
Weekly Cybersecurity Briefing (24 November – 30 November 2025)

CyberSecBrief Team

CyberSecBrief delivers high-impact, concise cybersecurity updates, cutting through the noise to focus on what matters most. Every day, you will find a curated briefing featuring essential news, supported by trusted feeds and advisories from reputable sources. Weekly and monthly recaps offer broader analysis, highlighting key trends, emerging threats, and significant developments — helping you stay informed with minimal effort.

For more briefings, visit CYBERSECBRIEF.COM.



December 1, 2025

Overview of the Week

The week saw a significant rise in supply-chain threats, ransomware disruptions, and breaches at major institutions.

- **Shai-Hulud campaign expanded** across both npm and Maven Central repositories, infecting thousands of packages to steal credentials and compromise multi-cloud environments.
- **ClickFix campaign** utilised steganographic PNG files and fake Windows Update screens to deliver infostealer malware, marking a new trend in browser-based attacks.
- **Matrix Push C2** abused browser push notifications for phishing and malware delivery, taking advantage of notification permissions to track and redirect users.
- **Harvard University and Dartmouth College** disclosed breaches, with attackers exploiting Oracle E-Business Suite zero-days to access sensitive data.
- **Ransomware attack on OnSolve CodeRED** led to nationwide emergency alert system disruptions in the US, highlighting growing vulnerabilities in critical infrastructure.
- **Gainsight breach** revealed unauthorised access to Salesforce-linked applications, affecting multiple clients and prompting integration suspensions.

Hot Topics, CVEs and APTs This Week

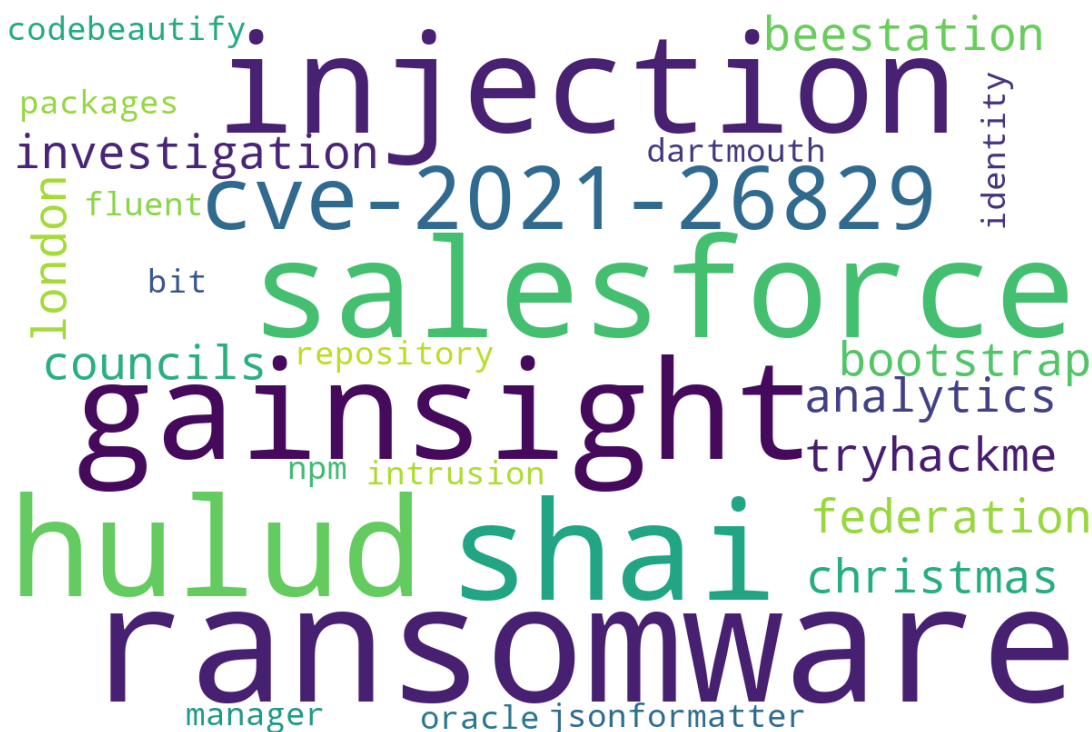
Hot topics:

- Ransomware
- Shai Hulud
- Dartmouth
- Gainsight
- Injection
- Salesforce
- Federation
- Across The
- Jsonformatter And Codebeautify

- Scattered Lapsus Hunters

APT groups:

- LAPSUS\$
- INC Ransom
- Salt Typhoon
- TA569
- ToddyCat
- Akira
- Moonstone Sleet
- Patchwork
- Scattered Spider
- Charming Kitten
- Contagious Interview

Key cybersecurity topics of the week:

Highlights of the Week

Shai-Hulud Campaign Expands Through Trojanised npm Packages

The Shai-Hulud supply-chain attack expanded its reach by injecting credential-stealing malware into npm packages, impacting thousands of repositories and cloud environments. Attackers used compromised maintainer accounts to propagate the attack.

