DAILY CYBER HEADLINES

Daily Cyber Headlines

 TLP:WHITE

Oct 24, 2025

Today's Headlines:

Leading Story

- Motex LANSCOPE Endpoint Manager Vulnerability Actively Exploited in the Wild

Data Breaches & Data Leaks

- Western Sydney University Confirms Personal Data Stolen in Latest Cyber Attack

Cyber Crimes & Incidents

- Phantom's Net: Spy Campaign Deploys WebSocket RAT Against Ukraine Aid
- New PassiveNeuron Attacking Servers of High-Profile Organizations to Implant Malware

Vulnerabilities & Exploits

- Threat Actors Exploiting Adobe Magento RCE Vulnerability Exploited in the Wild

Trends & Reports

- Cyber Incidents in Texas, Tennessee, and Indiana Impacting Critical Government Services

- Verizon Says Attacks Soar, AI-Powered Threats Raise Alarm

Privacy, Legal & Regulatory

- China Moves to Strengthen Regulation of AI Safety and Ethics
- UK Cyber Law Delays Causing Deep Concern

Upcoming Health-ISAC Events

- Global Monthly Threat Brief
  - Americas - October 28, 2025, 12:00-01:00 PM ET
  - European – October 29, 2025, 03:00-04:00 PM CET
- Fall Americas Summit – Carlsbad, California – December 1-5, 2025

Leading Story

Motex LANSCOPE Endpoint Manager Vulnerability Actively Exploited in the Wild

Summary

- A severe flaw has been discovered in Motex LANSCOPE Endpoint Manager, permitting malicious actors to impersonate legitimate sources.

Analysis & Action

CISA has issued warnings of a severe flaw in Motex LANSCOPE Endpoint Manager, tracked as CVE-2025-61932, after observing active exploitation in the wild.

CISA warns of rising endpoint management exploits, where threat actors use crafted packets to mimic trusted traffic, enabling remote

access, malware deployment, or system compromise without user interaction.

Health-ISAC published a bulletin for this and advises its members to apply the latest patches to vulnerable systems, additionally considering network segmentation as a mitigating practice.

Data Breaches & Data Leaks

Western Sydney University Confirms Personal Data Stolen in Latest Cyber Attack

Summary

- Western Sydney University confirmed that sensitive student information has been breached following unauthorized access to a third-party provider that hosts the university's Student Management System.

Analysis & Action

Western Sydney University recently confirmed a cyber-attack on a third-party provider that compromised sensitive student information, including financial and health records, stored in the university's Student Management System.

Threat actors accessed university systems from June 19 to September 03, stealing sensitive data and using it for phishing. Two instances of suspicious activities were first detected on August 06

and 11. Authorities were notified immediately, and impacted individuals have received official notifications.

Health-ISAC encourages its members to establish comprehensive encryption standards for all data, conduct regular risk assessments of third-party providers, and regularly monitor system activity as mitigation measures against potential breaches.

Cyber Crimes & Incidents

Phantom's Net: Spy Campaign Deploys WebSocket RAT Against Ukraine Aid

Summary

- New research from SentinelLABS showed that a recent highly coordinated campaign, dubbed PhantomCaptcha, has targeted several humanitarian and government organizations that support war relief efforts in Ukraine.

Analysis & Action

The campaign, dubbed PhantomCaptcha, was initially launched on October 08, 2025. The attackers spent six months preparing the infrastructure for this attack, which was only active for a day. This campaign mainly targeted organizations such as the International Red Cross, UNICEF, the Norwegian Refugee Council, and the Ukrainian government administrations in regions like Donetsk and Dnipropetrovsk, among others.

The attack started with official-looking emails impersonating the Ukrainian President’s Office, which included a malicious PDF attachment. The PDF contained a link to a domain appearing as a

legitimate Zoom website hosted on a Russian provider-owned server based in Finland.

Health-ISAC advises its members to enhance phishing detection methodologies, monitor PowerShell activity, enforce security policies to defend against this WebSocket RAT threat, and continuously raise employees' awareness of social engineering attacks.

New PassiveNeuron Attacking Servers of High-Profile Organizations to Implant Malware

Summary

- A sophisticated cyberespionage campaign, dubbed PassiveNeuron, has resurfaced, targeting high-profile government, financial, and industrial organizations.

Analysis & Action

PassiveNeuron, a cyberespionage campaign detected initially in 2024, has resurfaced, targeting government, financial, and industrial organizations in Africa, Asia, and Latin America.

Threat actors involved in the campaign primarily look to exploit Microsoft SQL servers, allowing them to gain initial remote command execution on systems upon successful exploitation. Threat actors seek access through leveraging SQL vulnerabilities, injection flaws, or compromised database credentials, allowing them to deploy Active Server Pages Extended (ASPX) web shells to maintain access. Analysis of the campaign points to Chinese-speaking threat actors, alongside tactics associated with APT31, APT27, and APT41 groups.

Health-ISAC advises its members to consider validating and sanitizing user input and additionally ensuring memory is being managed securely to mitigate risks of attacks via threat actors.

Vulnerabilities & Exploits

Threat Actors Exploiting Adobe Magento RCE Vulnerability Exploited in the Wild

Summary

- Sansec has recently observed 250 exploitation attempts targeting an Adobe Commerce remote code execution vulnerability, CVE-2025-54236, and noted that 62% of stores using the platform are still vulnerable.

Analysis & Action

Threat actors have been observed targeting a critical remote code execution vulnerability, tracked as SessionReaper, in the Adobe Commerce–formerly Adobe Magento–platform.

CVE-2025-54236, a Commerce REST API flaw that stems from an improper input validation process in several Adobe Commerce and Magento Open-Source versions, was patched in September 2025. On October 22, 250 exploitation attempts were observed. Despite this, only 38% of stores updated, prompting concerns as exploit attempts surged following the public release of PoC code.

