Conseil de
l'Union européenne

Bruxelles, le 7 juillet 2026
(OR. en)

8643/26

LIMITE

CORLX 388
CFSP/PESC 584
CYBER 192
JAI 505
FIN 592

ACTES LÉGISLATIFS ET AUTRES INSTRUMENTS

Objet:	DÉCISION DU CONSEIL modifiant la décision (PESC) 2019/797 concernant des mesures restrictives qui menacent l'Union ou ses États membres

DÉCISION (PESC) 2026/… DU CONSEIL

du …

modifiant la décision (PESC) 2019/797 concernant des mesures restrictives 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) Dans le cadre d'une action continue, adaptée et coordonnée de l'Union contre les acteurs persistants de cybermenaces, il convient d'ajouter huit personnes physiques et quatre entités sur 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. Ces personnes et entités sont responsables de cyberattaques ayant des effets importants qui constituent une menace extérieure pour l'Union ou ses États membres, les soutiennent ou y participent.

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

A ADOPTÉ LA PRÉSENTE DÉCISION:

[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 129I du 17.5.2019, p. 13, ELI: http://data.europa.eu/eli/dec/2019/797/oj).

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 de sa publication au *Journal officiel de l'Union européenne*.

Fait à …, le ...

Par le Conseil
Le président/La présidente

ANNEXE

L'annexe de la décision (PESC) 2019/797 est modifiée comme suit:

1) Les mentions ci-après sont ajoutées sous la rubrique "A. Personnes physiques":

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
"20.	Vitaly Nikolayevich KOVALEV	Виталий Николаевич КОВАЛЕВ Alias: "Bentley", "Bergen", "Alex Konor", "Benny", "Ben", "Stern" Date de naissance: 23.6.1988 Adresse: Serebristy Bulvar 34 (Serebristyy Bul'var); krp 1; flt 528; 197341; Saint-Pétersbourg, Fédération de Russie Nationalité: russe Sexe: masculin Entités associées: TrickBot, Wizard Spider, Conti	Vitaly Kovalev est un personnage de premier plan dans les programmes malveillants "Trickbot" et "Conti". Il est également connu par ses surnoms en ligne "Bentley", "Bergen", "Alex Konor", "Benny", "Ben" et "Stern". À l'origine, 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, 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 et TrickBot, sont responsables de préjudices économiques substantiels dans l'Union européenne. Par conséquent, Vitaly Kovalev est responsable de cyberattaques ayant des effets importants et constituant une menace extérieure pour l'Union ou pour ses États membres , et y participe.	+

+ JO: prière d'insérer la date de publication de la présente décision.

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
21.	Alexander Alexandrovich VOLOSOVIK	Александр Александрович ВОЛОСОВИК Date de naissance: 30.1.1983 Lieu de naissance: URSS Nationalité: russe Numéro de passeport: 762988138 Sexe: masculin Entités associées: Yalishanda, LARVA-34, podzemniyl, Ohyeahhellno, Stas_vl, downlow	Alexander Volosovik est le propriétaire de Media Land LLC. Depuis 2016, le service d'hébergement pare-balles Media Land LLC facilite toute une série d'attaques par logiciel malveillant contre l'Union et le monde entier, en proposant des services d'hébergement qui dissimulent l'identité des utilisateurs et résistent aux suppressions de contenus par les services répressifs. Media Land LLC a permis le déploiement d'opérations de rançongiciel à grande échelle, de services de commandement et de contrôle et d'opérations d'hameçonnage ciblant des infrastructures critiques et des services essentiels dans les États membres, ce qui a entraîné des pertes financières importantes. Les opérations facilitées par Media Land LLC comprennent, entre autres, LockBit, EvilCorp et BlackBasta. Par conséquent, Media Land LLC est impliquée dans des cyberattaques ayant des effets importants qui constituent une menace extérieure pour l'Union et ses États membres. En tant que propriétaire de Media Land LLC, Alexander Volosovik est responsable de ces cyberattaques et y participe. Il est également associé à Media Land LLC.	[+]

[+] JO: prière d'insérer la date de publication de la présente décision.

