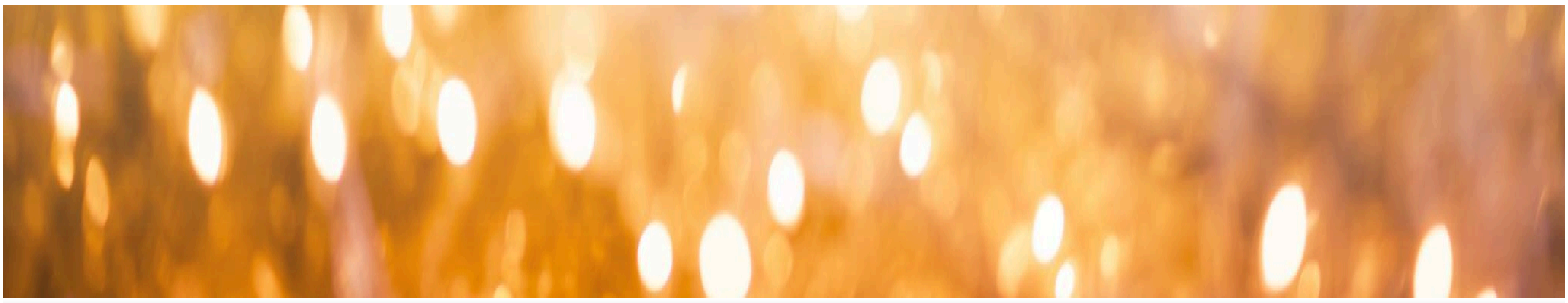


Week of December, 9, 2024

Cybersecurity Headlines

Official Security Bulletins

Headlines from List of Official Government Sources

CISA Updates Toolkit with Seven New Resources to Promote Public Safety Communications and Cyber Resiliency

www.cisa.gov

The Cybersecurity and Infrastructure Security Agency (CISA) collaborates with public safety, national security, and emergency preparedness communities to enhance seamless and secure communications to keep America safe, secure, and resilient.

Cyber Back on Top but AI Makes a Big Move on State CIO's Priorities for 2025 - NASCIO

www.nascio.org

LEXINGTON, Ky., Thursday, December 12, 2024—Today, the National Association of State Chief Information Officers (NASCIO) released the State CIO Top 10 for 2025. The Top 10 represents state technology leaders' top policy and technology priorities for ...

Northern District of Indiana | China-Based Hacker Charged for Conspiring to Develop and Deploy Malware That Exploited Tens of Thousands of Firewalls Worldwide - United States Department of Justice

www.justice.gov

A federal court in Hammond, Indiana, unsealed an indictment today charging Guan Tianfeng, a citizen of the People's Republic of China (PRC) for his involvement in a conspiracy to hack indiscriminately into firewall devices worldwide in 2020.

Office of Public Affairs | Rydox Cybercrime Marketplace Shut Down and Three Administrators Arrested - United States Department of Justice

www.justice.gov

The Justice Department today announced the seizure of Rydox, an illicit website and marketplace dedicated to selling stolen personal information, access devices, and other tools for carrying out cybercrime and fraud, and the arrest of Rydox administr...

Cybercrimes, Scams & Incidents

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

Hackers Using Fake Video Conferencing Apps to Steal Web3 Professionals' Data

thehackernews.com

Industry News

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

Beyond Compliance: The Advantage of Year-Round Network Pen Testing - The Hacker News

thehackernews.com

IT leaders know the drill—regulators and cyber insurers demand regular network penetration testing to keep the bad guys out. But here's the thing: hackers don't wait around for compliance schedules. Most companies approach network penetration testing...

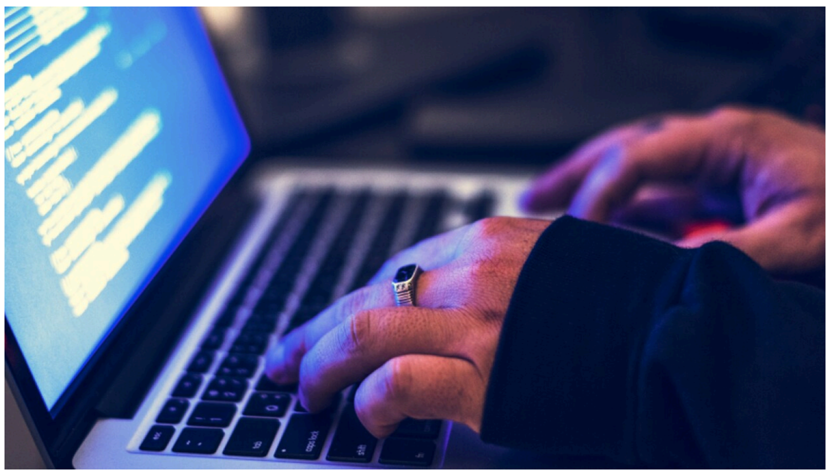
Cybersecurity researchers have warned of a new scam campaign that leverages fake video conferencing apps to deliver an information stealer called Realst targeting people working in Web3 under the guise of fake business meetings. "The threat actors be...

