

# WEEKLY INTELLIGENCE REPORT

## TOP ATTACKS AND BREACHES

- Two US banks, Artisans' Bank and VeraBank, [disclosed](#) that customer data was exposed in an August ransomware attack on their vendor, Marquis Software. The vendor was breached via SonicWall vulnerability, and while the banks' own systems were not compromised, researchers estimate the incident may have affected in total up to 1.35 million people across dozens of financial institutions.
- Romania's largest coal-based power producer, Oltenia Energy Complex, has [faced](#) a ransomware attack attributed to the Gentlemen group. The company said files were encrypted and Enterprise Resource Planning systems, email, and the website were disrupted, partially affecting operations, while power supply remained stable and recovery continues.
- Emurasoft, maker of EmEditor software, [reported](#) a website compromise that redirected the homepage download button to a fake installer for 4 days. The installer deployed infostealer malware that harvested credentials and added a rogue extension enabling remote control and cryptocurrency swapping.
- US-based Sedgwick Government Solutions, which manages claims, workforce health, risk, and productivity for government agencies and federal employees, has [experienced](#) a cybersecurity incident. The incident was limited to an isolated file transfer system, with no evidence of access to claims servers. The company notified law enforcement and clients after the TridentLocker ransomware group claimed an attack on December 31.
- Korean Air, South Korean airline, has [suffered](#) a data breach via KC&D Service, a vendor managing inflight catering and duty free. The incident exposed personal data of roughly 30,000 employees, including names and bank account numbers, while customer information was not affected. ClOp claimed responsibility and reportedly exploited an Oracle E-Business Suite flaw.

*Check Point IPS, Threat Emulation and Harmony Endpoint provide protection against this threat (Oracle Multiple Products Remote Code Execution; Ransomware.Win.Clop; Ransomware.Wins.Clop; Ransomware.Wins.Clop.ta.\*)*

- Trust Wallet, a cryptocurrency wallet provider, has [disclosed](#) a second Shai-Hulud supply-chain compromise of its Chrome extension, resulting in approximately \$8.5 million in losses. Using a leaked Chrome store key, attackers published tampered v2.68 which exfiltrated wallet recovery phrases upon unlock.
- European Space Agency (ESA), has [confirmed](#) a cybersecurity incident affecting a very small number of external servers outside its corporate network. ESA began forensic analysis and secured potentially affected devices after a threat actor claimed to have stolen 200GB of source code and access credentials in mid-December.

## VULNERABILITIES AND PATCHES

- Researchers [highlighted](#) CVE-2025-14346, a critical missing-authentication flaw in WHILL Model C2 and Model F power wheelchairs that enables attackers within Bluetooth range to take control. CISA urged immediate mitigations, warning that compromise could manipulate wheelchair movements and cause physical harm in healthcare and public settings. No public exploitation has been reported yet
- Security researchers [disclosed](#) CVE-2025-20700, CVE-2025-20701 (CVSS 8.8) and CVE-2025-20702 (CVSS 9.6) affecting Airoha Bluetooth SoCs. The flaws enabling unauthenticated access to the RACE protocol, arbitrary memory operations, and nearby takeover of headphones to extract link keys and impersonate devices to access paired smartphones.
- A patch has been [released](#) for CVE-2025-47411, an important privilege escalation in Apache StreamPipes 0.69.0 to 0.97.0 caused by flawed user ID creation enabling JWT token manipulation. Attackers can impersonate existing administrators to gain full control.
- IBM API Connect, an enterprise API management platform, is [affected](#) by a critical authentication bypass vulnerability (CVE-2025-13915, CVSS 9.8) enabling remote unauthorized access without credentials. The flaw impacts versions 10.0.8.0 through 10.0.8.5 and 10.0.11.0, with patches and iFixes available; no exploitation has been reported.

## THREAT INTELLIGENCE REPORTS

- Researchers [exposed](#) a new APT36 cyber espionage campaign targeting Indian government, academic, and strategic institutions. The Pakistan affiliated group delivers ZIP attachments disguised as PDFs that install ReadOnly and WriteOnly malware, which enables remote control, steals data, monitors clipboards, captures screenshots, and maintains access.
- DarkSpectre, a Chinese affiliated threat actor, has [compromised](#) 8.8 million Chrome, Edge, and Firefox users globally via campaigns including ShadyPanda, Zoom Stealer, and GhostPoster. The group employs malicious browser extensions with tactics such as time-bomb activation, dormant sleepers, PNG steganography, and heavy JavaScript obfuscation, exfiltrating corporate meeting data while impersonating videoconferencing tools and abusing browser platform permissions.
- Security researchers [discovered](#) two Chrome Web Store extensions, Chat GPT for Chrome with GPT-5 and AI Sidebar, that exfiltrate ChatGPT and DeepSeek chat histories, along with users' browsing activity, every 30 minutes. The extensions collectively have over 900,000 installations, and one holds a Google Featured badge.
- Researchers [identified](#) the rapid expansion of the Kimwolf botnet, which has infected more than 2 million devices globally by abusing residential proxy networks to reach local devices behind home routers. The campaign leverages insecure Android TV boxes and digital photo frames to enable DDoS, ad fraud, account takeover, and mass scraping.