



Week of September 9, 2024

Cybersecurity Headlines

Official Security Bulletins

Headlines from List of Official Government Sources

CISA Releases Election Security Focused Checklists for Both Cybersecurity and Physical Security

www.cisa.gov
Election officials around the country are unwavering in their commitment to enhance the cyber and physical security of election infrastructure to meet an evolving threat environment. As election officials and their teams enter into final preparations for November, these checklists help highlight some of the most common threat vectors, security practices, and resilience measures for consideration

FBI and CISA Release Joint PSA, Just So You Know: False Claims of Hacked Voter Information Likely ...

www.cisa.gov
(CISA) jointly issued the Just So You Know: False Claims of Hacked Voter Information Likely Intended to Sow Distrust of U.S. Elections PSA to raise awareness of attempts to undermine public confidence in the security of U.S. election infrastructure through the spread of disinformation falsely claiming that cyberattacks compromised U.S. voter registration databases.



2023 Cryptocurrency Fraud Report Released | Federal Bureau of Investigation

www.fbi.gov
Losses related to cryptocurrency fraud totaled over \$5.6 billion in 2023, a 45% increase in losses since 2022.



FBI Philadelphia Provides Back-to-School Tips for a Safe and Successful School Year | Federal Bureau of Investigation

www.fbi.gov
As the school year begins, the FBI Philadelphia Field Office wants to remind students, parents, and educators of a few important back-to-school cyber safety topics.

Cybercrimes, Scams & Incidents

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



Feds warn of broad Russia-linked CVE exploits targeting critical infrastructure
www.cybersecuritydive.com

Industry News

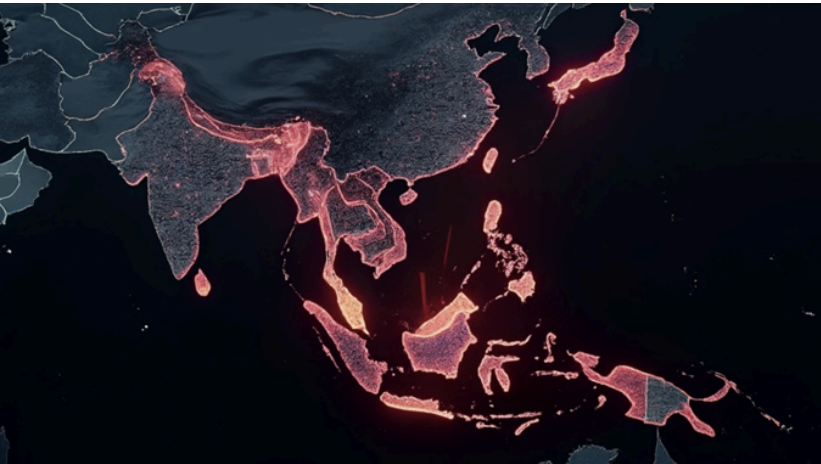
Headlines collected from across the cybersecurity industry related to legislation, business, and big tech



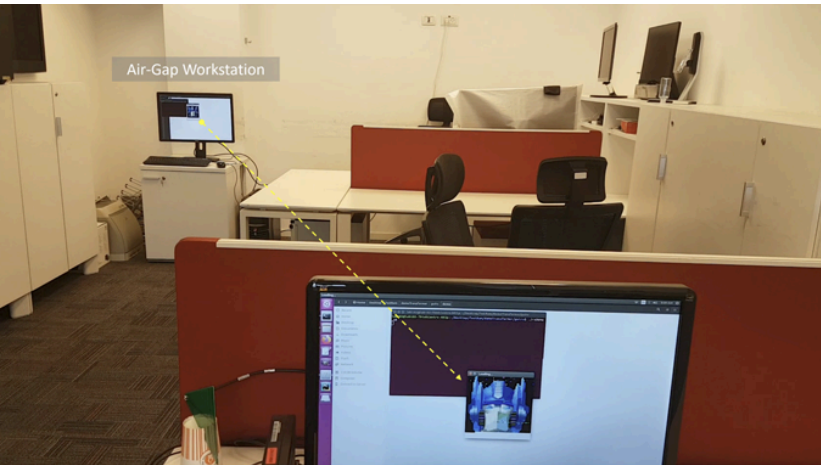
White House cyber czar launches a new hiring sprint
www.govexec.com

Attackers operating under the direction of Russia’s military intelligence service are targeting governments, finance, transportation, energy and healthcare.

