ISS GLOBAL / ANALYSE COMPARATIVE

Cyberattaques contre la chaîne du froid des supermarchés européens

France en octobre, perturbations dans plusieurs pays en novembre

PÉRIODE EXAMINÉE
Du 11 octobre au 9 novembre 2026 · heure de Londres

DATE DE PUBLICATION
2026-11-10

La France a attribué à l'Iran le sabotage des installations frigorifiques en octobre. Des incidents similaires en novembre ont exposé plusieurs pays européens au même type de risque, sans qu'un auteur commun soit établi par les éléments publics.

Ce rapport compare l'attaque des 11 et 12 octobre visant la distribution alimentaire en France et les incidents des 1er et 2 novembre dans plusieurs pays européens. Il couvre les faits rendus publics jusqu'au 9 novembre 2026 à 23 h 59 GMT, dont l'attribution française. Les pays et enseignes présentés constituent une sélection de cas. [1][2][3]

L'analyse distingue les pertes liées à la chaîne du froid des perturbations informatiques subies en octobre par le groupe Ahold Delhaize. Elle dégage des priorités pour les enseignes, les franchisés et les prestataires frigoristes. [10][11]

01 / SYNTHÈSE

Les faits et la portée de la menace

PAYS	OÙ	QUAND
France et plusieurs pays européens	Sites français de la grande distribution. Exemples en novembre : Belgique, Luxembourg, Suède, Irlande, Estonie, Allemagne et Finlande. [1][3][5][6][16]	11 et 12 octobre (France) ; 1er et 2 novembre (plusieurs pays) ; 9 novembre (attribution française). [1][2][3]

Que s’est-il passé ?

Le Centre de coordination des crises cyber (C4) indique que l’attaque d’octobre a visé les contrôleurs frigorifiques d’environ 700 sites français de la grande distribution. Elle a entraîné d’importantes pertes de marchandises et au moins 15 départs de feu. En novembre, des enseignes de plusieurs pays ont signalé des perturbations et retiré de la vente les produits concernés. [2][3][5][6][7]

Portée de la menace

Une intrusion informatique a eu des conséquences sur la sécurité sanitaire des aliments, la continuité d’activité et, en France, la sécurité incendie. Un magasin peut perdre ses produits frais alors que les caisses et les livraisons fonctionnent. Des magasins indépendants peuvent être exposés à la même défaillance s’ils utilisent le même matériel ou mode de maintenance. [2][5][6][7]

> APPRÉCIATION GÉNÉRALE
>
> La France désigne l’unité Shahid Kaveh, liée au Corps des gardiens de la révolution islamique d’Iran, pour l’attaque des 11 et 12 octobre. Les éléments publics examinés ne permettent pas d’étendre cette attribution aux incidents de novembre. Les enseignes doivent restreindre les accès à distance et vérifier que des alarmes indépendantes préviennent le personnel en mesure d’intervenir, y compris la nuit. [1][2][3][4]

02 / RECONSTITUTION

Que s’est-il passé ?

France | nuit du 11 au 12 octobre

Selon le C4, les auteurs ont compromis des contrôleurs frigorifiques et modifié les paramètres de dégivrage. Le centre cite Casino, Leclerc, Coopérative U, Metro, Carrefour et Intermarché parmi les groupes touchés et signale d’autres victimes dans le secteur alimentaire. L’exploitant de l’Intermarché de Gradignan a témoigné séparément de la mise au rebut de marchandises à la suite de l’incident nocturne. [2][9]

Plusieurs pays | nuit du 1er au 2 novembre

La déclaration conjointe de l’UE confirme une nouvelle vague dans plusieurs États membres. Le centre suédois de cybersécurité a signalé des incidents dans la distribution alimentaire et pris contact avec les organisations touchées. En Irlande, Musgrave indique que la surveillance a donné l’alerte. Par précaution, 13 magasins SuperValu ont retiré de la vente des produits réfrigérés et surgelés. Le groupe a annoncé le rétablissement et le réapprovisionnement le 2 novembre. [3][4][7]

Incident parallèle | informatique d’Ahold Delhaize

Le groupe a annoncé son incident informatique le 12 octobre et mis des systèmes hors ligne par précaution. Il a ensuite précisé que ses services en ligne au Benelux et aux États-Unis, ainsi que sa chaîne logistique au Benelux, avaient été touchés. Ses résultats publiés en novembre n’apportent aucun élément reliant cette panne d’octobre aux attaques frigorifiques. [10][11]

03 / COMPARAISON GÉOGRAPHIQUE

Où les perturbations ont été signalées

Chaque exemple s'appuie sur les déclarations d'un exploitant identifié ou d'une autorité nationale. Les chiffres portent sur les exploitants cités, sauf indication contraire.

