DAILY CYBER HEADLINES

Daily Cyber Headlines

TLP:WHITE

Oct 30, 2025

Today's Headlines:

Leading Story

- New Phishing Attack Using Invisible Characters Hidden in Subject Line Using MIME Encoding

Data Breaches & Data Leaks

- Advertisement and PR Giant Dentsu Says Threat Actors Stole Merkle Data
- Conduent Says Data Breach Originally Began with 2024 Intrusion

Cyber Crimes & Incidents

- Nothing to Report

Vulnerabilities & Exploits

- CISA Warns of Dassault Systèmes Vulnerabilities Actively Exploited in Attacks

Trends & Reports

- Cyber Breaches Go Unreported as AI-Driven Threats Surge
- Nearly Half of Ransomware Victims Who Pay Ransom Cannot Recover Data

Privacy, Legal & Regulatory

- China Amends Cybersecurity Law and Incident Reporting Regime to Address AI and Infrastructure Risks

Upcoming Health-ISAC Events

- Global Monthly Threat Brief
    1. Americas - November 25, 2025, 12:00-01:00 PM ET
    2. European – November 26, 2025, 03:00-04:00 PM CET
- Fall Americas Summit – Carlsbad, California – December 1-5, 2025

Leading Story

New Phishing Attack Using Invisible Characters Hidden in Subject Line Using MIME Encoding

Summary

- Threat actors have been observed leveraging a sophisticated phishing technique, embedding invisible characters into email subject lines to evade security filters.

Analysis & Action

A new phishing attack leveraged MIME encoding alongside Unicode soft hyphens to disguise malicious intent, utilizing embedded invisible characters to appear legitimate to human readers.

The technique targets email filtering mechanisms reliant on keyword detection and pattern matching. Victims of the campaign receive emails with subject lines claiming their password is about to expire to garner their attention. However, unbeknownst to the victim, these subject lines contain invisible character fragments, triggering words that would typically alert security systems if they were visible. Upon interaction, the phishing messages direct recipients to compromised domains, allowing for credential harvesting, capturing log information, and leaving targets vulnerable.

Health-ISAC advises its members to remain skeptical of emails from foreign senders and confirm their legitimacy before interacting with foreign links or attachments as a mitigating tactic.

Data Breaches & Data Leaks

Advertisement and Public Relations Giant Dentsu Says Threat Actors Stole Merkle Data

Summary

- Dentsu's subsidiary, Merkle, has been recently targeted in a cyber attack that compromised supplier, customer, and employee data.

Analysis & Action

Merkle, a subsidiary of Dentsu and a well-established customer experience management company, has confirmed that threat actors gained access to their internal network and, subsequently, to company files.

Dentsu disclosed the breach shortly after abnormal activity was detected on the subsidiary's network, which was immediately followed by the temporary shutdown of its systems. Some compromised data included information on suppliers, customers, and staff. United Kingdom employees, specifically, were warned separately of potential exposure to personal contact details, financial records, national insurance numbers, and salaries. No threat actors have claimed responsibility for the attack yet.

Health-ISAC advises its members to monitor network activity actively, encrypt all stored and in-transit data, and deploy Endpoint Detection and Response (EDR) systems to mitigate network and data breaches.

Conduent Says Data Breach Originally Began with 2024 Intrusion

Summary

- Several government agencies and healthcare insurance providers have been confirmed victims of a four-month intrusion into Conduent systems, exposing sensitive information from millions of individuals.

Analysis & Action

Conduent, a major back-end processing service provider to government agencies and other organizations, recently disclosed a

four-month-long intrusion into its systems that breached the information of millions of individuals.

The company first disclosed the intrusion in January of this year, shortly after discovering that threat actors had been in its systems since October 2024. Conduent has since been working with third-party forensic teams and other local government entities to investigate the attack. In April of this year, the company released a regulatory filing confirming that many individuals had their information compromised. Local agencies from four different US states and some healthcare insurance providers are known to have been impacted.

Health-ISAC recommends that its members establish comprehensive incident response plans, actively monitor network activity, and conduct regular risk assessments of third-party providers to mitigate similar breaches.

Cyber Crimes & Incidents

Nothing to Report.

Vulnerabilities & Exploits

Several Dassault Systèmes Vulnerabilities Actively Exploited in Attacks

Summary

- Two critical flaws impacting Dassault Systèmes DELMIA Apriso permit threat actors to execute arbitrary code and bypass mechanisms for elevated privileges.