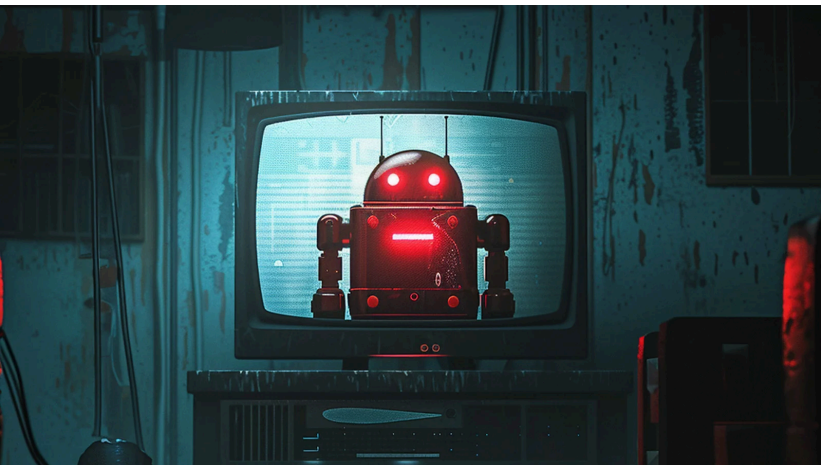
The Dark Nexus Between Harm Groups The Dark Nexus Between Harm Groups and ‘The Com’
krebsonsecurity.com
In September 2023, a Russian ransomware group known as ALPHV/Black Cat claimed credit for an intrusion at the MGM Resorts hotel chain that quickly brought MGM’s casinos in Las Vegas to a standstill.



Chinese Hackers Exploit Visual Studio Code in Southeast Asian Cyberattacks
thehackernews.com
Chinese hackers exploit Visual Studio Code in cyberattacks on Southeast Asian governments. New technique uses reverse shell for espionage and data the



New RAMBO Attack Uses RAM Radio Signals to Steal Data from Air-Gapped Networks
thehackernews.com
New RAMBO attack exploits radio signals from RAM to steal data from air-gapped networks, posing cybersecurity risks.



New Vo1d malware infects 1.3 million Android streaming boxes
www.bleepingcomputer.com
Threat actors have infected over 1.3 million TV streaming boxes running Android with a new Vo1d backdoor malware, allowing the attackers to take full control of the devices.

<https://www.bleepingcomputer.com/news/security/hackers-targeting-whatsup-gold-with-public-exploit-since-august/>

The federal government’s main occupational series for IT jobs saw 3,000 open positions in fiscal 2024.



Cyber Command leader says budget powers are shaving time to complete tasks that once took years
cyberscoop.com
One example, said Gen. Timothy Haugh, was moving \$140 million swiftly for training improvements.



The Department of State’s pilot project approach to AI adoption
fedscoop.com
Senior IT leaders at State argue that small-scale pilots of AI technology can help bring a wealth of benefits to federal government, such as increased transparency.



Adobe evolves its risk management strategy with homegrown framework
www.csoonline.com
The software maker’s Security Risk Management Framework (SRMF) helps leadership prioritize mitigation decisions and ensures everyone is informed about the latest cybersecurity challenges and risks.

Bug Left Some Windows PCs Dangerously Unpatched
krebsonsecurity.com
Microsoft Corp. today released updates to fix at least 79 security vulnerabilities in its Windows operating systems and related software, including multiple flaws that are already showing up in active attacks.



Hackers targeting WhatsUp Gold with public exploit since August

www.bleepingcomputer.com

Hackers have been leveraging publicly available exploit code for two critical vulnerabilities in the WhatsUp Gold network availability and performance monitoring solution from Progress Software.



Apple Vision Pro Vulnerability Exposed Virtual Keyboard Inputs to Attackers

thehackernews.com





















Apple patches Vision Pro vulnerability after GAZEexploit attack exposes keystroke inference risk via gaze tracking.

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.

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](#)