PAYS / ZONE	DÉCLARATION ET LIMITE DU BILAN
France · octobre	Selon le C4, environ 700 sites de plusieurs groupes ont été visés. Le rapport ne publie pas la liste des sites. [2]
Belgique / Luxembourg	Delhaize a signalé plusieurs dizaines de sites, principalement en Belgique. Carrefour a déclaré 15 sites belges touchés. Selon Delhaize, ses centres de distribution et ses livraisons fonctionnaient normalement. [5]
Suède	ICA a indiqué à Reuters que 23 magasins étaient touchés. Pour Coop, AP a d'abord rapporté six magasins ; Reuters a ensuite cité sept. Le bilan le plus récent de l'enseigne est retenu. [4][5][6]
Irlande	Musgrave a déclaré 13 magasins SuperValu touchés. Ils sont restés ouverts. Le réapprovisionnement a commencé après le rétablissement annoncé par l'exploitant. [5][7]
Estonie	Selver a confirmé à ERR qu'un magasin était touché. L'autorité estonienne des systèmes d'information (RIA) avait reçu un signalement au moment de l'entretien. [8][15]
Allemagne	Edeka a confirmé à Reuters un cas à Reisbach. Il s'agit d'un exemple, sans portée nationale. [6]
Finlande	Yle cite l'autorité nationale confirmant une cyberattaque et signale des perturbations dans quelques petits magasins du groupe K. Aucun chiffre précis. [16]
Pays-Bas / Italie · secteurs connexes	NOS cite un fournisseur qui recense au moins 17 entreprises néerlandaises, dont de petits magasins et des sites hors distribution. ANSA cite l'autorité italienne sur deux cas, en restauration collective et dans la production de surgelés. Aucun bilan national des supermarchés. [17][18]
Royaume-Uni · secteur connexe	La fédération AIMS a signalé trois fournisseurs britanniques de viande touchés. Ce chiffre ne porte pas sur les supermarchés. [13]

La déclaration conjointe de l'UE ne fournit pas de décompte harmonisé. Cette sélection ne permet ni d'identifier les pays épargnés ni de classer leur niveau d'exposition. [3]

04 / CHRONOLOGIE

Faits et annonces publiques

DATE DES FAITS	ÉVÉNEMENT OU DÉTECTION
11 et 12 oct. · heure locale	France : compromission nocturne de contrôleurs frigorifiques. Le C4 est alerté le 12 octobre. [2]
12 et 13 oct. · heure locale	Le Monde a fait état par la suite d'un second épisode français, plus limité, la nuit suivante. Son inclusion dans l'attribution publique reste incertaine. [12]
1er et 2 nov. · heure locale	Les autorités de l'UE situent la nouvelle vague dans cet intervalle. Les heures de détection varient selon les exploitants ; aucune heure commune de début n'est établie. [3][5][7]

DATE DE PUBLICATION	ÉLÉMENT RENDU PUBLIC
12 et 19 oct.	Ahold Delhaize annonce son incident informatique le 12 octobre, puis explique ses mises hors ligne par précaution le 19. [10]
2 et 3 nov.	Des autorités nationales et des exploitants signalent les perturbations frigorifiques de novembre. Certains bilans par enseigne sont actualisés. [4][5][6][7][8]
4 nov.	Des organismes de l'UE appellent ensemble à réduire l'exposition. Ahold Delhaize publie séparément ses estimations financières. [3][11]
9 nov.	La France désigne publiquement l'unité Shahid Kaveh. Le parquet de Paris annonce avoir requis des mandats d'arrêt internationaux. La France indique qu'elle proposera des sanctions européennes. [1][2][12]

Les dates des faits sont données en heure locale. La collecte s'arrête le 9 novembre à 23 h 59 GMT. La date de publication ou de détection ne permet pas de dater l'accès initial.

