INFOGRAPHIC · CYBERSECURITY & AI

# AI THREATS NOV-2026

Refrigeration sabotage across Europe, AI-found flaws, the NCSC warning and the largest crypto theft on record

**Aridio Silva — Independent Researcher**
**ORCID 0009-0008-2411-6995**

© 2026 Aridio Silva @aridiosilva · November 2026 · Facts checked up to 3 Nov 2026

OVERVIEW

# Three threat fronts in two weeks

1

## OT sabotage in retail

Two waves forced supermarket fridges into defrost in France (Oct) and at least 7 other European countries (Nov).

2

## AI in vulnerability discovery

AI helped find PHP2Shell; the UK NCSC expects AI attacks on critical infrastructure by 2028.

3

## State-scale crypto theft

About US$6.3bn left Binance; analysts point to North Korea's TraderTraitor/Lazarus.

**7+**

countries in the 2nd wave (Nov 1–2)

**76+**

stores hit in Belgium alone

**US$6.3bn**

Binance's own estimate

**2028**

horizon of the NCSC warning

⚠️ **Note: no official source says AI was used in the refrigeration attacks.**

© Aridio Silva @aridiosilva · November 2026

TIMELINE

# How the crisis unfolded



**Jan 2026**

Pro-Russian hacktivists start targeting refrigeration (20+ claimed attacks this year, per Forescout)

**Oct 11–12**

1st wave in France: forced defrost cycles; up to 50 °C for ~6 h

**Oct 12–13**

CERT-FR issues alert ALE-012 (Danfoss), then extends it to Copeland and Dixell

**Oct 21**

PHP Foundation patches PHP2Shell, found with AI assistance

**Oct 29–30**

Binance loses about US$6.3bn; TRM Labs points to TraderTraitor

**Nov 1–2**

2nd wave: Belgium, Sweden, Luxembourg, Estonia, Ireland, Netherlands, Finland

**Nov 3**

UK NCSC publishes its Annual Review with an AI warning

© Aridio Silva @aridiosilva · November 2026

THREAT 1 · FIRST WAVE

# France: fridges turned into ovens

- Night of Oct 11–12: forced defrost on central refrigeration managers, up to 50 °C for about 6 hours
- Hundreds of stores: Intermarché (~150), Carrefour (80), Netto, Coopérative U, Monoprix and E.Leclerc
- Food thrown away and fires at some stores; Intermarché's parent estimates losses of several million euros
- The Paris prosecutor opened an inquiry and the prime minister called in ANSSI

**WHY IT MATTERS**

Large-scale cyberattack with direct physical damage to the food chain.

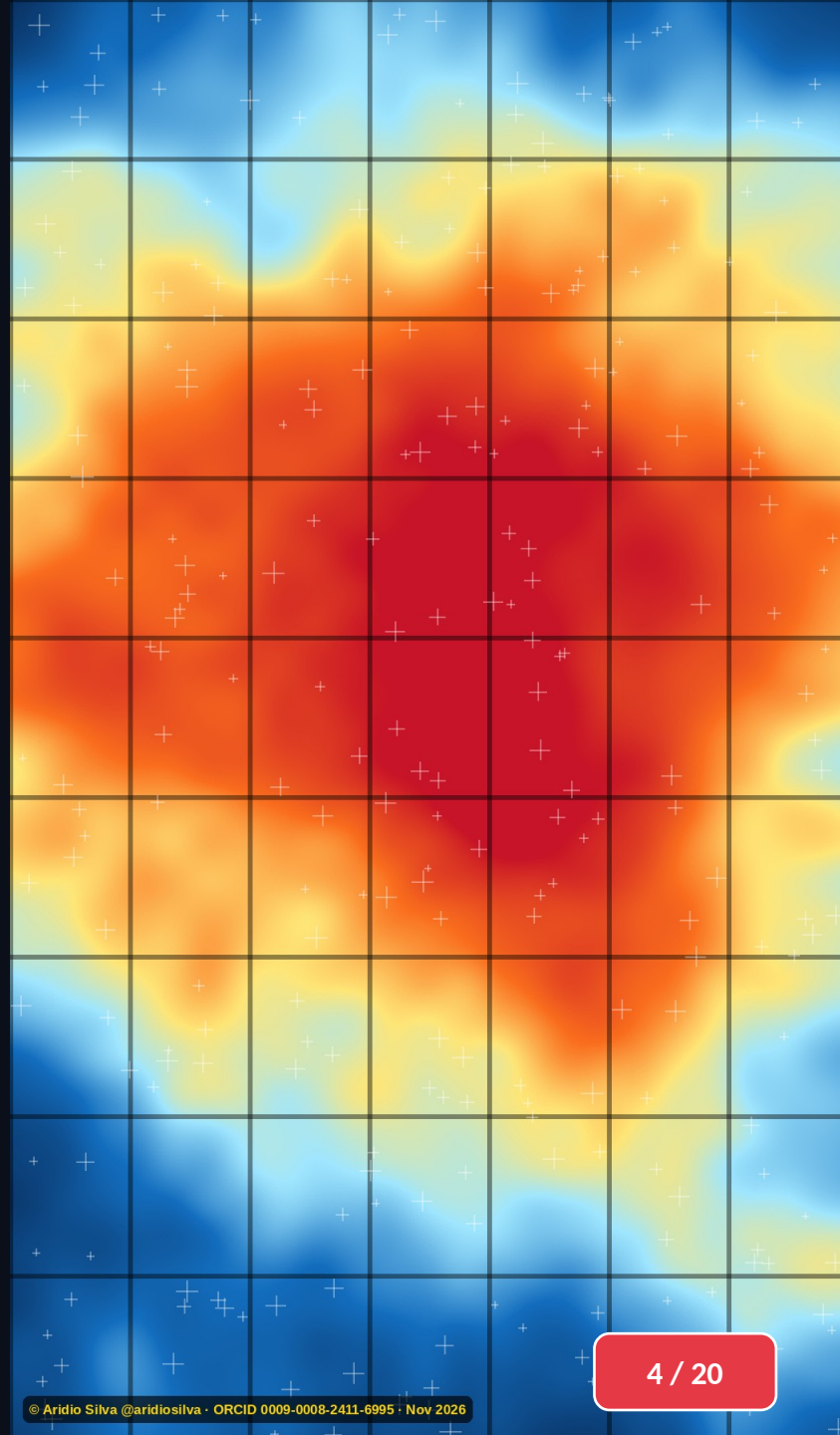
**(+) POSITIVE**

A CERT-FR alert within 24 h guided containment.

