DÉCISION (PESC) 2020/1748 DU CONSEIL

du 20 novembre 2020

modifiant la décision (PESC) 2019/797 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres

LE CONSEIL DE L'UNION EUROPÉENNE,

vu le traité sur l'Union européenne, et notamment son article 29,

vu la proposition du haut représentant de l'Union pour les affaires étrangères et la politique de sécurité,

considérant ce qui suit:

(1) Le 17 mai 2019, le Conseil a adopté la décision (PESC) 2019/797 ([1]).

(2) Le 30 juillet 2020, le Conseil a adopté la décision (PESC) 2020/1127 ([2]), par laquelle six personnes physiques et trois entités ou organismes ont été ajoutés à la liste des personnes physiques et morales, des entités et des organismes faisant l'objet de mesures restrictives qui figure à l'annexe de la décision (PESC) 2019/797.

(3) Des informations actualisées ont été reçues pour deux personnes inscrites sur la liste des personnes physiques.

(4) Il y a donc lieu de modifier la décision (PESC) 2019/797 en conséquence,

A ADOPTÉ LA PRÉSENTE DÉCISION:

Article premier

L'annexe de la décision (PESC) 2019/797 est modifiée conformément à l'annexe de la présente décision.

Article 2

La présente décision entre en vigueur le jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Fait à Bruxelles, le 20 novembre 2020.

Par le Conseil
Le président
M. ROTH

([1]) Décision (PESC) 2019/797 du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres (JO L 129 I du 17.5.2019, p. 13).

([2]) Décision (PESC) 2020/1127 du Conseil du 30 juillet 2020 modifiant la décision (PESC) 2019/797 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres (JO L 246 du 30.7.2020, p. 12).

ANNEXE

À l'annexe de la décision (PESC) 2019/797, sous le titre «A. Personnes physiques», les mentions 1 et 2 sont remplacées par les mentions suivantes:

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
«1.	GAO Qiang	Date de naissance: 4 octobre 1983 Lieu de naissance: Province de Shandong, Chine Adresse: Chambre 1102, Guanfu Mansion, 46 Xinkai Road, District de Hedong, Tianjin, Chine Nationalité: chinoise Sexe: masculin	GAO Qiang est impliqué dans "*Operation Cloud Hopper*", une série de cyberattaques ayant des effets importants, provenant de l'extérieur de l'Union et constituant une menace extérieure pour l'Union ou ses États membres, et de cyberattaques ayant des effets importants dirigés contre des pays tiers. "*Operation Cloud Hopper*" a ciblé les systèmes d'information d'entreprises multinationales sur six continents, y compris d'entreprises établies dans l'Union, et a permis d'obtenir un accès non autorisé à des données sensibles sur le plan commercial, causant ainsi d'importantes pertes économiques. L'acteur connu sous le nom de "APT10" ("*Advanced Persistent Threat 10*") (alias "Red Apollo", "CVNX", "Stone Panda", "MenuPass" et "Potassium") a mené "*Operation Cloud Hopper*". GAO Qiang peut être relié à APT10, y compris par son association avec l'infrastructure de commandement et de contrôle de APT10. De plus, GAO Qiang a été employé par Huaying Haitai, une entité désignée comme apportant un soutien à "*Operation Cloud Hopper*" et facilitant celle-ci. Il a des liens avec ZHANG Shilong, qui est également désigné en liaison avec "*Operation Cloud Hopper*". GAO Qiang est donc associé à la fois à Huaying Haitai et à ZHANG Shilong.	30.7.2020
2.	ZHANG Shilong	Date de naissance: 10 septembre 1981 Lieu de naissance: Chine Adresse: Hedong, Yuyang Road n° 121, Tianjin, Chine Nationalité: chinoise Sexe: masculin	ZHANG Shilong est impliqué dans "*Operation Cloud Hopper*", une série de cyberattaques ayant des effets importants, provenant de l'extérieur de l'Union et constituant une menace extérieure pour l'Union ou ses États membres, et de cyberattaques ayant des effets importants dirigés contre des pays tiers. "*Operation Cloud Hopper*" a ciblé les systèmes d'information d'entreprises multinationales sur six continents, y compris d'entreprises établies dans l'Union, et a permis d'obtenir un accès non autorisé à des données sensibles sur le plan commercial, causant ainsi d'importantes pertes économiques. L'acteur connu sous le nom de "APT10" ("*Advanced Persistent Threat 10*") (alias "Red Apollo", "CVNX", "Stone Panda", "MenuPass" et "Potassium") a mené "*Operation Cloud Hopper*". ZHANG Shilong peut être relié à "APT10", y compris par le logiciel malveillant qu'il a développé et testé en liaison avec les cyberattaques menées par "APT10". De plus, ZHANG Shilong a été employé par Huaying Haitai, une entité désignée comme apportant un soutien à "*Operation Cloud Hopper*" et facilitant celle-ci. Il a des liens avec GAO Qiang, qui est également désigné en liaison avec "*Operation Cloud Hopper*". ZHANG Shilong est donc associé à la fois à Huaying Haitai et à GAO Qiang.	30.7.2020»