Week of September 30, 2024

Cybersecurity Headlines

Official Security Bulletins

Headlines from List of Official Government Sources

NSA Jointly Releases Guidance for Mitigating Active Directory Compromises

www.nsa.gov

The National Security Agency (NSA) joins the Australian Signals Directorate's Australian Cyber Security Centre (ASD ACSC) and others in releasing the Cybersecurity Technical Report (CTR), "Detecting

Readout of the Criminal Division's Symposium on Artificial Intelligence in the Justice Department

www.justice.gov

The Criminal Division's Computer Crime and Intellectual Property Section (CCIPS) co-hosted the Artificial Intelligence in the Department of Justice Symposium in Washington, D.C., at the Center for Strategic and International Studies (CSIS) on Oct. 2.

2024 Deloitte-NASCIO Survey Finds States Face Growing Cybersecurity Threats, Tight Budgets - NASCIO

www.nascio.org

Nearly three-quarters of state chief information security officers say the likelihood of AI-enabled threats is "high" New Orleans, LA., September 30, 2024 — The 2024 edition of the biennial cybersecurity report from Deloitte and the National Associat...

The 2024 State CIO Survey: Building Blocks of the Next Generation CIO - NASCIO

www.nascio.org

The 2024 NASCIO State CIO Survey includes responses from 49 state chief information officers to questions on nine topics. This year's survey includes a dive into how states are using generative artificial intelligence, accelerating digital government...

State CIOs Focus on the Fundamentals - NASCIO

www.nascio.org

New Orleans, LA., Tuesday, October 1, 2024 —The National Association of State Chief Information Officers (NASCIO) released today The 2024 State CIO Survey: Building Blocks of the Next Generation CIO. The report includes responses from 49 state CIOs o...

2024 Deloitte-NASCIO Cybersecurity Study - NASCIO

www.nascio.org

As information has become ever more central to how government functions, the role of the state chief information security officer (CISO) has continued to grow in importance. This year's survey, which includes responses from CISOs in all 50 states and...

Indiana Man Pleads Guilty to Conspiracies Involving Cyber Intrusion and $37 Million Cryptocurrency Theft

www.justice.gov

SIOUX FALLS - United States Attorney Alison J. Ramsdell announced that Evan Frederick Light, age 21, of Lebanon, Indiana, appeared before U.S. Magistrate Judge Veronica Duffy on September 30, 2024, and pleaded guilty to an Indictment that charged him with Conspiracy to Commit Wire Fraud and Conspiracy to Launder Monetary Instruments.

CISA Kicks Off 21st Anniversary of Cybersecurity Awareness Month

www.cisa.gov

2024 Cybersecurity Awareness Month Provides Resources and Tools to Secure Our World and Keep Individuals, Businesses and Organizations Resilient to Cyber Attacks

WASHINGTON – Today, the Cybersecurity and Infrastructure Security Agency (CISA) announced the kickoff of the 21stCybersecurity Awareness Month. Throughout October, CISA and the National Cybersecurity Alliance (NCA) will focus on ways to

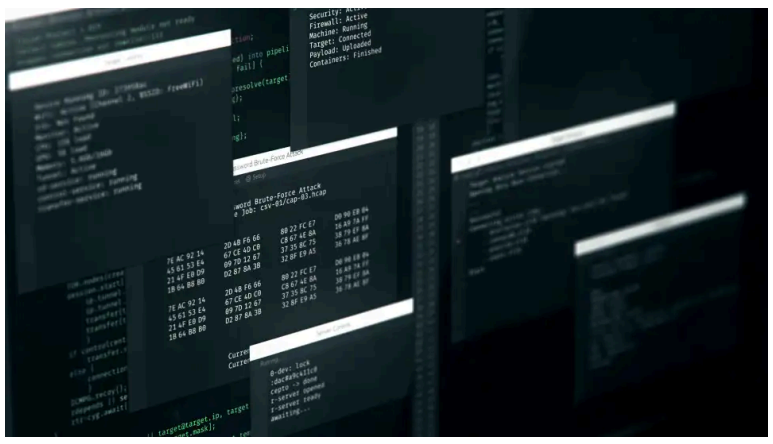
Cybercrimes, Scams & Incidents

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

Fake browser updates spread updated WarmCookie malware

www.bleepingcomputer.com

A new 'FakeUpdate' campaign targeting users in France leverages compromised websites to show fake browser and application updates that spread a new version of the WarmCookie malware.



