
Weekly Cybersecurity Briefing (12 October – 18 October 2026)

CyberSecBrief Team

CyberSecBrief provides clear, concise cybersecurity briefings that summarise the most relevant developments of the week. The report highlights notable incidents, key themes, and significant activity across the threat landscape, supported by daily updates sourced from trusted feeds and advisories. Its purpose is to offer a practical, time-efficient overview for readers who need a reliable snapshot of current cybersecurity events.

For more briefings, visit [CYBERSECBRIEF.COM](https://cybersecbrief.com).



October 19, 2026

Editorial Analysis

The **Danfoss attack** on French supermarkets caused reported stock losses across hundreds of stores, with attackers manipulating refrigeration controls to force continuous defrosting. Around 300 Intermarché and Netto stores and fewer than 100 Système U stores were initially reported affected, with later reports naming Coopérative U, Carrefour, E.Leclerc and Monoprix. Some accounts described defrost cycles extended from one hour to eight, delaying alarms and leaving staff less time to respond. The retailers do not share a parent company, pointing to their common supplier as the connection. Danfoss says affected stores were running outdated firmware, but authorities have not confirmed whether vulnerabilities disclosed in 2025 were used or identified the attacker. ANSSI is working with European counterparts to establish whether the same software versions are deployed elsewhere.

Ledger confirmed that a hardware wallet sold through Southeast Asian reseller CryptoBilis contained an unauthorised implant. The company says its own systems and direct sales channels were unaffected, and all confirmed cases involve devices sold through that reseller. The stage at which the implants were added and the number of affected devices remain unknown. Estimates of suspected cryptocurrency losses also differ, with on-chain researchers putting them above \$93 million, compared with an earlier estimate of more than \$86 million cited by The Hacker News. Ledger has paused sales through CryptoBilis, which has stopped selling all hardware wallet inventory. Ledger advises affected customers to move their funds to a new device using a new seed, as a seed generated on a tampered device cannot be considered secure.

The **ConnectWise Cloud Backup** compromise affected at least 162 customer tenants, according to Huntress, while other reports cite 173. Sign-ins from a single hosting IP address occurred over roughly two hours on 15 October. The attacker used the application's own credential, authenticating without a user session, device check or MFA prompt and inheriting permissions already granted by customers. In one tenant, a second ConnectWise application granted itself Global Administrator and added client secrets to two other trusted applications. This activity created additional access paths beyond the original credential. Previously issued tokens can also remain valid for up to 90 minutes after an application is disabled. ConnectWise has not disclosed how the credential was obtained and reports no evidence that partner backup data was compromised.

Highlights of the Week

Cyberattack on Danfoss Refrigeration Software Destroys Fresh Stock at French Supermarkets

A cyberattack on Danfoss refrigeration control software hit about 300 Intermarché and Netto stores and fewer than 100 Système U stores on 12 October 2026. Attackers reportedly forced continuous defrosting at a 50-degree setpoint on older software versions, spoiling fresh and frozen products. France's ANSSI identified a vulnerability in the software and is coordinating with European counterparts.

Sources:

- [BFMTV](#)

Ledger Finds Hardware Implant in CryptoBilis-Sold Wallet After Reported Fund Thefts

Ledger paused sales through reseller CryptoBilis after reports of stolen funds from users in Southeast Asia, with a blockchain investigator estimating losses above \$86 million. Ledger said one affected device contained an unauthorised hardware implant, and that all confirmed cases involve devices sold through CryptoBilis. CryptoBilis has stopped selling all hardware wallet inventory while the investigation continues.

Sources:

- [The Hacker News](#)

Attackers Hijack ConnectWise Cloud Backup Credential to Enter Microsoft 365 Tenants

On 15 October 2026, an attacker used the ConnectWise Cloud Backup application's credential to obtain Microsoft Graph tokens in customer tenants. Huntress confirmed unauthorised sign-ins in 162 tenants, all originating from a single hosting provider IP address within a roughly two-hour window. ConnectWise has disabled application access while investigating, and it has not disclosed how the credential was obtained.

Sources:

- [SpecterOps](#)

China-Linked Hackers Exploit BeyondTrust Remote Support Zero-Day

BeyondTrust disclosed CVE-2026-102764, a critical Remote Support vulnerability exploited as a zero-day by a suspected China-nexus actor tracked as ARMORY CASTLE, also known as UNC5221. The attacker compromised one BeyondTrust-hosted instance and one self-hosted appliance on

29 August, installing a web shell, escalating privileges and deleting logs. BeyondTrust released patch BT26-05 on 8 October and has found no further activity since August.