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
22.	Denis Olegovich DEGTYARENKO	Денис Олегович ДЕГТЯРЕНКО Alias: "Dena" Date de naissance: 9.10.1989 Lieu de naissance: URSS Nationalité: russe Sexe: masculin Adresse: 130 Lenina Avenue, microdistrict de Novy Gorod, Orsk, région d'Orenbourg, Fédération de Russie	Denis Degtyarenko, alias, Dena, est un pirate russe opérant pour la CARR (Cyber Army of Russia Reborn). CARR est responsable de cyberattaques visant des services nécessaires au maintien d'activités économiques essentielles et de fonctions critiques de l'État dans les États membres, ainsi que des infrastructures en Ukraine et dans d'autres pays tiers. CARR bénéficie du soutien du Centre principal des technologies spéciales (GTsST), qui est liée à la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GRU). Le GTsST continue de mener activement des cyberattaques contre l'Union ou ses États membres. Parmi les cibles de CARR figurent des agences gouvernementales, des institutions financières, des médias et des infrastructures critiques dans les États membres et aux États-Unis. CARR a mené des attaques par déni de service distribué (DDoS) en Ukraine ainsi que contre des gouvernements et des entreprises situés dans des pays ayant apporté leur soutien à l'Ukraine. Par conséquent, Denis Degtyarenko, l'un des principaux pirates informatiques de CARR, est impliqué dans des cyberattaques ayant un impact significatif, y compris des tentatives de cyberattaques susceptibles d'avoir un impact significatif, qui constituent une menace extérieure pour les États membres, ainsi que pour des États tiers. En tant que membre de CARR, il est également associé au GTsST.	+

+ JO: prière d'insérer la date de publication de la présente décision.

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
23.	Yuliya Vladimirovna PANKRATOVA	Юлия Владимировна ПАНКРАТОВА Autre dénomination: "YUliYA" Date de naissance: 6.4.1984 Lieu de naissance: URSS Nationalité: russe Sexe: féminin Adresse: 130 Lenina Avenue, microdistrict de Novy Gorod, Orsk, région d'Orenbourg, Fédération de Russie	Yuliya Pankratova est une pirate informatique russe qui a travaillé pour CARR (Cyber Army of Russia Reborn) avant de fonder Z-Pentest, pour laquelle elle continue de travailler. CARR est responsable de cyberattaques visant des services nécessaires au maintien d'activités économiques essentielles et de fonctions critiques de l'État dans les États membres, ainsi que des infrastructures en Ukraine et dans d'autres pays tiers. CARR bénéficie du soutien du Centre principal des technologies spéciales (GTsST), qui est liée à la direction générale du renseignement de l'état-major des forces armées de la Fédération de Russie (GRU). Le GTsST continue de mener activement des cyberattaques contre l'Union ou ses États membres. Parmi les cibles de CARR figurent des agences gouvernementales, des institutions financières, des médias et des infrastructures critiques dans les États membres de l'UE et aux États-Unis. CARR a mené des attaques par déni de service distribué (DDoS) en Ukraine ainsi que contre des gouvernements et des entreprises situés dans des pays ayant apporté leur soutien à l'Ukraine.	+

+ JO: prière d'insérer la date de publication de la présente décision.

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
			Z-Pentest est responsable de cyberattaques ayant un impact significatif, notamment sur les services nécessaires au maintien d'activités essentielles dans les États membres. Par conséquent, Yuliya Pankratova, l'une des principales pirates informatiques de CARR et de Z-Pentest, est impliquée dans des cyberattaques ayant un impact significatif, y compris des tentatives de cyberattaques susceptibles d'avoir un impact significatif, qui constituent une menace extérieure pour les États membres, ainsi que pour des États tiers. Elle est également associée à Z-Pentest.	

