DAILY CYBER HEADLINES

Daily Cyber Headlines

TLP:WHITE

Oct 29, 2025

Today's Headlines:

Leading Story

- Critical Authentication Bypass Vulnerability in Asseco mMedica Exposes Healthcare Databases

Data Breaches & Data Leaks

- Threat Actors Target Swedish Power Grid Operator

Cyber Crimes & Incidents

- Water Saci Threat Actors Leverage WhatsApp to Deliver Multi-Vector Persistent SORVEPOTEL Malware
- Massive China-Linked Smishing Campaign Leveraged 194,000 Domains

Vulnerabilities & Exploits

- Italian Spyware Menace: LeetAgent Delivered via Critical Chrome Zero-Day

Trends & Reports

- 81% Router Users Have Not Changed Default Admin Passwords, Exposing Devices to Threat Actors
- CrowdStrike: 76% of Organizations Struggle to Combat AI Attacks

Privacy, Legal & Regulatory

- Cybersecurity Executive Charged with Stealing and Selling Trade Secrets to Russia
- United Nations' First Global Cybercrime Treaty Sparks Debate Over Privacy and Surveillance

Upcoming Health-ISAC Events

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

Leading Story

Critical Authentication Bypass Vulnerability in Asseco mMedica Exposes Healthcare Databases

Summary

- Asseco Poland's mMedica software with versions before 11.9.5 has a critical authentication bypass (CVE-2025-9313), allowing unauthenticated users to access healthcare databases via the mmBackup application.

Analysis & Action

Asseco Poland S.A.'s mMedica software, utilized by healthcare providers across Europe, has been identified with a severe authentication bypass vulnerability (CVE-2025-9313). The flaw permits unauthorized access to sensitive patient data by exploiting a backup application's authenticated session, bypassing standard authentication mechanisms. This issue underscores significant security concerns within healthcare IT infrastructures.

The vulnerability arises from the mmBackup application's ability to maintain an authenticated session, which can be leveraged by unauthenticated users to connect to the database. This design flaw allows attackers to bypass authentication controls, granting them full access to sensitive data. The CVSS score of 9.3 indicates a critical risk, with high impact on confidentiality, integrity, and availability. The flaw is remotely exploitable without user interaction, making it a significant threat to organizations using affected versions of mMedica.

Health-ISAC recommends members to check for mMedica versions before 11.9.5 and upgrade promptly. Meanwhile, restrict network access, monitor unusual database activity, review authentication for backups, and ensure data encryption.

Data Breaches & Data Leaks

Threat Actors Target Swedish Power Grid Operator

Summary

- Svenska kraftnät, a Swedish power grid operator, has confirmed a recent attack allegedly orchestrated by Everest ransomware, in which data from an external file transfer solution was stolen.

Analysis & Action

Sweden's state-owned power grid operator, Svenska kraftnät, recently confirmed that threat actors gained access to external systems and exfiltrated company data.

The attack, discovered on October 25, affected an external file transfer solution. The company has confirmed that no other departments or the power grid had been affected by the breach, but has yet to disclose the type of information compromised in the attack. Everest ransomware group claimed to have stolen 280 GB of data, which the company has yet to verify. Svenska kraftnät is investigating the incident and has reported it to local authorities.

Health-ISAC recommends that its members encrypt all data, consider network segmentation, and establish strong access controls to mitigate potential breaches.

Cyber Crimes & Incidents

Water Saci Threat Actors Leverage WhatsApp to Deliver Multi-Vector Persistent SORVEPOTEL Malware

Summary

- A campaign dubbed Water Saci by Trend Micro in September 2025, which delivers SORVEPOTEL malware, had evolved dramatically by October 2025.

Analysis & Action

Trend Micro analysts recently observed a campaign leveraging SORVEPOTEL malware and exploiting WhatsApp to distribute viral propagation throughout victim networks.

The malware campaign primarily targets Brazilian users and has dramatically evolved since being identified in September 2025. Infection mechanisms start once a user has downloaded and extracted these malicious ZIP files containing an Orcamento.vbs, an obfuscated VBS downloader. Afterwards, the component executes a PowerShell command to perform fileless execution, downloading and executing tadeu.ps1, a PowerShell script, into memory directly. Threat actors can use the SORVEPOTEL backdoor to execute more than twenty commands, including capturing screenshots, file operations, granting remote access, etc.

Health-ISAC advises its members to consider implementing regulated network monitoring and leveraging reputable antivirus software as mitigating measures against similar attack vectors.

Massive China-Linked Smishing Campaign Leveraged 194,000 Domains

Summary

- According to Palo Alto reports, threat actors are being observed impersonating both critical and general services in widespread smishing campaigns.

Analysis & Action

Palo Alto Networks is issuing warnings about an extensive phishing campaign, Smishing Triad, led by a Chinese-speaking threat actor.

The cybersecurity firm reports that over 194,000 malicious domains have been leveraged as part of these smishing attacks since the beginning of 2024. While attacks initially leveraged impersonation of toll and package delivery services, they have more recently been observed impersonating other critical sectors such as health organizations, banks, e-commerce platforms, law enforcement, and social media platforms. The attacks primarily target users in the United States, Argentina, Mexico, the UK, France, Germany, Malaysia, and other countries. Palo Alto has claimed Smishing Triads attacks constantly evolve, warning those in targeted sectors.

Health-ISAC advises its members to treat any foreign or unsolicited messages with caution. As a mitigating practice, members should verify senders before interacting with potentially malicious links or attachments.

