Week of March 16, 2026

Cybersecurity Headlines

Digital Threat Landscape

Cybercrimes, Scams, Threats, Vulnerabilities and Incidents

CISA official says agency has not seen uptick in cyber threats amid Iran war

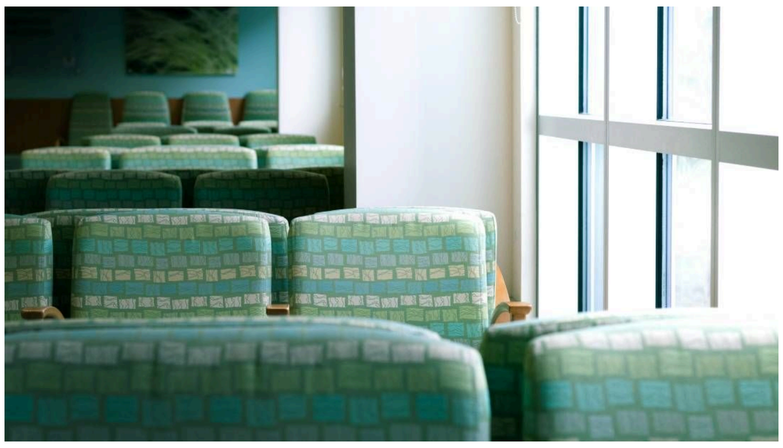
therecord.media

Cybersecurity and Infrastructure Security (CISA) Acting Director Nick Andersen said the agency has been working closely with industry and sector-based groups on threats from Iran in the past couple of weeks.

Stryker says hospital tools are safe, but digital ordering systems still down after cyberattack

therecord.media

Electronic ordering systems belonging to the medical device company Stryker are still down a week after a cyberattack believed to have wiped thousands of company devices of all information. The company said its digital products are safe for use.



Health plan information for over 2.6 million stolen from third-party admin Navia

therecord.media

Navia confirmed a breach in a notice on its website and with regulators in Maine, where the company said 2,697,540 people were affected.

Industry Updates

Legislation, Business, Privacy, Updates, Related Technologies

Energy Department’s CESER office to release strategic plan to fortify US energy sector

therecord.media

Alex Fitzsimmons, the acting director of the Office of Cybersecurity, Energy Security, and Emergency Response (CESER), said the plan is meant to supplement the recently-published national cyber strategy and will focus on how the agency will strengthe...

US intel chiefs urge lawmakers to extend Section 702 surveillance power without changes

therecord.media

The remarks at the House Intelligence Committee’s annual hearing on worldwide threats offered the most vocal support for President Donald Trump’s strategy to date.

Eastern Washington Earns NSA Accreditation for Cyber Operations

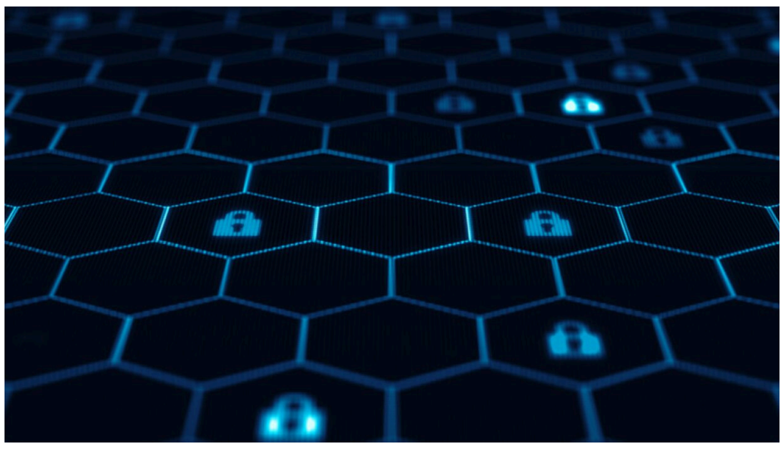
www.govtech.com

The National Security Agency has designated Eastern Washington University as a National Center of Academic Excellence in Cyber Operations, following encouragement by the federal government to ...

Interlock ransomware gang exploited Cisco firewall zero-day weeks before disclosure: Amazon

therecord.media

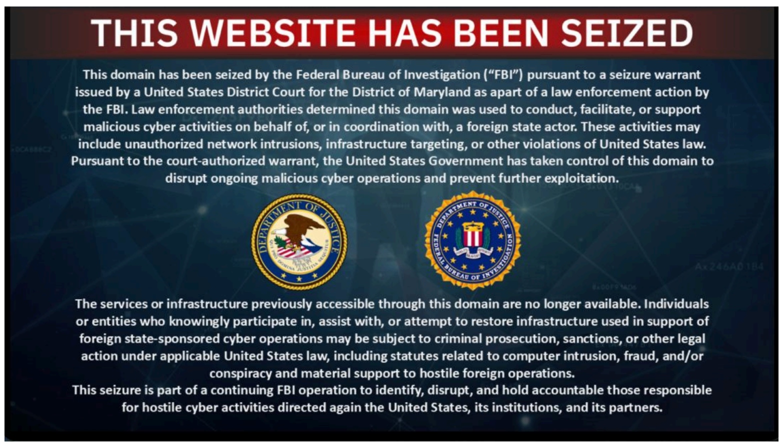
The Interlock ransomware gang recently exploited a zero-day vulnerability in a popular line of Cisco firewalls before the bug was disclosed publicly, according to an Amazon report.