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
24.	Maksim Evgenevich VORONIN	Максим Евгеньевич ВОРОНИН Autre dénomination: "Daugn0" Nationalité: prétendument russe Sexe: masculin	Maksim Voronin alias Daugn0 participe au développement, à la distribution et à la vente du logiciel malveillant LummaC2 (également connu sous les noms de Lumma Infostealer et Lumma Stealer), destiné à voler des informations. LummaC2 est une plateforme de type "Malware-as-a-Service" (MaaS) utilisée pour voler des données sensibles, identifiants de navigateur, portefeuilles cryptographiques ou informations système, pour déployer d'autres logiciels malveillants sur les appareils infectés, ainsi que pour le vol de cryptomonnaies et des campagnes d'espionnage. Les cyberattaques impliquant le logiciel malveillant LummaC2 sont également utilisées par des acteurs de cybermenaces motivés par l'appât du gain, tels que Storm-113, Storm-1607, Storm-1674, Octo Tempest et d'autres. Le logiciel malveillant LummaC2 a été utilisé dans le cadre de cyberattaques visant des fonctions et services critiques de l'État nécessaires au maintien des activités sociales et économiques essentielles des États membres. En 2024 et 2025, LummaC2 a été l'un des outils les plus utilisés au monde pour voler des informations. Par conséquent, Maksim Voronin, en tant que développeur, distributeur et vendeur de LummaC2, est impliqué dans des cyberattaques ayant un impact significatif et en facilite la mise en œuvre, ce qui constitue une menace extérieure pour les États membres.	[+]

[+] JO: prière d'insérer la date de publication de la présente décision.

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
25.	Maksim Aleksandrovich GORDIENKO alias: Maxim Alexandrovich GORDIENKO	Максим Александрович ГОРДИЕНКО Autre dénomination: "Lummaseller" Nationalité: prétendument russe Sexe: masculin	Maksim Gordienko alias Lummaseller participe au développement et à la distribution du logiciel malveillant LummaC2 (également connu sous les noms de Lumma Infostealer et Lumma Stealer), destiné à voler des informations. LummaC2 est une plateforme de type "Malware-as-a-Service" (MaaS) utilisée pour voler des données sensibles, identifiants de navigateur, portefeuilles cryptographiques ou informations système, pour déployer d'autres logiciels malveillants sur les appareils infectés, ainsi que pour le vol de cryptomonnaies et des campagnes d'espionnage. Les cyberattaques impliquant le logiciel malveillant LummaC2 sont également utilisées par des acteurs de cybermeances motivés par l'appât du gain, tels que Storm-113, Storm-1607, Storm-1674, Octo Tempest et d'autres. Le logiciel malveillant LummaC2 a été utilisé dans le cadre de cyberattaques visant des fonctions et services critiques de l'État nécessaires au maintien des activités sociales et économiques essentielles des États membres. En 2024 et 2025, LummaC2 a été l'un des outils les plus utilisés au monde pour voler des informations. Par conséquent, Maksim Gordienko, en tant que développeur, distributeur et vendeur de LummaC2, est impliqué dans des cyberattaques ayant un impact significatif et en facilite la mise en œuvre, ce qui constitue une menace extérieure pour les États membres.	+

+ JO: prière d'insérer la date de publication de la présente décision.

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
26.	Evgeniy Viktorovich BASHEV	Евгений Викторович БАШЕВ Date de naissance: 25.1.1980 Lieu de naissance: URSS Nationalité: russe Sexe: masculin Personnes associées: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin Entités associées: Unité 29155 de la GRU, "Impuls" LLC	Evgeniy Bashev est membre de l'unité 29155 de l'agence de renseignement militaire russe GRU. Au sein de cette unité, il soutient et facilite des cyberattaques ayant un impact significatif à l'encontre des États membres, entre autres en contrôlant le serveur "Aegon", utilisé pour des opérations de piratage. En particulier, il apporte un soutien technique et matériel aux cyberattaques menées par l'unité 29155 de la GRU par l'intermédiaire de sa société "Impuls" LLC, qui a facilité une couverture opérationnelle, des infrastructures et des moyens de paiement, et a géré des ressources techniques, notamment les serveurs, utilisées pour ces cyberattaques. Il a également coordonné la coopération entre les structures de la GRU et les réseaux de pirates informatiques externes. Les cyberattaques qu'il a facilitées visaient des fonctions, systèmes et services critiques de l'État nécessaires au maintien d'activités sociales ou économiques essentielles dans les États membres, notamment dans le secteur des transports. Dans le cadre de la campagne WhisperGate, l'unité 29155 de la GRU a également pris pour cible des infrastructures critiques de l'Ukraine.	+

+ JO: prière d'insérer la date de publication de la présente décision.