Sources:

- [Wiz](#)

Matrix Push C2 Uses Browser Alerts for Phishing and Malware

The Matrix Push C2 platform leveraged browser notifications to deceive users into visiting phishing pages and downloading malware. The attack exploits notification permissions for real-time user tracking and data theft.

Sources:

- [Malwarebytes](#)

Gainsight Reports Larger Set of Affected Customers

Gainsight expanded its list of impacted clients following a breach involving unauthorised access to Salesforce-linked applications. The ShinyHunters group claimed responsibility, leading to integration suspensions for some third-party platforms.

Sources:

- [The Hacker News](#)

FBI Reports Rising Losses from Account Takeover Fraud

The FBI reported more than 5,100 cases of account takeover fraud this year, leading to over \$262 million in losses. Social engineering and phishing were the primary methods for accessing financial, payroll, and health accounts.

Sources:

- [IC3](#)

Ransomware Hits US Emergency Alert System

OnSolve's CodeRED emergency notification system suffered a ransomware attack, disrupting services across multiple US states. The incident exposed user data and prompted an investigation into the breach.

Sources:

- [SecurityWeek](#)

Threats

Dartmouth Confirms Data Theft After Clop Exploits Oracle Zero-Day

Clop ransomware exploited a zero-day in Oracle E-Business Suite, leading to data theft at Dartmouth College. Personal and financial records were exposed, and the stolen data was later published online.

Sources:

- [BleepingComputer](#)

ShadowV2 Botnet Targets IoT Devices Worldwide

The ShadowV2 botnet targeted vulnerabilities in Internet of Things devices during a significant AWS outage. The Mirai-derived malware infected devices globally, supporting distributed attacks.

Sources:

- [Fortinet](#)

Infrastructure & Exploits

Fluent Bit Flaws Enable File Manipulation and Remote Code Execution

Five vulnerabilities in the Fluent Bit telemetry agent exposed cloud environments to remote code execution and log manipulation. The flaws affected widely used cloud platforms and Kubernetes environments.

Sources:

- [Oligo Security](#)

Tor Introduces Counter Galois Onion Encryption

The Tor Project introduced Counter Galois Onion encryption, replacing the older tor1 algorithm. This upgrade improves forward secrecy and prevents tagging attacks, enhancing user security on the Tor network.

Sources:

- [The Tor Project](#)

Tools & Techniques

RomCom Deploys Mythic Agent Through SocGholish Infection Chain

The RomCom malware used the SocGholish framework to deliver its Mythic Agent loader to a US engineering firm, following the fake-update attack chain commonly associated with SocGholish.

Sources:

- [Arctic Wolf Labs](#)

North Korean Operation Expands npm Supply-Chain Intrusions

The North Korean-linked Contagious Interview campaign added nearly 200 malicious npm packages, distributing updated OtterCookie malware. These packages targeted blockchain and Web3 developers through typosquatted utilities.

Sources:

- [Socket](#)

Policy & Legal

WA Man Jailed for Airport 'Evil Twin' WiFi Attacks

A West Australian man was sentenced to seven years for operating an 'evil twin' WiFi network at airports to steal traveller credentials, accessing personal online accounts.

Sources:

- [Australian Federal Police](#)

French Football Federation Reports Major Data Breach

The French Football Federation reported a data breach due to a compromised account, exposing personal details of millions of players. The breach prompted system remediation and notifications to authorities.

Sources:

- [Infosecurity Magazine](#)

Highlights from the Daily Briefings

25 November 2025

- RomCom deploys Mythic Agent via SocGholish: Arctic Wolf Labs observed RomCom delivering its loader to a US engineering firm using the SocGholish fake-update chain.
- Dartmouth data stolen after Clop exploits Oracle zero-day: Attackers accessed personal and financial records via a zero-day in Oracle E-Business Suite, later posting the data online.
- Massive credential leaks found in code-formatting platforms: watchTowr Labs identified tens of thousands of exposed credentials from governments, banks, and enterprises on JSONFormatter and CodeBeautify.
- SitusAMC breach affects major US banks: Corporate and client files were accessed during a 12 November incident, with some banking data confirmed compromised.
- Malicious LLMs increase AI-driven cybercrime: Unit 42 highlighted tools like WormGPT 4 and KawaiiGPT enabling automated phishing, malware creation, and lateral movement.
- Fluent Bit vulnerabilities permit file tampering and RCE: Oligo Security disclosed five flaws allowing tag manipulation, arbitrary file writes, and potential remote code execution.
- Tor introduces Counter Galois Onion encryption: New relay-encryption replaces tor1, enhancing forward secrecy, preventing tagging attacks, and increasing authentication to 16 bytes.
- HashJack exploits AI browser URL fragments: Cato CTRL revealed a technique injecting hidden instructions into AI assistants, enabling misinformation, data exfiltration, and credential theft.