05 / ATTRIBUTION

Le périmètre de l’attribution

Position officielle | attribution française établie

La France attribue à l’Iran le sabotage frigorifique des 11 et 12 octobre. Le C4 désigne le Corps des gardiens de la révolution islamique (CGRI) comme commanditaire et l’unité Shahid Kaveh comme exécutante. Le ministère et le C4 relèvent de la même démarche d’attribution. Ils font autorité sur la position française, mais les journaux techniques et la chaîne de preuve complète n’ont pas été publiés. [1][2]

Portée des indices publics | analyse ISS Global

Le C4 cite des recoupements entre l’infrastructure d’attaque et des activités antérieures, le relais de l’attaque par un média associé à l’unité et des traces de persan dans l’infrastructure. Un recoupement d’infrastructure pèse davantage s’il est vérifié indépendamment. Les traces linguistiques et le relais médiatique ne suffisent pas à établir une responsabilité. Le Monde rapporte les réquisitions du parquet de Paris, qui ne constituent ni des mandats délivrés ni des condamnations. [2][12]

Novembre | auteur indéterminé

Le calendrier, le secteur et les effets justifient d’examiner un lien. Des acteurs différents peuvent toutefois viser le même type de matériel et provoquer des pannes similaires. La déclaration de l’UE confirme la vague de novembre sans l’attribuer. SVT a rapporté des revendications de groupes prorusses, qui ne sont pas vérifiées et ne permettent pas d’identifier les auteurs. [19] Le rapport du C4 évoque aussi une autre unité iranienne, Shahid Shoostari, pour d’autres opérations. L’attribution française de l’attaque frigorifique d’octobre désigne Shahid Kaveh. [1][2][3]

> ÉLÉMENTS QUI CHANGERAIENT L’ANALYSE
>
> Des concordances transfrontalières authentifiées dans les journaux techniques, les infrastructures ou d’autres indices distinctifs, vérifiées par des enquêteurs indépendants, pèseraient davantage que la similitude des dégâts.

06 / CONSÉQUENCES

Dégâts et effets sur l’activité

France | ampleur et évaluation des pertes

Le C4 indique qu’environ 700 sites ont été visés ; le ministère des affaires étrangères en indique plus de 700. Ces chiffres portent sur les sites visés. Ils ne dénombrent ni incendies ni fermetures ni pertes vérifiées dans chaque site. Le C4 rapporte au moins 15 départs de feu. Le ministère estime les pertes alimentaires à plusieurs dizaines de millions d’euros, sans ventilation auditée dans les publications citées. [1][2]

Novembre | perturbations locales

Les enseignes signalent des retraits de produits et une disponibilité réduite dans certains magasins. Delhaize indique que les livraisons ont continué ; Musgrave annonce un rétablissement le jour même. En Estonie, ERR a rapporté une modification de consigne. Une consigne ne mesure ni la température de l’air du meuble ni celle des produits. Les sources retenues n’établissent ni bilan financier européen ni nombre de blessés. [3][5][7][8]

Ahold Delhaize | estimation financière distincte

Le 4 novembre, le groupe a estimé que son incident informatique d’octobre réduirait de 200 à 250 millions d’euros le chiffre d’affaires net et de 75 à 100 millions d’euros le résultat d’exploitation sous-jacent et au sens des normes IFRS. Il s’agit d’estimations portant sur des indicateurs distincts, qui ne s’additionnent pas et ne chiffrent pas les dégâts frigorifiques. La plupart des perturbations ont été maîtrisées en deux semaines ; le rétablissement se poursuivait à la date du communiqué. [11]

Hors distribution | dossiers distincts

Au Royaume-Uni, les signalements de novembre concernent des fournisseurs de viande. En France, le ministère de la Santé a signalé un incident touchant des équipements frigorifiques utilisés pour le stockage du sang, sans produit sanguin compromis, selon AP. Ces cas sont exclus du bilan des supermarchés et ne prouvent pas l’existence d’un auteur commun. [13][14]