FY2025 NDAA targets spyware threats to U.S. diplomats, military devices

www.nextgov.com

The U.S. government's must-pass defense policy bill includes a measure that aims to shield military servicemembers and diplomats from ensnarement by commercial spyware programs.

The provision, slotted into the $895.2 billion National Defense Authorization Act for the 2025 fiscal year, seeks to secure U.S. government-issued devices used by diplomats, armed forces personnel and staffers in the U.S.



L.A.-Area Cyber Attack Could Impact 17M Patient Records

www.govtech.com

(TNS) — Hackers claim they have retrieved 17 million patient records, including confidential personal and medical information, in a ransomware attack on PIH Health that has paralyzed operations ...

Critical 'AuthQuake' bug let attackers bypass Microsoft MFA

www.scworld.com

A critical vulnerability in Microsoft's multi-factor authentication (MFA) — dubbed "AuthQuake" — could let attackers bypass MFA and gain unauthorized access to a user's account.. Discovered by Oasis Security, the researchers reported in a Dec. 11 blo...

Ransomware sends Ohio county emergency services back to pen and paper

statescoop.com

Wood County, Ohio, located about 116 miles west of Cleveland, discovered a ransomware attack early Monday morning. Officials told StateScoop that fire and emergency services, including 911, are still operational, but that the cyberattack disrupted op...

IAM: It's not sexy, but it saves your bacon | SC Media

www.scworld.com

Identity and access management (IAM) proved its worth by quietly saving organizations from disaster. As breaches like MOVEit, Okta's credential compromise, and the Microsoft email hack rocked the cybersecurity world, IAM emerged as a critical, if uns...

House passes agency software licensing bill

www.govexec.com

The House passed a bipartisan proposal with new transparency requirements for government software spending on Wednesday. Dubbed the Strengthening Agency Management and Oversight of Software Assets ...

Pentagon sunsets generative AI task force, launches rapid capabilities cell

defensescoop.com

The initiative will be led by the CDAO in partnership with the Silicon Valley-headquartered Defense Innovation Unit ().The cell will be charged with identifying and testing technology through rapid experimentation and prototyping, assessing the effec...

Missoula, Mont., Police Evaluating AI Report Software

www.govtech.com

Idaho City Loses $480K to Fraudster Posing as Contractor

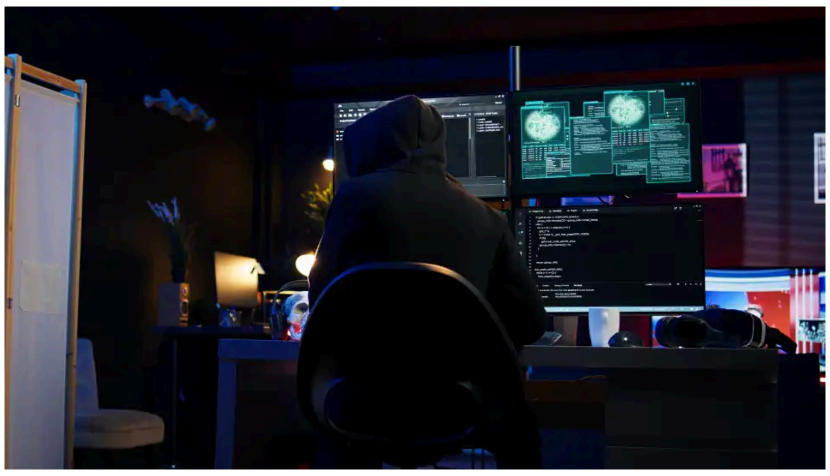
www.govtech.com

A so-called “man-in-the-middle” cyber attack last month compromised the city’s transfer of nearly half a million dollars to pay for excavation during a water infrastructure replacement project.

Krispy Kreme cyberattack impacts online orders and operations - BleepingComputer

www.bleepingcomputer.com

US doughnut chain Krispy Kreme suffered a cyberattack in November that impacted portions of its business operations, including placing online orders.



AWS customers face massive breach amid alleged ShinyHunters regroup

www.csoonline.com

AWS keys were tested for access to IAM, SES, SNS, and S3 services, enabling attackers to establish persistence, send phishing emails, and steal sensitive data.

Over 300K Prometheus Instances Exposed: Credentials and API Keys Leaking Online - The Hacker News

thehackernews.com

City officials have approved a request from Missoula police for 120 new Tasers and a bundle of add-on services, including AI software that writes up to 80 percent of police reports.