More info: [Daily Briefing 25 November 2025](#)

26 November 2025

- FBI reports surge in account takeover fraud: more than 5,100 incidents since January 2025 led to over \$262m in losses, largely driven by social engineering and phishing targeting financial, payroll, and health accounts.
- London councils disrupted by cyber incident: three boroughs reported outages across shared IT systems while working with national authorities to assess the cause and any potential data exposure.
- Ransomware hits US emergency alert platform: an attack on OnSolve's legacy CodeRED system caused multi-state outages and exposed user information, with Inc Ransom claiming responsibility.

- ShadowV2 botnet exploits global IoT flaws: Mirai-based malware abused multiple device vulnerabilities during an AWS outage, compromising devices across numerous regions and sectors for distributed attacks.
- PostHog outlines supply-chain compromise: several JavaScript packages were weaponised to deploy the Shai-Hulud 2.0 worm after an attacker leveraged a misconfigured GitHub workflow to access publishing credentials.

More info: [Daily Briefing 26 November 2025](#)

27 November 2025

- Gainsight expands scope of customer impact: unauthorised access to Salesforce-connected applications affected more organisations than first reported, prompting some partners to suspend integrations while investigations continue.
- Scattered Lapsus\$ Hunters spoof Zendesk in phishing wave: over 40 typosquatted domains and malicious support tickets were used to steal credentials and attempt malware delivery to legitimate portals.
- OpenAI details Mixpanel data exposure: an intrusion into Mixpanel systems revealed limited analytics data for some API users, with no access to OpenAI infrastructure or sensitive credentials.
- Asahi confirms 1.9m records exposed in ransomware attack: the September incident compromised customer and employee information across Japan-based systems, though no leaked data has been found online.
- Bloody Wolf broadens NetSupport RAT operations: new campaigns in Kyrgyzstan and Uzbekistan used government-themed lures and customised loaders to deploy the remote-administration tool via geo-fenced infrastructure.

More info: [Daily Briefing 27 November 2025](#)

28 November 2025

- French Football Federation reports major data breach: a compromised account exposed personal details of millions of licensed players, prompting notification of national authorities and system remediation.
- Calendar subscription abuse affects millions of Apple devices: more than 4 million iOS and macOS systems continue syncing to abandoned or hijacked calendar domains used to deliver unsolicited events with links or attachments.

- North Korean npm campaign expands with nearly 200 new packages: malicious uploads distribute an updated OtterCookie variant through typosquatted tools and cloned crypto projects targeting Web3 developers.
- Scan of public GitLab repositories uncovers 17,000 live secrets: analysis of 5.6 million repositories revealed widespread exposure of active credentials, including Google Cloud Platform keys and GitLab tokens.
- WA man jailed for airport 'evil twin' WiFi attacks: a Perth court sentenced him to more than seven years for deploying fake WiFi networks, harvesting credentials, and accessing victims' online accounts.

More info: [Daily Briefing 28 November 2025](#)

Copyright and Legal Notice

© CyberSecBrief. All rights reserved.

Reproduction, redistribution, or modification of this document or its contents without explicit written permission is strictly prohibited.

Disclaimer & Terms of Use

CyberSecBrief is a personal, non-commercial project operated from Germany and is not affiliated with any company or organisation. The information provided is intended solely for general informational and educational purposes and does not constitute professional cybersecurity, legal, or financial advice. Security-related information changes rapidly; although accuracy and timeliness are sought, no guarantee is given regarding completeness, correctness, or applicability. Users must verify details with official sources or qualified professionals before making decisions.

The owner disclaims liability for any indirect, incidental, or consequential damages arising from reliance on this material. External links and third-party feeds are offered for convenience; their content, accuracy, availability, and privacy practices are outside our control and are not endorsed. Sponsored or promoted material may appear, yet inclusion does not imply endorsement.

Original content is protected by copyright. Where external material is used, appropriate attribution is provided. Reproduction of original content without prior written consent is prohibited. Content may be updated, modified, or removed at any time without notice.

This disclaimer and the Terms of Use are governed by the laws of Germany and applicable European Union regulations. Should any provision be deemed invalid, the remaining provisions shall continue in full force and effect.

Credits and Sources

Definitions for CVEs are sourced from the [National Vulnerability Database \(NVD\)](#), maintained by the National Institute of Standards and Technology (NIST). The NVD is provided “as is” without warranty of any kind.

Definitions for APT groups are derived from the [MITRE ATT&CK® knowledge base](#), reproduced and distributed with the permission of The MITRE Corporation. © 2025 The MITRE Corporation.

Malware statistics are based on data from [MalwareBazaar](#), provided by abuse.ch under CC0. Data is supplied on an as-is basis in accordance with the project’s terms.

Definitions for malware families are derived from the [Malpedia cluster via MISP galaxy](#), provided under CC0 1.0 Universal. Data is supplied on an as-is basis for informational use and may include curated material.

Statistics based on vulnerability disclosures incorporate information from the [Zero Day Initiative](#). Content is used solely for analytical purposes and remains the property of its original publishers.

All feeds and advisories are acknowledged and linked to their respective original sources.

Logo icon created by Ida Desi Mariana — [Flaticon](#).

Powered by [CyberFeedBites](#).

Source

This briefing is published by *CyberSecBrief* –
<https://www.cybersecbrief.com/>