INFOGRÁFICO · CIBERSEGURANÇA & IA

AI THREATS NOV-2026

Sabotagem de refrigeração na Europa, falhas achadas por IA, alerta do NCSC e o maior roubo de cripto já registrado

Aridio Silva — Pesquisador Independente
ORCID 0009-0008-2411-6995

© 2026 Aridio Silva @aridiosilva · Novembro 2026 · Dados conferidos até 03/11/2026

PANORAMA

Três frentes de ameaça em duas semanas

1

Sabotagem de OT no varejo

Duas ondas forçaram o degelo de refrigeradores de supermercados na França (out) e em pelo menos 7 outros países europeus (nov).

2

IA na descoberta de falhas

IA ajudou a achar o PHP2Shell; o NCSC britânico projeta ataques com IA à infraestrutura crítica até 2028.

3

Roubo de cripto em escala estatal

Cerca de US$ 6,3 bi saíram da Binance; analistas apontam o grupo norte-coreano TraderTraitor/Lazarus.

7+

países na 2ª onda (1–2/nov)

76+

lojas atingidas só na Bélgica

US$ 6,3 bi

estimativa da Binance

2028

horizonte do alerta do NCSC

⚠️ **Atenção: nenhuma fonte oficial afirma que IA foi usada nos ataques aos refrigeradores.**

© Aridio Silva @aridiosilva · Novembro 2026

LINHA DO TEMPO

Como a crise se desenrolou



jan/2026	11–12/out	12–13/out	21/out	29–30/out	1–2/nov	3/nov
Hacktivistas pró-Rússia passam a mirar refrigeração (20+ ataques reivindicados no ano, segundo a Forescout)	1ª onda na França: ciclos de degelo forçados; até 50 °C por ~6 h	CERT-FR emite o alerta ALE-012 (Danfoss) e o amplia para Copeland e Dixell	PHP Foundation corrige o PHP2Shell, achado com apoio de IA	Binance perde cerca de US$ 6,3 bi; TRM Labs aponta TraderTraitor	2ª onda: Bélgica, Suécia, Luxemburgo, Estônia, Irlanda, Países Baixos, Finlândia	NCSC (Reino Unido) publica a Annual Review com alerta sobre IA

© Aridio Silva @aridiosilva · Novembro 2026

AMEAÇA 1 · 1ª ONDA

França: refrigeradores viram fornos

- Noite de 11 para 12/out: degelo forçado nos gerenciadores centrais de refrigeração, até 50 °C por cerca de 6 horas
- Centenas de lojas: Intermarché (~150), Carrefour (80), Netto, Coopérative U, Monoprix e E.Leclerc
- Alimentos descartados e incêndios em algumas lojas; o grupo da Intermarché estima perdas de vários milhões de euros
- A promotoria de Paris abriu inquérito e o primeiro-ministro acionou a ANSSI

POR QUE IMPORTA

Ataque cibernético em larga escala com dano físico direto à cadeia alimentar.

