Le 09/11/2026

Activités cyber offensives menées par des acteurs iraniens liés au CGRI

Imputation d'attaques à but de sabotage et de déstabilisation ciblant la France

---

Les membres du **Centre de Coordination des Crises Cyber** (C4)[1] ont observé plusieurs attaques à but de déstabilisation menées à l'encontre des intérêts français, qu'ils sont en mesure d'imputer **aux unités cyber-offensives Shahid Shoostari et Shahid Kaveh, opérant au sein du Centre électronique et cyber du Corps des Gardiens de la Révolution Islamique iranien (CGRI-CEC).**

L'attaque ciblant des contrôleurs de réfrigération industriels français les 11 et 12 octobre 2026 constitue une **attaque inédite** par son ampleur et son niveau d'agressivité, s'ajoutant à d'autres attaques observées depuis *a minima* 2020, parmi lesquelles des attaques à but de déstabilisation menées contre Charlie Hebdo en 2023, ainsi que contre une entreprise française d'affichage vidéo en 2024 dans le cadre de l'organisation des Jeux Olympiques et Paralympiques de Paris 2024.

1- Attaque menée les 11 et 12 octobre 2026 par l'unité Shahid Kaveh, affiliée au Centre électronique et cyber du Corps des Gardiens de la Révolution Islamique d'Iran

Le 12 octobre 2026, le Centre de Coordination des Crises Cyber est alerté d'une attaque ayant ciblé les **contrôleurs de froid d'environ 700 sites de la grande distribution en France**. À la suite de leur compromission dans la nuit du dimanche 11 au lundi 12 octobre 2026, les paramètres de dégivrage des équipements ont été modifiés pour être fixés à de hautes températures, entraînant des pertes de marchandise importantes et dans au moins **15 cas des départs de feu**.

Les entités affectées sont principalement celles de la grande distribution (notamment les groupes Casino, Leclerc, Coopérative U, Metro, Carrefour et Intermarché). Le Centre de Coordination des Crises Cyber a également connaissance d'autres victimes dans le secteur de l'agroalimentaire, dont plusieurs petites boucheries, un abattoir et des usines agroalimentaires coopératives.

[1] Le C4 est une instance interministérielle traitant de l'analyse de la menace informatique. Le C4 rassemble l'ANSSI, le COMCYBER, la DGA, la DGSE et la DGSI.

Le Centre de Coordination des Crises Cyber a par ailleurs observé le ciblage concomitant, qu'il relie à la même attaque, de plusieurs équipements Schneider Electric appartenant à de petites installations hydroélectriques en France, avec des effets modérés sur les équipements ciblés.

La cyberattaque menée à l'encontre des contrôleurs de réfrigération français présente un faisceau d'indices indiquant **le Corps des Gardiens de la Révolution Islamique iranien comme commanditaire de l'attaque et l'unité cyber-offensive Shahid Kaveh comme exécutante**.

L'unité **Shahid Kaveh**, dirigée par Reza Salarvand et Mahdi Lashgarian, est principalement connue à travers ses avatars numériques hacktivistes, parmi lesquels *CyberAveng3rs, Soldiers of Solomon, Mr. Soul, Cyber Isnaad Front*, ainsi que par son organe de communication en ligne *CyberbanNews*. Ces avatars sont chargés de revendiquer publiquement certaines des attaques menées par l'unité Shahid Kaveh.

Cette unité 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 États-Unis, mais aussi de la France et d'autres pays européens. Elle a notamment revendiqué (via son avatar *CyberAveng3rs*) une campagne menée en novembre 2023, ciblant la société israélienne Unitronics, qui produit des systèmes de contrôle industriel utilisés aux États-Unis et en Europe. L'unité a également revendiqué une campagne de sabotage à grande échelle contre des intérêts israéliens et américains, touchant des équipements de contrôle industriel, dont des équipements frigorifiques israéliens, en mars et avril 2026.

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. En avril 2026, l'unité Shahid Kaveh a été vue utilisant le protocole Modbus sur le port 502 pour effectuer des actions massives de reconnaissance sur des systèmes de contrôle industriel Schneider Electric, notamment en France.

Éléments d'imputation de l'attaque des contrôleurs de réfrigération des 11 et 12 octobre 2026 à l'unité Shahid Kaveh :

La cyberattaque menée à l'encontre des contrôleurs de réfrigération français présente un faisceau d'indices indiquant le Corps des Gardiens de la Révolution Islamique comme commanditaire, et l'unité Shahid Kaveh comme exécutante :

- L'infrastructure utilisée pour mener l'attaque a également été utilisée, au cours de la même période, pour mener des actions de reconnaissance sur des

équipements Schneider Electric, utilisés notamment dans des petites et moyennes unités de production d'énergie et d'eau. Les techniques utilisées lors de ces actions sont connues pour être utilisées par l'unité Shahid Kaveh depuis avril 2026 a minima (protocole Modbus / port 502) ;

- Pour mener l'attaque sur les systèmes de réfrigération français, les opérateurs ont utilisé l'outil de scan FOFA. Cet outil est habituellement utilisé par le mode opératoire d'attaque[2] dans les différentes actions qu'il mène ;
- La cyberattaque ciblant les contrôleurs de réfrigération a été relayée sur l'organe de propagande *CyberbanNews*, associé à l'unité Shahid Kaveh, dès le 13 octobre 2026 ;
- Des traces d'utilisation du farsi ont été retrouvées dans l'infrastructure d'attaque.