New ICIT report urges better resilience to threats of a digitally consolidated world

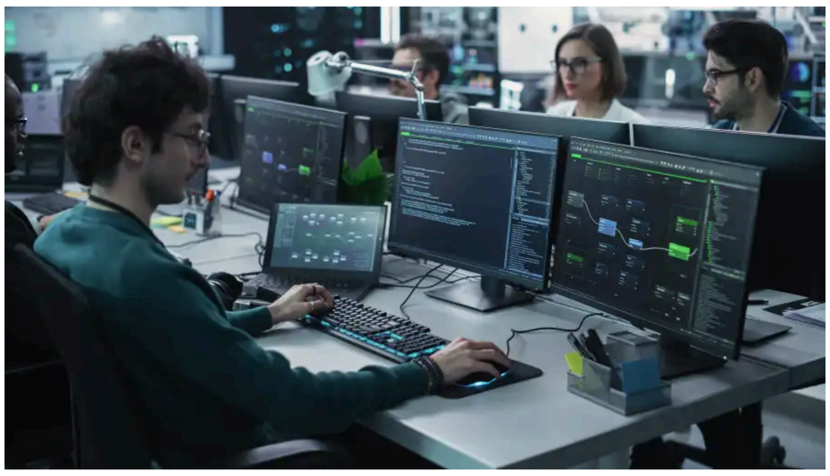
www.scworld.com

The geopolitical context exacerbates these risks. Nations like China have leveraged state-controlled digital ecosystems for economic and strategic gains, presenting an alternative to the open, private-sector-led model of democracies.

8 biggest cybersecurity threats manufacturers face | CSO Online

www.csoonline.com

The manufacturing sector remains a prominent target for cybercriminals, due to complex supply chains, legacy industry control and IoT systems, and a lack of appetite for downtime.

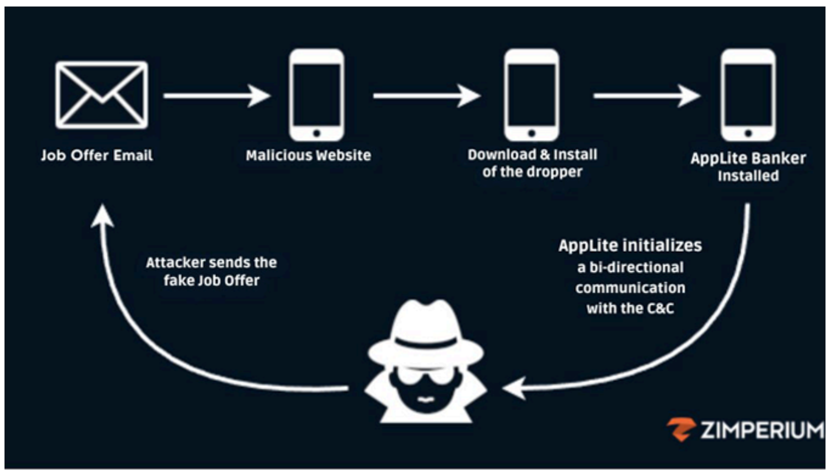


Gen AI use cases rising rapidly for cybersecurity - CSO Online

www.csoonline.com

The usefulness of gen AI tools is evidenced by their proliferation in intrusion detection, anomaly detection, malware identification, and anti-fraud systems, says Peter Garraghan, CEO and CTO of ...

As many as 296,000 Prometheus Node Exporter instances and 40,300 Prometheus servers have been estimated to be publicly accessible over the internet, making them a huge attack surface that could put data and services at risk.. The fact that sensitive ...


Job Offer Email
Malicious Website
Download & Install of the dropper
AppLite Banker Installed
Attacker sends the fake Job Offer
AppLite initializes a bi-directional communication with the C&C
ZIMPERIUM

Fake Recruiters Distribute Banking Trojan via Malicious Apps in Phishing Scam - The Hacker News

thehackernews.com

Cybersecurity researchers have shed light on a sophisticated mobile phishing (aka mishing) campaign that's designed to distribute an updated version of the Antidot banking trojan. "The attackers presented themselves as recruiters, luring unsuspecting...

OMB releases its federal technology impact report as the Biden administration winds down

www.govexec.com

The Biden administration's government tech policy shop released a new impact report on federal technology on Thursday, highlighting work done on artificial intelligence, cybersecurity ...

Vermont CISO's New Role Entails Learning from Policymakers

www.govtech.com

Vermont CISO John Toney will expand his knowledge in a new, supplemental role as a visiting fellow at the George Mason University's Antonin Scalia Law School, joining the National Security ...

***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