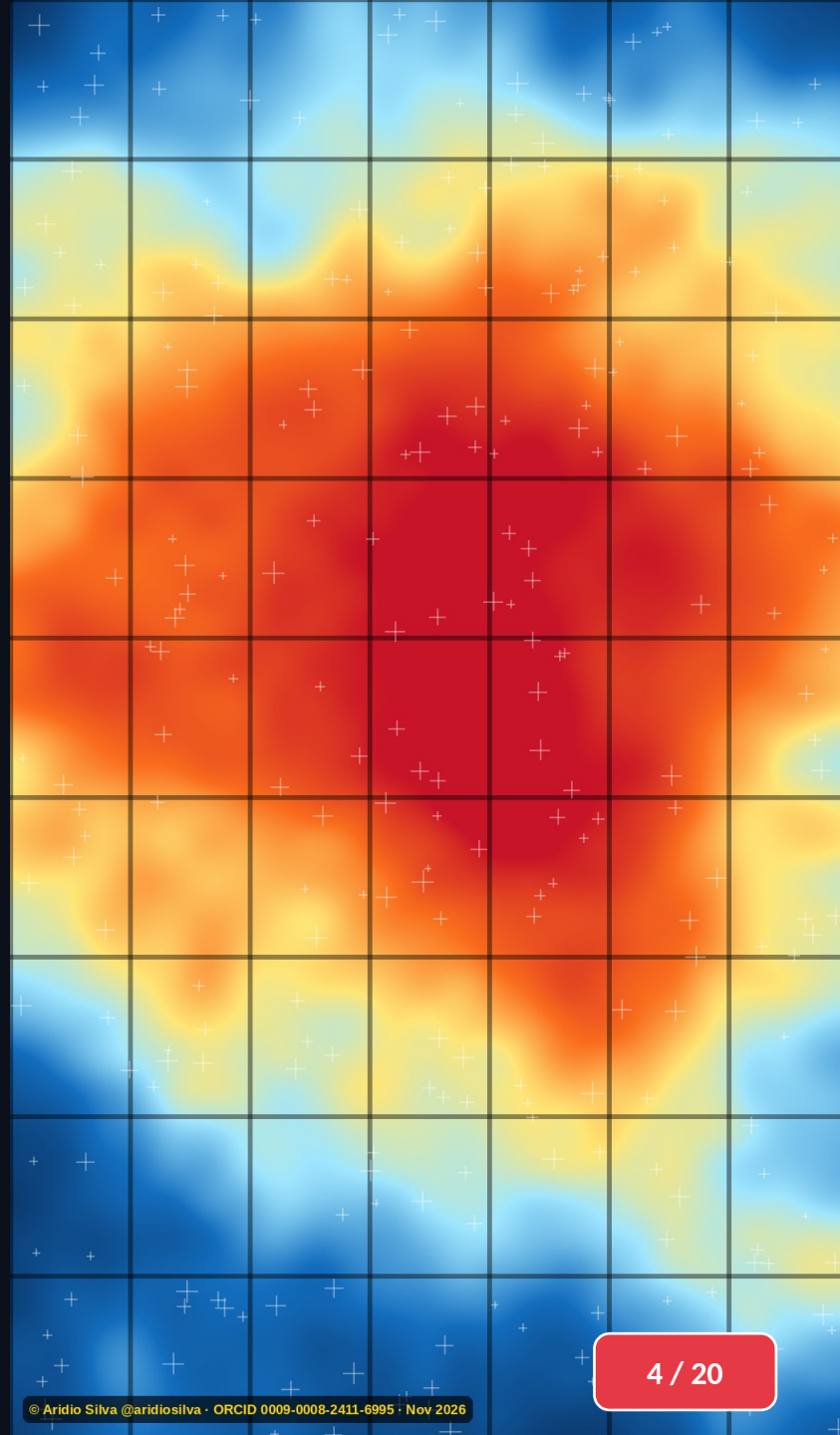
(+) POSITIVO

Alerta do CERT-FR em menos de 24 h orientou a contenção.

(–) NEGATIVO

Sabotagem sem resgate e sem malware divulgado: difícil de prever e de atribuir.

© Aridio Silva @aridiosilva · Novembro 2026



AMEAÇA 1 · 2ª ONDA

Novembro: a onda cruza a Europa



- Sete países: Bélgica, Suécia, Luxemburgo, Estônia, Irlanda, Países Baixos e Finlândia
- Bélgica: ao menos 76 pontos de venda; a promotoria federal abriu investigação
- Mesma técnica da França: evaporadores forçados ao modo degelo
- Delhaize (várias dezenas) e ICA não divulgaram números exatos

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

POR QUE IMPORTA

Repetição em 3 semanas indica campanha, não incidente isolado.

(+) POSITIVO

Varejistas isolaram sistemas e lojas seguiram abertas.

(–) NEGATIVO

Pequenos comércios, sem equipe de TI, também foram atingidos.



© Aridio Silva @aridiosilva · Novembro 2026

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

ORIGENS TÉCNICAS

Controladores obsoletos expostos à internet

- Danfoss AK-SM 800 (sem suporte desde mai/2021) e AK-SC 355 (descontinuado em 2016): não recebem mais correções
- O alerta do CERT-FR também cita Copeland XWEB e Dixell XWEB
- Mais de 4.500 interfaces Danfoss expostas (Shodan, out/2026), mais da metade na França
- Pesquisa prévia da Claroty Team82: bypass de autenticação e injeção de comando no AK-SM 800A (CISA ICSA-25-140-03)
- Vetor de entrada não confirmado; nenhuma CVE ligada oficialmente; sem IOCs públicos até 03/11

POR QUE IMPORTA

Ativos de OT legados, sem dono claro, viraram porta de entrada.

