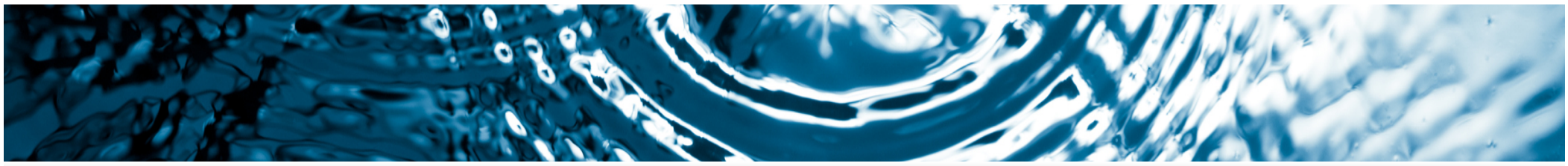


Week of August 26, 2024

Cybersecurity Headlines

Official Security Bulletins

Headlines from List of Official Government Sources

CISA Launches New Portal to Improve Cyber Reporting

www.cisa.gov

CISA Services Portal and Voluntary Cyber Incident Reporting webpage, with resources and frequently asked questions, is now live

WASHINGTON – Today, the Cybersecurity and Infrastructure Security Agency (CISA) announces its cyber incident reporting form moved to the new CISA Services Portal as part of its ongoing effort to improve cyber incident reporting.

Justice Department to Monitor Compliance with Federal Voting Rights Laws in Massachusetts

www.justice.gov

The Justice Department announced today that it will monitor compliance with federal voting rights laws in two cities in Massachusetts for the Sept. 3 primary election. The department will monitor in the Cities of Methuen (in Essex County) and Lowell ...

Election Security Partners Host 7th Annual Tabletop the Vote Exercise for 2024

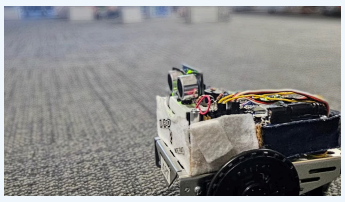
www.cisa.gov

WASHINGTON – The Cybersecurity and Infrastructure Security Agency (CISA), in close coordination with the National Association of Secretaries of State (NASS) and National Association of State Election Directors (NASED), hosted the seventh annual Tabletop the Vote election security exercise this month. Tabletop the Vote brings together federal, state, and local officials as well as private sector...

NSA releases copy of internal lecture delivered by computing giant Rear Adm. Grace Hopper

www.nsa.gov

FORT MEADE, Md. — In one of the more unique public proactive transparency record releases for the National Security Agency (NSA) to date, NSA has released a digital copy of a lecture that then-Capt.



Robots on the Plains: NSA Helps Native Students Engage in Cybersecurity Learning

www.nsa.gov

Last month, National Security Agency (NSA) affiliates traveled to North Dakota's Turtle Mountain Indian Reservation to teach Native high school students about programming, cybersecurity, and robotics.

Iran-based Cyber Actors Enabling Ransomware Attacks on US Organizations

www.cisa.gov

The Federal Bureau of Investigation (FBI), Cybersecurity and Infrastructure Security Agency (CISA), and the Department of Defense Cyber Crime Center (DC3) are releasing this joint Cybersecurity Advisory (CSA) to warn network defenders that, as of August 2024, a group of Iran-based cyber actors continues to exploit U.S. and foreign organizations..

DHS Partners with Japanese Counterparts to Strengthen Maritime Cybersecurity Cooperation | Homeland Security

www.dhs.gov

From August 21-22, the U.S. Department of Homeland Security (DHS) and the Government of Japan conducted a successful tabletop exercise focused on enhancing maritime cybersecurity and incident response capabilities.

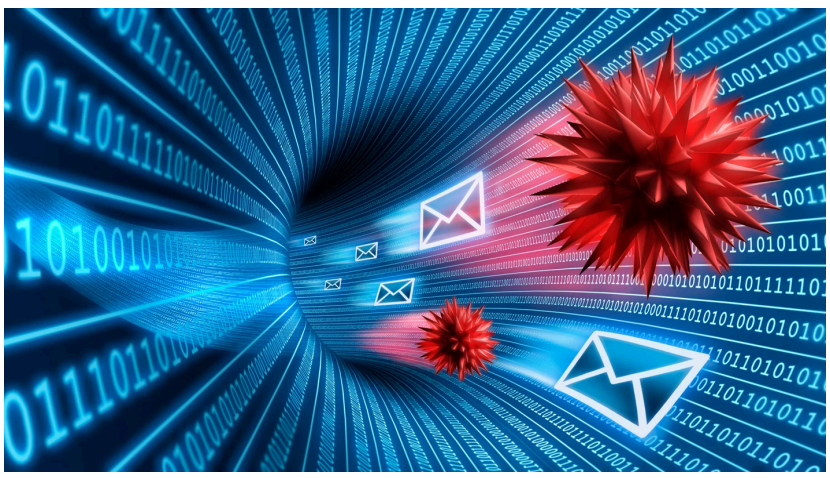
NSA to Launch 'No Such Podcast,' Pulling Back Curtain on Mission, Culture, People

www.nsa.gov

The National Security Agency (NSA) is launching a podcast on September 5 to share the stories of the world's best codemakers and codebreakers.

