Réservé aux abonnés

Plongée dans les opérations secrètes de Shahid Kaveh, l'armée de l'ombre iranienne suspectée d'avoir saboté les frigos de supermarchés français

Par **Steve Tenré**

Publié le 09/11/2026 à 20h42



Des Gardiens de la Révolution iraniens défilent à Téhéran, en février dernier (photo d'illustration). *ATTA KENARE / AFP*

DÉCRYPTAGE - Aussi connus sous le nom de «CyberAv3ngers» et de «Intelligence Team 13», ces hackeurs iraniens, liés au régime de Téhéran, sont considérés par nombre d'observateurs comme l'«une des unités les plus agressives» des Gardiens de la Révolution islamique.

700 commerces ciblés, des tonnes de nourritures jetées, des *«départs d'incendie»*… Le bilan de la surprenante cyberattaque ayant touché les réfrigérateurs connectés français les 11 et 12 octobre derniers est lourd, très lourd. Si lourd, et si déconcertant, que les autorités françaises ont travaillé

d'arrache-pied depuis sa survenue pour retrouver les coupables de cet assaut d'envergure, duquel ont également pâti d'autres pays européens, tels que le Royaume-Uni, l'Allemagne, l'Italie, le Portugal ou les Pays-Bas.

Le couperet est tombé ce lundi 9 novembre: selon le chef de la diplomatie française, Jean-Noël Barrot, les autorités sont ce jour *«en mesure de confirmer que la responsabilité de cette attaque revient au corps des Gardiens de la révolution de la République islamique d'Iran»*. *«C'est une attaque d'une ampleur inédite et d'une agressivité inédite (…) Nous prendrons des sanctions à l'échelle européenne contre tous les responsables de cette attaque.»* Auprès du *Figaro*, le parquet de Paris, dont la section cybercriminalité s'est saisie de l'affaire au titre de sa compétence nationale, a confirmé les soupçons évoqués par Jean-Noël Barrot, et a annoncé dans un communiqué l'ouverture d'une information judiciaire *«contre le chef du groupe iranien Shahid Kaveh»*.

Une hiérarchie très structurée

Le groupe Shahid Kaveh est loin d'être un petit nouveau dans le paysage cybercriminel: le réseau a fait l'objet de multiples fiches de renseignements et de notices rouges, tantôt émises par des agences de cybersécurité internationales, tantôt rédigées par des organismes indépendants spécialisés. D'après DomainTools Investigations, programme de recherche dédié au renseignement sur les cybermenaces, Shahid Kaveh est l'*«une des unités les plus agressives sur le plan opérationnel et les plus solidement ancrées idéologiquement de l'arsenal cyber des Gardiens de la révolution islamique».* Selon la CISA, l'agence de cybercriminalité américaine, Shahid Kaveh représente une *«menace persistante avancée»*, expression employée pour désigner des acteurs organisés, disposant de capacités techniques hors du commun pouvant cibler des infrastructures critiques. Enfin, pour Orion Policy, institut de recherche localisé à Washington, Shahid Kaveh, aussi connu sous les noms *«CyberAv3ngers, Hydro Kitten, Storm-0784, APT Iran, Bauxite, Mr. Soul, Soldiers of Solomon, UNC5691»*, le groupuscule est directement lié aux Gardiens de la Révolution iraniens, avec une structure organisationnelle majoritairement secrète, mais bien établie en interne.

Et pour cause: selon les informations disponibles à date, Shahid Kaveh est sous la houlette directe d'Hamid Reza Lashgarian, responsable du Commandement cyber-électronique de Téhéran et l'un des commandants des forces Qods, la

branche des Gardiens de la révolution chargée des opérations extérieures et du soutien aux groupes armés alliés de Téhéran. Sous son autorité, Shahid Kaveh est divisé en deux équipes: l'Intelligence Groupe 13, guidée par Reza Salarvand, chargée d'identifier les infrastructures occidentales critiques exposées à Internet, les vulnérabilités de certains logiciels massivement utilisés et les failles dans les comptes utilisateurs des entreprises et des institutions; et les CyberAv3ngers, soit la main armée de Shahid Kaveh, qui mène les cyberattaques, revendique sur Telegram, et produit de la propagande à la gloire du régime iranien sur les réseaux sociaux.

Les deux équipes ont fait de la *«guerre psychologique»* leur terrain de jeux, selon les multiples rapports consultés. Leur objectif n'est pas seulement de *«déstabiliser»* les adversaires de Téhéran avec des cyberattaques, mais de montrer que ces derniers ne sont à l'abri d'aucun assaut numérique - preuve en sont les attaques contre les frigos français.

Propagande religieuse et nationaliste

Ainsi, les CyberAv3ngers sont souvent vus en train de publier via leurs canaux Telegram, via leurs comptes Instagram et via les *«réseaux liés à la diaspora»* iranienne d'après DomainTools, des photos des dégradations qu'ils provoquent et des captures d'écran de fenêtres informatiques prouvant leur prise de contrôle sur des systèmes électroniques. Ils accompagnent leurs photos et vidéos de messages *«souvent émaillés de références au nationalisme religieux, de citations de martyrs et de rhétorique antisioniste, contribuant ainsi à renforcer le discours idéologique des Gardiens de la révolution. CyberAv3ngers ne se contente pas de réagir aux événements: le groupe publie des avertissements avant ses attaques, s'en glorifie une fois les opérations menées et menace de lancer de nouvelles campagnes»*, explique DomainTools.