Health-ISAC encourages its members to mitigate all vulnerable software, implement web application firewalls, and actively scan for suspicious activity to mitigate potential exploits.

Trends & Reports

Cyber Incidents in Texas, Tennessee, and Indiana Impacting Critical Government Services

Summary

- Local United States government entities have experienced a surge in cyberattacks in the past weeks, which have disrupted several critical services.

Analysis & Action

Several local government agencies in the United States have been hit by cyberattacks in the past weeks, indicating a potential trend in government targeting.

Kaufman County, Texas, discovered an attack on October 20 that took down several county systems, including the county courthouse. Similarly, an attack on La Vergne, Tennessee, city networks impacted water and property tax billing systems, forcing the shutdown of several city offices throughout the week. In September, Chester County, Pennsylvania, and DeKalb County, Indiana, experienced widespread outages due to targeted cyberattacks. The attacks reveal an ongoing trend of local government targeting that aligns with the end of significant federal partnerships and legislation on cybersecurity.

Health-ISAC advises its members to actively monitor network activity, consider network segmentation, and implement strong authentication measures to mitigate similar attacks that compromise critical services.

Verizon Says Attacks Soar, AI-Powered Threats Raise Alarm

Summary

- Verizon’s latest Mobile Security Index reveals a rising trend of AI-powered attacks, particularly targeting mobile devices.

Analysis & Action

Verizon’s 2025 Mobile Security Index reveals a sharp rise in mobile-targeted cyberattacks, with 85% of companies reporting increased incidents.

Most believe AI significantly enhances these threats, especially in phishing and deepfake tactics. Despite growing concerns, only 17% have implemented defenses against AI-driven attacks. The report also notes employees' widespread use of generative AI tools, raising further security risks. Organizations anticipate that the sophistication of AI will continue to grow, increasing their vulnerability to future mobile and AI-assisted exploits.

Health-ISAC recommends that its members review mobile device security protocols, establish clear guidelines for mobile device usage, and train staff on AI-powered social engineering campaigns as mitigation measures.

Privacy, Legal & Regulatory

China Moves to Strengthen Regulation of AI Safety and Ethics

Summary

- As China looks to strengthen regulations of AI safety, the country's cybersecurity law is expected to be amended to address new challenges and illegal activities.

Analysis & Action

Following a surge in threats leveraging artificial intelligence (AI), top legislative bodies in China state they require stronger AI safety and ethics regulations, amending the country's Cybersecurity Law.

The new development comes as challenges and illegal online activities have increased since China's Cybersecurity Law was enacted in 2016. The amendment intends to create a framework provision on AI security and development, alongside support for basic AI theory research and the development of critical technologies. Moreover, the amendment will see clauses on basic infrastructure such as ethical norms, risk monitoring and assessment, and security regulations related to AI.

Health-ISAC advises its members to encrypt sensitive data and establish guidelines for third-party AI models and/or services as proactive mitigations.

UK Cyber Law Delays Causing Deep Concern

Summary

- UK lawmakers express concern as new cybersecurity laws have yet to be introduced to Parliament amid several substantial cyberattacks.

Analysis & Action

British lawmakers express their concern as their government has yet to introduce new cybersecurity laws to Parliament, allowing for gaps in legislation and growth in cyberthreats.

The development follows the frequently delayed Cyber Security and Resilience Bill, which saw delays again in September. Lawmakers push for new cybersecurity laws to minimize gaps in their legislation, as the United Kingdom has faced several cyberattacks on British businesses such as Marks & Spencer, the Co-op, Harrods, and Jaguar Land Rover within the year. In response, the British government has claimed to be still consulting on its new ransomware policy, expecting to introduce the long-awaited Cyber Security and Resilience Bill shortly.

Health-ISAC advises its members to consider performing regular data backups, segmenting networks, and implementing strong access controls as mitigating strategies.

Health-ISAC Cyber Threat Level

On October 16, 2025, the Health-ISAC Threat Intelligence Committee (TIC) evaluated the current Cyber Threat Level and collectively decided to maintain the Cyber Threat Level to **Blue (Guarded)**. The Threat Level of **Blue (Guarded)** is due to threats from:

F5 Security Incident, Oracle E-Business Suite (Cl0p) Campaign, Ongoing ClickFix Campaign, Remote IT Worker Fraud, and **RedHat Incident.**

For more information about the Health-ISAC Cyber Threat Level, including definitions and response guidelines for each of the alert levels, please review the Threat Advisory System.

You must have Cyware Access to reach the Threat Advisory System document. Contact membership@h-isac.org for access to Cyware.

Report Source(s)	Health-ISAC

Alert ID bad4e196

View Alert

Share Feedback

was this helpful?  | 

Tags PassiveNeuron, WebSocket RAT, PhantomCaptcha, Motex, Lanscope Endpoint Manager, RCE, Artificial Intelligence, Magento, Remote Code Execution, Adobe

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

Share Threat Intel

For guidance on sharing indicators with Health-ISAC via HTIP, please visit the Knowledge Base article "HTIP - Share Threat Intel" here.

The "Share Threat Intel" feature allows for attributed or anonymous sharing across ISACs and other cybersecurity-related entities.

Turn off Categories

For guidance on disabling alert categories, please visit the Knowledge Base article "HTIP Alert Categories" here.

Access the Health-ISAC Threat Intelligence Portal

Enhance your personalized information-sharing community with improved threat visibility, alert notifications, and incident sharing in a trusted environment delivered to you via email and mobile apps. Contact membership@h-isac.org for access to Health-ISAC Threat Intelligence Portal (HTIP).

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.  

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**