Conseil de
l'Union européenne

Bruxelles, le 5 mai 2026
(OR. en)

7283/26

LIMITE

CORLX 273
CFSP/PESC 390
RELEX 352
CYBER 115
JAI 340
FIN 408

ACTES LÉGISLATIFS ET AUTRES INSTRUMENTS

Objet:	RÈGLEMENT D'EXÉCUTION DU CONSEIL mettant en œuvre le règlement (UE) 2019/796 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres

RÈGLEMENT D'EXÉCUTION (UE) 2026/… DU CONSEIL

du …

mettant en œuvre le règlement (UE) 2019/796 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres

LE CONSEIL DE L'UNION EUROPEENNE,

vu le traité sur le fonctionnement de l'Union européenne,

vu le règlement (UE) 2019/796 du Conseil du 17 mai 2019 concernant des mesures restrictives contre les cyberattaques qui menacent l'Union ou ses États membres[1], et notamment son article 13,

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

[1] JO L 129 I du 17.5.2019, p. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj.

considérant ce qui suit:

(1) Le 17 mai 2019, le Conseil a adopté le règlement (UE) 2019/796.

(2) Le Conseil a réexaminé la liste des personnes physiques et morales, des entités et des organismes figurant à l'annexe I du règlement (UE) 2019/796. Sur la base de ce réexamen, il convient de mettre à jour les motifs d'inscription de quatre personnes et une entité sur la liste des personnes physiques et morales, des entités et des organismes faisant l'objet de mesures restrictives.

(3) Il y a donc lieu de modifier l'annexe I du règlement (UE) 2019/796 en conséquence,

A ADOPTÉ LE PRÉSENT RÈGLEMENT:

Article premier

L'annexe I du règlement (UE) 2019/796 est modifiée conformément à l'annexe du présent règlement.

Article 2

Le présent règlement entre en vigueur le jour suivant celui de sa publication au *Journal officiel de l'Union européenne*.

Le présent règlement est obligatoire dans tous ses éléments et directement applicable dans tout État membre.

Fait à …, le

Par le Conseil
Le président/La présidente

ANNEXE

L'annexe I du règlement (UE) 2019/796 est modifiée comme suit:

1) Sous le titre "A. Personnes physiques", les mentions 1, 2, 13 et 14 sont remplacées par les mentions correspondantes suivantes:

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
"1.	GAO Qiang	Date de naissance: 4.10.1983 Lieu de naissance: Province du Shandong, Chine Adresse: Room 1102, Guanfu Mansion, 46 Xinkai Road, District de Hedong, Tianjin, Chine Nationalité: chinoise Sexe: masculin	Gao Qiang est lié au groupe parapluie "APT10" ("Advanced Persistent Threat 10") (également connu sous les noms de "Red Apollo", "CVNX", "Stone Panda", "MenuPass" et "Potassium") et a été 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, dirigées 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. Gao Qiang est associé à l'infrastructure de commandement et de contrôle de APT10. De plus, Gao Qiang a été employé par Huaying Haitai, une entité utilisée par APT10 et désignée comme apportant un soutien à "Operation Cloud Hopper" et facilitant celle-ci. Il est également associé à Zhang Shilong, qui est lié à APT10 et qui a également été employé par Huaying Haitai.	30.7.2020

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
2.	ZHANG Shilong	Date de naissance: 10.9.1981 Lieu de naissance: Chine Adresse: Hedong, Yuyang Road n° 121, Tianjin, Chine Nationalité: chinoise Sexe: masculin	Zhang Shilong est lié au groupe parapluie "APT10" ("Advanced Persistent Threat 10") (également connu sous les noms de "Red Apollo", "CVNX", "Stone Panda", "MenuPass" et "Potassium") et a été 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, dirigées 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. Zhang Shilong est associé 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 utilisée par APT10 et désignée comme apportant un soutien à "Operation Cloud Hopper" et facilitant celle-ci. Il est associé à Gao Qiang, qui est lié à APT10 et qui a également été employé par Huaying Haitai.	30.7.2020