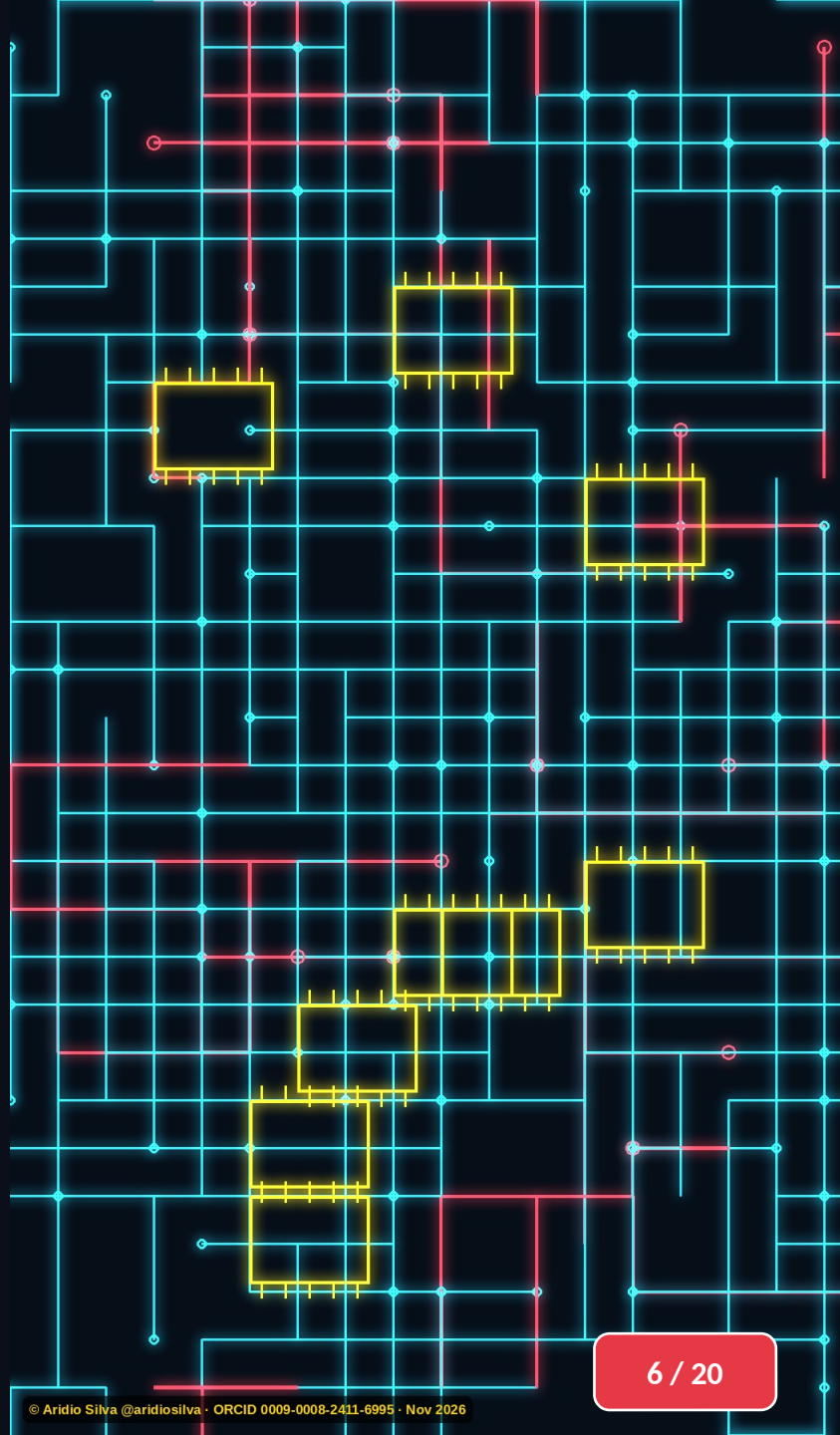
(+) POSITIVO

Contenção é simples: tirar da internet, VPN, trocar senhas padrão.

(–) NEGATIVO

Hardware em fim de vida não tem patch; fornecedor e varejista disputam a responsabilidade.

© Aridio Silva @aridiosilva · Novembro 2026



AUTORIA

Quem está por trás? Ainda não se sabe

- Ninguém reivindicou; nenhuma família de malware nomeada; nenhum resgate; motivo não confirmado
- Contexto: os grupos pró-Rússia Z-Pentest Alliance e NoName057(16) miram refrigeração desde jan/2026 (Forescout)
- Analistas veem na falta de resgate um indício de motivação estatal ou de sabotagem; é hipótese, não fato
- Duas rotas possíveis: canal de manutenção remota comprometido (atinge todos os clientes) ou varredura oportunista de dispositivos expostos

POR QUE IMPORTA

A rota de entrada define a resposta: auditar terceiros ou fechar portas.

(+) POSITIVO

Investigações penais abertas em Paris e Bruxelas.

(–) NEGATIVO

Sem atribuição, não há dissuasão e novas ondas não podem ser descartadas.



© Aridio Silva @aridiosilva · Novembro 2026

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

AMEAÇA 2 · IA

PHP2Shell: IA encontra falhas críticas

- CVE-2026-109618 e CVE-2026-109619: falhas críticas corrigidas pela PHP Foundation em 21/out
- Calif (no programa Patch the Planet, da OpenAI) e Wiz usaram IA para achar e demonstrar as falhas
- NSA e ENISA pediram ação imediata; sites de governos e empresas saíram do ar temporariamente
- Ressalvas: 70% é a fatia de sites que usam PHP, não de sites vulneráveis; cerca de metade roda versões antigas sem patch

POR QUE IMPORTA

Marco da IA acelerando a descoberta de falhas antigas em software base.

