Week of January 27, 2025

Cybersecurity Headlines

Official Security Bulletins

Headlines from List of Official Government Sources

Office of Public Affairs | Cracked and Nulled Marketplaces Disrupted in International Cyber Operation - United States Department of Justice

www.justice.gov

The Justice Department today announced its participation in a multinational operation involving actions in the United States, Romania, Australia, France, Germany, Spain, Italy, and Greece to disrupt and take down the infrastructure of the online cybe...

Justice Department Announces Seizure of Cybercrime Websites Selling Hacking Tools to Transnational Organized C

www.justice.gov

The Justice Department today announced the coordinated seizure of 39 domains and their associated servers in an international disruption of a Pakistan-based network of online marketplaces selling hacking and fraud-enabling tools operated by a group known as Saim Raza (also known as HeartSender). The seizures were conducted in coordination with the Dutch National Police.

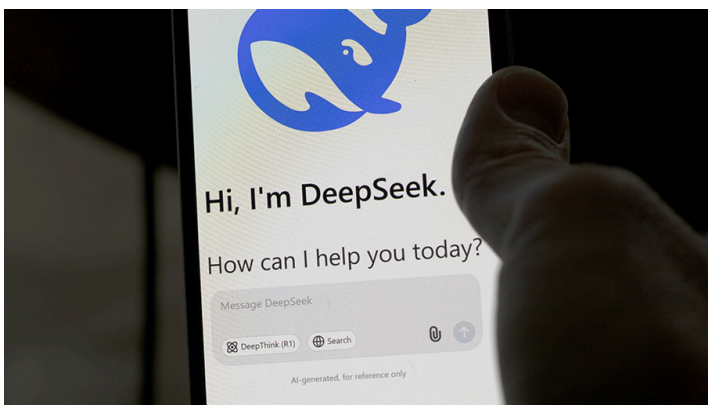
Cybercrimes, Scams & Incidents

Headlines related to cybercrimes and scams including international cybersecurity news and high-profile incidents like ransomware and malware attacks

DeepSeek exposes database with over 1 million chat records

www.bleepingcomputer.com

DeepSeek, the Chinese AI startup known for its DeepSeek-R1 LLM model, has publicly exposed two databases containing sensitive user and operational information.



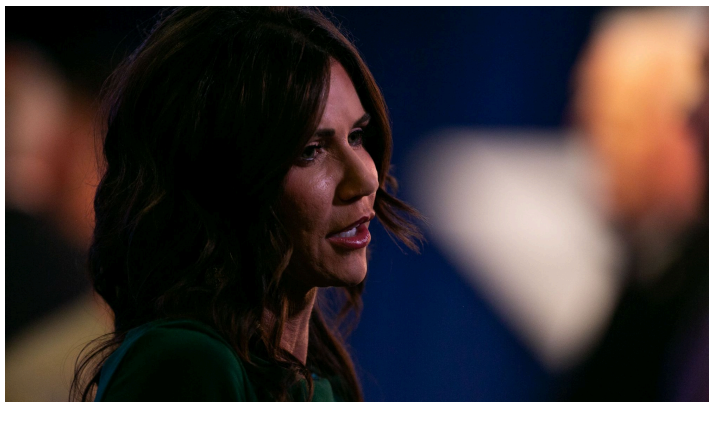
Six ways threat actors will weaponize DeepSeek | SC Media

www.scworld.com

Spear phishing: AI-powered spear phishing attacks are capable of tricking more than 50% of their targets. With DeepSeek's advanced language generation capabilities, threat actors, including non-native English speakers, can create convincing and targe...

Industry News

Headlines collected from across the cybersecurity industry related to legislation, business, and big tech



State and local governments should prepare for changes to CISA, cyber experts say

statescoop.com

Cybersecurity experts told StateScoop that state and local governments should brace themselves for changes to the Cybersecurity Infrastructure and Security Agency under Kristi Noem, former governor of South Dakota, who was sworn last weekend as the 8...

