of Russia-linked hackers adapting their tactics.



Nevada government declined to pay ransom, says cyberattack traced to breach in May

therecord.media

The state government of Nevada did not pay a ransom to cybercriminals who took down critical government systems in August, the state said in a post-mortem review of the attack.



New malware uses AI to adapt during attacks, report finds

therecord.media

Researchers at Google said Wednesday that they recently observed malware "that employed AI capabilities mid-execution to dynamically alter the malware's behavior."



Cybersecurity Experts Seek to Build Volunteer Defense Force

www.govtech.com

As state and local agencies worry about cybersecurity budget cuts and increased attacks, public officials and researchers try to build a network to boost digital defenses. Leaders of the effort ...



Newly identified Android spyware appears to be from a commercial vendor

therecord.media

Researchers spotted a 9-month-long campaign involving previously undiscovered spyware they call LANDFALL, which leveraged a zero-day bug in Samsung Galaxy phones.

Please be advised that the following resources and materials are for informational purposes only. The opinions and views expressed in these materials are the opinions of the designated authors and do not reflect the opinions or views of the Commonwealth of Massachusetts, the Executive Office of Technology Services and Security, and/or the Enterprise Risk Management Office, (the Commonwealth). The information posted on this website includes hypertext links or pointers to information created and maintained by other public and/or private organizations. These links and pointers are provided solely for the information and convenience of the user. By selecting a link to an outside website, the user is subject to the privacy, copyright, security, and information quality policies of that website. The Commonwealth is not responsible for transmissions users receive from linked websites.

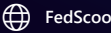
External Quick links



AI



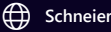
Cybersecurity Dive



FedScoop



Krebs on Security



Schneier on Security



BleepingComputer



Cyware



Government Executive



MITRE ATT&CK®



SC Media



Cisco Talos Intelligence Group



CyberWire



Government Technology



NASCIO



StateScoop



CSO Online



ISACA



The Hacker News



CyberScoop



ISSA International



The Record