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
			Par conséquent, Evgeniy Bashev apporte un soutien technique et matériel à des cyberattaques ayant un impact significatif, y compris des tentatives de cyberattaques ayant un impact significatif potentiel qui constituent une menace extérieure pour les États membres, ainsi qu'à des cyberattaques ayant un impact significatif contre un pays tiers, ou y participe d'une autre manière. En tant que propriétaire et directeur général, il est associé à la société "Impuls" LLC. En tant que membre de l'unité 29155 de la GRU, il est également associé à cette entité.	

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
27.	Roman Alexandrovich PUNTUS	Роман Александрович ПУНТУС Lieu de naissance: Fédération de Russie Nationalité: russe Sexe: masculin Personnes associées: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin, Evgeniy Viktorovich Bashev Entités associées: Unité 29155 de la GRU	Roman Puntus est membre de l'unité 29155 de l'agence de renseignement militaire russe GRU. Au sein de cette unité, il joue un rôle de premier plan dans l'organisation et la coordination de cyberattaques ayant un impact significatif à l'encontre des États membres. Il soutient également le développement des cybercapacités internes de l'unité, notamment en matière de recrutement et d'encadrement de personnel tel que des pirates informatiques et des programmeurs. En créant la société-écran "Aegeon-Impulse", il a facilité la gestion logistique et financière des cyberopérations. Sous sa coordination, cette unité a mené des cyberattaques visant des fonctions, systèmes et services critiques de l'État nécessaires au maintien d'activités sociales ou économiques essentielles dans les États membres, notamment dans le secteur des transports. Dans le cadre de la campagne WhisperGate, l'unité 29155 de la GRU a également pris pour cible des infrastructures critiques de l'Ukraine.	[+]".

[+] JO: prière d'insérer la date de publication de la présente décision.

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
			Par conséquent, Roman Puntus est responsable de cyberattaques ayant un impact significatif, y compris de tentatives de cyberattaques ayant un impact significatif potentiel, et constituant une menace extérieure pour les États membres, ou y est impliquée d'une autre manière, ainsi que de cyberattaques ayant un impact significatif à l'encontre d'un pays tiers. En tant que membre de l'unité 29155 de la GRU, il est également associé à cette entité.	

2) Les mentions ci-après sont ajoutées sous la rubrique "B. Personnes morales, entités et organismes":

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
"8.	Media Land LLC	Adresse: Tsvetnochnaya st., 16 Litera P, Room 27 District municipal de Moskovskaya Zastava Saint-Pétersbourg, 196006, Fédération de Russie Type d'entité: société à responsabilité limitée Lieu d'enregistrement: Saint-Pétersbourg Date d'enregistrement: 19.10.2015 Numéro d'enregistrement: 1152536009900 Principal établissement: Saint-Pétersbourg, Fédération de Russie Entités associées: ML.Cloud	Depuis 2016, le service d'hébergement pare-balles Media Land LLC facilite toute une série d'attaques par logiciel malveillant contre les États membres et le monde entier, en proposant des services d'hébergement qui dissimulent l'identité des utilisateurs et résistent aux suppressions de contenus par les services répressifs, ce qui a entraîné des pertes financières considérables. Media Land LLC a permis le déploiement d'opérations de rançongiciel à grande échelle, de services de commandement et de contrôle et d'opérations d'hameçonnage ciblant des infrastructures critiques et des services essentiels dans les États membres. Les opérations facilitées par Media Land LLC comprennent, entre autres, LockBit, EvilCorp et BlackBasta. Par conséquent, Media Land LLC est impliquée dans des cyberattaques ayant des effets importants qui constituent une menace extérieure pour les États membres.	[+]

[+] JO: prière d'insérer la date de publication de la présente décision.

