DAILY CYBER HEADLINES

Daily Cyber Headlines

TLP:GREEN

Nov 14, 2025

Today's Headlines:

Leading Story

- New ClickFix Attack Tricks Users with Fake OS Update to Execute Malicious Commands

Data Breaches & Data Leaks

- Everest Ransomware Claims Leading Italian Gas Producer Breach
- Threat Actor Everest Claims Breach of Korpath, Vikor Scientific, and Korgene

Cyber Crimes & Incidents

- Major Cyberattack Disrupts Operations Across Normandy Regional Institutions
- Black Shrantac Ransomware Group Targets Multiple Global Enterprises in Coordinated Attack

Vulnerabilities & Exploits

- Palo Alto PAN-OS Firewall Vulnerability Let Attackers Reboot Firewall by Sending Malicious Packet

Trends & Reports

- Qilin Ransomware Gang Ramps Up Attacks

Privacy, Legal & Regulatory

- Extended State, Local Cybersecurity Grants Present in Shutdown Deal

Upcoming Health-ISAC Events

- Global Monthly Threat Brief
  - Americas – November 25, 2025, 12:00-01:00 PM ET
  - European – November 26, 2025, 03:00-04:00 PM CET
- Fall Americas Summit – Carlsbad, California – December 1-5, 2025

Leading Story

New ClickFix Attack Tricks Users with Fake OS Update to Execute Malicious Commands

Summary

- A new ClickFix campaign has been observed tricking users into installing fake Windows updates that deliver malware, exploiting users' trust.

Analysis & Action

A new ClickFix campaign has been identified, tricking users into installing false Windows updates by leveraging their trust in Microsoft's blue screen of death (BSOD) to deliver malware.

The campaign primarily operates through the groupewadesecurity[.]com domain, often distributed via malvertising or spam links. Once the domain is visited, the link generates a full-screen overlay that mimics Windows OS crashes or update prompts, instructing victims to perform three manual fixes: a Ctrl+Alt+Del restart, entering a bogus command, and downloading a recovery tool. Following these actions permits a threat actor with remote access or the ability to install infostealers and ransomware loaders.

Health-ISAC advises its members to consider restricting unnecessary system utilities, implementing application controls, and enforcing the principle of least privilege as mitigating practices.

Data Breaches & Data Leaks

Everest Ransomware Claims Leading Italian Gas Producer Breach

Summary

- SIAD, a major Italian industrial and chemical gas producer, has had 159 GB of data stolen by Everest Ransomware, now threatening to expose the data.

Analysis & Action

The Everest ransomware gang has stolen 159 gigabytes of data from the major Italian industrial and chemical gas producer, SIAD Group. It is now threatening to expose the data within eight days.

The extent of the breach is unknown at the time of reports, as Everest has not provided any sample data alongside the breach claims, and SIAD Group has yet to acknowledge Everest's assertions. Everest's claims follow the group's targeting of Collins Aerospace's automatic check-in and boarding software, resulting in disruptions at numerous European airports. If Everest's claims are valid, the exposure may result in the producer's inability to deliver consumables to their clients, creating disruptions in the manufacturing, health, and energy sectors, primarily in the EU.

Health-ISAC advises its members to secure data backups, encrypt sensitive data, and conduct regular audits and assessments as mitigative practices.

Threat Actor Everest Claims Breach of Korpath, Vikor Scientific, and Korgene

Summary

- Korpath, Vikor Scientific, and Korgene were reportedly compromised by the threat actor group Everest, who claim to have accessed sensitive internal data from all three organizations. The group has published samples of the alleged stolen information and is threatening to release more.

Analysis & Action

The breach involved unauthorized access to confidential documents, internal communications, and data archives belonging to Korpath,

Vikor Scientific, and Korgene. The affected entities are in the biotechnology and diagnostics sectors, making the incident particularly sensitive.

Everest published samples of the compromised data on its leak site, including financial records, employee details, and operational documents. This suggests a potentially deep intrusion, possibly involving compromised credentials or unpatched system vulnerabilities across multiple organizations.

Health-ISAC recommends that its members enhance monitoring of remote access points, review access controls on sensitive repositories, and enforce multi-factor authentication to prevent unauthorized data exfiltration by threat actors.

Cyber Crimes & Incidents

Major Cyberattack Disrupts Operations Across Normandy Regional Institutions

Summary

- Several regional institutions in Normandy experienced a major cyberattack that disrupted digital services and raised concerns over potential unauthorized access to sensitive data. Authorities have launched investigations to assess the scope of the incident and mitigate further impact.

Analysis & Action

The cyberattack affected multiple public sector organizations, including local governments and healthcare institutions, disrupting online services and internal systems. Emergency protocols were activated, and incident response teams began containment efforts to restore operations.

