

Week of September 2, 2024

Cybersecurity Headlines

Official Security Bulletins

Headlines from List of Official Government Sources



Service for America: Cyber Is Serving Your Country | ONCD | The White House

www.whitehouse.gov

By National Cyber Director Harry Coker, Jr. Throughout our history, generation after generation of Americans have stepped up to meet the challenges of their day, protecting and serving our Nation in a variety of ways. Rationing everyday essentials li...

CIS Controls Successfully Mapped to Healthcare and Public Health Sector-Specific Cybersecurity Performance Goals

www.cisecurity.org

The Center for Internet Security, Inc. (CIS®) is pleased to announce the successful mapping of CIS Critical Security Controls® (CIS Controls®) v8.1 to the U.S. Department of Health and Human Services' Healthcare and Public Health (HHS HPH) cybersecur...



Russian Disinformation Campaign “DoppelGänger” Unmasked: A Web of Deception

www.cybercom.mil

The European Union’s Disinformation Lab (EU DisinfoLab) has recently exposed a sophisticated Russian influence campaign known as “DoppelGänger.”



NSA, FBI, CISA, and Allies Issue Advisory about Russian Military Cyber Actors

www.nsa.gov

FORT MEADE, Md. – The National Security Agency (NSA) joins the Federal Bureau of Investigation (FBI), the Cybersecurity and Infrastructure Security Agency (CISA), and international allies in

Cybercrimes, Scams & Incidents

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

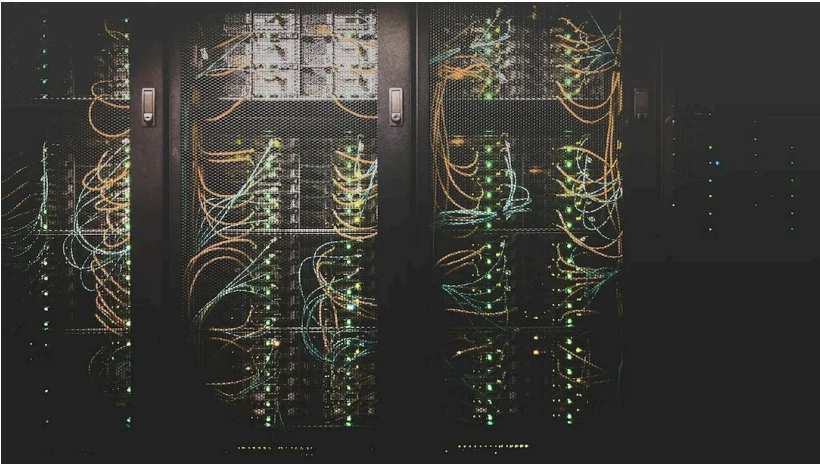


RansomHub Ransomware Group Targets 210 Victims Across Critical Sectors

thehackernews.com

Industry News

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



White House calls attention to ‘hard problem’ of securing internet traffic routing

therecord.media

RansomHub ransomware group targets 210 victims across critical sectors. US government warns of rising attacks on infrastructure using advanced tactics



Linux version of new Cicada ransomware targets VMware ESXi servers

www.bleepingcomputer.com

A new ransomware-as-a-service (RaaS) operation named Cicada3301 has already listed 19 victims on its extortion portal, as it quickly attacked companies worldwide.

SQL Injection Attack on Airport Security - Schneier on Security

www.schneier.com

SQL Injection Attack on Airport Security
Interesting vulnerability:

...a special lane at airport security called Known Crewmember (KCM). KCM is a TSA program that allows pilots and flight attendants to bypass security screening, even when flying on domestic personal trips.



FTC issues \$3 million fine for security camera firm, issuing penalties for a range of violations

therecord.media

The Federal Trade Commission (FTC) plans to fine the security camera company Verkada \$2.95 million over allegations that the firm’s poor security practices led to a hacker breaking into customers’ devices as well as accessing personal data.