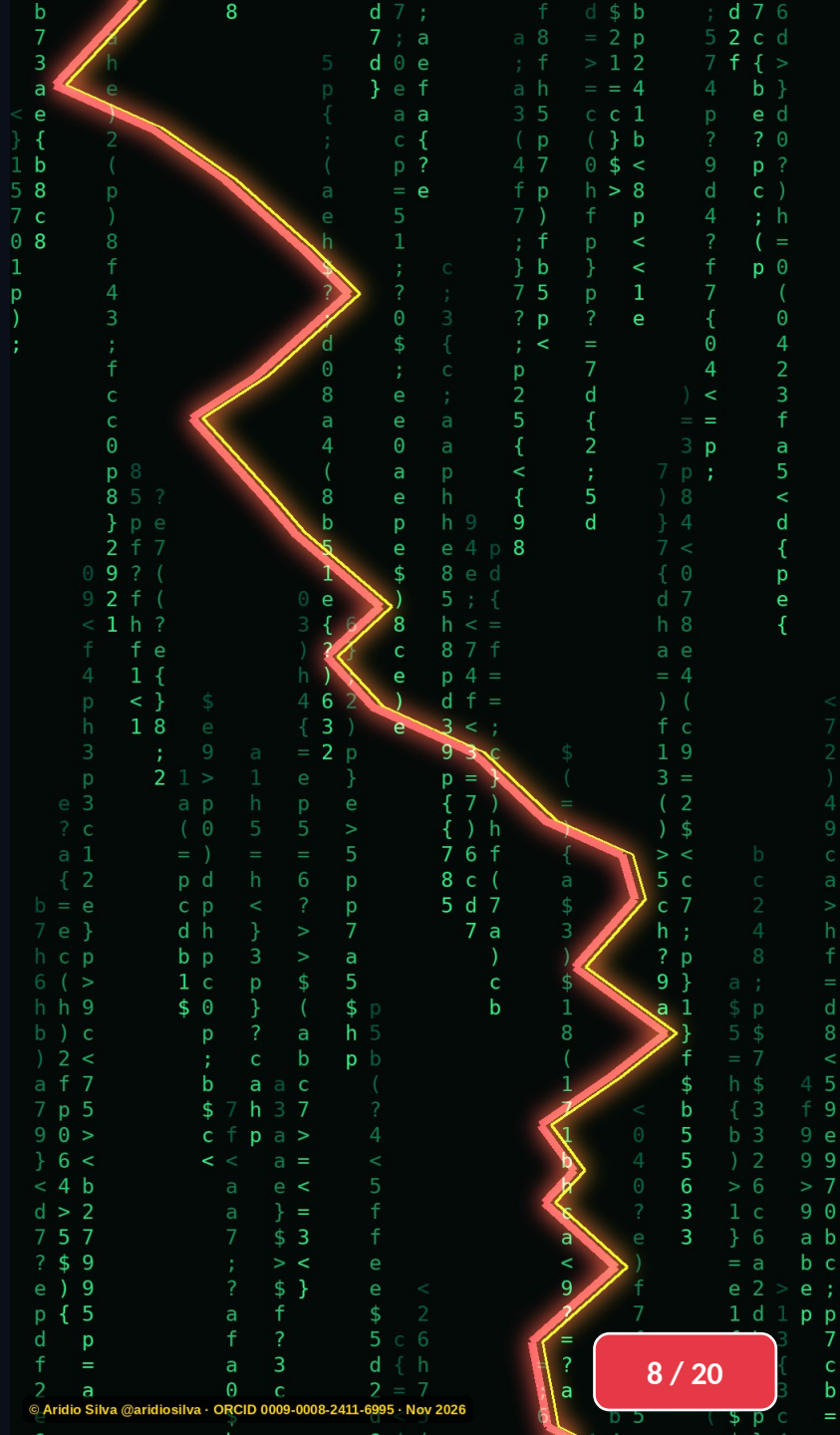
(+) POSITIVO

IA a serviço da defesa: falha corrigida antes de exploração conhecida.

(–) NEGATIVO

A mesma capacidade está ao alcance de atacantes; legado sem patch.

© Aridio Silva @aridiosilva · Novembro 2026

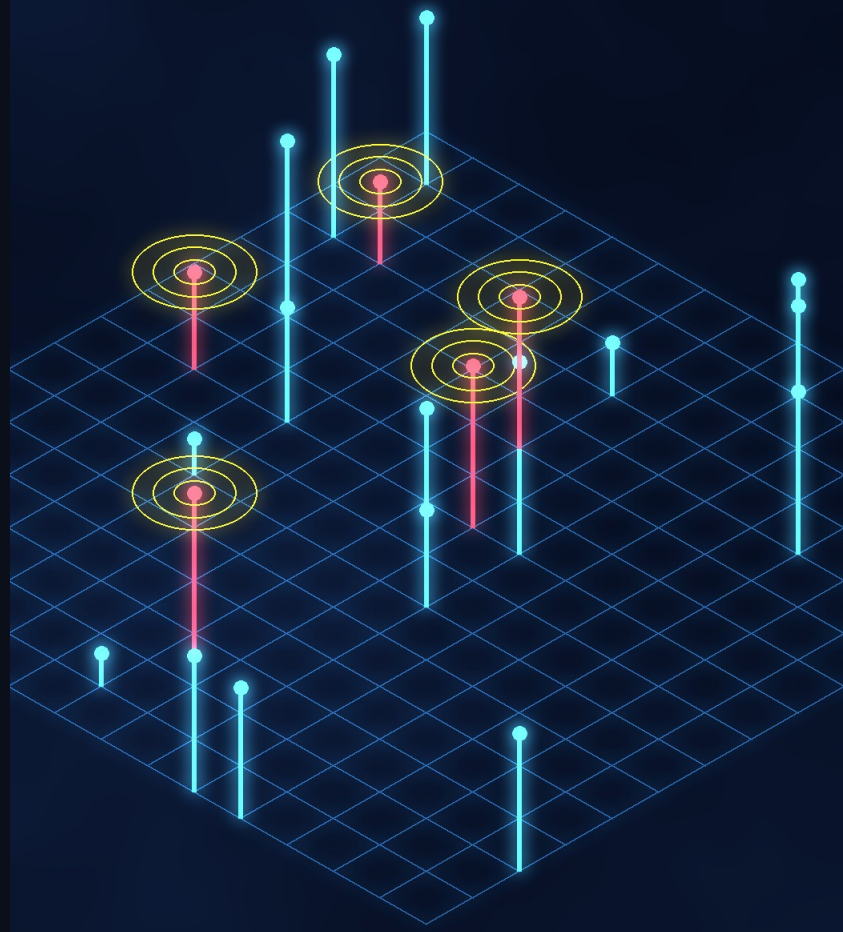


© Aridio Silva @aridiosilva · ORCID 0009-0008-2411-6995 · Nov 2026

AMEAÇA 3 · IA

NCSC: IA contra infraestrutura até 2028

- Annual Review (3/nov): ataques com IA à infraestrutura crítica britânica são prováveis até 2028
- Atores: China (o desafio mais sofisticado e persistente), Rússia, Irã e grupos criminosos
- Alvos citados: comutação elétrica, comportas e barragens, linhas de produção, aquecimento e refrigeração
- Nuance do relatório: a IA deve escalar táticas existentes mais do que achar vulnerabilidades inéditas
- Richard Horne: líderes que pouparam em tecnologia terão de explicar prateleiras vazias e luzes apagadas



POR QUE IMPORTA

Agência oficial liga IA, legado e sabotagem física no mesmo diagnóstico.

