DAILY CYBER HEADLINES

Daily Cyber Headlines

TLP:WHITE

Oct 17, 2025

Today's Headlines:

Leading Story

- Windows Improper Access Control Vulnerability Exploited in Attacks

Data Breaches & Data Leaks

- Prosper Data Breach Exposed 17.6 Million People's Information

Cyber Crimes & Incidents

- PhantomVAI Loader Attacking Organizations Worldwide to Deliver AsyncRAT, XWorm, FormBook, and DCRAT
- Chinese Threat Group Jewelbug Quietly Infiltrated Russian IT Network for Months

Vulnerabilities & Exploits

- Adobe Experience Manager Forms Zero-Day Vulnerability Exploited in Attacks

Trends & Reports

- Extortion and Ransomware Drive Over Half of Cyberattacks

Privacy, Legal & Regulatory

- New Cybersecurity Law Protects Oklahoma's Data, Pressures Businesses to Act
- California Enacts 30-Day Data Breach Notification Deadline

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

Windows Improper Access Control Vulnerability Exploited in Attacks

Summary

- CISA has added a critical flaw in Microsoft Windows that allows threat actors to gain higher-level permissions and compromise networks to its KEV catalog.

Analysis & Action

CISA has recently added a critical flaw in Microsoft Windows, tracked as CVE-2025-59230 (CVSS v3.1 score of 7.8), to its Known Exploited Vulnerabilities (KEV) catalog.

The vulnerability, classified under CWE-284, stems from improper access control within the Windows Remote Access Connection Manager service. The flaw allows a user with authorized access to escalate their privileges to higher-level permissions, potentially compromising entire networks. Successful exploitation could result in threat actors manipulating system files, installing malware, or pivoting to other machines within the same network. Microsoft has since released patches for the flaw as part of its October 2025 Patch Tuesday, urging users to deploy the update immediately.

Health-ISAC advises its members to consider leveraging reputable endpoint protection software, deploying firewalls, and ensuring secure device configurations as additional mitigative strategies.

Data Breaches & Data Leaks

Prosper Data Breach Exposed 17.6 Million People's Information

Summary

- Prosper, a peer-to-peer lending platform, has experienced a significant data breach, compromising the data of 17.6 million individuals.

Analysis & Action

Prosper has confirmed that it suffered a data breach that affected the sensitive personal and financial data of 17.6 million individuals.

The breach was initially acknowledged on September 18, 2025, although the scope of individuals impacted only recently became clear after adding a dataset to HIBP. Compromised data from the breach includes full names, email addresses, physical addresses, dates of birth, government IDs, Social Security Numbers, employment statuses, income levels, credit statuses, IP addresses, and browser user-agent strings. The breach impacted both current and prospective customers. The company has yet to release any information regarding the initial attack vector at the time of the reports. Those impacted face heightened risk of targeted phishing, fraud, and/or identity theft, cautioned to maintain elevated vigilance.

Health-ISAC advises its members to consider encrypting all sensitive data, regularly backing up data, and segmenting networks when possible as mitigations against data breaches and leaks.

Cyber Crimes & Incidents

PhantomVAI Loader Attacking Organizations Worldwide to Deliver AsyncRAT, XWorm, FormBook, and DCRat

Summary

- A multi-stage malware campaign leveraging PhantomVAI Loader has been observed targeting organizations globally, distributing information-stealing malware.

Analysis & Action

A multi-staged malware campaign targeting organizations globally has been observed utilizing the PhantomVAI loader to distribute malicious information-stealing malware.

The chain of attack originates from crafted phishing emails, targeting sectors such as manufacturing, education, health, technology, utilities, and government. Injection begins once an unsuspecting user receives the malicious email, which contains attachments disguised to look like legitimate business communications such as sales inquiries, payment notifications, and/or legal matters. Upon opening, malicious Base64-encoded PowerShell commands execute, concealing the loader payload. The PowerShell script then decodes, allowing PhantomVAI Loader to execute and deploy a final payload, establishing persistence and injecting into legitimate system processes to deliver information-stealing malware.

Health-ISAC advises its members to remain cautious of emails from foreign senders, confirming validity before interacting with links or attachments as a proactive mitigation against similar attacks.

Chinese Threat Group Jewelbug Quietly Infiltrated Russian IT Network for Months

Summary

- Jewelbug, a Chinese-based threat actor, has been attributed to a five-month-long intrusion on a Russian IT service provider’s network earlier this year, along with attacks on South American and APAC organizations.

Analysis & Action

The Chinese threat group, Jewelbug–associated with the CL-STA-0049, Earth Alux, and REF7707 clusters–has been linked to a five-month-long intrusion on a Russian IT service provider's network.

The attack on the IT service provider leveraged a renamed version of the Microsoft Console Debugger executable file to run commands on the shell, bypass the allowlisting protocols, and disable security tools. Jewelbug also gained access to the company's code repositories, exfiltrated data to Yandex Cloud, and cleared Windows Event Logs to avoid detection. The group is also known for targeting government entities and critical infrastructure in Latin America and the Asia-Pacific (APAC) region, leveraging malware such as Vargeit, Cobeacon, and FinalDraft. Recent incidents involved an attack on a large South American government organization in July 2025 and two companies in the APAC region in late 2024.

