Cybersecurity Headlines

Digital Threat Landscape

Cybercrimes, Scams, Threats, Vulnerabilities and Incidents

New Advanced Phishing Kits Use AI and MFA Bypass Tactics to Steal Credentials at Scale - The Hacker News

thehackernews.com

Researchers detail new AI and phishing kits that steal credentials, bypass MFA, and scale attacks across major services.

More than $2 billion in payments from 4,000 ransomware incidents reported to Treasury in recent years

therecord.media

The Financial Crimes Enforcement Network (FinCEN) released a study covering 4,194 ransomware incidents that were reported through the Bank Secrecy Act over the three-year period.

DOJ, CISA warn of Russia-linked attacks targeting meat processing plants, nuclear regulatory entities and other critical infrastructure

therecord.media

The Cybersecurity and Infrastructure Security Agency (CISA), alongside several other U.S. and international agencies, released an advisory covering the cyberattacks launched by CyberArmyofRussia_Reborn (CARR), NoName057(16) and several related groups...
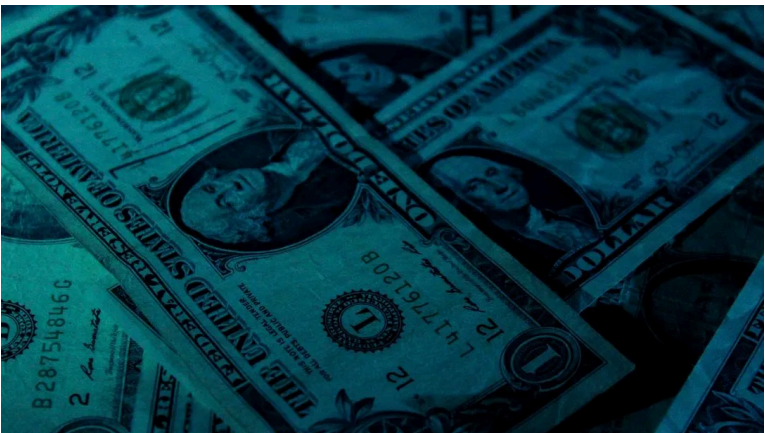
Industry Updates

Legislation, Business, Privacy, Updates, Related Technologies

Canada's privacy regulator to probe billboards equipped with facial scanning tech

therecord.media

The billboards, located near Toronto's Union Station, reportedly analyze only the age and gender of people nearby, according to their owner.

Meta proposal for less data sharing is approved by European Commission

therecord.media

Instagram and Facebook users in the EU will now have the option to share less personal data and see fewer personalized ads.

New York Program to Help Local Governments Pay for Tech
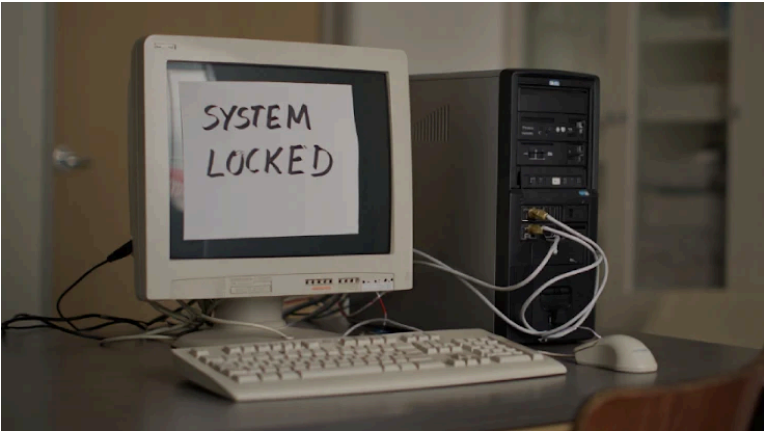
www.govtech.com

The renewal of a state grant program for local public agencies focuses on cybersecurity and other areas that involve gov tech. Officials encourage governments to partner on projects that could ...

Google Adds Layered Defenses to Chrome to Block Indirect Prompt Injection Threats - The Hacker News

thehackernews.com

Chrome adds new layered defenses to block prompt injections, restrict origin access, and prevent unsafe AI actions.

Federal agencies now only have one more day to patch React2Shell bug

therecord.media

Wide exploitation of the vulnerability known as React2Shell has prompted CISA to reduce the amount of time federal agencies have to patch the bug.

Storm-0249 Escalates Ransomware Attacks with ClickFix, Fileless PowerShell, and DLL Sideloading - The Hacker News

thehackernews.com

Storm-0249 now employs ClickFix, fileless PowerShell, and DLL sideloading to gain stealthy access that enables ransomware operations.

CISA, Partners Release Guidance on AI in Critical Systems

www.govtech.com

The document emphasizes governance, risk assessment and safety principles to protect operational technology as AI adoption grows. Understanding security concerns during development is one ...