**(–) NEGATIVE**

Sabotage with no ransom and no disclosed malware: hard to predict or attribute.

© Aridio Silva @aridiosilva · November 2026



THREAT 1 · SECOND WAVE

# November: the wave crosses Europe




- Seven countries: Belgium, Sweden, Luxembourg, Estonia, Ireland, the Netherlands and Finland
- Belgium: at least 76 outlets; the federal prosecutor opened an investigation
- Same technique as France: evaporators forced into defrost mode
- Delhaize (several dozen) and ICA gave no exact counts

*Intermarché BE: 10–15; Coop SE: 6–7. Sources: Reuters/CNBC, The Hacker News, Nordisk Post, Cybernews.*

**WHY IT MATTERS**

A repeat within 3 weeks points to a campaign, not a one-off.

**(+) POSITIVE**

Retailers isolated systems and stores stayed open.

**(–) NEGATIVE**

Small shops with no IT staff were hit too.



© Aridio Silva @aridiosilva · November 2026

© Aridio Silva @aridiosilva · ORCID 0009-0008-2411-6995 · Nov 2026

TECHNICAL ORIGINS

# Obsolete controllers exposed online

- Danfoss AK-SM 800 (unsupported since May 2021) and AK-SC 355 (discontinued in 2016): no more fixes
- The CERT-FR alert also names Copeland XWEB and Dixell XWEB
- Over 4,500 exposed Danfoss interfaces (Shodan, Oct 2026), more than half in France
- Prior Claroty Team82 research: authentication bypass and command injection in the AK-SM 800A (CISA ICSA-25-140-03)
- Entry vector unconfirmed; no CVE officially linked; no public IOCs as of Nov 3

**WHY IT MATTERS**

Legacy OT assets with no clear owner became the way in.

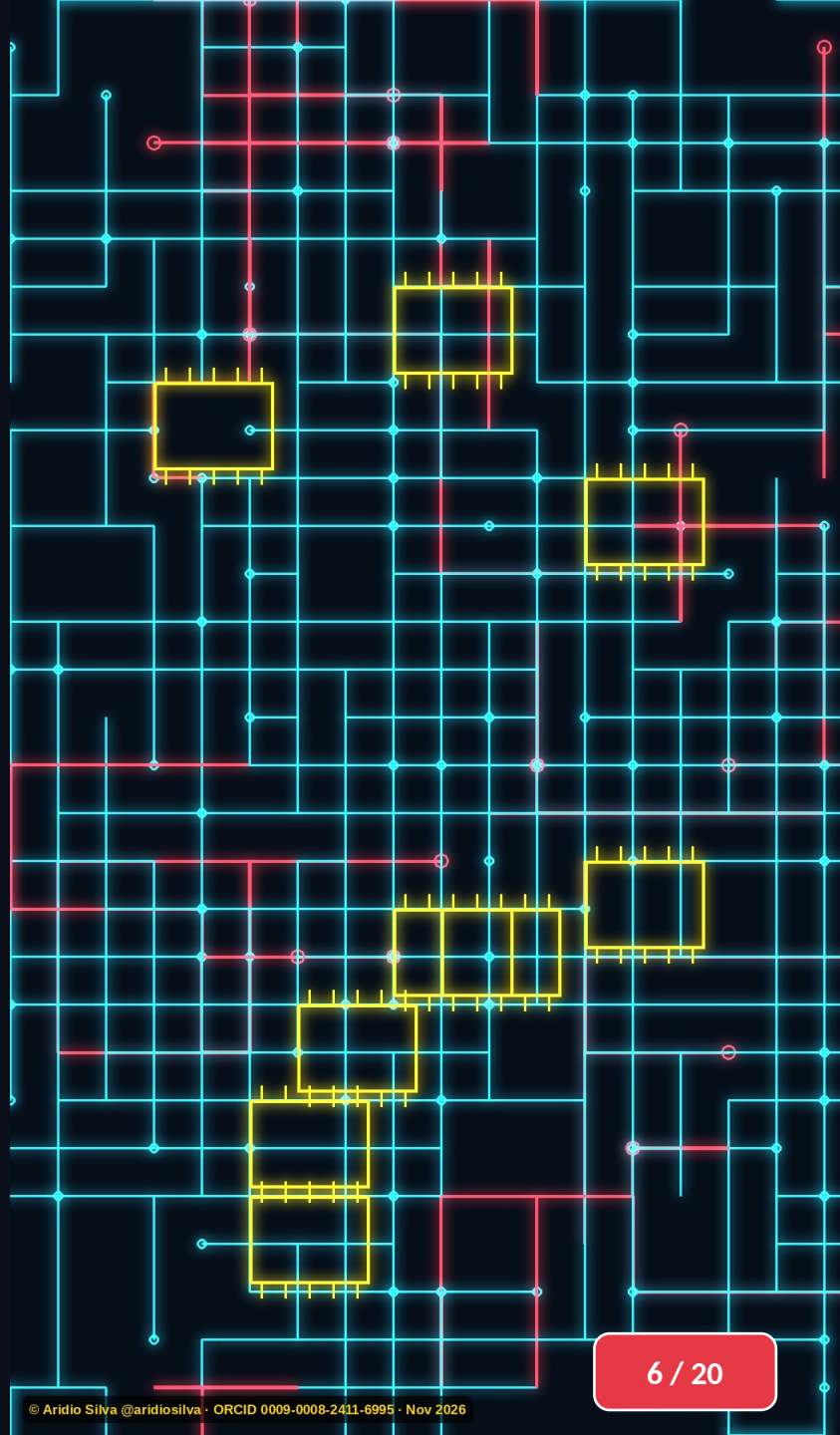
**(+) POSITIVE**

Containment is simple: take them offline, VPN, change default passwords.