AI sandbox generates new solutions, talent pipeline in Massachusetts

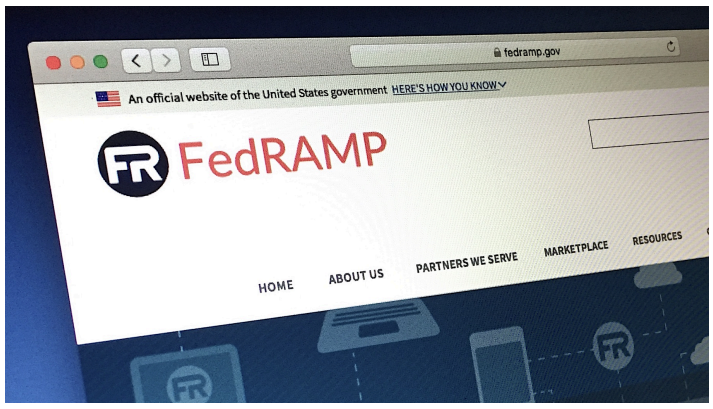
statescoop.com

Massachusetts Chief Information Officer Jason Snyder joins the latest episode of StateScoop's Priorities Podcast to break down a new program designed to spur innovative AI solutions in the state.

DeepSeek Blames Disruption on Cyberattack as Vulnerabilities Emerge

www.securityweek.com

Kela has tested a few known jailbreaks — methods used to trick chatbots into bypassing or ignoring mechanisms designed to prevent malicious use — and found that DeepSeek R1 is vulnerable.. Jailbreak methods such as Evil Jailbreak (instructs the chatb...



Trump administration scraps AI-focused framework for FedRAMP

fedscoop.com

The framework, which had highlighted generative AI as a focus, comes as AI companies have increasingly encountered FedRAMP, short for the Federal Risk and Authorization Management program.. Created in 2011, FedRAMP serves as the federal government's ...

New VPN Backdoor - Schneier on Security

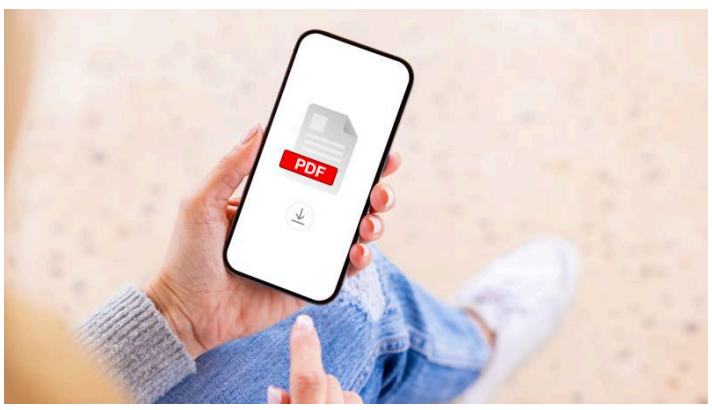
www.schneier.com

A newly discovered VPN backdoor uses some interesting tactics to avoid detection: When threat actors use backdoor malware to gain access to a network, they want to make sure all their hard work can't be leveraged by competing groups or detected by de...

Cyberrisk Quantification: A Strategic Imperative for Financial Resilience

www.isaca.org

As enterprise risk becomes increasingly intricate, the strategic execution of addressing multifaceted threats has grown more critical than ever. Among these threats, cyberrisk has emerged as especially consequential for enterprises, necessitating the...



New USPS text scam uses unique method to hide malicious PDF links

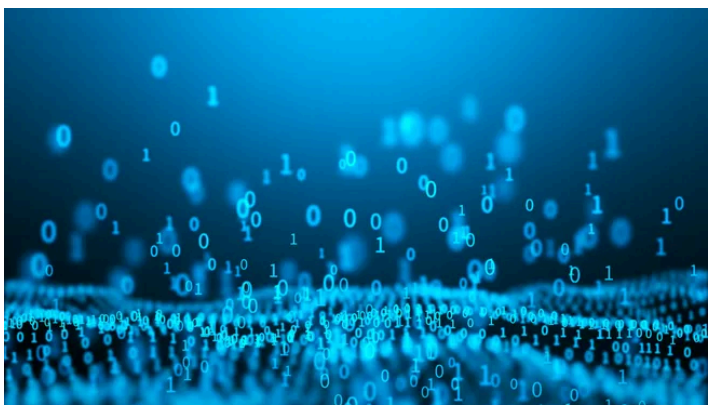
www.scworld.com

A new phishing scam targeting mobile devices was observed using a "never-before-seen" obfuscation method to hide links to spoofed United States Postal Service (USPS) pages inside PDF files, Zimperium reported Monday. The method manipulates elements o...

