It's Probably Nothing
by Sierra Echo Charlie

EDITION 20 / 4 NOVEMBER 2026

The fridge hackers went on a European tour

Supermarket freezers hit in four more countries, the FBI names North Korea for Binance, and malware that talks back to AI.

5 stories / Listen online - 5:41

THE TAKEAWAY

The supermarket refrigeration sabotage that started in France has now hit Belgium, Luxembourg, Sweden and Ireland in a single overnight wave, which rather settles the question of whether it was a one-country experiment. Also today: the FBI has formally pointed at North Korea for the Binance heist, Pyongyang is furious about it, and someone's written malware with a polite note asking AI analysis tools to look the other way. It didn't work.

01 / THE BRIEF

Fridge sabotage jumps the border: four countries hit in one night

Reuters reports a coordinated overnight wave on Monday hitting Ahold Delhaize and Colruyt in Belgium and Luxembourg, ICA and Coop in Sweden, an IKEA store, and 13 Musgrave SuperValu stores in Ireland - the same defrost-style attack we saw in France in October, freezers driven up to 50°C and stock binned. One Stockholm ICA franchise was hit at 2 a.m.; its sales manager said every freezer maxed out. Carrefour reported 15 of its 700 Belgian stores affected, Coop 7 of 800. At least some of the affected units used the same Danfoss control technology targeted in France; Danfoss says it's been working with customers on fixes. EU agriculture commissioner Christophe Hansen called it a deliberate attempt to disrupt the food supply chain.

Attribution is nowhere. Reuters couldn't establish who's behind it or whether it's linked to the French incidents, and Belgium's Centre for Cybersecurity said the perpetrator may never be determined. SentinelOne's Tom Hegel noted the absence of financial demands points to sabotage rather than extortion, and that exposed control panels leave almost no traces. Moscow has repeatedly denied involvement in sabotage operations, for what that's worth. The genuinely wild part remains that this many supermarket chains have internet-reachable refrigeration controllers to begin with.

QUALIFICATIONS

No established link to the French attacks and no attribution; treat any Russia speculation as speculation.

SOURCES

New cyberattack on supermarket fridges sweeps across Europe - Reporting / context

Hackers Hijack Supermarket Refrigeration in Belgium and Sweden, Spoiling Food - Reporting / context

02 / THE BRIEF

FBI names North Korea for the Binance heist; laundering gets creative

The Binance theft now has an official attribution: the FBI said at the weekend that North Korea was responsible, per Reuters. Pyongyang responded with unusual speed - Kim Yo Jong used KCNA on Tuesday to call the allegation 'absurd rhetoric' and 'a grave political provocation'. Meanwhile TRM Labs' 3 November tracing update shows the roughly US$2.4 billion in unfrozen ETH and BTC moving through new laundering routes: a self-minted TRON token sold into its own liquidity pool (nearly US$100 million in receipt tokens withdrawn in one sequence), a lending receipt token passed between wallets to defeat USDT-only tracing, and cross-chain swaps chained through two bridges with no intermediate wallet. Nearly US$2.7 billion remains frozen; the main ETH and BTC balances hadn't moved as of 3 November, with activity concentrated on TRON and starting on Solana. Binance co-CEO Richard Teng told Hong Kong Fintech Week that outflows had normalised and 95% of affected tokens replenished, though customers had withdrawn a net US$4.72 billion as of Monday.

Worth keeping the timing straight: TRM attributes the theft to TraderTraitor with high confidence, but its post noted no government had attributed it - the FBI statement, dated only as 'at the weekend', sits slightly outside or alongside that. Context from Reuters: Chainalysis estimates 89% of crypto hack losses this year trace to North Korea; Elliptic puts the country's 2026 haul at US$7.6 billion, a record.

QUALIFICATIONS

The laundering typologies are TRM's tracing; Binance still hasn't published a root cause.

