Health-ISAC

Collaborating for Resilience in Health

DAILY CYBER HEADLINES

Daily Cyber Headlines

TLP:GREEN

Dec 03, 2025

Today's Headlines:

Leading Story

- Microsoft Defender Portal Outage Disrupts Security Alert Visibility

Data Breaches & Data Leaks

- Brsk Investigates Security Incident Involving Stolen Customer Records

Cyber Crimes & Incidents

- Fake Calendly Invites Spoof Top Brands to Hijack Ad Manager Accounts
- Cybercrime Becomes a Service Economy: Tools, Access, and Infrastructure for Rent
- North Korea's IT Worker Fraud: Engineers Enticed to Rent Identities for State-Sponsored Remote Jobs

Vulnerabilities & Exploits

- Apache Struts Vulnerability Lets Attackers Trigger Disk Exhaustion Attacks

Trends & Reports

- Trend Micro Warns of Autonomous AI Ransomware Threats by 2026

Privacy, Legal & Regulatory

- Australia Rolls Out AI Roadmap, Steps Back From Tougher Rules

Upcoming Health-ISAC Events

- Global Monthly Threat Brief
    - Americas – December 16, 2025, 12:00-01:00 PM ET
    - European – December 17, 2025, 03:00-04:00 PM CET
- Fall Americas Summit – Carlsbad, California – December 1-5, 2025

Leading Story

Microsoft Defender Portal Outage Disrupts Security Alert Visibility

Summary

- Microsoft reported a widespread outage in its Defender portal that prevented many organizations from accessing critical security alerts and threat-hunting data.

Analysis & Action

The outage affected users’ ability to access alert dashboards and device listings within the Defender portal, inhibiting normal visibility into potential threats and hindering ongoing security monitoring across impacted environments.

The incident was caused by a surge in traffic that led to high CPU usage on core components responsible for portal operations. As a result, advanced threat-hunting alerts failed to surface, and some devices disappeared from the portal’s view, undermining alert correlation, incident tracking, and response workflows.

Health-ISAC advises its members to manually cross-verify endpoint logs and threat-detection outputs from alternative sources outside the portal, and to ensure logging and telemetry ingestion continue uninterrupted until portal functionality is fully verified. Additionally, Health-ISAC published an advisory for this.

Data Breaches & Data Leaks

Brsk Investigates Security Incident Involving Stolen Customer Records

Summary

- Investigations have begun following a reported security incident at internet provider Brsk, as claims were made that up to 230,105 customer records had been stolen.

Analysis & Action

British internet provider Brsk has launched investigations into a security incident which reportedly saw 230,105 customer records stolen from its systems.

Information believed to have been stolen in the breach includes names, contact details, installation information, location data, phone numbers, and other notes, as seen posted on a cybercrime forum. The company has claimed that only basic contact details were involved, as no financial information, passwords, or account login credentials were exposed. Furthermore, the company has claimed that there is no evidence of the stolen information being used at the time of the reports, alongside statements claiming that its leading network and broadband services were not impacted either.

Health-ISAC advises its members to follow the principle of least privilege, limit data exposure, and leverage strong encryption as mitigating measures against data breaches and leaks.

Cyber Crimes & Incidents

Fake Calendly Invites Spoof Top Brands to Hijack Ad Manager Accounts

Summary

- An ongoing phishing campaign leverages Calendly-themed lures to steal Google Workspace and Facebook business account credentials.

Analysis & Action

A persistent phishing campaign sees threat actors impersonate popular brands, sending Calendly-themed lures to steal Google Workspace and Facebook business account credentials.

The campaign features brands such as Unilever, Disney, MasterCard, LVMH, and Uber, among others, that are impersonated. The attack vector targets business ad manager accounts, providing threat actors with opportunities to launch malvertising campaigns, enact AiTM (Adversary-in-the-Middle) phishing, distribute malware, and/or execute ClickFix attacks. Attacks begin with threat actors impersonating recruiters, sending fake meeting invitations crafted through AI tools that impersonate more than 75 different brands. Upon interaction, the victim is met with a CAPTCHA, followed by an AiTM phishing page, which steals login sessions and exposes users to further malicious attacks.

Health-ISAC advises its members to hover over links and check URLs before interaction, and to leverage reputable antivirus software and block spam as additional mitigations.

Cybercrime Becomes a Service Economy: Tools, Access, and Infrastructure for Rent

Summary

- Cybercriminals now rent out phishing platforms, stolen data feeds, access brokers, and malware via subscription-style services, lowering the barrier to launching attacks and increasing cybercrime activity across multiple sectors.

Analysis & Action

The underground cybercrime ecosystem has transformed into a subscription-driven marketplace offering phishing kits, stolen credentials, initial network access, and remote-access malware. This accessible model enables cybercriminals to scale their operations without requiring advanced technical knowledge.

Crime-as-a-service platforms offer comprehensive service packages that include infrastructure, support, and automation. Infostealers, phishing-as-a-service tools, and network access brokers enable rapid deployment of attack campaigns. This commercialized model accelerates operations and broadens the reach of adversaries.

Health-ISAC advises its members to strengthen credential protection and enforce multi-factor authentication. Regular auditing of access logs, restricting privileged accounts, applying segmentation, and enhancing anomaly detection can help mitigate attacks that leverage commercialized threat offerings.

