Journal officiel
de l'Union européenne

FR
Série L

2024/1778

24.6.2024

RÈGLEMENT D'EXÉCUTION (UE) 2024/1778 DU CONSEIL

du 24 juin 2024

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 EUROPÉENNE,

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, paragraphe 1,

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 le règlement (UE) 2019/796.

(2) Des mesures restrictives ciblées contre les cyberattaques ayant des effets importants qui constituent une menace extérieure pour l'Union ou ses États membres font partie des mesures prévues dans le cadre de l'Union pour une réponse diplomatique conjointe face aux actes de cybermalveillance (la boîte à outils cyberdiplomatique) et sont un instrument essentiel pour prévenir, dissuader, décourager et contrer de telles activités.

(3) Les actes de cybermalveillance contre les infrastructures critiques ou services essentiels, y compris par l'utilisation de rançongiciels et de logiciels malveillants d'effacement de données (*wipers*), le ciblage de chaînes d'approvisionnement et le cyberespionnage, y compris les activités de vol de propriété intellectuelle, sont de plus en plus nombreux, fréquents et sophistiqués. En raison de leurs effets perturbateurs et destructeurs, ces activités constituent une menace systémique pour la sécurité, l'économie, la démocratie et la société de l'Union dans son ensemble.

(4) Le recours à des cyberopérations facilitant et accompagnant la guerre d'agression non provoquée et injustifiée menée par la Russie contre l'Ukraine nuit à la stabilité et à la sécurité mondiales, représente un risque important d'escalade et vient s'ajouter à la multiplication déjà importante des actes de cybermalveillance commis ces dernières années en dehors des conflits armés. L'augmentation des risques liés à la cybersécurité et la complexité globale du panorama des menaces, ainsi que le risque évident de propagation rapide des incidents de cybersécurité d'un État membre à d'autres, et de pays tiers à l'Union, exigent la mise en place de nouvelles mesures restrictives au titre du règlement (UE) 2019/796.

(5) Dans le cadre d'une action continue, adaptée et coordonnée de l'Union contre les acteurs persistants de cybermenaces, il convient d'inscrire six personnes physiques sur la liste des personnes physiques et morales, des entités et des organismes faisant l'objet de mesures restrictives qui figure à l'annexe I du règlement (UE) 2019/796. Ces personnes sont responsables de cyberattaques ayant des effets importants qui constituent une menace extérieure pour l'Union ou ses États membres, ou y ont participé.

(6) 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.

[1] JO L 129 I du 17.5.2019, p. 1.

Article 2

Le présent règlement entre en vigueur le jour 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 Luxembourg, le 24 juin 2024.

Par le Conseil

Le président

J. BORRELL FONTELLES

ANNEXE

Les mentions ci-après sont ajoutées à la section «A. Personnes physiques» de l'annexe I du règlement (UE) 2019/796:

	Nom	Informations d'identification	Exposé des motifs	Date d'inscription
«9.	Ruslan Aleksandrovich PERETYATKO	Руслан Александрович ПЕРЕТЯТЬКО Date de naissance: 3.8.1985 Nationalité: russe Sexe: masculin	Ruslan PERETYATKO a participé à des cyberattaques ayant des effets importants, qui constituent une menace extérieure pour l'Union ou ses États membres. Ruslan PERETYATKO fait partie du "groupe Callisto", composé de membres du renseignement militaire russe qui mènent des cyberopérations contre des États membres de l'Union et des états tiers. Le groupe Callisto (autrement connu sous le nom "Seaborgium", "Star Blizzard", "ColdRiver" ou "TA446") a lancé des campagnes d'hameçonnage pluriannuelles destinées à voler des identifiants et données liés à des comptes. En outre, le groupe Callisto est responsable de campagnes ciblant des personnes et des fonctions critiques de l'État, y compris dans les domaines de la défense et des relations extérieures. Par conséquent, Ruslan PERETYATKO est impliqué dans des cyberattaques ayant des effets importants, qui constituent une menace extérieure pour l'Union ou ses États membres.	24.6.2024
10.	Andrey Stanislavovich KORINETS	Андрей Станиславович КОРИНЕЦ Date de naissance: 18.5.1987 Lieu de naissance: Syktyvkar, Russie Nationalité: russe Sexe: masculin	Andrey Stanislavovich KORINETS a participé à des cyberattaques ayant des effets importants, qui constituent une menace extérieure pour l'Union ou ses États membres. Andrey Stanislavovich KORINETS est un officier du "Centre 18" du Service fédéral de sécurité (FSB) de la Fédération de Russie. Andrey Stanislavovich KORINETS fait partie du "groupe Callisto", composé de membres du renseignement militaire russe qui mènent des cyberopérations contre des États membres de l'Union et des états tiers. Le groupe Callisto (autrement connu sous le nom "Seaborgium", "Star Blizzard", "ColdRiver" ou "TA446") a lancé des campagnes d'hameçonnage pluriannuelles destinées à voler des identifiants et données liés à des comptes. En outre, le groupe Callisto est responsable de campagnes ciblant des personnes et des fonctions critiques de l'État, y compris dans les domaines de la défense et des relations extérieures. Par conséquent, Andrey Stanislavovich KORINETS est 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
11.	Oleksandr SKLIANKO	Александр СКЛЯНКО (en russe) Олександр СКЛЯНКО (en ukrainien) Date de naissance: 5.8.1973 Passeport: EC 867868, délivré le 27.11.1998 (Ukraine) Sexe: masculin	Oleksandr SKLIANKO a participé à des cyberattaques ayant des effets importants dirigées contre des États membres de l'Union, ainsi qu'à des cyberattaques ayant des effets importants dirigées contre des états tiers. Oleksandr SKLIANKO fait partie du groupe de pirates informatiques "Armageddon", soutenu par le Service fédéral de sécurité (FSB) de la Fédération de Russie, qui a mené diverses cyberattaques ayant des effets importants sur le gouvernement ukrainien et sur des États membres de l'Union et des fonctionnaires de leurs gouvernements, y compris en utilisant des courriels d'hameçonnage et des attaques par logiciels malveillants. Par conséquent, Oleksandr SKLIANKO est impliqué dans des cyberattaques ayant des effets importants dirigées contre des états tiers, ainsi que dans des cyberattaques ayant des effets importants, qui constituent une menace extérieure pour l'Union ou ses États membres.	24.6.2024
12.	Mykola CHERNYKH	Николай ЧЕРНЫХ (en russe) Микола ЧЕРНИХ (en ukrainien) Date de naissance: 12.10.1978 Passeport: EC 922162, délivré le 20.1.1999 (Ukraine) Sexe: masculin	Mykola CHERNYKH a participé à des cyberattaques ayant des effets importants dirigées contre des États membres de l'Union et à des cyberattaques ayant des effets importants dirigées contre des états tiers. Mykola CHERNYKH fait partie du groupe de pirates informatiques "Armageddon", soutenu par le Service fédéral de sécurité (FSB) de la Fédération de Russie, qui a mené diverses cyberattaques ayant des effets importants sur le gouvernement ukrainien et sur des États membres de l'Union et les représentants de leurs gouvernements, y compris en utilisant des courriels d'hameçonnage et des attaques par logiciels malveillants. En tant qu'ancien employé des services de sécurité ukrainiens, il est accusé, en Ukraine, de trahison et d'intervention non autorisée dans l'exploitation de matériel informatique et de systèmes automatisés électroniques. Par conséquent, Mykola CHERNYKH est 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
13.	Mikhail Mikhailovich TSAREV	Михаил Михайлович ЦАРЕВ Date de naissance: 20.4.1989 Lieu de naissance: Serpukhov, Fédération de Russie Nationalité: russe Adresse: Serpukhov 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. 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" et TrickBot, 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 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" et TrickBot, 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»