DDoS attacks are increasingly targeting critical infrastructure

www.csoonline.com

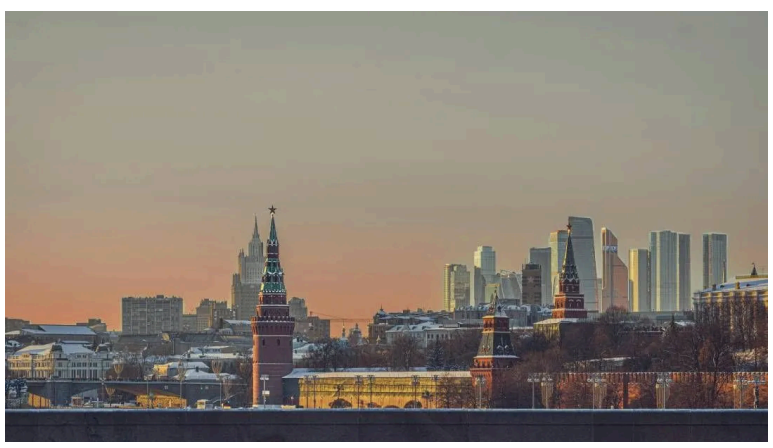
An upswing in hacktivist activity is behind the big rise in attacks aiming to saturate and overwhelm the resources of governments, utilities, and financial services, a report from Netscout reveals.

FBI raids government IT and cyber contractor Carahsoft

www.govexec.com

The FBI raided the Reston, Va., headquarters of IT, software and cybersecurity services provider Carahsoft Technology Corp. on Tuesday, according to two people familiar with the matter.

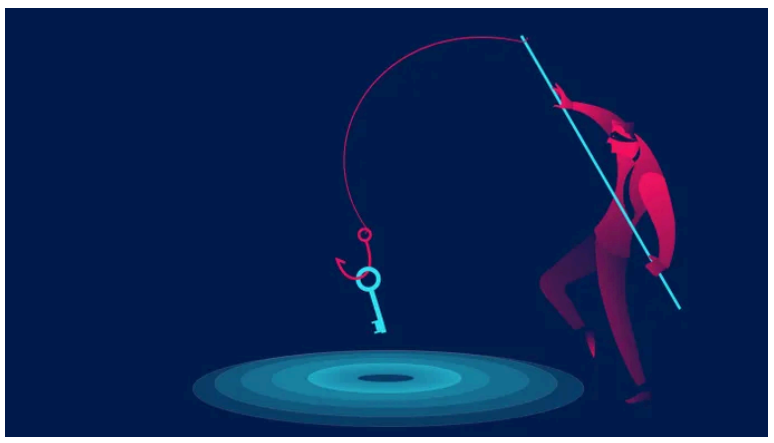
The raid was conducted sometime Tuesday morning, said one of the people, who asked not to be identified due to the matter's sensitivity.



DOJ, Microsoft seize dozens of domains 'used by Russian intelligence agents'

Industry News

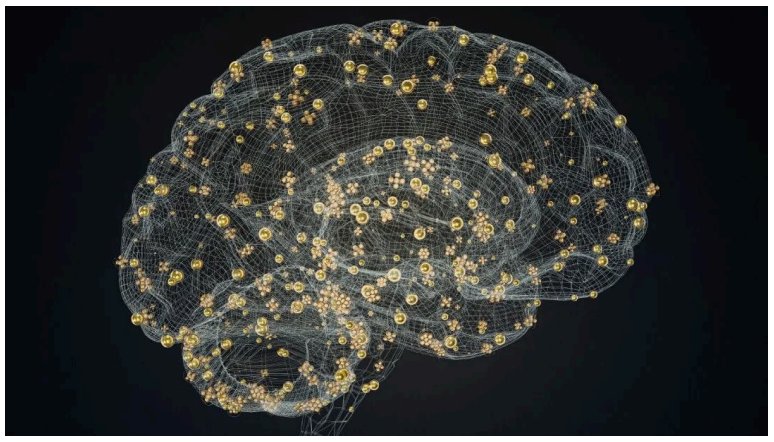
Headlines collected from across the cybersecurity industry related to legislation, business, and big tech



Phishing remains cloud intrusion tactic of choice for threat groups

www.cybersecuritydive.com

The long-lasting effectiveness and success of phishing campaigns underscores the most central challenge in cybersecurity — people are the weakest link.