The disruption primarily affected IT infrastructure, limiting access to internal networks and online portals. Preliminary assessments indicate coordinated activity targeting centralized systems, resulting in operational slowdowns and temporary service unavailability.

Health-ISAC recommends that its members implement advanced endpoint detection, regularly audit system configurations, and maintain segmented network architectures to minimize lateral movement during incidents of this scale.

Black Shrantac Ransomware Group Targets Multiple Global Enterprises in Coordinated Attack

Summary

- Several global firms have been targeted in a ransomware campaign carried out by the cybercriminal group known as Black Shrantac. The attackers reportedly encrypted critical systems and are demanding payment in exchange for the decryption keys, as well as to prevent the exposure of public data.

Analysis & Action

The attack disrupted operations across various industries, with victims reporting system lockouts and encrypted files. The affected organizations are currently assessing the damage and coordinating

incident response efforts to contain the impact and restore operations.

The group deployed ransomware that appears to have bypassed traditional defenses, encrypting files and displaying ransom notes. Preliminary technical indicators point to the use of custom payloads and potential exploitation of remote access vulnerabilities for initial access.

Health-ISAC recommends that its members apply patches to exposed services, monitor for indicators of compromise related to known ransomware behaviors, and maintain offline, encrypted backups to support rapid recovery in the event of system encryption.

Vulnerabilities & Exploits

Palo Alto PAN-OS Firewall Vulnerability Let Attackers Reboot Firewall by Sending a Malicious Packet

Summary

- Palo Alto has disclosed a denial-of-service flaw that allows threat actors to remotely reboot firewalls.

Analysis & Action

A critical denial-of-service flaw has been disclosed by Palo Alto Networks, tracked as CVE-2025-4619 (CVSS v4.0 score: 6.6), posing risks to organizations that rely on Palo Alto firewalls.

The flaw, identified as CWE-754, allows unauthenticated threat actors to remotely reboot firewalls by sending specially crafted packets. Threat actors can exploit the flaw without requiring credentials, authentication, or user interaction. Successful instances result in malicious packets triggering an unexpected firewall reboot. Furthermore, repeated exploitation attempts pose a risk of forcing the firewall into maintenance mode, which can result in disruptions to network operations and potentially leave organizations vulnerable during downtime.

Health-ISAC advises its members to consider increasing bandwidth, implementing rate limiting, and utilizing reputable anti-DDoS services as mitigation measures.

Trends & Reports

Qilin Ransomware Gang Ramps Up Attacks

Summary

- Current trends show an increase in attacks from Qilin ransomware gang, exploiting vulnerable appliances and interfaces in the health, finance, and construction industries.

Analysis & Action

Qilin ransomware has shown an increase in activity throughout the year, targeting small and mid-sized organizations in the health, finance, and construction sectors.

The operation, known for its data exfiltration and file encryption, primarily targets vulnerable VPN appliances and management interfaces within these organizations. The growth of the ransomware group coincides with its adoption of a ransomware-as-a-service model, which has been prevalent over the past two years. Multiple affiliates, such as Scattered Spider, now leverage the platform, making attribution and defense significantly more challenging for organizations and investigators.

Health-ISAC advises its members to regularly patch VPN and remote access devices, consider implementing network segmentation, and assess their ransomware risk as proactive measures for mitigation.

Privacy, Legal & Regulatory

The 2025 Healthcare Cyber Crisis: Unified AI Defense Against $10.3M Breaches

Summary

- Healthcare's fragmented security is failing to keep pace with escalating attacks, necessitating a unified, AI-driven platform to protect patient safety and data.

Analysis & Action

The U.S. healthcare sector is the top-attacked industry, suffering from soaring breach costs and disruptions to patient care due to ransomware, primarily attributed to its rapid digital expansion.

Fragmentation across 20-35 disconnected security tools creates blind spots and alert fatigue, making the sector's inherent complexity its most significant exploit risk.

Health-ISAC advises its members to achieve resilience mandates by transitioning to a unified and advanced, AI-driven platform that provides real-time detection, automated response, and comprehensive visibility across all clinical and operational assets.

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)	scworld, dailydarkweb, paris-normandie, scworld 1, securityboulevard, cybersecuritynews, cybersecuritynews 1, dailydarkweb 1
Report Source(s)	Health-ISAC

Alert ID e0a795f6

View Alert

Share Feedback

was this helpful? |

Tags Black Shrantac, Everest Ransomware, ClickFix, Qilin, PAN-OS, Palo Alto, Firewall

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.  

For more updates and alerts, visit: **https://health-isac.cyware.com/webapp/**