Cybercrimes, Scams & Incidents

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



Fake Palo Alto GlobalProtect used as lure to backdoor enterprises

www.bleepingcomputer.com

Threat actors target Middle Eastern organizations with malware disguised as the legitimate Palo Alto GlobalProtect Tool that can steal data and execute remote PowerShell commands to infiltrate internal networks further.

After a wave of attacks, Snowflake insists security burden rests with customers

www.cybersecuritydive.com

The cloud-based data warehouse vendor remains “slightly muted” about the attacks on its customers because it wasn’t breached, CEO Sridhar Ramaswamy said.

New 0-Day Attacks Linked to China's 'Volt Typhoon'

krebsonsecurity.com

Malicious hackers are exploiting a zero-day vulnerability in Versa Director, a software product used by many Internet and IT service providers. Researchers believe the activity is linked to Volt Typhoon, a Chinese cyber espionage group focused on infiltrating critical U.S. networks and laying the groundwork for the ability to disrupt communications between the United States and Asia...

Seattle's airport, seaport isolate systems after cyberattack

therecord.media

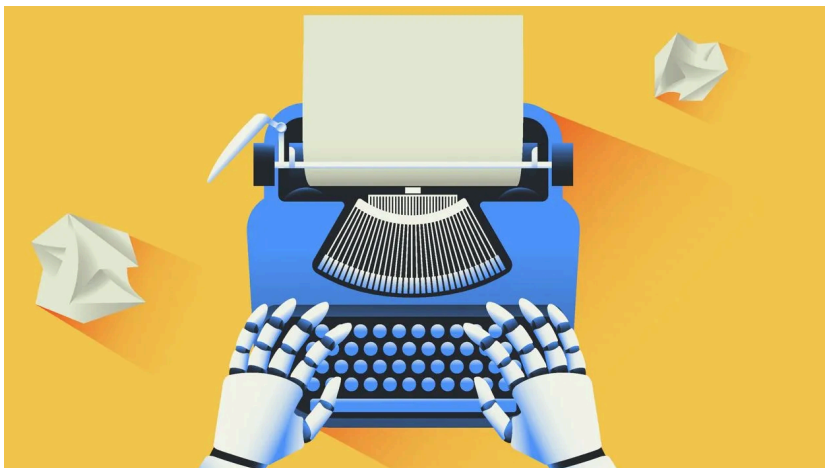
Industry News

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

CISA Urges Federal Agencies to Patch Versa Director Vulnerability by September

thehackernews.com

The U.S. Cybersecurity and Infrastructure Security Agency (CISA) has placed a security flaw impacting Versa Director to its Known Exploited Vulnerabilities (KEV) catalog based on evidence of active exploitation.



Police have begun using AI to write incident reports | StateScoop

statescoop.com

Some police departments have begun using generative AI to help officers write incident reports, concerning watchdogs.

In-depth security news and investigation

krebsonsecurity.com

The proliferation of new top-level domains (TLDs) has exacerbated a well-known security weakness: Many organizations set up their internal Microsoft authentication systems years ago using domain names in TLDs that didn’t exist at the time. Meaning, they are continuously sending their Windows usernames and passwords to domain names they do not control and which are freely available for anyone to re

Audit finds notable security gaps in FBI's storage media management

www.bleepingcomputer.com

An audit from the Department of Justice's Office of the Inspector General (OIG) identified "significant weaknesses" in FBI's inventory management and disposal of electronic storage media containing sensitive and classified information.

US Federal Court Rules Against Geofence Warrants - Schneier on Security

www.schneier.com

This is a big deal. A US Appeals Court ruled that geofence warrants—these are general warrants demanding information about all people within a geographical boundary—are unconstitutional.

The decision seems obvious to me, but you can’t take anything for granted.

The Port of Seattle, which oversees the Seattle-Tacoma airport, said there was no timetable for when certain systems would return to normal after an incident disrupted services over the weekend.