Neural data privacy an emerging issue as California signs protections into law

therecord.media

Neurobiologist Rafael Yuste had what he calls his "Oppenheimer moment" a decade ago after he learned that he could take over the minds of mice by turning on certain neurons in their brains with a laser.

White House official says insurance companies must stop funding ransomware payments

therecord.media

Some insurance policies incentivize holders to make ransomware payments that ultimately "fuel cyber crime ecosystems," White House cyber adviser Anne Neuberger wrote in an op-ed. "This is a troubling practice that must end."

Stress Levels on the Rise for Cybersecurity Professionals

www.isaca.org

therecord.media

The domains are believed to be used "to commit computer fraud and abuse in the United States" and to launch spearphishing campaigns on sensitive political targets.

A Single Cloud Compromise Can Feed an Army of AI Sex Bots

krebsonsecurity.com

Organizations that get relieved of credentials to their cloud environments can quickly find themselves part of a disturbing new trend:

https://www.scworld.com/news/ivanti-warns-critical-flaws-in-endpoint-manager-exploited-in-the-wild

Ivanti warns critical flaws in Endpoint Manager exploited in the wild

www.scworld.com

Ivanti is advising administrators to get up to date on their patches following a new spell of exploits against Endpoint Manager (EPM).

Research reveals vulnerabilities in routers that left 700,000-plus exposed

cyberscoop.com

ForeScout said one of them warranted rating at the maximum severity level, although DrayTek has issued patches.

https://www.cybersecuritydive.com/news/crowdstrike-recovery-repair/728810/

What's next for CrowdStrike on the road to repair its reputation?

www.cybersecuritydive.com

The cybersecurity vendor finds itself operating from a vulnerable position. Efforts to earn back trust are complex and some require industrywide support.

Cybersecurity professionals increasingly are feeling stress, primarily in response to an escalating threat landscape, new ISACA research shows.

What's new from this year's Counter Ransomware Initiative summit, and what's next

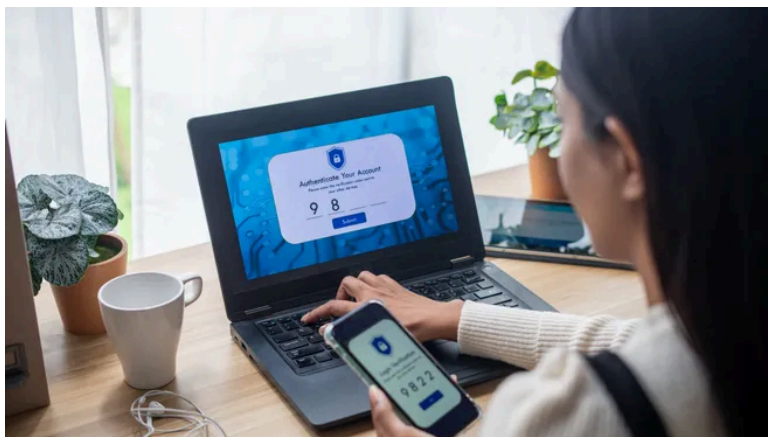
cyberscoop.com

Action plans, different kinds of meetings and more have all been in the mix, top administration officials told CyberScoop.

White House issues guidance for purchasing AI tools to US agencies

fedscoop.com

The Office of Management and Budget memo is the latest action by the Biden administration seeking to effectuate responsible artificial intelligence use in the federal government.



Customers are done with passwords. Do businesses have a solution?

www.cybersecuritydive.com

Research shows customers are frustrated with the login experience, and the friction can cost businesses customers.

DOJ, Microsoft seize more than 100 domains used by the FSB

cyberscoop.com

The simultaneous actions targeted the Star Blizzard espionage operation, which targeted government and civil society around the world.

LockBit Ransomware and Evil Corp Members Arrested and Sanctioned in Joint Global Effort

thehackernews.com

Europol and allies dismantle LockBit ransomware's infrastructure, arresting key figures and sending a strong message to cybercriminals.

Official Quick Links

- CISA
- CIS/MS-ISAC
- CyberCom
- DHS
- DOJ
- FBI
- NIST
- NSA
- White house | ONCD

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