Analysis & Action

Warnings were raised regarding two critical flaws in Dassault Systèmes DELMIA Apriso. After identifying active exploitation in real-world attacks, the flaws were added to the CISA's Known Exploited Vulnerabilities (KEV) catalog.

The first vulnerability, CVE-2025-6204, categorized under CWE-94, is a code injection flaw, allowing threat actors to execute arbitrary code on systems, possibly allowing for total system compromise on vulnerable systems. The second flaw, tracked as CVE-2025-6205, categorized under CWE-862, details missing authorization controls, allowing threat actors to escalate privileges, infiltrate manufacturing environments, manipulate production data, and/or deploy ransomware to industrial networks. The alert from CISA requires all federal agencies to implement the mitigations by November 18, 2025, urging organizations to update the software immediately.

Health-ISAC advises its members to consider regularly reviewing access logs and implementing network segmentation as mitigating strategies against exploitation of similar vulnerabilities.

Trends & Reports

Cyber Breaches Go Unreported as AI-Driven Threats Surge

Summary

- New studies reveal that almost half of cyber breaches go unreported, while threats leveraging AI continue to grow, amongst other threats.

Analysis & Action

As AI-driven threats continue to surge, a recent study unveiled that nearly half (48%) of cybersecurity leaders failed to report breaches to their organizations in the past year.

The findings surveyed leaders in the US, UK, and Ireland, representing sectors such as retail (45%), health (34%), hospitality (12%), travel (4%), and restaurant/food service (6%). These findings come when cyber incidents are rising in frequency and severity, as reports state a 61% increase in attacks compared to 2024. Over half of organizations saw at least 5% financial losses, posing significant risks to small and mid-sized businesses. On top of threats presented by AI, the report highlights the prevalent dangers of insider threats, as 63% of respondents attested that internal actors are accounted for recent incidents. Moreover, nation-state cyberattacks were also an increased risk for organizations, as 80% of leaders expressed concern about nation-state targeting within the following year.

Health-ISAC advises its members to consider automating defense operations and possibly adopting AI-driven defense tools as mitigation strategies to combat expanding AI threats.

Nearly Half of Ransomware Victims Who Pay Ransom Cannot Recover Data

Summary

- Hiscox found that paying ransomware attackers often fails: 41% still rebuilt systems, 31% faced new demands, and 27% suffered new attacks.

Analysis & Action

Recent findings from Hiscox's Cyber Readiness Report 2025 revealed that data recovery after ransom payments fails more frequently than expected.

The report collected information on 5,750 organizations across seven countries, of which 27% experienced ransomware attacks in the preceding year. Out of the organizations that paid threat actors ransom, 41% could not recover all of the data. While they did get the corresponding recovery keys, they failed to regain access to the affected files.

Health-ISAC advises its members to prioritize strong data backups and employee training, regularly patch vulnerabilities, secure IoT devices, and develop a clear incident response plan.

Privacy, Legal & Regulatory

China Amends Cybersecurity Law and Incident Reporting Regime to Address AI and Infrastructure Risks

Summary

- China has approved an amendment to its cybersecurity law, focusing on AI safety and obligations regarding incident reporting on onshore infrastructures.

Analysis & Action

China recently approved an amendment to its Cybersecurity Law, which enhances a framework for regulating network operations, protecting personal information, and securing critical information infrastructure.

The new amendments to China's Cybersecurity Law (CSL) align with addressing emerging risks associated with artificial intelligence and cross-border cyber threats. Detailed in the provision, these new implementations intend to encourage AI usage alongside other continued emerging technologies to bolster cybersecurity management, advance basic research and algorithmic innovation, and strengthen ethical norms and oversight, among other adjustments. The amendments are expected to go into effect on January 1, 2026, at the beginning of the new year.

Health-ISAC advises its members to consider implementing role-based access controls and encrypting sensitive data at rest and in transit as proactive mitigations to looming threats.

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.

Reference(s)	programbusiness, insideprivacy, securityweek, cybersecuritydive, cybersecuritynews, cybersecuritynews 1, thecyberexpress

Report Source(s)	Health-ISAC

Alert ID e1d42e2f

View Alert

Share Feedback

was this helpful?  | 

Tags Dessault Systemes, MIME, Windows Subsystem for Linux (WSL), Artificial Intelligence, Data Breaches, Phishing, Ransomware

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/**