07 / EXAMEN DES ÉLÉMENTS

Ce qui reste à établir

POINT À VÉRIFIER	APPRÉCIATION À LA DATE DE CLÔTURE
Périmètre français en octobre	Retenir le chiffre approximatif du C4 pour l'analyse et conserver séparément la formulation du ministère. Un relevé par site est nécessaire pour ventiler les pertes, fermetures ou incendies par enseigne. [1][2]
Seconde nuit en France	Le Monde distingue l'épisode des 12 et 13 octobre. L'attribution du C4 vise les 11 et 12 octobre. Traiter la seconde nuit à part dans l'attente d'une clarification des enquêteurs français. [2][12]
Bilans de novembre par pays	Les bilans des exploitants sont provisoires et leurs définitions peuvent différer. Ne pas additionner signalements, magasins, appareils et fournisseurs. Vérifier les identifiants des sites et incidents avant tout total. [3][5][6][13][15]
Ahold et Delhaize	L'incident informatique du groupe en octobre et le signalement frigorifique de l'enseigne Delhaize en novembre diffèrent par leur date, leur périmètre et leurs effets. Les traiter séparément en l'absence de lien établi. [5][10][11]
Photographies des magasins	Des photos publiées à propos de Caen et de Lucan illustrent l'état des magasins selon les médias. Faute de métadonnées originales, de couverture de tous les sites et de droits de reproduction établis, aucune image ne sert à établir les températures ou l'attribution. [7][9]

LIMITES DE L'ANALYSE

Cette étude en sources ouvertes porte sur une sélection de cas. Elle ne permet ni de dénombrer tous les sites touchés, ni de reproduire indépendamment l'attribution française, ni d'écarter un lien entre les vagues.

08 / PRIORITÉS OPÉRATIONNELLES

Protéger les stocks et maintenir l’activité

Dès aujourd’hui | équipes techniques, sécurité informatique et prestataires

Désigner un responsable des installations frigorifiques par site, franchisés compris. Vérifier quels accès distants sont nécessaires. Supprimer l’exposition directe à Internet et limiter les accès nécessaires à des canaux authentifiés et surveillés. Coordonner les changements avec les frigoristes pour préserver le fonctionnement local en toute sécurité. [3][4]

Dès aujourd’hui | magasins et sécurité sanitaire

Tester les capteurs indépendants, la transmission des alarmes et l’astreinte de nuit. Si les relevés ne sont pas fiables, isoler les produits concernés et consigner les heures et températures avant toute décision de remise en vente, de transfert ou de destruction, selon les procédures sanitaires. Signaler toute surchauffe selon les consignes de sécurité du site.

Cette semaine | maintenance et réponse à incident

Inventorier les contrôleurs et les dépendances de maintenance. Prioriser les mises à jour et les équipements qui ne sont plus pris en charge. Conserver si possible l’historique des configurations, les journaux d’accès et les relevés indépendants. Consigner l’heure locale et l’heure UTC, le moment de détection et la différence entre la température mesurée et la consigne. Tester séparément le rétablissement et le réapprovisionnement.

Pour les enquêteurs | distinguer les liens des similitudes

Demander un registre de sites sans doublons, les journaux d’origine des exploitants et prestataires et les rapports des services d’incendie pour les cas français. Solliciter une comparaison transfrontalière des éléments de novembre auprès des autorités nationales. Relever les matériels communs à titre de contexte et laisser l’attribution ouverte jusqu’à preuve suffisante. [2][3][4]

> SUIVRE LES MESURES MISES EN PLACE
>
> Recenser les sites dotés d’un responsable identifié, d’un accès restreint vérifié et d’une alarme indépendante testée. Réapprovisionner seulement après validation du responsable de la sécurité sanitaire.

REGISTRE DES SOURCES

Sources 01–05

Le registre précise l’origine des sources et les limites d’accès. La reprise d’une déclaration ne constitue pas une preuve indépendante.