(+) POSITIVO

Prazo explícito dá às diretorias tempo para investir e substituir legado.

(–) NEGATIVO

IA escala ataques baratos contra falhas toleradas há anos.

© Aridio Silva @aridiosilva · Novembro 2026

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

AMEAÇA 4 · FORA DA EUROPA

Binance: o maior roubo de cripto registrado

- 29–30/out: cerca de US$ 6,3 bi retirados em ~10 blockchains (estimativa da Binance; TRM Labs: US$ 6,36 bi)
- TRM Labs e Chainalysis: alta confiança em TraderTraitor, subunidade do Lazarus (Coreia do Norte); Elliptic concorda
- Binance: ataque partiu do laptop comprometido de um engenheiro de DevOps; sem evidência de vazamento de chave privada
- Atribuição ainda não é oficial: os EUA investigam; a Binance promete cobrir as perdas

POR QUE IMPORTA

Escala inédita: cerca de 4 vezes o roubo da Bybit (2025).

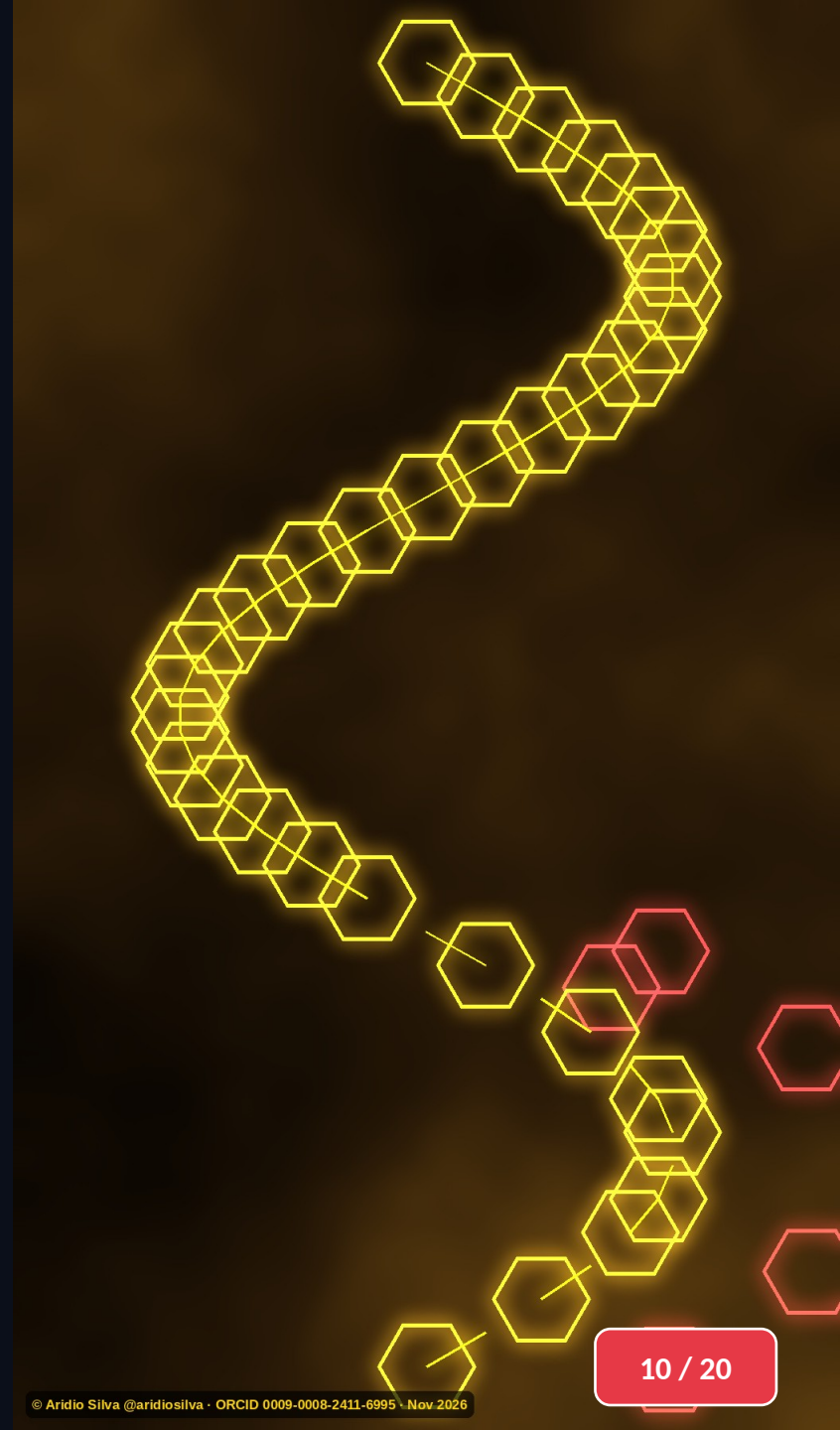
(+) POSITIVO

Rastreio on-chain permitiu apontar suspeitos em horas.