Fait à noter d'ailleurs, le groupe *«Shahid Kaveh»* tire directement son nom de Mohammad Kaveh, un commandant du CGRI fait *«martyr pendant la guerre Iran-Irak en 1986 à l'âge de 25 ans»*, d'après DomainTools. *«Il a dirigé des opérations d'élite du CGRI au Kurdistan et dans l'ouest de l'Iran et était considéré comme un modèle révolutionnaire de sacrifice, de bravoure et d'obéissance (…) En invoquant le martyre, ces unités présentent leurs opérations non seulement comme des missions tactiques, mais comme des continuations sacrées d'une lutte*

historique et spirituelle. Le Shahid Kaveh Group s'inspire directement de cet héritage pour insuffler à ses opérations cyber une légitimité idéologique et une résonance émotionnelle», souligne le site de recherches.

Un mode opératoire bien rodé

L'une des premières traces documentaires liées au groupe remonte à l'année 2021, lorsque la chaîne britannique SkyNews parvient à obtenir 57 pages de rapports produits par la cellule Intelligence Team 13. Trois documents sortent alors du lot: l'un d'eux est consacré à l'entreprise allemande Wago, fabricant de composants électriques. L'autre porte sur les systèmes électroniques qui permettent de gérer les lumières, la ventilation ou le chauffage des bâtiments connectés. Un troisième est dédié au transport maritime, et aborde les systèmes de communication satellitaire, les équipements de navigation, la gestion des eaux de ballast des navires… Les trois rapports, très techniques, étaient affublés de la mention *«Très confidentiel»*, écrit en farsi, et accompagnés d'une phrase attribuée à l'ex-guide suprême iranien, Ali Khamenei, qui appelait la *«République islamique d'Iran à devenir l'un des acteurs les plus puissants au monde»*.

Ces tout premiers documents retrouvés démontraient déjà le cœur du mode opératoire de Shahid Kaveh, dont l'objectif affiché est de nuire aux *«ennemis»* de Téhéran de façon *«asymétrique»*, en ne cherchant pas seulement à pénétrer des sites internet pour y voler des données, mais en exploitant les systèmes informatiques permettant de contrôler des installations, quant à elles, bien physiques.

Le groupe, qui a émergé en 2020, a dès ses débuts revendiqué sur ses réseaux sociaux l'attaque de plus de 150 serveurs industriels du réseau ferroviaire israélien, perturbant, selon lui, 28 gares et stations de métros. Fin 2020, ils ont publié une vidéo dans laquelle ils clamaient avoir momentanément pris le contrôle d'une installation hydraulique en Israël, grâce à une faille selon la firme de cybersécurité Otorio. *«Cela offrait aux attaquants un accès direct au système, leur permettant d'en modifier librement les paramètres: pression de l'eau, température, et bien d'autres valeurs. Une simple connexion à Internet et un navigateur web leur suffisaient pour prendre le contrôle de ces réglages»*, écrivait la société dans un billet de blog.

Depuis, le groupe multiplie les faits d'armes à l'international, qui lui servent, surtout, d'entraînements. En novembre 2023, les hackeurs accèdent à un automate Unitronics de la compagnie municipale des eaux d'Aliquippa, en Pennsylvanie (États-Unis), mettant hors service une pompe régulant la pression de l'eau. Entre novembre 2023 et janvier 2024, ils compromettent 75 appareils aux États-Unis, dont 34 dans le secteur de l'assainissement de l'eau, selon le FBI. Sur la même période, ils lancent l'assaut contre une usine et un système de fontaines à eau en République tchèque, et une entreprise de distribution d'eau en Roumanie. Le groupe revendique en janvier 2024 l'attaque de quelque 200 stations-service situées en Israël et aux États-Unis. En août 2024, la société de cybersécurité Claroty découvre IOControl, un logiciel malveillant conçu par l'Iran pour s'en prendre aux infrastructures civiles, et pour infecter des équipements connectés fonctionnant sous le système d'exploitation Linux, tels que des routeurs, des caméras, des automates industriels, des systèmes de gestion de carburant… La même année, OpenAI, maison-mère de ChatGPT, a également tiré le signal d'alarme, annonçant avoir banni de nombreux comptes appartenant aux CyberAv3ngers. *«Les comptes exploités par cet acteur malveillant utilisaient nos modèles pour rechercher des vulnérabilités, déboguer du code et demander des conseils sur l'écriture de scripts»*, indiquait l'entreprise dans un communiqué.

Les attaques se sont grandement aggravées cette année, puisque les fabricants Rockwell, Schneider Electric et Siemens ont été ciblés, ainsi que des cantines militaires américaines où des défaillances frigorifiques ont été constatées en août. Shahid Kaveh a atteint son pic d'activités en octobre, lorsque le groupe a attaqué les frigos connectés français. Il est également probable que les pirates aient ciblé l'Établissement français du sang le 3 novembre dernier, dont plusieurs équipements frigorifiques ont vu leur température grimper à des niveaux extrêmes.