**(–) NEGATIVE**

End-of-life hardware has no patch; vendor and retailers dispute responsibility.

© Aridio Silva @aridiosilva · November 2026



© Aridio Silva @aridiosilva · ORCID 0009-0008-2411-6995 · Nov 2026

ATTRIBUTION

# Who is behind it? Still unknown

- No claim; no malware family named; no ransom; no confirmed motive
- Context: pro-Russian groups Z-Pentest Alliance and NoName057(16) have targeted refrigeration since Jan 2026 (Forescout)
- Analysts read the lack of ransom as a hint of state or sabotage motives; a hypothesis, not a fact
- Two possible routes: a compromised remote-maintenance channel (hits every client) or opportunistic scanning of exposed devices

**WHY IT MATTERS**

The entry route sets the response: audit third parties or close ports.

**(+) POSITIVE**

Criminal investigations open in Paris and Brussels.

**(–) NEGATIVE**

Without attribution there is no deterrence; new waves cannot be ruled out.



© Aridio Silva @aridiosilva · November 2026

© Aridio Silva @aridiosilva · ORCID 0009-0008-2411-6995 · Nov 2026

THREAT 2 · AI

# PHP2Shell: AI finds critical flaws

- CVE-2026-109618 and CVE-2026-109619: critical flaws patched by the PHP Foundation on Oct 21
- Calif (in OpenAI's Patch the Planet programme) and Wiz used AI to find and demonstrate the flaws
- NSA and ENISA urged immediate action; government and corporate sites went offline temporarily
- Caveats: 70% is the share of sites using PHP, not of vulnerable sites; about half run old versions with no patch

**WHY IT MATTERS**

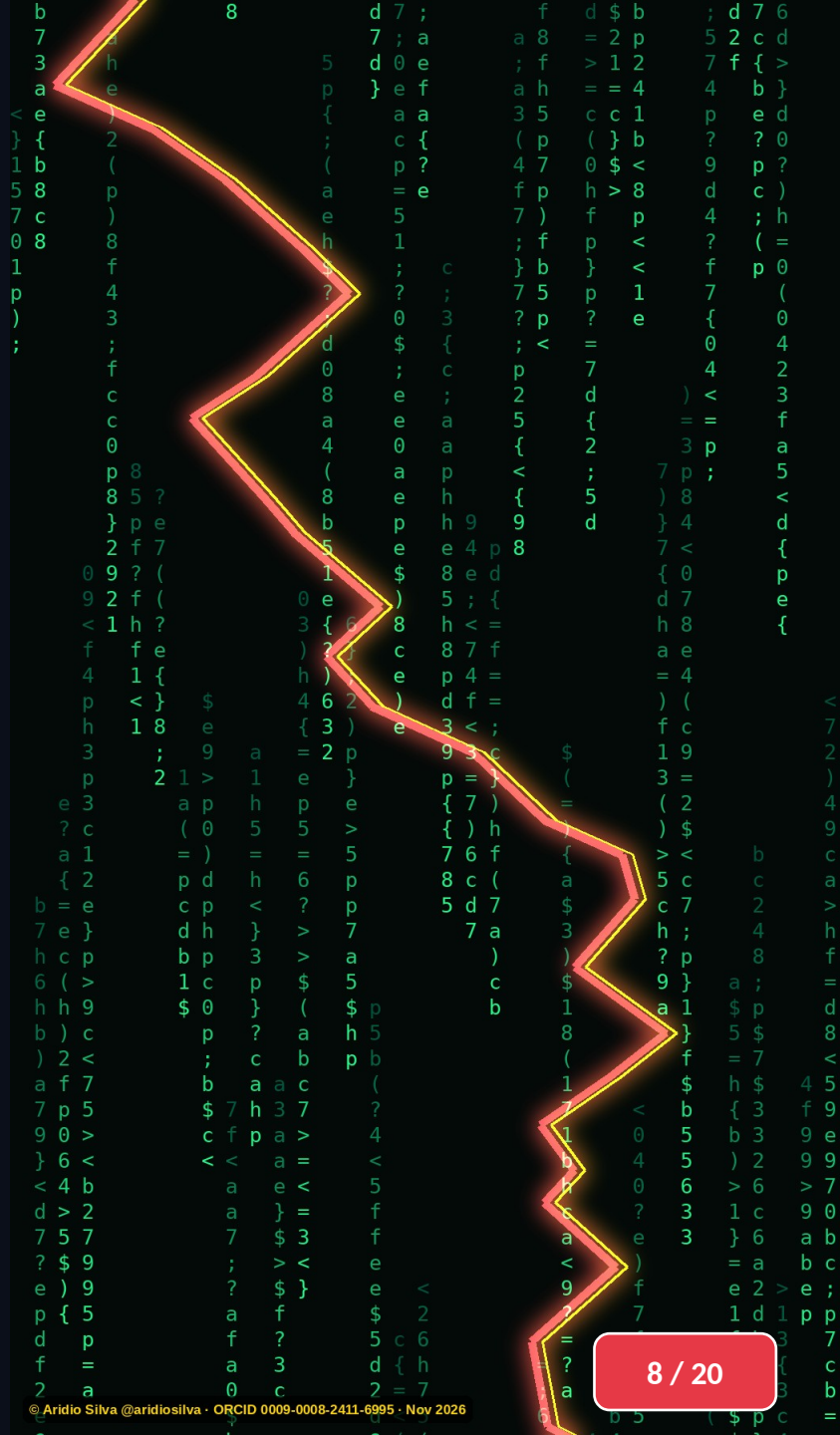
A milestone of AI speeding up discovery of old flaws in core software.