(–) NEGATIVO

Um único endpoint de funcionário bastou para drenar carteiras.

© Aridio Silva @aridiosilva · Novembro 2026



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

GRAVIDADE E ABRANGÊNCIA

Matriz comparativa das ameaças

Ameaça	Tipo de dano	Abrangência	Gravidade*	Confiança na autoria
Sabotagem de refrigeração	Físico, econômico e alimentar	França + 7 países	**ALTA**	Baixa: sem autor
PHP2Shell	Sistêmico (potencial)	Global: ~70% dos sites usam PHP	**CRÍTICA (potencial)**	Não se aplica: descoberta defensiva
Alerta do NCSC	Estratégico (projeção)	Reino Unido, até 2028	**ALTA (projeção)**	Estados citados: China, Rússia, Irã
Roubo da Binance	Financeiro	Global (cripto)	**ALTA**	Média-alta: setor privado

**Avaliação qualitativa do autor com base nas fontes citadas; não é métrica oficial.*

© Aridio Silva @aridiosilva · Novembro 2026

IMPLICAÇÕES

O que muda para empresas e governos

Negativas

- Comida e varejo entram no mapa de alvos de sabotagem
- Equipamento em fim de vida vira passivo sem solução técnica
- Prestadores com acesso remoto ampliam o risco de terceiros
- IA encurta o tempo entre falha e exploração

Positivas

- CERTs nacionais alertaram em menos de 24 h
- Divulgação coordenada do PHP2Shell com IA defensiva
- Investigações penais transnacionais em curso
- Rastreio on-chain acelera a atribuição de roubos

Para GRC

- Inventariar ativos de OT expostos à internet
- Exigir cláusulas de segurança de quem faz manutenção remota
- Plano de substituição de equipamentos EOL
- Monitorar setpoints e alarmes de temperatura

© Aridio Silva @aridiosilva · Novembro 2026

TENDÊNCIAS

Para onde as ameaças apontam

1. **Sabotagem físico-cibernética**
   Setores cotidianos, como varejo e alimentos, somam-se a energia e água.

2. **IA comprimindo prazos**
   Descoberta e exploração de falhas ficam mais rápidas e baratas (PHP2Shell, NCSC).

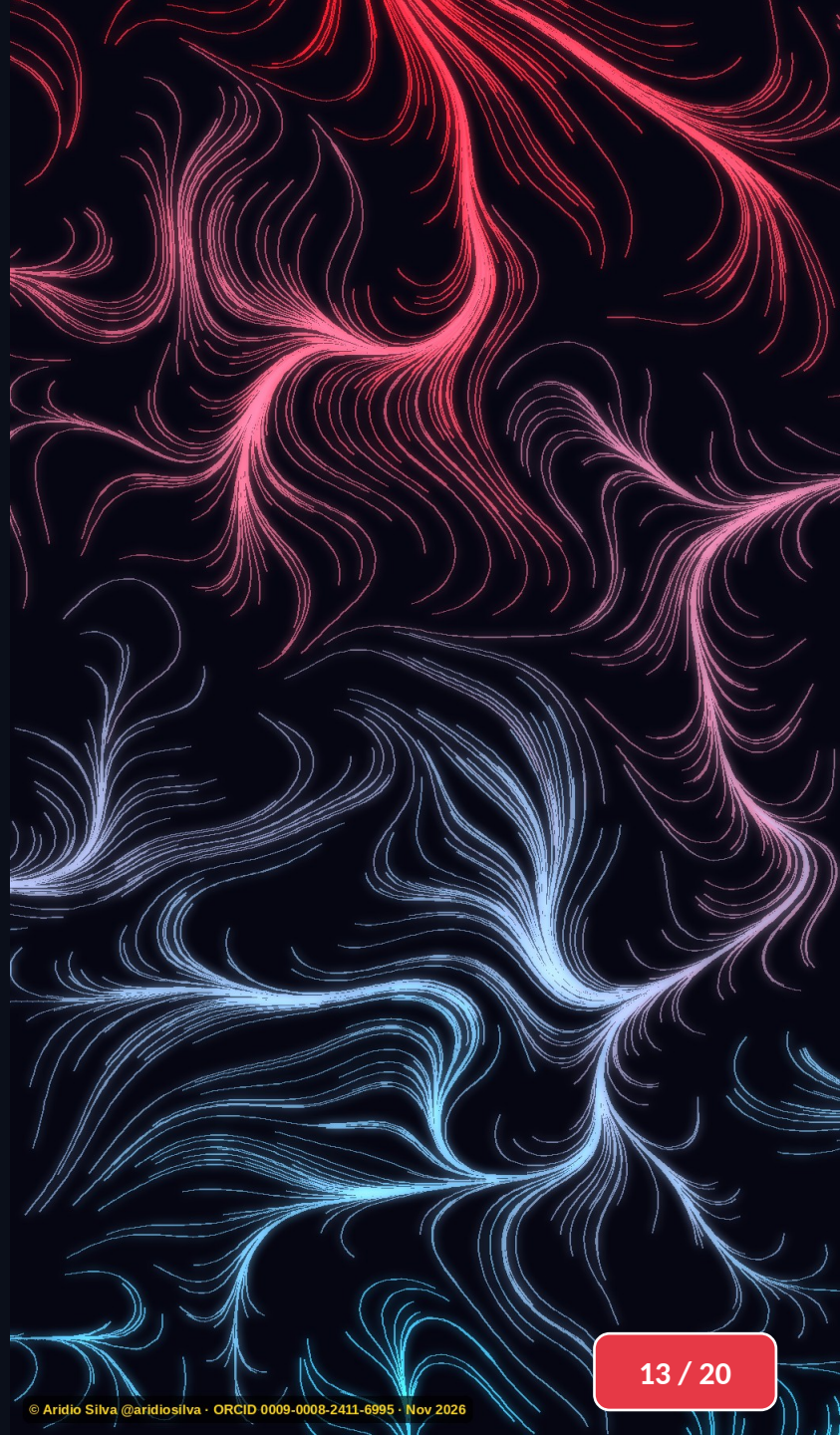
3. **Legado como risco da diretoria**
   Tecnologia barata e desatualizada passa a ser questão de responsabilização.