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
13.	Mikhail Mikhailovich TSAREV	Михаил Михайлович ЦАРЕВ Date de naissance: 20.4.1989 Lieu de naissance: Serpukhov, Fédération de Russie Nationalité: russe Adresse: Serpoukhov Sexe: masculin	Mikhail Mikhailovich Tsarev a participé à des cyberattaques ayant des effets importants, qui constituent une menace extérieure pour les États membres de l'Union. Mikhail Mikhailovich Tsarev, également connu par ses surnoms en ligne "Mango", "Alexander Grachev", "Super Misha", "Ivanov Mixail", "Misha Krutysha" et "Nikita Andreevich Tsarev", est un acteur clé du déploiement des programmes malveillants "Conti" et "TrickBot", et fait partie du groupe de menace "Wizard Spider" basé en Russie. Wizard Spider continue d'évoluer et d'intensifier ses activités. Les programmes malveillants Conti et TrickBot ont été créés et développés par Wizard Spider. Wizard Spider a mené des attaques par rançongiciel dans divers secteurs, y compris des services essentiels tels que la santé et le secteur bancaire. Le groupe a infecté des ordinateurs dans le monde entier et son logiciel malveillant a été développé en une série de logiciels malveillants hautement modulaires. Les attaques menées par Wizard Spider, en utilisant des logiciels malveillants tels que Conti, "Ryuk", TrickBot ou Black Basta, sont responsables de préjudices économiques substantiels dans l'Union européenne. Mikhail Mikhailovich Tsarev est donc impliqué dans des cyberattaques ayant des effets importants, qui constituent une menace extérieure pour l'Union ou ses États membres.	24.6.2024

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
14.	Maksim Sergeevich GALOCHKIN	Максим Сергеевич ГАЛОЧКИН Date de naissance: 19.5.1982 Lieu de naissance: Abakan, Fédération de Russie Nationalité: russe Sexe: masculin	Maksim Galochkin a participé à des cyberattaques ayant des effets importants, qui constituent une menace extérieure pour les États membres de l'Union. Maksim Galochkin est également connu par ses surnoms en ligne "Benalen", "Bentley", "Volhvb", "volhvb", "manuel", "Max17" et "Crypt". Maksim Galochkin est un acteur clé du déploiement des programmes malveillants "Conti" et "TrickBot", et fait partie du groupe de menace "Wizard Spider" basé en Russie. Il a dirigé un groupe de testeurs chargé du développement, de la supervision et de la mise en œuvre de tests pour le programme malveillant TrickBot, créé et déployé par Wizard Spider. Wizard Spider continue d'évoluer et d'intensifier ses activités. Wizard Spider a mené des attaques par rançongiciel dans divers secteurs, y compris des services essentiels tels que la santé et le secteur bancaire. Le groupe a infecté des ordinateurs dans le monde entier et son logiciel malveillant a été développé en une série de logiciels malveillants hautement modulaires. Les attaques menées par Wizard Spider, en utilisant des logiciels malveillants tels que Conti, "Ryuk", TrickBot ou Black Basta, sont responsables de préjudices économiques substantiels dans l'Union européenne. Maksim Galochkin est donc impliqué dans des cyberattaques ayant des effets importants, qui constituent une menace extérieure pour l'Union ou ses États membres.	24.6.2024".

2) Sous le titre "B. Personnes morales, entités et organismes", la mention 1 est remplacée par la mention suivante:

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
"1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	Alias: Haitai Technology Development Co. Ltd Lieu: Tianjin, Chine	Huaying Haitai a apporté un soutien financier, technique ou matériel à "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, dirigées contre des pays tiers, et l'a facilitée. "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". Huaying Haitai peut être reliée à "APT10". De plus, Huaying Haitai a employé Gao Qiang et Zhang Shilong, tous deux désignés en liaison avec "Operation Cloud Hopper". Huaying Haitai est donc également associée à Gao Qiang et à Zhang Shilong.	30.7.2020".