01 Déclaration d’attribution à l’Iran de cyberattaques visant la France

France Diplomatie · 2026-11-09

Origine : Attribution du gouvernement français · Consulté le 10 nov. 2026. Déclaration lue en français ; position et estimations de l’État.

https://www.diplomatie.gouv.fr/fr/presse-et-ressources/decouvrir-et-informer/actualites/declaration-d-attribution-a-l-iran-de-cyberattaques-visant-la-france

02 Activités cyber offensives ciblant la France menées par des acteurs iraniens liés au CGRI

C4 / **CERT-FR** · 2026-11-09

Origine : Attribution du gouvernement français · Consulté le 10 nov. 2026. Rapport public lu en français ; données d’investigation sous-jacentes non publiées.

https://www.cert.cyber.gouv.fr/uploads/CERTFR-2026-CTI-009.pdf

03 Joint statement on cyber incidents in refrigeration systems across the EU

European Commission / **EU cyber partners** · 2026-11-04

Origine : Déclaration conjointe des autorités de l’UE · Consulté le 10 nov. 2026. Déclaration lue en anglais ; ni décompte des sites ni attribution.

https://digital-strategy.ec.europa.eu/en/news/joint-statement-cyber-incidents-refrigeration-systems-across-eu

04 Cyberangrepp mot uppkopplade frys- och kylsystem

Nationellt cybersäkerhetscenter (Sweden) · 2026-11-02

Origine : Autorité nationale suédoise de cybersécurité · Consulté le 10 nov. 2026. Note lue en suédois ; aucun bilan par enseigne.

https://www.ncsc.se/sv/aktuellt/cyberangrepp-mot-kylsystem

05 Supermarket freezers in several European countries hit by apparent cyberattacks

Associated Press · 2026-11-02

Origine : Enquête AP / exploitants identifiés · Consulté le 10 nov. 2026. Dépêche lue en anglais ; premiers témoignages d’exploitants et d’agences.

https://apnews.com/article/a8ea5b30d67da47957769f29101fe686

REGISTRE DES SOURCES

Sources 06–10

Le registre précise l’origine des sources et les limites d’accès. La reprise d’une déclaration ne constitue pas une preuve indépendante.

06 European supermarkets rush to patch vulnerabilities after region-wide fridge hack

Reuters via Investing.com · 2026-11-03

Origine : Enquête Reuters / exploitants identifiés · Consulté le 10 nov. 2026. Dépêche reproduite lue en anglais ; bilans communiqués par les exploitants.

https://www.investing.com/news/stock-market-news/european-supermarkets-rush-to-patch-vulnerabilities-after-regionwide-fridge-hack-4995896

07 SuperValu says issues after cyberattack on its fridge systems ‘fully resolved’

The Irish Times · 2026-11-02

Origine : Enquête de The Irish Times / Musgrave · Consulté le 10 nov. 2026. Article lu en anglais ; rétablissement annoncé par Musgrave.

https://www.irishtimes.com/technology/data-security/2026/11/02/supervalu-removes-frozen-and-chilled-food-from-13-stores-after-cyber-attack-on-fridges/

08 Hackers raised freezer temperature at Selver supermarket to +50°C

ERR · 2026-11-02

Origine : Enquête ERR / Selver et prestataire · Consulté le 10 nov. 2026. Article lu en anglais ; le titre renvoie à une consigne, pas à une mesure sur les produits.

https://news.err.ee/1610183296/hackers-raised-freezer-temperature-at-selver-supermarket-to-50-c

09 A disastrous day for French supermarkets after massive cyberattack targets refrigeration systems

Le Monde · 2026-10-13

Origine : Enquête du Monde / exploitant du magasin · Consulté le 10 nov. 2026. Extrait abonnés lu en anglais ; témoignage direct à Gradignan.

https://www.lemonde.fr/en/economy/article/2026/10/13/a-disastrous-day-for-french-supermarkets-after-massive-cyberattack-targets-refrigeration-systems_6758535_19.html

10 Ahold Delhaize update on status of cybersecurity incident

Ahold Delhaize · 2026-10-19

Origine : Communications du groupe Ahold Delhaize · Consulté le 10 nov. 2026. Communiqué lu en anglais ; mesures de confinement, sans lien causal établi.

https://newsroom.aholddelhaize.com/ahold-delhaize-update-on-status-of-cybersecurity-incident/

REGISTRE DES SOURCES

Sources 11–15

Le registre précise l’origine des sources et les limites d’accès. La reprise d’une déclaration ne constitue pas une preuve indépendante.