4. **Ataques pela cadeia de serviço**
   Acesso remoto de manutenção e fornecedores como vetor de massa.

5. **Atribuição pelo setor privado**
   Firmas de análise blockchain e de OT apontam suspeitos antes dos governos.

Tendências: leitura analítica do autor a partir das fontes; não são previsões oficiais.

© Aridio Silva @aridiosilva · Novembro 2026



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

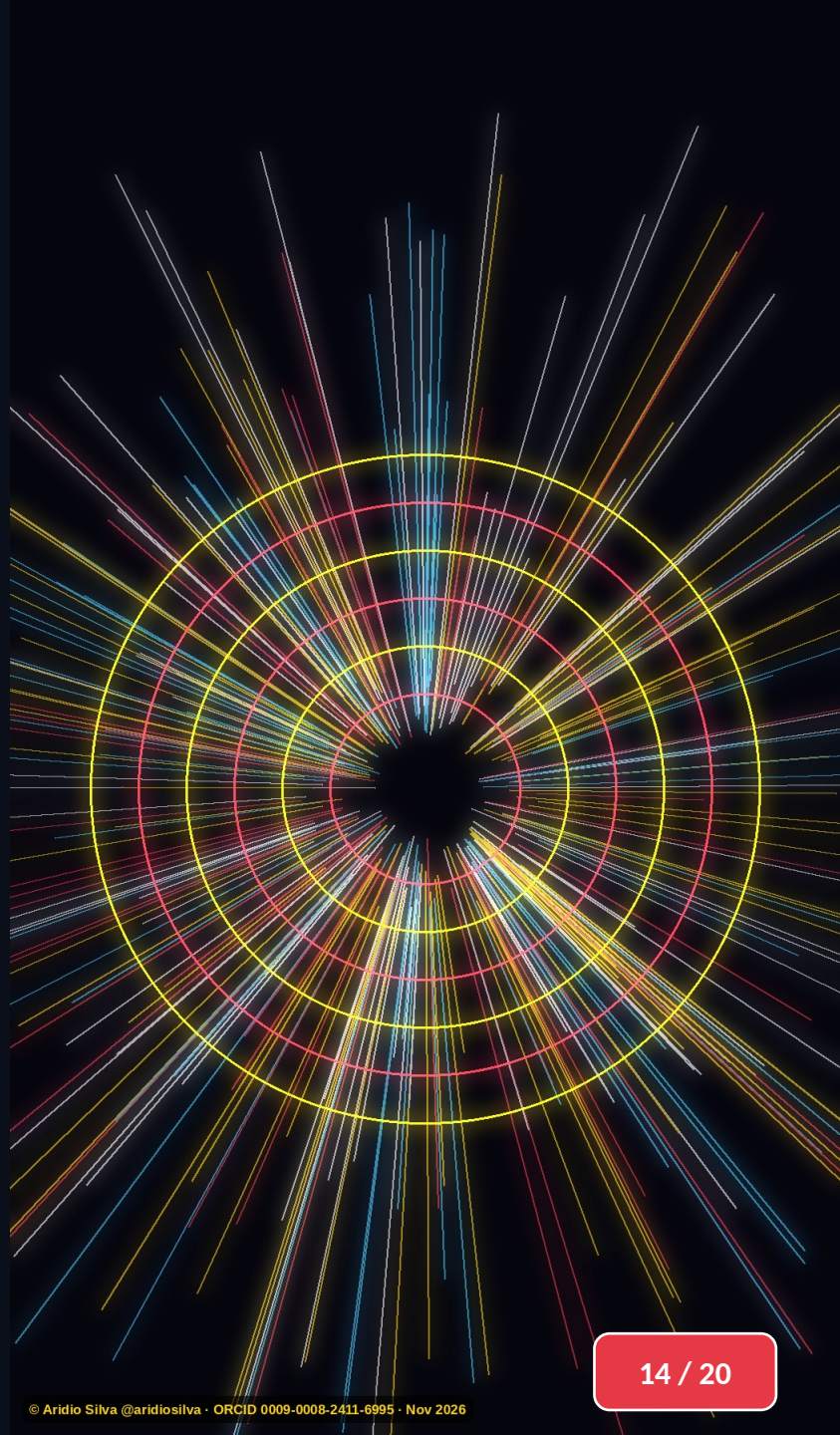
CONCLUSÃO

O risco saiu da tela e chegou à gôndola

Em três semanas, duas ondas de sabotagem forçaram o degelo de refrigeradores em centenas de lojas na França e em pelo menos sete outros países europeus. Os ataques exploraram controladores obsoletos expostos à internet, sem autor identificado e sem pedido de resgate. No mesmo período, a IA mostrou as duas faces: ajudou defensores a achar e corrigir falhas críticas no PHP, e o NCSC a aponta como multiplicador de ataques à infraestrutura crítica até 2028. O roubo de US$ 6,3 bilhões da Binance lembra que atores estatais seguem monetizando falhas operacionais.

A lição comum é de governança: inventariar e isolar ativos legados, controlar o acesso remoto de terceiros e encurtar o tempo de correção. Autoria e vetores ainda em aberto pedem cautela antes de conclusões.

© Aridio Silva @aridiosilva · Novembro 2026



GLOSSÁRIO (1/2)

Glossário de termos

OT (Tecnologia Operacional) Sistemas que controlam processos físicos: refrigeração, energia, água.

ICS Sistemas de Controle Industrial; controladores e supervisórios de OT.

Controlador de refrigeração Central (ex.: Danfoss AK-SM/AK-SC) que gerencia balcões e câmaras de uma loja.

Modo degelo (defrost) Ciclo que aquece o evaporador para tirar gelo; forçado, eleva a temperatura interna.

EOL (fim de vida) Produto que não recebe mais atualizações de segurança.

Firmware Software embarcado que roda dentro do equipamento.

CERT / CSIRT Equipe de resposta a incidentes; o CERT-FR integra a ANSSI.

ANSSI Agência nacional de cibersegurança da França.

CCB Centre for Cybersecurity Belgium, autoridade belga de cibersegurança.

NCSC National Cyber Security Centre, autoridade britânica de cibersegurança.

ENISA Agência da União Europeia para a Cibersegurança.

CVE Identificador público e único de uma vulnerabilidade.

CVSS Escala de 0 a 10 para a severidade de vulnerabilidades.

© Aridio Silva @aridiosilva · Novembro 2026

Glossário de termos

IOC Indicador de comprometimento: IP, hash, domínio ligados a um ataque.