**(+) POSITIVE**

AI on defence: flaw fixed before any known exploitation.

**(–) NEGATIVE**

Attackers have the same capability; legacy stays unpatched.

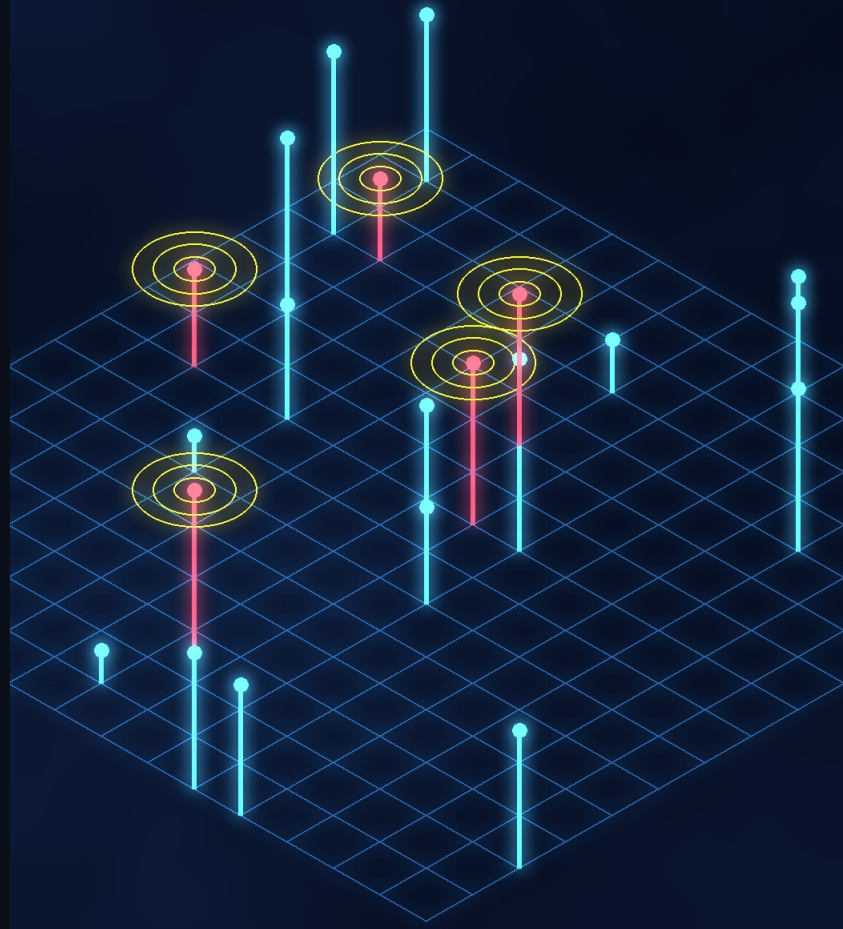



© Aridio Silva @aridiosilva · November 2026

THREAT 3 · AI

# NCSC: AI vs. infrastructure by 2028

- Annual Review (Nov 3): AI attacks on UK critical infrastructure are likely by 2028
- Actors: China (the most sophisticated and sustained challenge), Russia, Iran and criminal groups
- Named targets: electricity switching, sluice gates and dams, production lines, heating and refrigeration
- Report nuance: AI will scale existing tactics more than find brand-new vulnerabilities
- Richard Horne: leaders who skimped on tech will have to explain empty shelves and lights out



**WHY IT MATTERS**

An official agency ties AI, legacy tech and physical sabotage together.

**(+) POSITIVE**

An explicit deadline gives boards time to invest and replace legacy.

**(–) NEGATIVE**

AI scales cheap attacks on flaws tolerated for years.

© Aridio Silva @aridiosilva · November 2026

© Aridio Silva @aridiosilva · ORCID 0009-0008-2411-6995 · Nov 2026

THREAT 4 · BEYOND EUROPE

# Binance: the largest crypto theft on record

- Oct 29–30: about US$6.3bn drained across ~10 blockchains (Binance estimate; TRM Labs: US$6.36bn)
- TRM Labs and Chainalysis: high confidence in TraderTraitor, a Lazarus sub-unit (North Korea); Elliptic agrees
- Binance: the attack started on a DevOps engineer's compromised laptop; no evidence of private key leakage
- Attribution not yet official: the US is investigating; Binance pledges to cover losses

**WHY IT MATTERS**

Unprecedented scale: about 4 times the Bybit theft (2025).