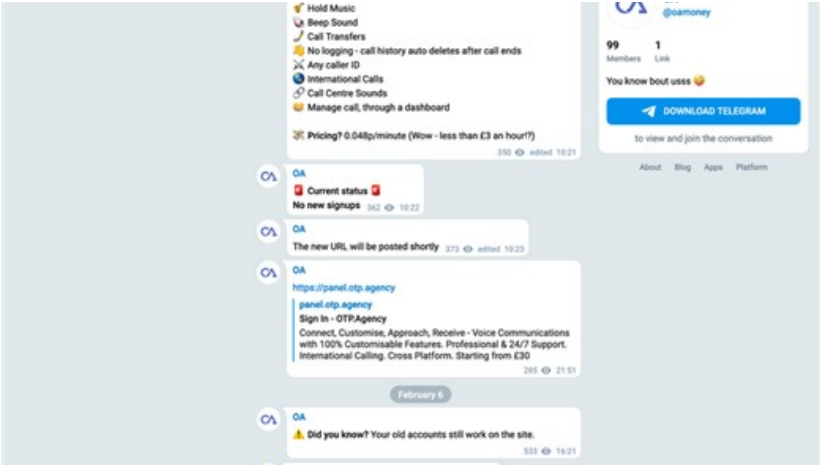


Chinese-Speaking Hacker Group Targets Human Rights Studies in Middle East

thehackernews.com

Tropic Trooper cyberattack targets Middle Eastern government entities with Crowdoor malware and China Chopper

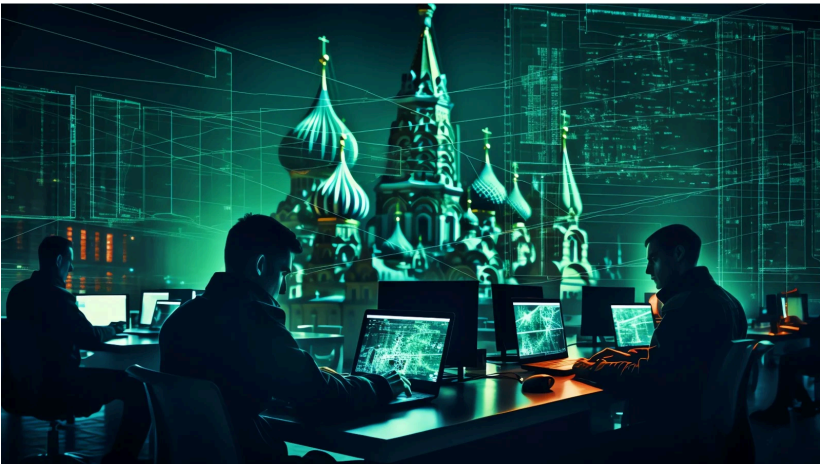
The new guidance on securing the Border Gateway Protocol (BGP) from the White House’s cyber office says the technology “does not provide adequate security and resilience features for the risks we currently face.”



Owners of 1-Time Passcode Theft Service Plead Guilty

krebsonsecurity.com

Three men in the United Kingdom have pleaded guilty to operating otp[.]agency, a once popular online service that helped attackers intercept the one-time passcodes (OTPs) that many websites require as a second authentication factor in addition to passwords.



US cracks down on Russian disinformation before 2024 election

www.bleepingcomputer.com

The FBI seized 32 web domains used by the Doppelgänger Russian-linked influence operation network in a disinformation campaign targeting the American public ahead of this year’s presidential election.



Zyxel warns of critical OS command injection flaw in routers

www.bleepingcomputer.com

Zyxel has released security updates to address a critical vulnerability impacting multiple models of its business routers, potentially allowing unauthenticated attackers to perform OS command injection.



Cisco warns of backdoor admin account in Smart Licensing Utility

www.bleepingcomputer.com





















Cisco has removed a backdoor account in the Cisco Smart Licensing Utility (CSLU) that can be used to log into unpatched systems with administrative privileges.

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](#)