Four Threat Clusters Using CastleLoader as GrayBravo Expands Its Malware Service Infrastructure - The Hacker News

thehackernews.com

GrayBravo drives four CastleLoader threat clusters using phishing, malvertising, and Booking-themed lures across multiple sectors.
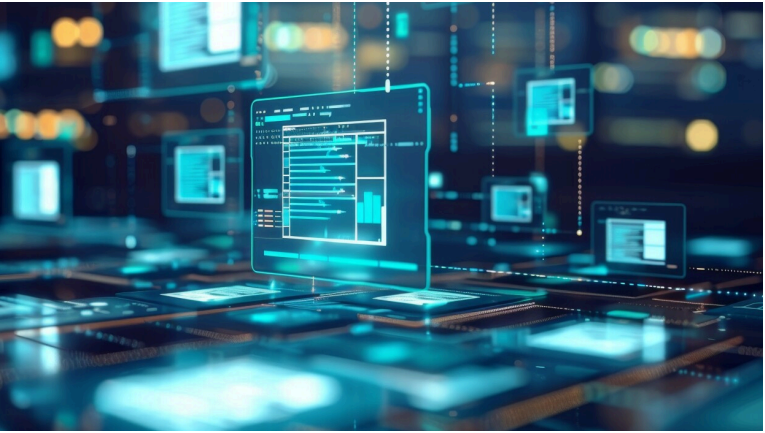

Senators return to effort to boost cybersecurity for commercial satellite industry

therecord.media

Sens. John Cornyn and Gary Peters are taking another crack at moving legislation meant to help commercial satellite providers defend their networks.

Fortinet, Ivanti, and SAP Issue Urgent Patches for Authentication and Code Execution Flaws - The Hacker News

thehackernews.com

Vendors fix critical flaws across Fortinet, Ivanti, and SAP to prevent authentication bypass and remote code execution.

Trump plans executive order curbing state AI laws

therecord.media

Legislators at both the state and federal level have increasingly scrutinized how AI models suck up data for training purposes. AI companies have repurposed data collected for one purpose to train models using data for different purposes and in the process inferred sensitive information.
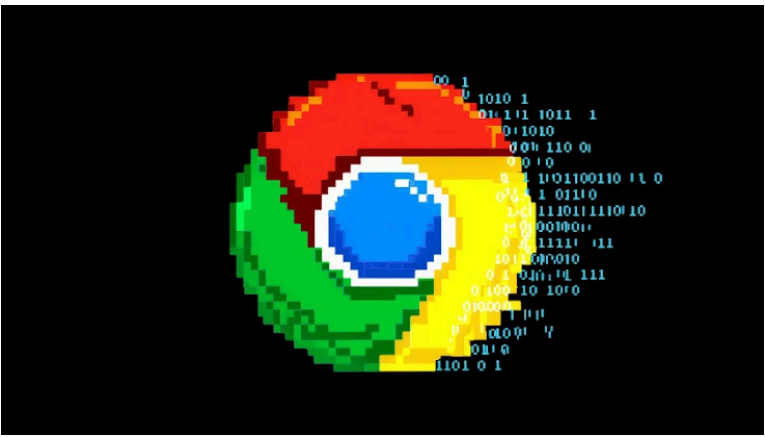
Chrome Targeted by Active In-the-Wild Exploit Tied to Undisclosed High-Severity Flaw - The Hacker News
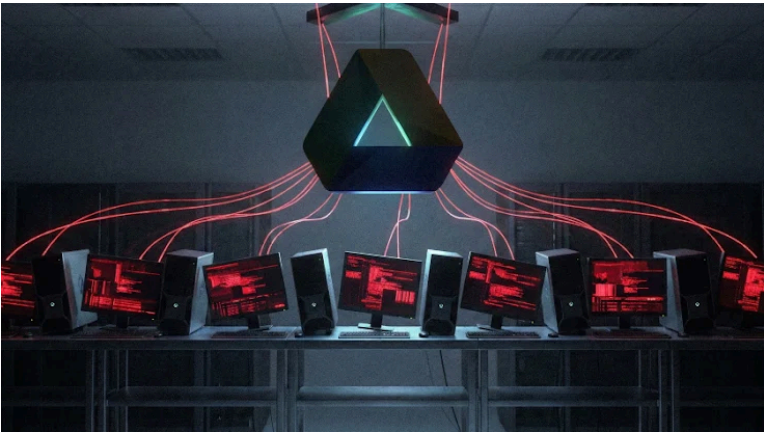
thehackernews.com

Google issues a Chrome update to fix actively exploited issue 466192044 and other confirmed 2025 security flaws.

Trump signs executive order on 'national framework' for AI regulation

therecord.media

Seeking to end a "patchwork" of state-level AI regulation, the president spelled out his administration's approach to letting companies "be free to innovate."

NANOREMOTE Malware Uses Google Drive API for Hidden Control on Windows Systems - The Hacker News

thehackernews.com

Researchers detail NANOREMOTE, a Windows backdoor using Google Drive API for covert control and data theft.

Announced pick for No. 2 at NSA won't get the job as another candidate surfaces

therecord.media

The Trump administration has changed its mind about who will be the new No. 2 at the National Security Agency, amid internal White House opposition to the pick and attacks from far-right conservatives.

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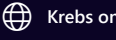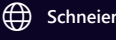
- AIScoop
- BleepingComputer
- Cisco Talos Intelligence Group
- CSO Online
- CyberScoop
- Cybersecurity Dive
- Cyware
- CyberWire
- FedScoop
- Government Executive
- Government Technology
- ISACA
- ISSA International
- Krebs on Security
- MITRE ATT&CK®
- NASCIO
- Schneier on Security
- SC Media
- StateScoop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