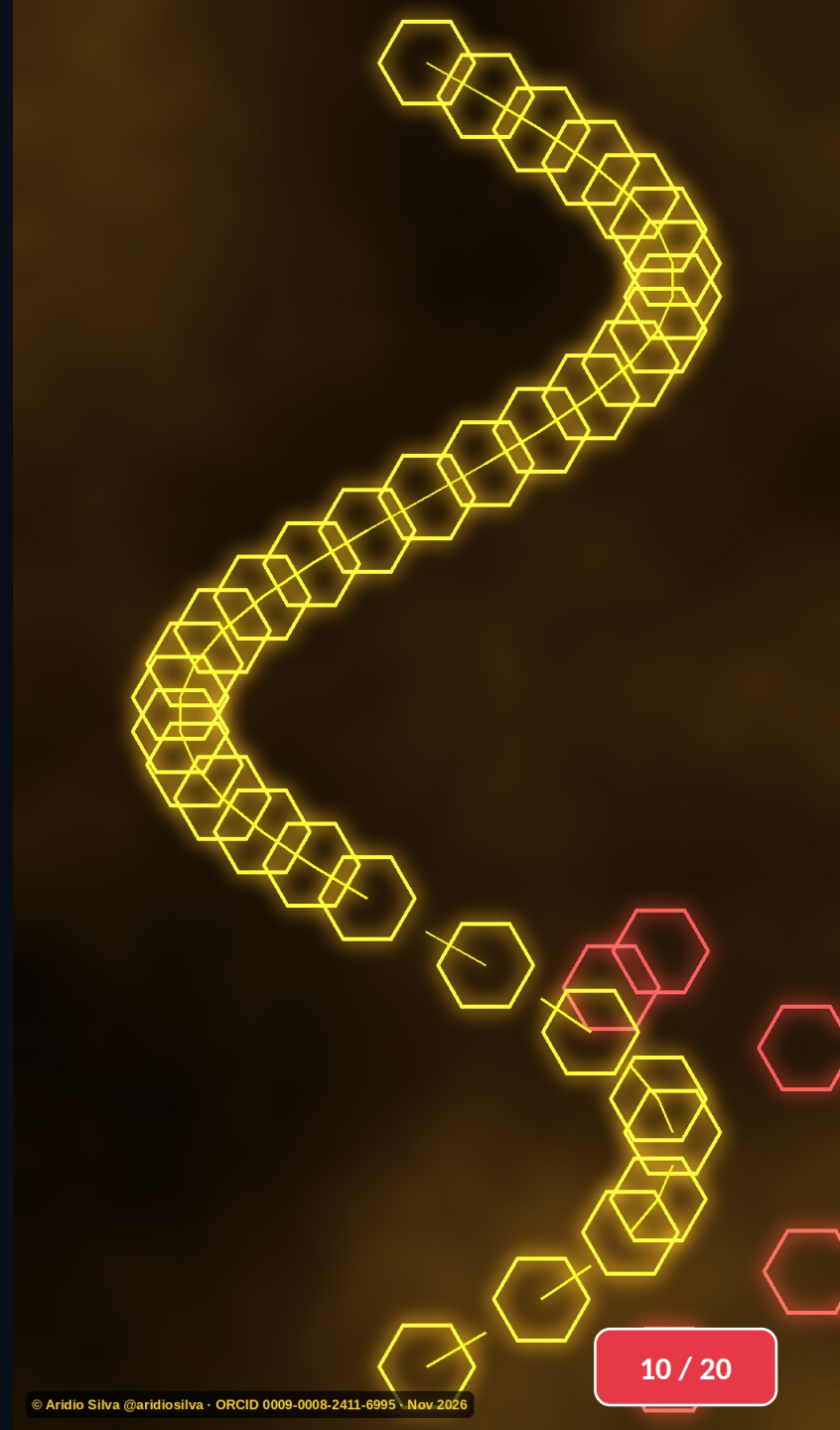
**(+) POSITIVE**

On-chain tracing named suspects within hours.

**(–) NEGATIVE**

A single employee endpoint was enough to drain wallets.

© Aridio Silva @aridiosilva · November 2026





© Aridio Silva @aridiosilva · ORCID 0009-0008-2411-6995 · Nov 2026

SEVERITY AND SCOPE

# Comparative threat matrix

| Threat | Damage type | Scope | Severity* | Attribution confidence |
|---|---|---|---|---|
| **Refrigeration sabotage** | Physical, economic, food supply | France + 7 countries | **HIGH** | Low: no actor |
| **PHP2Shell** | Systemic (potential) | Global: ~70% of sites use PHP | **CRITICAL (potential)** | N/A: defensive discovery |
| **NCSC warning** | Strategic (projection) | UK, by 2028 | **HIGH (projection)** | States named: China, Russia, Iran |
| **Binance theft** | Financial | Global (crypto) | **HIGH** | Medium-high: private sector |

**Author's qualitative assessment based on the cited sources; not an official metric.*

© Aridio Silva @aridiosilva · November 2026

IMPLICATIONS

# What changes for companies and governments

## Negative

- Food and retail join the sabotage target map
- End-of-life gear becomes a liability with no technical fix
- Contractors with remote access widen third-party risk
- AI shortens the time from flaw to exploitation

## Positive

- National CERTs alerted within 24 h
- Coordinated PHP2Shell disclosure with defensive AI
- Cross-border criminal investigations under way
- On-chain tracing speeds up theft attribution

## For GRC

- Inventory internet-exposed OT assets
- Require security clauses from remote-maintenance firms
- Plan replacement of EOL equipment
- Monitor temperature setpoints and alarms

© Aridio Silva @aridiosilva · November 2026

TRENDS

# Where the threats are heading

1. **Cyber-physical sabotage**
   Everyday sectors such as retail and food join energy and water.

2. **AI compressing timelines**
   Finding and exploiting flaws gets faster and cheaper (PHP2Shell, NCSC).