Health-ISAC recommends that its members deploy endpoint detection and response (EDR) tools and actively monitor network activity as mitigation measures.

Vulnerabilities & Exploits

Adobe Experience Manager Forms Zero-Day Vulnerability Exploited in Attacks

Summary

- After discovering recent in-the-wild exploits, CISA added a previously patched maximum-severity vulnerability in the Adobe Experience Manager Forms, CVE-2025-54253, to its KEV catalog.

Analysis & Action

CISA has added CVE-2025-54253, a vulnerability in the Adobe Experience Manager Forms (AEM Forms), to its Known Exploited Vulnerabilities (KEV) catalog after recent reports of in-the-wild exploitation.

The vulnerability, which had been patched earlier in August, affects the Java Enterprise Edition (JEE) and enables remote code execution. Threat actors can exploit the flaw without user interaction and gain full control of the compromised servers for further network compromise. Mandiant has noted the recent exploits targeted unpatched instances in cloud environments, with a particular incident in Europe involving the deployment of malware and data exfiltration. CISA is requiring all federal agencies to apply the patches by November 14.

Health-ISAC encourages its members to establish regular patching schedules, actively scan for system vulnerabilities, and monitor network activity as mitigation measures.

Trends & Reports

Extortion and Ransomware Drive Over Half of Cyberattacks

Summary

- Microsoft's latest Digital Defense Report highlights the trends and threats of the current cyber landscape, noting a

preference for financially motivated campaigns and a rise in identity-based attacks.

Analysis & Action

The latest Annual Microsoft Digital Defense Report shares findings on the trends and threats observed between July 2024 and June 2025.

Microsoft revealed that more than half of the cyberattacks in the past year were financially motivated, often driven by ransomware or extortion tactics. Large-scale campaigns by nation-state actors were also highlighted in the report, with mentions of attacks primarily targeting public service organizations and government entities. Microsoft also noted a sharp rise in the use of AI for automation within attack chains, with both independent threat actors and nation-state groups leveraging tools to target companies. Lastly, the report highlights a surge of 32% in identity-based attacks, facilitated mainly by credential leaks and the use of information-stealing malware.

Health-ISAC recommends that its members stay vigilant of the evolving threat landscape, deploy endpoint detection and response (EDR) solutions, and employ phishing-resistant multi-factor authentication to mitigate emerging threats.

Privacy, Legal & Regulatory

New Cybersecurity Law Protects Oklahoma’s Data, Pressures Businesses to Act

Summary

- Oklahoma’s new cybersecurity law, Senate Bill 626, mandates companies to report data breaches.

Analysis & Action

Oklahoma’s new cybersecurity law, Senate Bill 626, is expected to take effect soon. The law requires businesses to act according to it.

Also known as the Security Breach Notification Act, the bill was introduced in 2024, though not passed until 2025. The act will require companies to report data breaches to the attorney general's office, allowing for investigations to take place regarding how the breach happened and if reasonable safeguards were in place to prevent it. The bill intends to urge businesses to create more secure security standards, incentivizing practices that may have been procrastinated in the past. Civil penalties will be determined based on a breach's magnitude, the extent of the company or individual impacted, and any failure to provide notice. The law is expected to go into effect on January 1, 2026.

Health-ISAC advises its members to regularly conduct risk assessments and audits and maintain secure backups as proactive mitigations to persistent cyber threats.

California Enacts 30-Day Data Breach Notification Deadline

Summary

- California’s governor signed Senate Bill 446, which will become effective in 2026 and strengthen current data breach requirements for businesses operating in the state.

Analysis & Action

California's governor has signed Senate Bill 446, which is expected to strengthen the state's current stance on cybersecurity regulations, particularly for data breaches.

The legislation, set to become effective in 2026, will require all businesses operating in California to report any data breaches to state residents within 30 calendar days of discovering the incident. For companies with more than 500 affected customers, notifications must be submitted to the Attorney General within 15 days of notifying customers. In addition, the amendment clarifies collaboration between the government and organizations for more effective investigations.

Health-ISAC encourages its members to follow all local and federal regulations pertaining to cybersecurity requirements and incident reporting to mitigate the evolving threat landscape.

Health-ISAC Cyber Threat Level

On September 18, 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:

NPM Worm Impact, QR Code Phishing, Typosquatting Campaigns, Remote IT Worker Fraud, and **Job Posting Scams.**

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)	newson6, thehackernews, cybersecuritynews, cyberinsider, consumerfinanceandfintechblog, microsoft, cybersecuritynews 1, cybersecuritynews 2
Report Source(s)	Health-ISAC

Alert ID c6c1e3d6

View Alert

Share Feedback

was this helpful? |

Tags Adobe Experience Manager Forms, Jewelbug, PhantomVAI, Prosper, XWorm, dcRAT, AsyncRAT, FormBook, Microsoft Windows, Improper Access Control, 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/**