With Governance, States, Locals Shape Data Strategies

www.govtech.com

State and local governments are embracing data modeling and governance strategies to advance efficiency, sharpen decision-making, and elevate their service delivery. In so doing, they're helping ...



Attackers lodge backdoors into Ivanti Connect Secure devices

www.cybersecuritydive.com

Dive Brief: Researchers tracking a recently disclosed zero-day vulnerability in Ivanti Connect Secure said hundreds of instances may have been compromised through exploits of CVE-2025-0282.Shadowserver scans identified 379 new backdoored instances on...

Report: Almost half of state consumer privacy laws fail to protect individuals' data

therecord.media

Nearly half of state consumer privacy laws fail to adequately protect individuals' data and have made consumer protections weaker than they were before the laws were passed, according to a report released Tuesday.

Multiple Vulnerabilities in Apple Products Could Allow for Arbitrary Code Execution

www.cisecurity.org

Multiple vulnerabilities have been discovered in Apple products, the most severe of which could allow for arbitrary code execution. Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution in the co...

Multiple Vulnerabilities in Google Chrome Could Allow for Arbitrary Code Execution

www.cisecurity.org

Multiple vulnerabilities have been discovered in Google Chrome, the most severe of which could allow for arbitrary code execution. Google Chrome is a web browser used to access the internet. Successful exploitation of the most severe of these vulnera...

Cyber Incident Temporarily Halts Pa. Child Support Payments

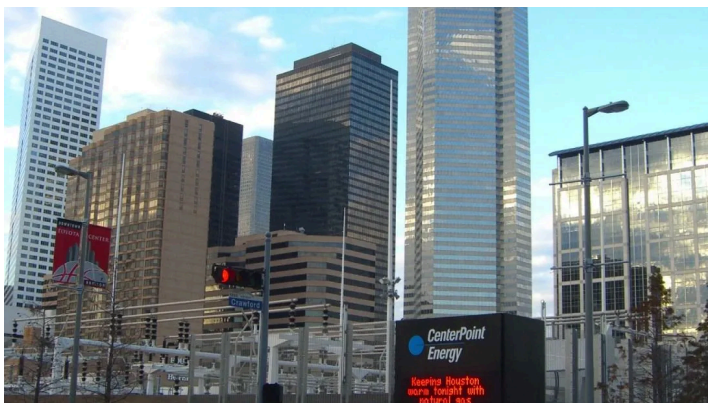
www.govtech.com

The matter, which has since been resolved, prevented an estimated 121,000 families from getting around $27 million in collective payments. The incident was contained and systems have been restored.

Microsoft Teams phishing attack alerts coming to everyone next month - BleepingComputer

www.bleepingcomputer.com

UnitedHealth now says 190 million impacted by 2024 data breach. Clone2Leak attacks exploit Git flaws to steal credentials. Microsoft Teams phishing attack alerts coming to everyone next month



Texas utility firm investigating potential leak of customer data tied to 2023 MOVEit breach

therecord.media

A large Texas energy company confirmed it is investigating reports of stolen customer data that has been published on a cybercriminal forum after it was allegedly taken during a 2023 breach.

The future of identity security: What we can expect | SC Media

www.scworld.com

Identity security will see several ongoing long-term trends continue over the next few years. These include greater adoption of phishing-resistant authentication; greater acceptance of passkeys and other passwordless protocols; further migration to c...

Change Healthcare Data Breach Impact Grows to 190 Million Individuals

www.securityweek.com

UnitedHealth Group has revealed that the number of individuals impacted by the Change Healthcare data breach resulting from a February 2024 ransomware attack is approximately 190 million. The healthcare technology giant previously reported that the i...

Apple Patches Actively Exploited Zero-Day Affecting iPhones, Macs, and More - The Hacker News

thehackernews.com

Apple has released software updates to address several security flaws across its portfolio, including a zero-day vulnerability that it said has been exploited in the wild.. The vulnerability, tracked as CVE-2025-24085 (CVSS scores: 7.3/7.8), has been...

Official Quick Links

- CISA
- CIS/MS-ISAC
- CyberCom
- DHS
- DOJ
- FBI
- NIST
- NSA

External Quick links

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