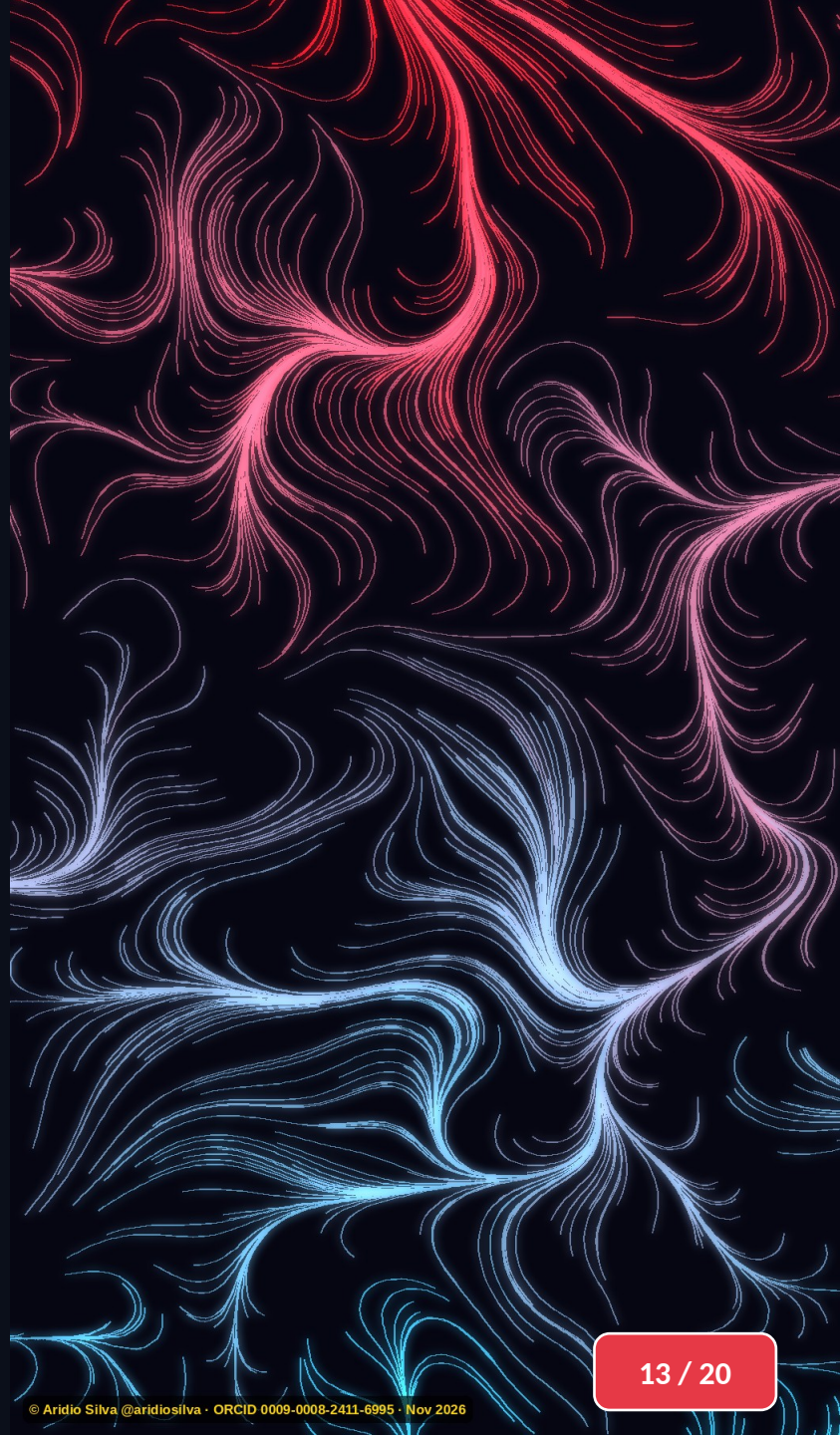
3. **Legacy as a board risk**
   Cheap, outdated tech becomes an accountability issue.

4. **Attacks via the service chain**
   Remote maintenance and suppliers as a mass vector.

5. **Private-sector attribution**
   Blockchain and OT analytics firms name suspects before governments do.

*Trends: the author's analytical reading of the sources; not official forecasts.*

© Aridio Silva @aridiosilva · November 2026



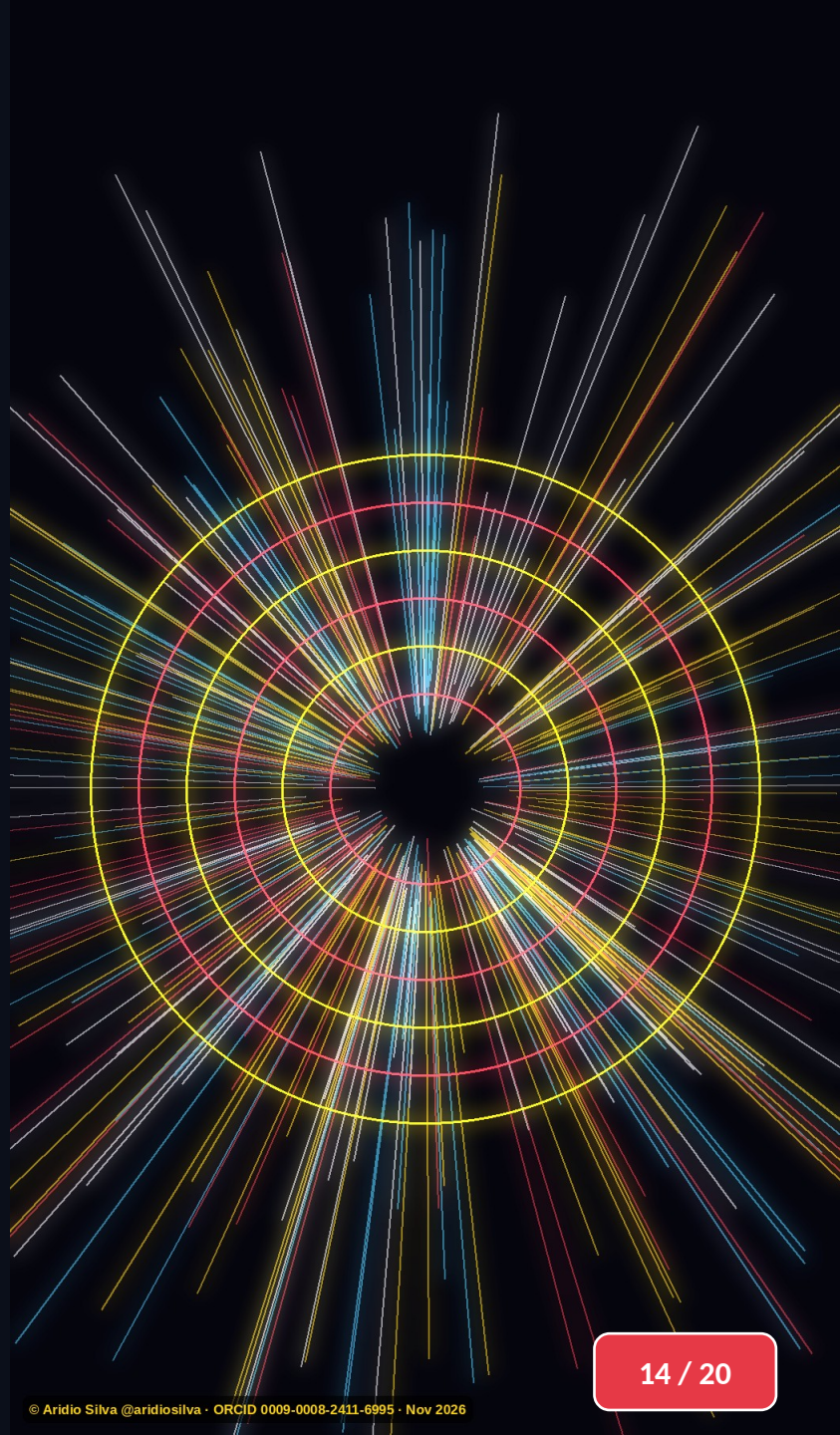
© Aridio Silva @aridiosilva · ORCID 0009-0008-2411-6995 · Nov 2026