11 Ahold Delhaize reports resilient Q3 2026 results and updates 2026 guidance to reflect business disruption caused by recent cybersecurity incident

Ahold Delhaize · 2026-11-04

Origine : Communications du groupe Ahold Delhaize · Consulté le 10 nov. 2026. Communiqué lu en anglais ; effets financiers prévisionnels.

https://newsroom.aholddelhaize.com/ahold-delhaize-reports-resilient-q3-2026-results-and-updates-2026-guidance-to-reflect-business-disruption-caused-by-recent-cybersecurity-incident

12 Cyberattaque contre des réfrigérateurs de supermarchés : la justice ouvre une enquête contre un groupe iranien lié aux gardiens de la révolution

Le Monde · 2026-11-09

Origine : Enquête du Monde / parquet de Paris · Consulté le 10 nov. 2026. Article lu en français dans sa version actualisée ; annonce du parquet du 9 novembre.

https://www.lemonde.fr/pixels/article/2026/11/09/cyberattaque-des-refrigerateurs-de-supermarche-la-justice-ouvre-une-enquete-contre-un-groupe-iranien-jean-noel-barrot-souhaite-des-sanctions-a-l-echelle-europeenne_6808673_4408996.html

13 British businesses caught in Europe-wide supermarket fridge attacks

The Record · 2026-11-03

Origine : Enquête de The Record / AIMS · Consulté le 10 nov. 2026. Article lu en anglais ; le témoignage de la fédération concerne des fournisseurs.

https://therecord.media/british-businesses-caught-in-europe-wide-supermarket-fridge-attacks

14 Cyberattack hits French blood bank site but no blood products are compromised

Associated Press · 2026-11-04

Origine : Enquête AP / ministère français de la Santé · Consulté le 10 nov. 2026. Dépêche lue en anglais ; déclaration du ministère de la Santé, hors grande distribution.

https://apnews.com/article/12b80bcf93b8404264209e519c204919

15 Kraft: millised on rünnakute motiivid, pole praegu teada

ERR · 2026-11-02

Origine : Entretien ERR / autorité estonienne RIA · Consulté le 10 nov. 2026. Entretien lu en estonien ; un seul signalement reçu par la RIA à cette heure.

https://www.err.ee/1610183710/kraft-millised-on-runnakute-motiivid-pole-praegu-teada

REGISTRE DES SOURCES

Sources 16–19

Le registre précise l’origine des sources et les limites d’accès. La reprise d’une déclaration ne constitue pas une preuve indépendante.

16 Kyberturvallisuuskeskus vahvistaa: kauppojen kylmälaitehäiriöt johtuivat kyberhyökkäyksestä

Yle · 2026-11-04

Origine : Enquête Yle / autorité finlandaise · Consulté le 10 nov. 2026. Article lu en finnois ; attaque confirmée par l’autorité, sans décompte précis des magasins.

https://yle.fi/a/74-20255142

17 Ook koelsystemen in Nederland aangevallen, bij 17 bedrijven temperatuur aangepast

NOS · 2026-11-02

Origine : Enquête NOS / fournisseur frigoriste · Consulté le 10 nov. 2026. Article lu en néerlandais ; décompte du fournisseur, incluant des sites hors distribution.

https://nos.nl/artikel/2637734-ook-koelsystemen-in-nederland-aangevallen-bij-17-bedrijven-temperatuur-aangepast

18 Attacchi hacker ai supermercati, alert Agenzia cyber in Italia

ANSA · 2026-11-02

Origine : Dépêche ANSA / autorité italienne · Consulté le 10 nov. 2026. Article lu en italien ; les cas cités concernent des acteurs de la filière, hors supermarchés.

https://www.ansa.it/sito/notizie/cronaca/2026/11/02/attacchi-hacker-ai-supermercati-alert-agenzia-cyber-in-italia_6a838d5b-aef2-48ac-b082-37c487819ded.html

19 Pro-ryska grupper påstår sig ligga bakom flera kylattacker

SVT Nyheter · 2026-11-04

Origine : Enquête SVT / revendications publiques · Consulté le 10 nov. 2026. Article lu en suédois ; revendications non vérifiées, sans attribution.

https://www.svt.se/nyheter/utrikes/pro-ryska-grupper-pastar-sig-ligga-bakom-flera-kylattacker