

Week of December 30, 2024

Cybersecurity Headlines

Cybercrimes, Scams & Incidents

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



Treasury says Chinese hackers remotely accessed several workstations and unclassified documents | AP News - Associated Press News

apnews.com

The Treasury Department says Chinese hackers remotely accessed several employee workstations and unclassified documents after compromising a third-party software service provider.

Industry News

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



HIPAA to be updated with cybersecurity regulations, White House says

therecord.media

The Biden administration is proposing an overhaul of the data security rules under the landmark Health Insurance Portability and Accountability Act (HIPAA).

Shedding Light on Shadow IT: Aligning Goals for Organizational Success - ISACA

www.isaca.org

In writing our article, "Navigating the Shadows: A Comprehensive Framework for Anticipating, Identifying, and Managing Shadow IT in Organizations," I was reminded of the conundrum that leads to why shadow IT exists in the first place. Before moving i...



US Treasury Department breached through remote support platform - BleepingComputer

www.bleepingcomputer.com

Chinese state-sponsored threat actors hacked the U.S. Treasury Department after breaching a remote support platform used by the federal agency.



Texas awards \$170M contract to SAIC for IT, cybersecurity services

statescoop.com

Texas' Department of Information Resources has awarded a \$170.9 million contract to technology integrator firm Science Applications International Corporation, or SAIC, to provide the state and its agency network with IT and cybersecurity services.



16 Chrome Extensions Hacked, Exposing Over 600,000 Users to Data Theft

thehackernews.com

16 Chrome extensions breached, exposing 600,000+ users to credential theft; risks persist on endpoints.



It's the 35th anniversary of ransomware - let's talk about the major shifts and changes

talostakes.talosintelligence.com

Ransomware is 35 years old this month, which isn't exactly something to celebrate. But in any case, do join Hazel and special guest Martin Lee to discuss what happened in the very first ransomware incident in December 1989 and why IT "wasn't ready". ...



White House: Salt Typhoon hacks possible because telecoms lacked basic security measures | CyberScoop

cyberscoop.com

The White House said Friday that as the U.S. government continues to assess the damage caused by the Salt Typhoon hacks, the breach occurred in large part due to telecommunications companies failing to implement rudimentary cybersecurity measures acr...



Apple to Pay Siri Users \$20 Per Device in Settlement Over Accidental Siri Privacy Violations - The Hacker News

thehackernews.com

Apple has agreed to pay \$95 million to settle a proposed class action lawsuit that accused the iPhone maker of invading users' privacy using its voice-activated Siri assistant.. The development was first reported by Reuters.. The settlement applies t...

U.S. Army Soldier Arrested in AT&T, Verizon Extortions

krebsonsecurity.com





















Federal authorities have arrested and indicted a 20-year-old U.S. Army soldier on suspicion of being Kiberphant0m, a cybercriminal who has been selling and leaking sensitive customer call records ...

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](#)