Vulnerabilities & Exploits

Italian Spyware Menace: LeetAgent Delivered via Critical Chrome Zero-Day

Summary

- Italian-made LeetAgent spyware exploited a Chrome zero-day flaw, tracked as CVE-2025-2783, to execute espionage attacks targeting Russian organizations via phishing.

Analysis & Action

On October 27, 2025, Kaspersky released a report regarding a now-patched zero-day vulnerability in Google Chrome, tracked as CVE-2025-2783 (CVSS Score: 8.3), being actively exploited in a campaign they dubbed Operation ForumTroll.

In this campaign, attackers used phishing emails disguised as invitations to a forum to target organizations in Russia. Simply clicking the malicious link in a Chromium browser triggers the exploit, which bypasses the sandbox to deliver LeetAgent spyware. The spyware is attributed to the Italian firm Memento Labs (formerly Hacking Team). This operation highlights the growing use of sophisticated commercial surveillance tools.

While the health sector was not explicitly listed as a primary target in this campaign, Health-ISAC still advises its members to immediately update Chrome and all Chromium-based browsers to patch the zero-day flaw (CVE-2025-2783).

Trends & Reports

81% Router Users Have Not Changed Default Admin Passwords, Exposing Devices to Threat Actors

Summary

- A late 2025 survey reveals that most router users have never changed their default admin password, putting devices at significant risk.

Analysis & Action

Recent Broadband Genie survey reports highlight 81% of broadband users have never changed administrative passwords for their routers, leaving them at risk of malware deployment from threat actors.

The findings suggest widespread negligence, highlighting that most users set up their routers with minimal configurations, leaving openings for threat actors to find admin credentials on the open web. Due to this, threat actors can gain access to devices, facilitate surveillance, instate DNS tampering, pivot internally, and install persistent malware. These oversights mark routers as a prime launchpad for phishing operations, botnets, and campaigns attempting data exfiltration.

Health-ISAC advises its members to consider modifying administrative credentials beyond their default settings, enabling firewalls, and backing up sensitive data to mitigate similar cyber risks.

CrowdStrike: 76% of Organizations Struggle to Combat AI Attacks

Summary

- Recent reports from CrowdStrike highlight a global struggle to keep up with continued attacks leveraging AI, leading to the consideration of AI-based protections.

Analysis & Action

CrowdStrike’s State of Ransomware 2025 report highlights a global issue of organizations' traditional defenses struggling to compete with growing AI-powered attacks.

The report states 76% of organizations have dealt with this struggle, with 89% now considering AI-based protections to weaken the gap. The report still tops phishing as a top attack vector, as 87% of survey respondents say AI use and deepfakes are becoming a primary driver for ransomware attacks in the future. Indicators from the report indicate that 83% of organizations that paid their ransom saw themselves hit again, and 93% of cases saw their data stolen anyway.

Health-ISAC advises its members to consider deploying API security and strengthening access controls as proactive mitigative practices against AI-powered threats.

Privacy, Legal & Regulatory

Cybersecurity Executive Charged with Stealing and Selling Trade Secrets to Russia

Summary

- Peter Williams, a former director for L3Harris’ Trenchant division, allegedly stole trade secrets belonging to two unnamed companies and sold them to a Russian-based buyer.

Analysis & Action

A former Trenchant director, Peter Williams, has been sued for stealing and selling trade secrets from the L3Harris cyber division to a Russian buyer.

The Australian national responsible for leading computer networks, vulnerability research, and offensive cyber weapon development operations for almost a year, allegedly obtained undisclosed information belonging to two companies between April 2022 and June 2025. The former employee reportedly gained $1.3 million from the associated sales. While the Department of Justice has not shared details on which trade secrets were involved, it has confirmed Williams shared the information with a buyer based in Russia.

Health-ISAC advises its members to employ a least privilege model, encrypt all stored and in-transit data, and use data loss prevention (DLP) tools to mitigate insider threats.

United Nations' First Global Cybercrime Treaty Sparks Debate Over Privacy and Surveillance

Summary

- During the recent summit in Hanoi, Vietnam, several nations signed the UN Convention against Cybercrime, the first global legal framework that combats cybercriminal activity.

Analysis & Action

More than 60 countries have signed the first global cybercrime treaty, the UN Convention against Cybercrime, over the weekend in Hanoi, Vietnam.

The treaty establishes the first global legal framework for investigating and prosecuting cybercriminal activity, with new mechanisms for cross-border evidence sharing. It will also focus on providing nations in the Global South with resources and support to counteract evolving threats. Some countries that agreed to the current terms include the United Kingdom, the European Union, China, Russia, Brazil, and more. The United States did not sign the treaty and continues reviewing its terms. The convention will go into effect 90 days after 40 nations formally ratify it.

Health-ISAC advises its members to monitor any updates about the treaty's ratification in the upcoming days, as legal requirements for participating nations may change.

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)	offseq, cybersecuritynews, securelist, cybernews, trendmicro, cyware, securityweek, redhotcyber, techrepublic, securityweek 1
Report Source(s)	Health-ISAC

Alert ID 4dc92096

View Alert

Share Feedback

was this helpful? |

Tags LeetAgent, SORVEPOTEL, Water Saci, Asseco mMedica, Smishing Triad, CrowdStrike, Artificial Intelligence, WhatsApp, Zero-Day, Google Chrome, Authentication Bypass

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/**