New Android Malware NGate Steals NFC Data to Clone Contactless Payment Cards

thehackernews.com

Discover how NGate, a new Android malware, steals contactless payment data using NFC relay attacks. Learn about the latest cybersecurity threat target

Hunters International ransomware gang threatens to leak US Marshals data

www.scmagazine.com

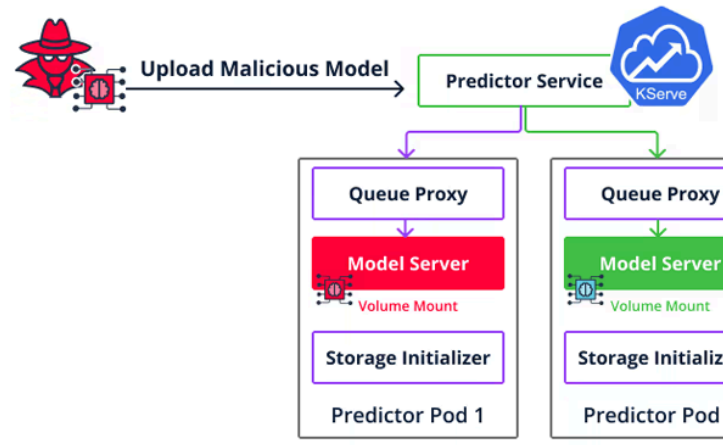
The U.S. Marshals Service previously suffered a major ransomware attack in early 2023.

US Marshals Service disputes ransomware gang's breach claims

www.bleepingcomputer.com

The U.S. Marshals Service (USMS) denies its systems were breached by the Hunters International ransomware gang after being listed as a new victim on the cybercrime group's leak site on Monday.

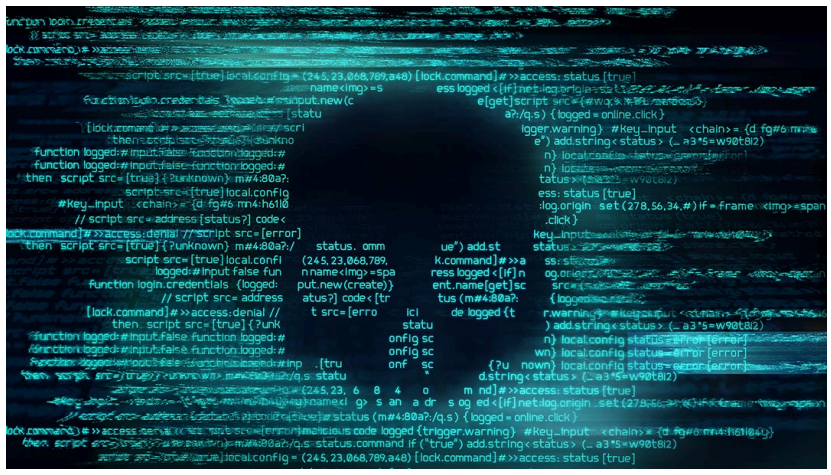
'ASCII Smuggling' attack exposes sensitive Microsoft Copilot data



Researchers Identify Over 20 Supply Chain Vulnerabilities in MLOps Platforms

thehackernews.com

Researchers Identify Over 20 Supply Chain Vulnerabilities in MLOps Platforms | Read more hacking news on The Hacker News cybersecurity news website and learn how to protect against cyberattacks and software vulnerabilities.



EDR killer ransomware: What it is, how to repel

www.scmagazine.com

Threat actors behind RansomHub ransomware are now using EDRKillShifter in attacks.

What is OWASP? A standard bearer for better web application security

www.csoonline.com

The Open Web Application Security Project (OWASP) is an international nonprofit dedicated to providing free documentation, tools, videos, and forums for anyone interested in improving the security of their web applications.

https://www.csoonline.com/article/3497138/how-not-to-hire-a-north-korean-it-spy.html

How not to hire a North Korean IT spy

www.csoonline.com

www.scmagazine.com

Security pros say the novel ASCII Smuggling technique underscores the evolving nature of AI-enabled attacks.

BlackSuit ransomware stole data of 950,000 from software vendor

www.bleepingcomputer.com

Young Consulting is sending data breach notifications to 954,177 people who had their information exposed in a BlackSuit ransomware attack on April 10, 2024.

Windows Downdate tool lets you 'unpatch' Windows systems

www.bleepingcomputer.com

SafeBreach security researcher Alon Leviev has released his Windows Downdate tool, which can be used for downgrade attacks that reintroduce old vulnerabilities in up-to-date Windows 10, Windows 11, and Windows Server systems.

CISOs looking for new IT hires already struggle with talent market shortages and bridging cybersecurity skills gaps. But now they face a growing challenge from an unexpected source: sanctions-busting North Korean software developers posing as potential hires.

The CIS Security Operations Center (SOC): The Key to Growing Your SLTT's Cyber Maturity

www.cisecurity.org

SLTTs can't address their top cybersecurity concerns on their own. They need access to experts who can help to manage their security operations in the context of their evolving security requirements and business needs. This is where a managed securit...

Official Quick Links

- CISA
- CIS/MS-ISAC
- CyberCom
- DHS
- DOJ
- FBI
- NIST
- NSA
- The 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