DAILY CYBER HEADLINES

Daily Cyber Headlines

TLP:WHITE

Oct 22, 2025

Today's Headlines:

Leading Story

- Windows SMB Vulnerability Actively Exploited in Attacks

Data Breaches & Data Leaks

- Eticex Hosting Data Breach Exposes Customer Databases
- Bovavet Breach Compromises 18K Veterinary User Records

Cyber Crimes & Incidents

- Threat Actors Used Snappybee Malware and Citrix Flaws to Breach a European Telecommunications Network
- Massachusetts Hospitals Experiencing Disruption Due to Cyberattack

Vulnerabilities & Exploits

- Apache Syncope Groovy RCE Vulnerability Let Attackers Inject Malicious Code

Trends & Reports

- Ransomware Payouts Surge to $3.6M Amid Evolving Tactics

Privacy, Legal & Regulatory

- Myanmar Military Shuts Down Major Cybercrime Center and Detains Over 2,000 People
- Italy Locks Down its Digital, 5G Security

Upcoming Health-ISAC Events

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

Leading Story

Windows SMB Vulnerability Actively Exploited in Attacks

Summary

- CISA has released an urgent alert, warning of a severe flaw in Microsoft Windows SMB Client, posing risks of privilege escalation from threat actors.

Analysis & Action

CISA is issuing warnings regarding a severe flaw in Microsoft Windows Server Message Block (SMB) Client, tracked as CVE-2025-33073.

The vulnerability, linked to CWE-284, stems from improper access control, posing risks of privilege escalation from threat actors. Exploitation of the flaw sees a malicious actor crafting a script intending to trick a victim's machine into initiating an SMB connection back to the system belonging to the attacker. This process forces authentication, granting the threat actor unauthorized access and allowing full control of compromised devices. CISA has warned that these attacks mirror techniques used by threat groups such as Conti and LockBit, warning of data exfiltration and malware deployment risks to organizations.

Health-ISAC advises its members to consider regulating vulnerability scans and enforcing least privilege access as mitigating strategies to prevent vulnerability exposure.

Data Breaches & Data Leaks

Eticex Hosting Data Breach Exposes Customer Databases

Summary

- Eticex Hosting suffered a data breach, exposing customer databases and payment information. The hacker demanded a $10,000 ransom to prevent data deletion and further exposure.

Analysis & Action

Eticex Hosting, a Turkish web hosting provider, has suffered a significant data breach, exposing customer databases, website files, and payment-related data. The threat actor demands a $10,000 ransom to prevent deletion or further distribution of the stolen information.

The attacker claims access to complete SQL databases and critical customer information, suggesting a significant compromise of Eticex's servers. The incident points to potential weaknesses in data protection, access controls, and overall cybersecurity hygiene within the hosting infrastructure.

Health-ISAC recommends that its members immediately assess the security posture of third-party vendors, monitor for leaked customer or credential data, and review backup integrity and incident response plans to ensure readiness against similar data breach and extortion threats.

Bovavet Breach Compromises 18K Veterinary User Records

Summary

- Bovavet suffered a data breach exposing over 18,000 user records, including personal, professional, and payment information. The stolen database is reportedly being sold on the dark web.

Analysis & Action

Bovavet, an Australian online supplier for veterinary professionals, reportedly suffered a data breach that exposed over 18,000 user records, including full names, email addresses, phone numbers, billing/shipping addresses, and veterinary registration & tax numbers.

The breach exposed a wide range of sensitive personal, professional, tax, and registration details, highlighting major security failures. The attackers reportedly sell the entire database, posing significant risks to affected individuals and organizations.

Health ISAC recommends that its members immediately review vendors handling professional and sensitive datasets, monitor for exposed credentials or records tied to their workforce or partners, and ensure strong access controls, encryption, and incident response plans are in place to minimise exposure.

Cyber Crimes & Incidents

Threat Actors Used Snappybee Malware and Citrix Flaws to Breach a European Telecommunications Network

Summary

- Salt Typhoon has been observed targeting a European telecommunications company's Citrix NetScaler Gateway appliance to deploy the Snappybee malware for persistence.

Analysis & Action

Darktrace reported that a Chinese cyber-espionage group, Salt Typhoon, exploited a Citrix NetScaler Gateway appliance to infiltrate a European telecommunications company's network. The exact vulnerabilities exploited were undisclosed.

The threat actors allegedly obtained initial access in July of this year, masquerading their activity with SoftEther VPN and using their foothold to target the Citrix Virtual Delivery Agent (VDA) hosts in the victim's Machine Creation Services (MCS). Salt Typhoon then leveraged DLL-side loading techniques to deliver the Snappybee malware via legitimate antivirus software to establish persistence. The company quickly identified the intrusion and contained the malicious activity.

Health-ISAC recommends that its members deploy endpoint detection software and actively monitor network activity to mitigate potential intrusions.

Massachusetts Hospitals Experiencing Disruption Due to Cyberattack

Summary

- Two Heywood Healthcare hospitals were recently impacted by a cyberattack that caused major network outages and temporary operational disruptions.

Analysis & Action

Heywood Hospital and Athol Hospital were recently impacted by a cyberattack that resulted in a significant network outage.

