

Daily Cyber Headlines

Daily Cyber Headlines

TLP:WHITE

Alert ID : 4c78d3c5

Oct 13, 2025, 05:20 AM



Today's Headlines:

Leading Story

- FBI Takes Down BreachForums Portal Used for Salesforce Extortion

Data Breaches & Data Leaks

- Georgia DHS Warns Threat Actors Accessed Employee Email Accounts with Personal Data

Cyber Crimes & Incidents

- Cisco, Fortinet, Palo Alto Networks Devices Targeted in Coordinated Campaign
- Microsoft Warns of Threat Actors Compromising Employee Accounts to Steal Salary Payments

Vulnerabilities & Exploits

- 7-Zip Vulnerabilities Let Attackers Execute Arbitrary Code Remotely
- Juniper Networks Patches Critical Junos Space Vulnerabilities

Trends & Reports

- 59% of Organizations Hit by MF Security Incidents Amid Weak Encryption and Oversight

Privacy, Legal & Regulatory

- New Cyber Crime Bill and RM32 Million Boost to Tackle Scams in Malaysia

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
- [European Summit](#) – Rome, Italy – October 14-16, 2025
- [Fall Americas Summit](#) – Carlsbad, California – December 1-5, 2025

Additional Information

Leading Story

[FBI Takes Down BreachForums Portal Used for Salesforce Extortion](#)

Summary

- The FBI has seized all domains from BreachForums' web infrastructure, previously used to leak corporate data stolen in ransomware attacks.

Analysis & Action

The FBI has seized all domains from the ShinyHunters-operated BreachForums web infrastructure, which was formerly used to leak corporate data stolen in ransomware attacks.

ShinyHunters confirmed BreachForums had been seized, adding that all BreachForums database backups since 2023 have been compromised, along with all escrow databases and backend servers. Despite this, the group's dark web data leak site remains online. The cybercriminals have further stated that the seizure has not impacted their Salesforce campaign, as their leak site lists several companies affected, including FedEx, Disney/Hulu, Home Depot, Google, McDonald's, and many others.

Health-ISAC advises its members to regulate offline backups and encrypt sensitive data as a mitigating strategy against similar campaigns.

Data Breaches & Data Leaks

Georgia DHS Warns Threat Actors Accessed Employee Email Accounts With Personal Data

Summary

- Georgia's Department of Human Services has warned that residents' personal information might have been exposed in a breach earlier this year.

Analysis & Action

Georgia's Department of Human Services has issued warnings, cautioning that some personal information belonging to residents may have been exposed after a breach earlier in the year.

Information reportedly exposed in the breach included names, Social Security numbers, driver's license details, medical and insurance information, and financial account numbers. Officials don't believe any misuse of the exposed data has occurred at the time of the reports. Furthermore, it remains unclear how long impacted email accounts were exposed or when the unauthorized access occurred. Despite no evidence of information being stolen or used for fraud, residents have been advised to monitor their bank accounts and credit reports.

Health-ISAC advises its members to conduct regular security audits and monitor network activity as mitigative strategies against data breaches and leaks.

Cyber Crimes & Incidents

Cisco, Fortinet, Palo Alto Networks Devices Targeted in Coordinated Campaign

Summary

- GreyNoise identified that the recent Cisco and Palo Alto infrastructure scanning activities were launched from IP addresses under a shared subnet and may be linked to a recent spike in Fortinet VPN brute force attempts.

Analysis & Action

GreyNoise researchers discovered that the recent attacks on Cisco and Palo Alto infrastructure originated from IP addresses under the same subnet, indicating a coordinated campaign potentially by the same threat actor.

The research team had recently released information on a significant spike in scanning activity on the Palo Alto Networks GlobalProtect login portals. Similarly, the threat

intelligence company disclosed a series of scanning attempts targeting Cisco ASA in early September, soon followed by two zero-day vulnerability disclosures by Cisco. The latest reports, however, indicate that the scanning campaigns on both companies' infrastructure were launched from IPs in the same subnets. GreyNoise also identified the campaign as possibly linked to recent brute forcing attacks on Fortinet VPNs, which share the same source subnet and TCP fingerprints as Cisco and Palo Alto attacks.

Health-ISAC advises its members to scan for system vulnerabilities, monitor network activity, and promptly apply any available patches to mitigate potential intrusions.

[Microsoft Warns of Threat Actors Compromising Employee Accounts to Steal Salary Payments](#)

Summary

- Microsoft disclosed a new campaign by Storm-2657 that targets employee accounts lacking phishing-resistant MFA protections to steal salary payments from human resources software and SaaS platforms.

Analysis & Action

The Microsoft Threat Intelligence Group has identified a new campaign by Storm-2657 targeting US organizations and universities to redirect salary payments.

The threat actors primarily exploit employees' access to third-party human resources software and software-as-a-service (SaaS) platforms, such as Workday. The campaign, labeled payroll pirate, leverages adversary-in-the-middle (AitM) phishing techniques to harvest credentials and multi-factor authentication (MFA) codes. Storm-2657 then uses the compromised credentials to gain initial access to Exchange Online accounts, particularly from accounts lacking phishing-resistant MFA protections. Threat actors then establish their phone numbers as MFA devices and block notification emails from the compromised SaaS management platforms to hide any modifications to payroll configurations that may alert victims of the intrusion.