Sources:

- [BeyondTrust](#)
- [Google Threat Intelligence Group](#)

CISA Flags Exploited Ivanti Connect Secure Zero-Day Enabling Remote Command Execution

CISA added CVE-2026-104935, an authentication bypass in Ivanti Connect Secure, to its Known Exploited Vulnerabilities Catalogue on 13 October 2026. The zero-day allows remote, unauthenticated execution of arbitrary commands on versions 25.1.1.1, 25.1.2.2 and 22.8R2.4 and earlier. Threat actors are exploiting it for credential theft and data exfiltration, with commands running in memory so Ivanti's Integrity Checker Tool may miss evidence.

Sources:

- [CISA](#)
- [Ivanti](#)

Threats

Hirudo Android Trojan Replaces Indonesian Banking Apps With Patched Copies

ThreatFabric identified Hirudo, an Android banking trojan delivered through shopping, adult video and short drama apps behind a fake update prompt. It replaces eight Indonesian banking apps with modified copies containing a hooking engine that disables signature, Accessibility, screen-capture and Play Integrity checks.

Sources:

- [ThreatFabric](#)

Ad Platform Delivered Candiru Spyware to Al Jazeera Devices

Citizen Lab linked zero-click attacks on at least 45 Al Jazeera devices in 2024 and 2025 to Candiru spyware delivered through advertisements bought by Israeli firm Discover-Tech. Google, IAB Europe, Beeswax and Eskimi cut off Discover-Tech, while Liftoff paused its access during a review.

Sources:

- [Citizen Lab](#)

Aoki Infostealer Adds Theft of AI Coding Assistant Credentials

Symantec found that recent Aoki infostealer samples harvest credential and session files for AI coding assistants, including Claude, Codex, Cursor, Codeium and Gemini. The malware also takes browser, cryptocurrency wallet and password manager data and sends it to its command-and-control server.

Sources:

- [Symantec](#)

Infrastructure & Exploits

Cisco Email Gateway Flaw Lets Attackers Gain Root Through Malicious Attachments

Cisco disclosed CVE-2026-76519, a critical arbitrary file write flaw in the Advanced Malware Protection feature of Cisco Secure Email Gateway. An unauthenticated attacker can send a crafted attachment to write files and execute commands as root, and Cisco became aware of active exploitation in October 2026.

Sources:

- [Cisco](#)

Microsoft Patches Record 1,411 Flaws in October Update, Including Three Zero-Days

Microsoft's October 2026 Patch Tuesday addresses a record 1,411 vulnerabilities, including 70 rated Critical, one actively exploited zero-day and two publicly disclosed ones. The exploited flaw is a Windows Shell command injection that bypasses the Mark of the Web security feature.

Sources:

- [BleepingComputer](#)

SiteGuard WAF Flaw Allows Root Command Execution and Is Under Active Exploitation

EG Secure Solutions disclosed CVE-2026-106931, an OS command injection vulnerability in the default-enabled statistics feature of SiteGuard Server Edition. Exploitation allows arbitrary commands with root or SYSTEM privileges, and attacks have already been observed.

Sources:

- [EG Secure Solutions](#)

Tools & Techniques

Chained PostgreSQL Features Enable Code Execution on Snowflake Servers

Varonis Threat Labs showed that a Snowflake Postgres role holding only CREATEROLE could grant itself data-access roles, hijack the pg_cron job table and reach superuser. The researchers then rebuilt blocked file functions and injected a shell command into archive_command. Snowflake fixed the issue server-side.

Sources:

- [Varonis Threat Labs](#)

Underground Forums Shift From Jailbroken Chatbots to AI Agents and Open Models

Bitsight analysed 16 underground forums from February to August 2026 and found AI-related discussion grew 45 per cent while ransomware mentions fell 49 per cent. Mentions of the Model Context Protocol, AI agents and indirect prompt injection rose 67 per cent.