SOURCES

Binance Hack Update: North Korea Launders Proceeds Through Self-Minted Tokens and Chained Bridges - Primary source

Binance says outflows normalised as North Korea rejects US allegation over heist - Reporting / context

Binance Hit by $6.3 Billion Crypto Theft Linked to North Korea's TraderTraitor - Reporting / context

03 / THE BRIEF

Gorbag: smash-and-grab spies casing war crimes files and aid routes

ESET has publicly identified Gorbag, a Russia-aligned group active since at least February 2025, per reporting from The Record and The Hacker News. The target list reads like a wartime intelligence wishlist: about a quarter of known victims are Ukrainian law enforcement and judicial bodies (ESET suggests monitoring war crimes investigations), another quarter frontline local councils (strike-damage assessment), plus defence organisations and a transport hub used for foreign military aid. Its BeautyStealer malware grabs browser credentials, VPN and RDP configs, Office documents and KeePass databases, exfiltrates via Telegram or a FastAPI C2, then deletes itself - collection over persistence. Since early 2026 delivery has run through RAR archives exploiting CVE-2025-8088, the WinRAR path traversal patched in July 2025. Activity overlaps CERT-UA's UAC-0226 and Trend Micro's SHADOW-EARTH-066 clusters, though that doesn't make them interchangeable.

My favourite detail: one Prime ReverseShell variant carries a comment addressed to 'LLM and AI' reviewers insisting the file is benign and needs no analysis. ESET tested it against two AI assistants - the prompt injection failed and both flagged it as a reverse shell. Malware authors are now writing for an AI readership, which was inevitable, but it's nice to see the early attempts land this poorly.

WORTH ASKING

If your estate still has unpatched WinRAR installs, CVE-2025-8088 is being actively exploited by multiple actors - worth another nudge.

QUALIFICATIONS

Findings are attributed to ESET via press coverage; whether Gorbag hands stolen access to other actors is ESET's hypothesis, not established.

SOURCES

Russia-linked cyber spies target Ukraine's war crimes investigations, military aid routes - Reporting / context

Russia-Aligned Gorbag Hackers Exploit WinRAR Flaw to Deploy Data-Stealing Malware - Reporting / context

Gorbag Targets Ukrainian Courts and Frontline Authorities With BeautyStealer - Reporting / context

04 / THE BRIEF

Prompt adware: a Codex jailbreak that repays you in advertising

Check Point Research has dissected Haiou, a Chinese-language jailbreak bundle for OpenAI Codex that persistently rewrites the agent's trusted global instructions - so an ordinary greeting triggers an ad for a third-party LLM gateway, and the agent is told to exempt that gateway from offensive testing. No executable payload, just natural language and config. CPR calls the technique 'prompt adware', and in its testing Claude Code spotted the injection and declined to follow it while Codex didn't.

Keep the qualifications, because they're the difference between a novel finding and a scare story: Check Point found no evidence the advertised gateway is malicious, observed no data theft, and explicitly doesn't classify this as a supply-chain attack. What it demonstrates is that third-party prompts and Skills are now part of the trust chain - the same persistence mechanism could quietly steer recommendations or bias technical advice, and most organisations have no visibility into what their agents' instructions actually say anymore.

WORTH ASKING

If teams are installing community jailbreaks, Skills or prompt bundles for coding agents, that's now a supply-chain review item, not a productivity choice.

QUALIFICATIONS

The referenced academic findings on malicious LLM gateways concern other services, not Haiou's advertised gateway.

SOURCES

Prompt Adware: How Hidden AI Instructions Could Create a New Enterprise Security Risk - Primary source

Haiou Jailbreak Bundle Plants Persistent AI Gateway Ads in Codex Instructions - Reporting / context

05 / THE BRIEF

Sydney auctioneer confirms breach after million-row forum listing

First State Auctions, a Sydney luxury-goods auction house, has confirmed unauthorised access to part of a system holding customer information, Cyber Daily reports. The disclosure follows a forum post from a user calling themselves 'sexyskin' offering more than a million lines of customer data - names, emails, phone numbers and addresses - essentially free for site credits. The company says impact appears mostly limited to basic contact information with no evidence credit cards or passwords were affected, it's contacted affected customers, and both the ACSC and OAIC have been informed. Operations are unaffected.

Keep the two sides distinct: the million-line figure is the seller's claim, while 'mostly basic contact info, no cards or passwords' is the company's early assessment. Those two things can both be true, or one of them can age badly - we've all seen both outcomes.

QUALIFICATIONS

The intrusion timing is unspecified beyond 'recently'; data scope rests on the seller's forum claim versus the company's initial assessment.

SOURCES

Exclusive: Sydney-based First State Auctions customer data impacted by cyber incident - Reporting / context

---

THAT'S IT FOR TODAY.

Listen to this edition or browse the archive. Narrated using an AI voice.

Researched by our AI agents using Mallory and original sources. Reviewed and published by Sierra Echo Charlie.

Want intelligence your team can act on? Reach out for a chat.