2- Attaques menées depuis 2020 contre la France par l'unité Shahid Shoostari, affiliée au Centre électronique et cyber du Corps des Gardiens de la Révolution Islamique d'Iran

Le CGRI-CEC est responsable de plusieurs opérations menées contre la France ou les intérêts français depuis 2020, à des fins de déstabilisation, *via* son unité **Shahid Shoostari**, également connue et documentée en source ouverte sous les noms de **Iliyanet** ou **Emennet Pasargad**.

Ainsi, le Centre de Coordination des Crises Cyber est en mesure de confirmer le ciblage mené en 2020 contre l'hebdomadaire ***Charlie Hebdo*** par Emennet Pasargad / Shahid Shoostari, révélé en 2021 par *Lab Dookhtegan,* un groupe se présentant comme une organisation hacktiviste dissidente iranienne. Ce plan de cyberattaque aurait été réalisé dans une logique de représailles et d'intimidation contre *Charlie Hebdo*, l'hebdomadaire ayant réédité en septembre 2020 des caricatures du Prophète.

Le 4 janvier 2023, date à laquelle *Charlie Hebdo* devait publier les résultats d'un concours de caricatures d'Ali Khamenei (alors Guide suprême de la République Islamique d'Iran) en soutien aux mouvements de protestations en cours en Iran depuis septembre 2022, les équipes de la société éditrice du journal ont constaté la défiguration de la boutique en ligne de l'hebdomadaire, ainsi que l'exfiltration des informations contenues dans la base de données de celle-ci.

Les investigations menées ont permis de retrouver des éléments techniques de l'infrastructure attaquante, ainsi que des preuves de l'exploitation de cette attaque

[2] Un mode opératoire d'attaque (MOA) est défini comme un ensemble de techniques, tactiques et procédures, codes et infrastructures, évolutifs mais cohérents dans le temps, qui est utilisé pour mener des attaques informatiques.

par le biais de revendications sur Internet. Ces éléments sont imputés à l'unité Shahid Shoostari, agissant pour le compte du CGRI.

Le Centre de Coordination des Crises Cyber est également en mesure d'imputer une attaque à des fins de déstabilisation ayant ciblé **une entreprise de gestion d'affichage vidéo** dans le cadre de **l'organisation des Jeux Olympiques et Paralympiques de Paris 2024**.

À partir du 20 juillet 2024, une société française opérant un système de gestion de bornes d'affichage vidéo a été compromise au moyen d'un mode opératoire d'attaque opéré par l'unité Shahid Shoostari.

Les attaquants ont tenté de détourner ces bornes pour diffuser des photos-montages dénonçant la participation des athlètes israéliens aux JOP2024. L'ensemble des clients de cette entreprise aurait pu être ciblé par cette tentative, mais la compromission a été découverte avant que l'attaquant ne parvienne à faire afficher ces images sur les bornes.

Les investigations menées à partir du 25 juillet 2024 ont permis de confirmer des activités malveillantes remontant a minima à plusieurs jours précédant la découverte de la compromission, et d'identifier des marqueurs techniques d'intérêt. Plusieurs outils observés lors des investigations comme étant employés par les attaquants ont également été documentés par des éditeurs de sécurité et des partenaires internationaux comme associés à Emennet Pasargad. Les analyses menées ont permis d'identifier des activités de navigation, en amont de l'ouverture des JOP2024, sur plusieurs sites de médias français.

Les investigations ont pu démontrer que les photos-montages utilisés par l'attaquant pour être diffusés via les bornes d'affichage de la société ciblée ont été publiés en premier lieu le 24 juillet 2024 (soit un jour avant la découverte de la compromission) sur un compte Instagram s'exprimant en persan, puis relayés par deux comptes X (ex-Twitter) ainsi que dans le journal iranien jahannews[.]com.

Ces investigations ont également permis d'observer l'utilisation par les attaquants de deux adresses IP appartenant à des FAI iraniens durant leurs activités menées sur le réseau de la victime.

Annexe : dirigeants du CGRI-CEC et de l'unité cyber-offensive Shahid Kaveh



Hamid Reza LASHGARIAN - Dirigeant du CGRI-CEC



Mahdi LASHGARIAN - Commandant de Shahid Kaveh



Reza SALARVAND - Commandant de Shahid Kaveh