Sources:

- [Bitsight](#)

Policy & Legal

Microsoft Disrupts Chinese-Language Phishing Kit Ecosystem Behind Billion Messages

Microsoft tracked the CoGUI, Haozi and Iron Man System phishing kits to developers it calls Storm-2990, linked to over one billion phishing emails and SMS messages since January 2026. Microsoft's Digital Crimes Unit worked with law enforcement and partners to disrupt the primary developers and infrastructure.

Sources:

- [Microsoft Threat Intelligence](#)

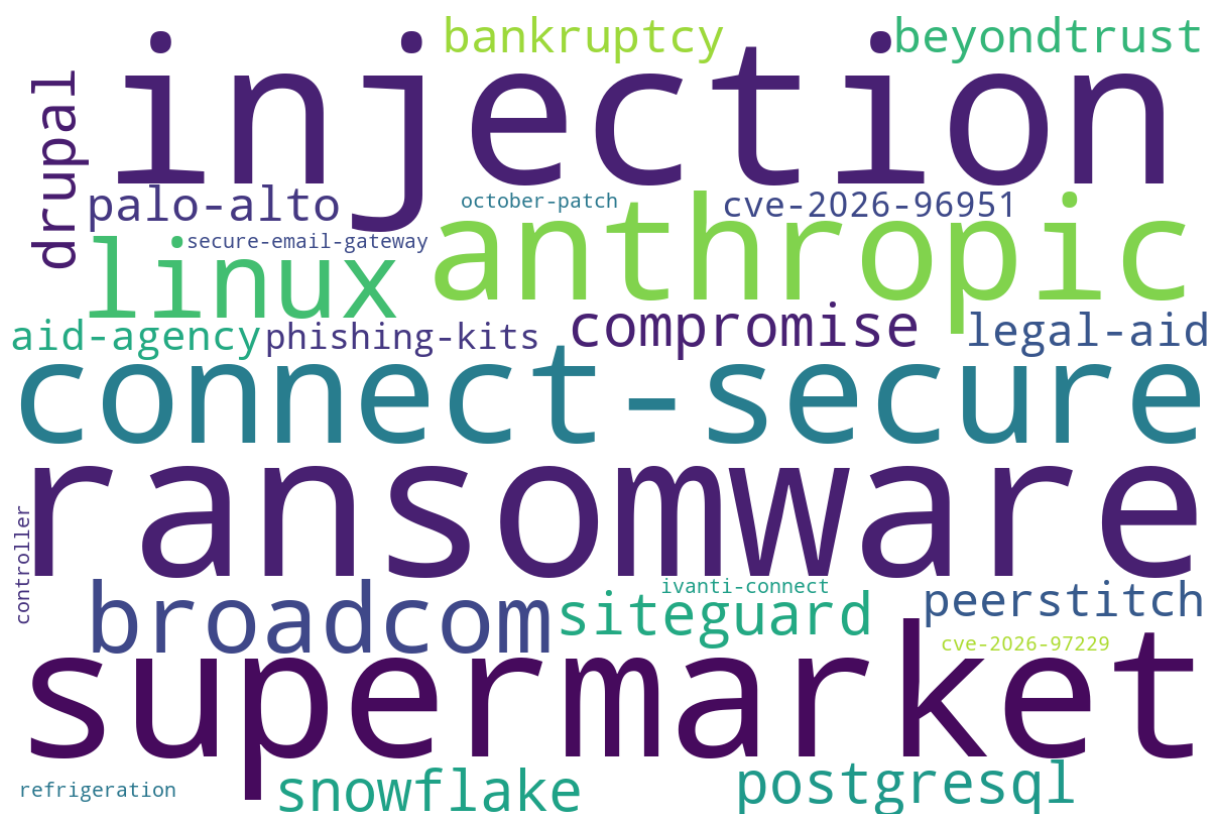
US Indicts 14 Over North Korean Remote IT Worker Scheme

A federal grand jury in Ohio charged U.S. citizens and Chinese nationals with wire fraud, money laundering and identity theft conspiracies tied to a North Korean remote IT worker scheme. US-based facilitators hosted company laptops, helping workers secure jobs at more than 70 US companies and generating roughly \$3 million in revenue.

Sources:

- U.S. Attorney's Office, Northern District of Ohio

Weekly Topic Distribution



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

CVE entries are sourced from the [CVE® Program](#), operated by [The MITRE Corporation](#), and 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.

All feeds and advisories are properly acknowledged and linked to their original sources where referenced, including within briefings.

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

Powered by [CyberFeedBites](#).

Source

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