The attack, detected last week, disrupted the hospital's network connection, email system, and phone lines. As a precautionary measure, the hospital immediately shut down the affected systems, resulting in the temporary closure of the emergency departments and delays in radiology and laboratory services. There are no indications

of a ransomware attack or that data has been exfiltrated, but investigations are ongoing.

Health-ISAC advises its members to consider network segmentation, actively monitor network activity, and establish comprehensive incident response plans as mitigation measures to potential threats.

Vulnerabilities & Exploits

Apache Syncope Groovy RCE Vulnerability Let Attackers Inject Malicious Code

Summary

- A vulnerability in Apache Syncope exposes the open-source identity management system to remote code execution.

Analysis & Action

A flaw in Apache Syncope, tracked as CVE-2025-57738, has been identified. It exposes the open-source identity management system to remote code execution (RCE) attacks.

The flaw stems from an absence of a sandbox environment, potentially allowing threat actors to compromise systems entirely. Threat actors can exploit this flaw by creating a Groovy implementation, binding it to a report, and triggering its execution through REST endpoints. In doing this, malicious code can be executed under the Syncope service account. The flaw has been identified to impact Apache Syncope versions before 3.0.14 and 4.0.2. Apache has since addressed the issue, introducing a Groovy

sandbox to block malicious operations and asking users to upgrade immediately.

Health-ISAC advises its members to consider network segmentations and regularly monitor log activity as proactive mitigations to similar vulnerabilities.

Trends & Reports

Ransomware Payouts Surge to $3.6M Amid Evolving Tactics

Summary

- Recent reports indicate the average ransomware payment has risen to $3.6 million this year, underscoring a significant increase from the previous year despite overall attacks lessening.

Analysis & Action

A 2025 Global Threat Landscape Report from ExtraHop highlights that ransomware payouts have increased to $3.6 million on average this year, indicating a 44% increase from the year prior.

The rise in average payouts comes despite a smaller number of overall attacks, rather than highlighting a higher level of attacks' intensity. Of the organizations surveyed, 70% paid ransom, health and government sectors were observed facing the highest financial burdens, both having payouts of around $7.5 million. Threat groups such as RansomHub, LockBit, and DarkSide were seen to be leading actors in these attacks. Moreover, the report underscores cloud

infrastructure (53.8%), third-party integrations (43.7%), and generative AI applications (41.9%) as the sources with the highest cybersecurity risks, as methods such as phishing (33.7%), software vulnerabilities (19.4%), and supply chain compromises (13.4%) remain leading methods for threat actor infiltration.

Health-ISAC advises its members to verify senders before interacting with foreign content, regularly back up data, and leverage reputable antivirus software as mitigating practices.

Privacy, Legal & Regulatory

Myanmar Military Shuts Down Major Cybercrime Center and Detains Over 2,000 People

Summary

- A major online scam operation has been shut down by the Myanmar military, seeing over 2,000 people detained, along with dozens of Starlink satellite internet terminals being seized.

Analysis & Action

An extensive online scam operation has been shut down by the Myanmar military, seeing over 2,000 detained individuals and dozens of seized Starlink satellite terminals.

The development came as part of the Myanmar military's operations to suppress online fraud, illegal gambling, and cross-border cybercrime. Details state the shutdown took place after Myanmar's army raided KK Park, a well-known and documented cybercrime

center, in early September. Centers such as these are known for recruiting workers under the guise of legitimate jobs, holding them captive to perform criminal activities. The operation found 260 buildings to have been unregistered, seizing their equipment along with 30 sets of Starlink satellite terminals. Furthermore, 2,198 individuals were detained as a part of the shutdown.

Health-ISAC advises its members to consider regularly backing up critical data and implementing access controls as proactive mitigations to looming threats.

Italy Locks Down its Digital 5G Security

Summary

- Undersecretary Alfredo Mantovano recently signed a decree implementing Italy's Law 90/2024, strengthening the nation's cybersecurity stance by including 4G and 5G devices in its list of IT goods and services.

Analysis & Action

Italy's undersecretary, Mantovano, signed a decree on October 2 to implement Law 90/2024, the nation's key cybersecurity reform.

The National Cybersecurity Agency (NCA) proposed the measure to counteract the evolving geopolitical threat landscape while strengthening the nation's stance on cybersecurity. The legislation updates the regulation for IT devices and services, adding 4G and 5G devices and systems under the same cybersecurity requirements. Future evolutions of these technologies are also included under the decree.

Health-ISAC encourages its members to follow any updates to federal regulations as mitigations to the evolving threat landscape.

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)	cyware, thehackernews, hipaajournal, securityweek, cyware 1, decode39, cybersecuritynews, infosecurity-magazine, dailydarkweb, cybersecuritynews 1, dailydarkweb 1, cyware 2
Report Source(s)	Health-ISAC

Alert ID 7fe666ac

View Alert

Share Feedback

was this helpful? |

Tags Snappybee, Bovavet, Eticex, Injection Attack, Apache Syncope, Citrix, Citrix ADC and Gateway, Citrix ADC, RCE, SMB, Apache, Remote Code Execution

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/**