Report: AI-Driven Cyber Attacks Outpace Public-Sector Defenses

www.govtech.com

As AI and growing software supply chains make cybersecurity more complicated, there are also ways that organizations can and should strengthen their defenses.



THIS WEBSITE HAS BEEN SEIZED

This domain has been seized by the Federal Bureau of Investigation ("FBI") pursuant to a seizure warrant issued by a United States District Court for the District of Maryland as apart of a law enforcement action by the FBI. Law enforcement authorities determined this domain was used to conduct, facilitate, or support malicious cyber activities on behalf of, or in coordination with, a foreign state actor. These activities may include unauthorized network intrusions, infrastructure targeting, or other violations of United States law. Pursuant to the court-authorized warrant, the United States Government has taken control of this domain to disrupt ongoing malicious cyber operations and prevent further exploitation.

The services or infrastructure previously accessible through this domain are no longer available. Individuals or entities who knowingly participate in, assist with, or attempt to restore infrastructure used in support of foreign state-sponsored cyber operations may be subject to criminal prosecution, sanctions, or other legal action under applicable United States law, including statutes related to computer intrusion, fraud, and/or conspiracy and material support to hostile foreign operations.

This seizure is part of a continuing FBI operation to identify, disrupt, and hold accountable those responsible for hostile cyber activities directed again the United States, its institutions, and its partners.

FBI, CISA warn on Microsoft Intune risks after Iran-linked cyberattack on Stryker

therecord.media

The attackers behind a recent attack on Stryker did not use malware, instead breaking into a legitimate Microsoft device management system called Intune and wiping the company's data that way.

Maine Courts Push for More Cybersecurity as Records Move Online

www.govtech.com

Maine's court system wants to hire its first full-time cybersecurity employee amid an ongoing shift that has seen most records starting to become available online

New Android malware hiding in streaming apps to spy on users' personal notes

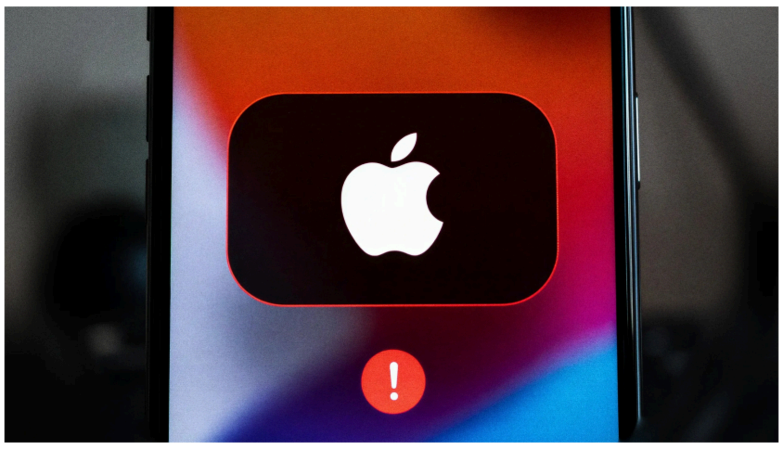
therecord.media

A newly discovered Android malware is masking itself within television streaming apps in order to steal users' passwords and banking data and spy on their personal notes, researchers have found.

Maryland Colleges to Host Cybersecurity Clinic

www.govtech.com

Howard, Carroll and Frederick community colleges will host a a 10-week paid internship program involving in-person meetings and virtual coaching for current cybersecurity students as well as IT ...



Apple Warns Older iPhones Vulnerable to Coruna, DarkSword Exploit Kit Attacks - The Hacker News

thehackernews.com

Apple is urging users who are still running an outdated version of iOS to update their iPhones to secure against web-based attacks carried out via powerful exploit kits like Coruna and DarkSword. These attacks employ malicious web content to target o...

Feds Disrupt IoT Botnets Behind Huge DDoS Attacks

krebsonsecurity.com

The U.S. Justice Department joined authorities in Canada and Germany in dismantling the online infrastructure behind four highly disruptive botnets that compromised more than three million ...

Speagle Malware Hijacks Cobra DocGuard to Steal Data via Compromised Servers - The Hacker News

thehackernews.com

Speagle malware exploits Cobra DocGuard servers to exfiltrate sensitive data, indicating targeted espionage risks for protected systems.

***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.*

External Quick links

- AIScoop
- BleepingComputer
- Cisco Talos Intelligence Group
- CSO Online
- CyberScoop
- Cybersecurity Dive
- Cyware
- CyberWire
- FedScoop
- Government Executive
- Government Technology
- ISACA
- ISSA International
- Krebs on Security
- MITRE ATT&CK®
- NASCIO
- Schneier on Security
- SC Media
- StateScoop
- The Hacker News
- The Record