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
9.	ML.Cloud	Adresse: Brivibas iela 52, Riga, LV-1011, Lettonie; Fédération de Russie, Kazan, Peterburgskaya st. 52 Lieu d'enregistrement: Riga Personne associée: Alexander Volosovik Autres entités associées: Media Land LLC	ML.Cloud est la société sœur de Media Land LLC et fournit l'infrastructure technique à Media Land LLC. Depuis 2016, le service d'hébergement pare-balles Media Land LLC facilite toute une série d'attaques par logiciel malveillant contre les États membres et le monde entier, en proposant des services d'hébergement qui dissimulent l'identité des utilisateurs et résistent aux suppressions de contenus par les services répressifs, ce qui entraîne des pertes financières considérables. Media Land LLC a permis le déploiement d'opérations de rançongiciel à grande échelle, de services de commandement et de contrôle et d'opérations d'hameçonnage ciblant des infrastructures critiques et des services essentiels dans les États membres. Les opérations facilitées par Media Land LLC comprennent, entre autres, LockBit, EvilCorp et BlackBasta. Par conséquent, ML. LLC est impliquée dans des cyberattaques qui constituent une menace extérieure ayant un impact significatif sur les États membres. Par conséquent, Media Land Cloud apporte un soutien technique face aux cyberattaques ayant un impact significatif constituant une menace extérieure pour les États membres.	[+]

[+] JO: prière d'insérer la date de publication de la présente décision.

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
10.	"Impuls" LLC	Общество с ограниченной ответственностью "Импульс" Adresse: 344015, Fédération de Russie, région de Rostov, Rostov-sur-le-Don, ul. Eremenko, d. 56, k. 6, apt. 88 Type d'entité: société à responsabilité limitée Lieu d'enregistrement: Inspection interdistrict du service fédéral des impôts n° 26 pour la région de Rostov, 344019, Rostov-sur-le-Don, ul. Myasnikova, d. 52/32, Fédération de Russie Date d'enregistrement: 27.9.2010	"Impuls" LLC est une société russe détenue par Evgeniy Viktorovich Bashev, membre de l'unité 29155 de l'agence de renseignement militaire russe GRU. La société apporte un soutien technique et matériel aux cyberattaques et aux tentatives de cyberattaques menées par l'unité 29155 de la GRU. Plus précisément, "Impuls" LLC fait office d'intermédiaire opérationnel permettant de mener des activités liées au piratage informatique par l'intermédiaire d'une société qui n'a, en apparence, aucun lien avec l'État russe. Elle a facilité la couverture opérationnelle, l'infrastructure et les paiements liés aux cyberattaques, et était reliée à des ressources techniques, y compris des serveurs utilisés pour soutenir des activités de piratage informatique. En particulier, la "Impuls" LLC a permis une coopération entre les structures de la GRU et des réseaux de pirates informatiques externes. Les cyberopérations facilitées par la "Impuls" LLC ciblent des fonctions et services critiques de l'État, nécessaires au maintien d'activités sociales etéconomiques essentielles dans les États membres , notamment dans le secteur des transports. Dans le cadre de la campagne WhisperGate, l'unité 29155 de la GRU a également pris pour cible des infrastructures critiques de l'Ukraine.	+

+ JO: prière d'insérer la date de publication de la présente décision.

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
		Numéro d'enregistrement: INN (ИНН): 6168033776; OGRN (ОГРН): 1106194004850 Principal établissement: Fédération de Russie Personnes associées: Evgeniy Bashev Entités associées: Unité 29155 de la GRU	Par conséquent, "Impuls" LLC apporte un soutien technique et matériel à des cyberattaques ayant un impact significatif et qui constituent une menace extérieure pour les États membres, ainsi qu'à des cyberattaques ayant un impact significatif contre un pays tiers, ou y participe d'une autre manière.	

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
11.	Z-Pentest	Alias: "Z-Pentest Alliance", "Z-Alliance" Principal établissement: Fédération de Russie Personnes associées: Yuliya Pankratova Entités associées: Cyber Army of Russia/CARR Compte sur X.com: ZPentest (compte suspendu) Compte sur Telegram: Zpentestalliance	Z-Pentest est un groupe d'hacktivistes pro-russes, composé de membres issus de CARR (Cyber Army of Russia Reborn) et de NoName057, qui, à l'échelle mondiale, cible les infrastructures critiques, en particulier dans les secteurs de l'énergie et de l'eau. Le groupe a notamment attaqué une compagnie danoise de distribution d'eau en décembre 2024. Par conséquent, Z-Pentest est responsable de cyberattaques ayant un impact significatif qui constituent une menace extérieure pesant sur les États membres.	[+]".

[+] JO: prière d'insérer la date de publication de la présente décision.