CONCLUSION

# Risk has moved from screen to shelf

In three weeks, two waves of sabotage forced refrigerators into defrost at hundreds of stores in France and in at least seven other European countries. The attacks used obsolete controllers exposed to the internet, with no identified actor and no ransom demand. In the same period, AI showed both faces: it helped defenders find and fix critical PHP flaws, and the NCSC names it as a force multiplier for attacks on critical infrastructure by 2028. The US$6.3bn Binance theft is a reminder that state actors keep monetising operational weaknesses.

**The common lesson is governance: inventory and isolate legacy assets, control third-party remote access and shorten patch times. Open questions on actors and vectors call for caution before conclusions.**




© Aridio Silva @aridiosilva · November 2026

# Glossary of terms

**OT (Operational Technology)** Systems that control physical processes: refrigeration, energy, water.

**ICS** Industrial Control Systems; OT controllers and supervisory systems.

**Refrigeration controller** Hub (e.g. Danfoss AK-SM/AK-SC) that runs a store's cases and cold rooms.

**Defrost mode** Cycle that heats the evaporator to remove ice; when forced, raises inside temperature.

**EOL (end of life)** A product that no longer gets security updates.

**Firmware** Embedded software that runs inside the device.

**CERT / CSIRT** Incident response team; CERT-FR is part of ANSSI.

**ANSSI** France's national cybersecurity agency.

**CCB** Centre for Cybersecurity Belgium, Belgium's cyber authority.

**NCSC** UK National Cyber Security Centre.

**ENISA** European Union Agency for Cybersecurity.

**CVE** Unique public identifier for a vulnerability.

**CVSS** 0-to-10 scale for vulnerability severity.

© Aridio Silva @aridiosilva · November 2026

GLOSSARY (2/2)

# Glossary of terms

**IOC** Indicator of compromise: IP, hash, domain tied to an attack.

**Shodan** Search engine for internet-connected devices.

**Authentication bypass** Access to a system without valid credentials.

**Command injection** Running arbitrary commands through unsanitised input.

**RCE** Remote code execution on the target.

**Hacktivism** Cyberattacks driven by political or ideological motives.

**Hybrid threat** State actions (cyber, sabotage, disinformation) below the threshold of war.

**Attribution** Identifying who carried out an attack, based on evidence.

**Lazarus / TraderTraitor** North Korea-linked groups; TraderTraitor focuses on crypto.

**Hot wallet** Internet-connected crypto wallet for fast operations.

**Coordinated disclosure** Publishing a flaw by agreement between finder and fixer.

**Third-party risk** Risk from suppliers and contractors with system access.

**VPN** Encrypted tunnel that restricts and protects remote access.

© Aridio Silva @aridiosilva · November 2026

# Primary sources (P) and the outlets that cite them


- [P] CERT-FR / ANSSI — Alert CERTFR-2026-ALE-012, incident on remote refrigeration controllers (12–13 Oct 2026). cert.ssi.gouv.fr — via SecurityWeek, The Hacker News, Brandefense
- [P] CISA — ICSA-25-140-03, vulnerabilities in Danfoss AK-SM 8xxA. cisa.gov — via Brandefense
- [P] Claroty Team82 — "Freeze the Controller, Defrost the Food" and DEF CON demo — via OCCRP
- [P] UK NCSC — Annual Review 2026 and Richard Horne's speech (3 Nov 2026). ncsc.gov.uk — via AP / SecurityWeek
- [P] PHP Foundation — PHP2Shell emergency security release (21 Oct 2026) — via CNN, Fortune, GovTech
- [P] Forescout — research on hacktivists and refrigeration systems (2026) — via Cybernews
- [P] Statements: Danfoss (DR, NOS, AFP, VTM), CCB (Belga, Euronews), Sabcobel (Belga), Carrefour, Coop, ICA, SuperValu, Selver/Kitman Coldtech (ERR)
- [P] Binance (X, 30 Oct 2026); TRM Labs, Chainalysis and Elliptic — theft attribution — via PA, Reuters, CNN