Shodan Buscador de dispositivos conectados à internet.

Bypass de autenticação Acesso a um sistema sem credenciais válidas.

Injeção de comando Execução de comandos arbitrários por entrada não tratada.

RCE Execução remota de código no alvo.

Hacktivismo Ataques cibernéticos com motivação política ou ideológica.

Ameaça híbrida Ações estatais (cibernéticas, sabotagem, desinformação) abaixo do limiar de guerra.

Atribuição Identificação do autor de um ataque com base em evidências.

Lazarus / TraderTraitor Grupos ligados à Coreia do Norte; o TraderTraitor foca em cripto.

Hot wallet Carteira de cripto conectada à internet para operações rápidas.

Divulgação coordenada Publicação da falha acertada entre quem a achou e quem a corrige.

Risco de terceiros Risco trazido por fornecedores e prestadores com acesso aos sistemas.

VPN Túnel cifrado que restringe e protege o acesso remoto.

© Aridio Silva @aridiosilva · Novembro 2026

Fontes primárias (P) e citadas por veículos

- [P] CERT-FR / ANSSI — Alerta CERTFR-2026-ALE-012, incidente em controladores remotos de refrigeração (12–13/10/2026). cert.ssi.gouv.fr — via SecurityWeek, The Hacker News, Brandefense
- [P] CISA — ICSA-25-140-03, vulnerabilidades no Danfoss AK-SM 8xxA. cisa.gov — via Brandefense
- [P] Claroty Team82 — "Freeze the Controller, Defrost the Food" e demonstração na DEF CON — via OCCRP
- [P] NCSC (Reino Unido) — Annual Review 2026 e discurso de Richard Horne (03/11/2026). ncsc.gov.uk — via AP / SecurityWeek
- [P] PHP Foundation — atualização de segurança emergencial PHP2Shell (21/10/2026) — via CNN, Fortune, GovTech
- [P] Forescout — pesquisa sobre hacktivistas e sistemas de refrigeração (2026) — via Cybernews
- [P] Declarações: Danfoss (DR, NOS, AFP, VTM), CCB (Belga, Euronews), Sabcobel (Belga), Carrefour, Coop, ICA, SuperValu, Selver/Kitman Coldtech (ERR)
- [P] Binance (X, 30/10/2026); TRM Labs, Chainalysis e Elliptic — atribuição do roubo — via PA, Reuters, CNN

Acesso em 03/11/2026. [P] = fonte primária; conteúdo conferido na cobertura indicada.

© Aridio Silva @aridiosilva · Novembro 2026

BIBLIOGRAFIA (2/4)

Fontes secundárias: ataques à refrigeração

- 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 · Novembro 2026

BIBLIOGRAFIA (3/4)

Fontes secundárias: ataques à refrigeração

- 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 · Novembro 2026

Fontes secundárias: IA, NCSC e 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 · Novembro 2026