North Korea’s IT Worker Fraud: Engineers Enticed to Rent Identities for State-Sponsored Remote Jobs

Summary

- Security researchers have exposed a scheme in which North Korean recruiters convinced software engineers to rent their identities, allowing North Korean operatives to secure remote IT jobs under false pretenses.

Analysis & Action

The scheme involves North Korean actors using identity renting arrangements with real engineers. These real engineers serve as front persons, allowing the regime to pass identity checks and secure remote IT contracts with Western companies.

According to reporting, operatives tied to the state-linked group often use stolen or fake identities, sometimes rented from legitimate engineers. They leverage remote access tools, VPNs, or virtual desktops, allowing North Korea to remain physically hidden while using the rented identity as a proxy. This method bypasses conventional employment verification, enabling the infiltration of high-value targets.

Health-ISAC advises organizations to strengthen their hiring and onboarding processes for remote IT staff. Implement multi-factor identity verification, insist on in-person or video-call interviews with live identity proof, and apply strict monitoring of remote access tools and network segmentation to detect and block suspicious remote activity early.

Vulnerabilities & Exploits

Apache Struts Vulnerability Let Attackers Trigger Disk Exhaustion Attacks

Summary

- A critical Apache Struts flaw enables threat actors to trigger disk exhaustion attacks, potentially leading to denial-of-service conditions.

Analysis & Action

An Apache Struts flaw, tracked as CVE-2025-64775, could allow threat actors to execute disk exhaustion attacks, rendering the impacted systems unusable.

The flaw stems from a file leak within multipart processing, allowing threat actors to exploit operations intended for file handling, resulting in uncontrolled file accumulation. Multiple Struts versions, including Struts 6.0.0-6.7.0 and 7.0.0-7.0.3, are impacted by the flaw, alongside two Struts versions that have reached end-of-life (EOL) status (versions 2.0.0 to 2.3.37 and 2.5.0 to 2.5.33). The vulnerability poses an increased risk to internet-facing applications, as threat actors need no authentication for exploitation. Apache has since recommended users upgrade to Struts 6.8.0 or newer to prevent possible service disruptions, data loss, or operational downtime as a result of the flaw.

Health-ISAC advises its members to continuously monitor network traffic, employ IP filtering, and implement disk quotas as mitigations against similar flaws.

Trends & Reports

Trend Micro Warns of Autonomous AI Ransomware Threats by 2026

Summary

- Trend Micro issues warnings about the evolution of AI-powered ransomware, which automates attacks, selects targets, and enacts extortion.

Analysis & Action

Recent reports from Trend Micro suggest a likely increase in threat actors utilizing agentic AI to automate and enhance malicious capabilities.

These actions are primarily seen by state-backed groups at this time, who are already experimenting with these tools. Due to recent trends, experts anticipate that by 2026, ransomware actors will streamline their operations, reducing human elements to minimize errors. This could result in AI agents handling reconnaissance, vulnerability exploitation, and negotiations. This comes at a time when 76% of organizations already struggle to keep up with AI-enhanced attacks, according to CrowdStrike's 2025 ransomware report, making these threats all the more dangerous for organizations.

Health-ISAC advises its members to consider leveraging AI for threat detection, implement a zero-trust architecture, and apply immutable backups as mitigating actions.

Privacy, Legal & Regulatory

Australia Rolls Out AI Roadmap, Steps Back From Tougher Rules

Summary

- Australia has released its roadmap for the adoption of AI throughout its economy, stepping back from prior plans to enact harsher rules on high-risk incidents.

Analysis & Action

Australia has unveiled its roadmap to increase the adoption of artificial intelligence (AI) in its economy, backing away from previous intentions to strengthen laws on high-risk scenarios involving AI.

The action comes as Australia currently lacks specific AI laws, despite its government signalling the introduction of guidelines last year due to concerns over privacy, safety, and transparency. This new plan will focus on investments in data centers, the development of AI skills to support and protect jobs, and ensuring public safety during the integration of AI into individuals' daily lives. Additionally, government officials in Australia have expressed their intention to continue refining and strengthening their plans, seizing new opportunities to keep Australian residents safe.

Health-ISAC advises its members to leverage strict access controls, encrypt both data at rest and in transit, and implement real-time monitoring as mitigating strategies against AI threats.

Health-ISAC Cyber Threat Level

On November 20, 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:

Glassworm, CEO Impersonation via WhatsApp, Holiday Staffing Shortages, ClickFix Campaigns, and Remote IT Worker Fraud.

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)	cyware, cybersecuritynews, bleepingcomputer, economictimes, webpronews, bleepingcomputer 1, bleepingcomputer 2, bleepingcomputer 3, scworld
Report Source(s)	Health-ISAC

Alert ID d93b49cc

View Alert

Share Feedback

was this helpful? 👍 | 👎

Tags Artificial Intelligence Ransomware, Disk Exhaustion Attack, Calendly, North Korea IT Worker Scheme, Apache Struts, Microsoft Defender, Outage, Apache, Microsoft

TLP:GREEN TLP:GREEN Limited disclosure, recipients can ONLY share this within their TRUST community. Recipients should consider the information proprietary and may ONLY share TLP:GREEN information with peers and partner organizations within their TRUST community, SHARING IS NOT PERMITTED via social media, public websites and/or other publicly accessible channels.

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.

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.