Health-ISAC recommends that its members actively monitor system activity and enforce multi-factor authentication for all accounts as mitigation measures.

Vulnerabilities & Exploits

[7-Zip Vulnerabilities Let Attackers Execute Arbitrary Code Remotely](#)

Summary

- Two severe vulnerabilities in the open-source file archiver, 7-Zip, permit remote threat actors to execute arbitrary code.

Analysis & Action

Two vulnerabilities in the open-source file archiver 7-Zip, tracked as CVE-2025-11001 and CVE-2025-11002 (both with a CVSS 3.0 score of 7.0), allow remote threat actors to execute arbitrary code.

The flaws impact all versions of the software before the most recent release. Both vulnerabilities stem from improper handling of symbolic links embedded in ZIP archives. With this, threat actors can create malicious ZIP files containing crafted data for exploitation. Once a user with a vulnerable version of 7-Zip decompresses the archive, processes can be manipulated for directory traversal, allowing for writing files outside the intended destination folder. Successful exploitation permits threat actors to execute arbitrary code, resulting in complete system compromise, data theft, or deployment of malware such as ransomware. Users have been advised to install the most recent patches for 7-Zip immediately to prevent exploitation.

Health-ISAC advises its members to consider employing firewalls, segmenting networks, and implementing the principle of least privilege as additional mitigations to similar vulnerabilities.

[Juniper Networks Patches Critical Junos Space Vulnerabilities](#)

Summary

- Juniper Networks has released security patches for nearly 220 vulnerabilities in its Junos OS, Junos Space, and Junos Space Security Director and Policy Enforcer platforms.

Analysis & Action

Juniper Networks has released security updates for approximately 220 vulnerabilities in several Junos Space products, including nine critical-severity flaws.

The October 2025 security advisory addressed 162 vulnerabilities in Junos Space, including a high-severity denial-of-service (DoS) flaw and 24 cross-site scripting (XSS) vulnerabilities that could enable threat actors to execute commands with administrative privileges. The company also addressed 15 medium-severity vulnerabilities in the Junos Space Security Director component and a high-severity flaw in Junos Space Director Policy Enforcer. Junos OS also presented several bugs, with the latest updates

addressing many medium-severity issues. The company has noted it is not aware of any active exploits in the wild.

Health-ISAC encourages its members to establish regular patching schedules and apply any emergency updates, as needed, to mitigate potential exploits.

Trends & Reports

[59% of Organizations Hit by MFT Security Incidents Amid Weak Encryption and Oversight](#)

Summary

- A new report connects a rise in MFT breaches to poor encryption, weak governance, and overlooked integrations.

Analysis & Action

The Kiteworks 2025 report details increased managed file transfer (MFT) incidents, linking them to poor encryption, weak governance, and overlooked integrations.

The report highlights that 59% of organizations experienced these MFT incidents in the past year. Organizations with mature governance reported significantly fewer incidents, including regular access reviews, time-limited credentials, and automated deprovisioning. Furthermore, 63% of organizations have not integrated MFT systems with SIEM/SOC platforms, creating blind spots for threat actors to exploit without triggering alerts or detection. These risks loom as AI-related threats continue to grow, with 28% of organizations stating that they have already experienced incidents involving AI misuse, emphasizing a need for strengthening security measures collectively.

Health-ISAC advises its members to consider automated patch management systems, ensure endpoint protection, and encrypt sensitive data as mitigating strategies.

Privacy, Legal & Regulatory

[New Cyber Crime Bill and RM32 Million Boost to Tackle Scams in Malaysia](#)

Summary

- The Malaysian government is expected to introduce the Cyber Crime Bill in early 2026 and invest approximately RM32 million for a more resilient cyber

infrastructure.

Analysis & Action

The Malaysian government is set to present a new Cyber Crime Bill and increase national budget plans to push against cybercrime and strengthen national security.

The new legislation is expected to replace outdated laws and respond more strongly to the evolving threat landscape in early 2026. In addition, the National Cyber Security Agency (NACSA) will be responsible for establishing a new Center for Cryptology and Cyber Security Development. The National Scam Response Centre (NSRC) will also be restructured to work under the Royal Malaysia Police (PDRM) for more effective investigation processes. The proposed 2026 budget plans would include an RM12 million investment in the expansion of the NSRC and an RM20 million investment for enhanced digital forensic systems.

Health-ISAC encourages its members to follow any emerging legislation on privacy and cybersecurity guidelines 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.**

Report Source(s)

Health-ISAC

Reference

[bleepingcomputer](#)
[fintechnews](#)
[cybersecuritynews](#)
[petri](#)
[securityweek](#)
[securityweek 1](#)
[cybersecuritynews 1](#)
[fox5atlanta](#)

Tags

7-Zip Vulnerability, BreachForums, Legislation, Extortion, ShinyHunters, Palo Alto, Data Breaches, Fortinet, Salesforce, Cisco, Microsoft

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