*Accessed 3 Nov 2026. [P] = primary source; content checked in the coverage indicated.*

© Aridio Silva @aridiosilva · November 2026

# Secondary sources: refrigeration attacks


- Euronews (02/11/2026) — Cyberattacks hit supermarket fridges and freezers in Europe
  https://www.euronews.com/2026/11/02/cyberattack-hits-belgian-supermarket-fridges-and-freezers
- CNBC / Reuters (02/11/2026) — New cyberattack on supermarket fridges sweeps across Europe
  https://cnbc.com/2026/11/02/cyberattack-on-fridges-hits-supermarkets-across-europe.html
- CNBC (03/11/2026) — Supermarket fridges are under attack in Europe
  https://www.cnbc.com/2026/11/03/supermarket-fridges-hack-cyberattack-europe.html
- NBC News (02/11/2026) — Supermarkets across Europe hit by new fridge cyberattacks
  https://www.nbcnews.com/world/europe/european-supermarkets-hit-new-fridge-cyberattack-rcna606972
- The Hacker News (11/2026) — New wave of refrigeration cyberattacks hits supermarkets
  https://thehackernews.com/2026/11/second-wave-of-cyberattacks-hits.html
- The Hacker News (10/2026) — Attackers heat French supermarket fridges up to 50°C
  https://thehackernews.com/2026/10/attackers-heat-french-supermarket.html
- SecurityWeek (10/2026) — Attack widens to Copeland, Dixell controllers
  https://www.securityweek.com/supermarket-refrigeration-attack-widens-to-copeland-dixell-controllers/
- The Register (13/10/2026) — Cyberattacks crank French refrigeration systems up to 50C
  https://www.theregister.com/security/2026/10/13/cyberattacks-crank-french-supermarket-refrigeration-systems-up-to-50c/5302784


© Aridio Silva @aridiosilva · November 2026

# Secondary sources: refrigeration attacks


- OCCRP (10/2026) — Hackers turn French supermarket refrigerators into furnaces
  https://www.occrp.org/en/news/hackers-turn-french-supermarket-refrigerators-into-furnaces
- Forbes (20/10/2026) — The French supermarket fridge hack
  https://www.forbes.com/sites/jonmarkman/2026/10/20/the-french-supermarket-fridge-hack-that-made-cyberattacks-physical/
- Cybernews (11/2026) — Who's behind the wave of refrigerator hacks?
  https://cybernews.com/security/europe-supermarket-refrigerator-hacks/
- SBS News (11/2026) — Who's behind Europe's freezer hacks?
  https://sbs.com.au/news/article/who-is-behind-europe-supermarket-fridge-hack/iq2ueze5o
- Nordisk Post (02/11/2026) — Danfoss systems hit in new cyberattacks
  https://www.nordiskpost.com/2026/11/02/danfoss-refrigeration-cyberattacks-europe/
- IT-Connect (11/2026) — After France, hackers overheat fridges in Belgium and Sweden
  https://www.it-connect.tech/after-france-hackers-overheat-supermarket-fridges-in-belgium-and-sweden/
- Rescana (03/11/2026) — What retailers and cold-chain vendors should do now
  https://www.rescana.com/post/europe-supermarket-refrigeration-cyberattack-ot-prepare-now
- Brandefense (11/2026) — Seven steps to isolate your controllers
  https://brandefense.io/security-news/supermarket-refrigeration-cyberattack-belgium-sweden-playbook/


© Aridio Silva @aridiosilva · November 2026

BIBLIOGRAPHY (4/4)

# Secondary sources: AI, NCSC and Binance


- SecurityWeek / AP (03/11/2026) — UK cyber chief: AI cyberattacks on critical infrastructure by 2028
  https://www.securityweek.com/uk-cyber-chief-says-the-uk-will-face-ai-cyberattacks-on-critical-infrastructure-by-2028/
- Dataconomy (03/11/2026) — UK warns of AI attacks on critical infrastructure
  https://dataconomy.com/2026/11/03/uk-warns-of-ai-attacks-on-critical-infrastructure-by-2028/
- CNN (21/10/2026) — Websites shut down after AI finds flaw affecting 70% of the internet
  https://www.cnn.com/2026/10/21/tech/php2shell-vulnerability-ai-intl
- Fortune (21/10/2026) — AI tools discovered the PHP vulnerability
  https://fortune.com/2026/10/21/ai-tools-discovered-the-php-vulnerability-that-could-take-down-70-of-the-internet-now-the-race-is-on-to-patch-it-before-ai-powered-hackers-attack/
- GovTech (11/2026) — PHP scare points to an AI-fueled new normal
  https://govtech.com/security/for-government-php-scare-points-to-an-ai-fueled-new-normal
- Tech-Insider (10/2026) — PHP2Shell: CVE-2026-109618 and CVE-2026-109619
  https://tech-insider.org/ai-php2shell-vulnerability-70-percent-web-2026/
- Irish News / PA (30/10/2026) — Intelligence firm links North Korea with Binance hack
  https://www.irishnews.com/news/world/intelligence-firm-links-north-korea-with-63-billion-dollar-binance-hack-RTCBVZ2ORRNWJBB2VZPPUP3QUM/
- Virginia Business / Reuters (30/10/2026) — Hackers steal $6.3B from Binance
  https://virginiabusiness.com/hackers-steal-6-3-billion-binance-north-korea-heist/
- CoinCentral (10/2026) — TRM Labs, Chainalysis, ZachXBT on the Binance hack
  https://coincentral.com/?p=216010
- Bitcoin.com News (10/2026) — Binance hack pinned on Lazarus by TRM Labs
  https://news.bitcoin.com/security/binance-hack-north-korea-lazarus-tradertraitor/


© Aridio Silva @aridiosilva · November 2026