Affaire des frigos piratés : comment la France a remonté la piste jusqu'à l'Iran

Paris accuse Téhéran d'une cyberattaque massive ayant touché 700 supermarchés en octobre. Les services de renseignement et de cybersécurité français ont identifié les auteurs présumés de l'opération.



La cyberattaque de mi-octobre avait affecté environ 700 supermarchés en France. (Photo Fred Tanneau/AFP)

Par Diane Jeantet, Marie Delumeau
Publié le 9 nov. 2026 à 18:01 | Mis à jour le 10 nov. 2026 à 14:33

Réservé à nos abonnés

Certains regards s'étaient tournés vers Moscou… mais c'est l'Iran que la France a accusé ce lundi d'être responsable du piratage de centaines de frigos dans des supermarchés français il y a quelques semaines. « La responsabilité de cette attaque revient au corps des Gardiens de la révolution de la République islamique d'Iran », a affirmé le ministre des Affaires étrangères, Jean-Noël Barrot, en marge du G7.

Le chef de la diplomatie a dénoncé une « attaque d'une ampleur inédite et d'une agressivité inédite », et promis « des sanctions à l'échelle européenne contre tous les responsables de cette attaque ». L'ambassadeur d'Iran en France a également été convoqué lundi.

De son côté, Téhéran a rejeté mardi « les accusations infondées et unilatérales du gouvernement français à l'encontre de l'Iran concernant de prétendues activités cyber en France ».

Un groupe lié aux gardiens de la révolution

Le 12 octobre, le Centre de coordination des crises cyber est alerté d'une attaque touchant les contrôleurs de froid d'environ 700 sites de la grande distribution sur

tout le territoire : Casino, Leclerc, Coopérative U, Metro, Carrefour… mais aussi plusieurs petites boucheries, un abattoir et des usines agroalimentaires coopératives, selon les autorités françaises.

Dans la nuit, les paramètres de dégivrage des équipements en question ont été modifiés pour être fixés à de fortes températures. La hausse subite des températures des frigos entraîne au moins 15 départs de feu, et des pertes de marchandise évaluées à plusieurs dizaines de millions d'euros. Plusieurs équipements Schneider Electric appartenant à de petites installations hydroélectriques en France sont aussi touchés, sans causer de dégâts majeurs.

Lire aussi :
DECRYPTAGE - Cybersécurité : à l'Assemblée, l'examen du projet de loi « résilience » rime avec urgence

Pour les agences françaises de renseignement et de cybersécurité, la piste iranienne est désormais établie. Dans un rapport publié ce lundi, cinq agences françaises dont la DGSE et la DGSI accusent les Gardiens de la révolution d'être commanditaires de l'attaque, et l'unité cyberoffensive Shahid Kaveh, son exécutante.

Cette dernière, dirigée par Reza Salarvand et Mahdi Lashgarian, « mène des campagnes de ciblage d'équipements industriels à grande échelle à des fins de sabotage, principalement dirigées à l'encontre d'Israël et des Etats-Unis, mais aussi de la France et d'autres pays européens », détaille le rapport.

Le parquet ouvre une information judiciaire

Ce groupe a par exemple revendiqué une attaque, fin 2023, contre la société israélienne Unitronics, qui produit des systèmes de contrôle industriel utilisés aux Etats-Unis et en Europe. Ou encore une campagne similaire à celle qui vient de se produire en France, visant des équipements frigorifiques israéliens en mars et avril 2026. Le rapport précise que l'unité Shahid Kaveh « possède, au moins depuis juin 2024, des scripts permettant de scanner, d'accéder et de contrôler des équipements de contrôle industriel des marques Schneider Electric, Siemens et Rockwell ».

Les agences de renseignement rappellent par ailleurs que la menace cyber iranienne contre les intérêts français n'est pas nouvelle. L'Iran a conduit plusieurs actes de déstabilisation contre la France, ciblant notamment l'hebdomadaire « Charlie Hebdo » en 2023 ainsi que l'organisation des Jeux Olympiques de Paris en 2024.

Lire aussi :
DECRYPTAGE - Après les frigos piratés, l'IA et la géopolitique aggravent la menace cyber

Les enquêteurs ont mis au jour un mode opératoire d'attaque caractéristique de cette unité de cyberoffensive iranienne. Les hackeurs ont par exemple utilisé l'outil de scan Fofa, « habituellement utilisé par le mode opératoire d'attaque dans les différentes actions qu'il mène ». L'utilisation du farsi et d'adresses IP renvoyant vers des terminaux localisés en Iran a aussi contribué à les orienter.

Des mandats d'arrêt internationaux à l'encontre des trois individus ont été requis par le parquet. En parallèle, la procureure de la République de Paris a annoncé que le parquet avait ouvert une information judiciaire visant le chef du groupe iranien Shahid Kaveh et ses deux adjoints. Les chefs d'accusation retenus contre eux sont aggravés puisque les faits auraient été commis « dans le but de servir une puissance étrangère », a précisé la procureure.

D'autres pays touchés en Europe

Il y a quelques jours, des magasins dans une dizaine d'autres pays européens,dont la Belgique et la Suède, ont également été perturbés par des incidents similaires. La cheffe de la diplomatie européenne, Kaja Kallas, a indiqué ce lundi que le sujet sera abordé lors du prochain Conseil des affaires étrangères, et que ces incidents « appellent également une réponse forte de notre part ».

Dans un premier temps, la presse spécialisée avait rapporté que deux groupes de hackeurs prorusses avaient revendiqué les cyberattaques visant des frigos de supermarchés en Europe. Le Kremlin avait néanmoins démenti le 5 novembre toute implication dans cette affaire et déclaré que ces accusations étaient « absolument absurdes ».