2024/1779

24.6.2024

COUNCIL DECISION (CFSP) 2024/1779

of 24 June 2024

amending Decision (CFSP) 2019/797 concerning restrictive measures against cyberattacks threatening the Union or its Member States

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on European Union, and in particular Article 29 thereof,

Having regard to the proposal from the High Representative of the Union for Foreign Affairs and Security Policy,

Whereas:

(1) On 17 May 2019, the Council adopted Decision (CFSP) 2019/797 concerning restrictive measures against cyberattacks threatening the Union or its Member States ([1]).

(2) Targeted restrictive measures against cyberattacks with a significant effect, which constitute an external threat to the Union or its Member States, are one of the measures included in the Union's framework for a joint diplomatic response to malicious cyber activities (the Cyber Diplomacy Toolbox), and are a vital instrument to prevent, deter, discourage and respond to such activities.

(3) Malicious cyber activities against critical infrastructure or essential services, including through the use of ransomware and wipers, the targeting of supply chains and cyberespionage, including intellectual property theft activities, are increasing in number, frequency and sophistication. With their disruptive and destructive effects, these activities pose a systemic threat to the Union's security, economy, democracy, and to society at large.

(4) The use of cyber operations that have enabled and accompanied Russia's unprovoked and unjustified war of aggression against Ukraine affects global stability and security, represents an important risk of escalation, and adds to the already significant increase of malicious cyber activities outside the context of armed conflict over recent years. The growing cybersecurity risks and an overall complex cyber threat landscape, with a clear risk of rapid spill-over of cyber incidents from one Member State to others, and from third countries to the Union, further call for restrictive measures under Decision (CFSP) 2019/797.

(5) As part of the sustained, tailored and coordinated Union action against persistent cyber threat actors, six natural persons should be included in the list of natural and legal persons, entities and bodies subject to restrictive measures set out in the Annex to Decision (CFSP) 2019/797. Those persons are responsible for, or were involved in, cyberattacks with a significant effect, which constitute an external threat to the Union or its Member States.

(6) Decision (CFSP) 2019/797 should therefore be amended accordingly,

HAS ADOPTED THIS DECISION:

Article 1

The Annex to Decision (CFSP) 2019/797 is amended as set out in the Annex to this Decision.

Article 2

This Decision shall enter into force on the date of its publication in the *Official Journal of the European Union*.

Done at Luxembourg, 24 June 2024.

For the Council

The President

J. BORRELL FONTELLES

([1]) Council Decision (CFSP) 2019/797 of 17 May 2019 concerning restrictive measures against cyberattacks threatening the Union or its Member States (OJ L 129 I, 17.5.2019, p. 13).

ANNEX

The following entries are added to section ‘A. Natural persons’ in the Annex to Decision (CFSP) 2019/797:

	Name	Identifying information	Reasons	Date of listing
‘9.	Ruslan Aleksandrovich PERETYATKO	Руслан Александрович ПЕРЕТЯТЬКО Date of birth: 3.8.1985 Nationality: Russian Gender: Male	Ruslan Peretyatko took part in cyberattacks with a significant effect, which constitute an external threat to the Union or its Member States. Ruslan Peretyatko is part of the “Callisto group” of Russian military intelligence officers conducting cyber operations against EU Member States and third states. Callisto Group (a.k.a. “Seaborgium”, “Star Blizzard”, “ColdRiver”, “TA446”) has launched multi-year phishing campaigns used to steal account credentials and data. Furthermore, the Callisto group is responsible for campaigns targeting individuals and critical state functions, including in the areas of defence and external relations. Therefore, Ruslan Peretyatko is involved in cyberattacks with a significant effect, which constitute an external threat to the Union or its Member States.	24.6.2024
10.	Andrey Stanislavovich KORINETS	Андрей Станиславович КОРИНЕЦ Date of birth: 18.5.1987 Place of birth: City of Syktyvkar, Russia Nationality: Russian Gender: Male	Andrey Stanislavovich Korinets took part in cyberattacks with a significant effect, which constitute an external threat to the Union or its Member States. Andrey Stanislavovich Korinets is an officer of “Center 18” of the Federal Security Service (FSB) of the Russian Federation. Andrey Stanislavovich Korinets is part of the “Callisto group” of Russian military intelligence officers conducting cyber operations against EU Member States and third states. Callisto Group (a.k.a. “Seaborgium”, “Star Blizzard”, “ColdRiver”, “TA446”) has launched multi-year phishing campaigns used to steal account credentials and data. Furthermore, the Callisto group is responsible for campaigns targeting individuals and critical state functions, including in the areas of defence and external relations. Therefore, Andrey Stanislavovich Korinets is involved in cyberattacks with a significant effect, which constitute an external threat to the Union or its Member States.	24.6.2024

ELI: http://data.europa.eu/eli/dec/2024/1779/oj

	Name	Identifying information	Reasons	Date of listing
11.	Oleksandr SKLIANKO	Александр СКЛЯНКО (Russian spelling) Олександр СКЛЯНКО (Ukrainian spelling) Date of birth: 5.8.1973 Passport: EC 867868, issued on 27.11.1998 (Ukraine) Gender: male	Oleksandr Sklianko took part in cyberattacks with a significant effect against EU Member States, as well as cyberattacks with a significant effect against third states. Oleksandr Sklianko is part of the "Armageddon" hacker group supported by the Federal Security Service (FSB) of the Russian Federation that carried out various cyberattacks with a significant effect on the government of Ukraine and on EU Member States and their government officials, including by using phishing emails and malware campaigns. Therefore, Oleksandr Sklianko is involved in cyberattacks with a significant effect against third states, as well as in cyberattacks with a significant effect, which constitute an external threat to the Union or its Member States.	24.6.2024
12.	Mykola CHERNYKH	Николай ЧЕРНЫХ (Russian spelling) Микола ЧЕРНИХ (Ukrainian spelling) Date of birth: 12.10.1978 Passport: EC 922162, issued on 20.01.1999 (Ukraine) Gender: male	Mykola Chernykh took part in cyberattacks with a significant effect against EU Member States, as well as cyberattacks with a significant effect against third states. Mykola Chernykh is part of the "Armageddon" hacker group supported by the Federal Security Service (FSB) of the Russian Federation that carried out various cyberattacks with a significant effect on the government of Ukraine and on EU Member States and their government officials, including by using phishing emails and malware campaigns. As a former employee of the Security Service of Ukraine, he is charged in Ukraine with treason and unauthorised interference in the operation of electronic computing machines and automated systems. Therefore, Mykola Chernykh is involved in cyberattacks with a significant effect, which constitute an external threat to the Union or its Member States.	24.6.2024

	Name	Identifying information	Reasons	Date of listing
13.	Mikhail Mikhailovich TSAREV	Михаил Михайлович ЦАРЕВ Date of birth: 20.4.1989 Place of birth: Serpukhov, Russian Federation Nationality: Russian Address: Serpukhov Gender: male	Mikhail Mikhailovich Tsarev took part in cyberattacks with a significant effect, which constitute an external threat to EU Member States. Mikhail Mikhailovich Tsarev, also known by the online monikers “Mango”, “Alexander Grachev”, “Super Misha”, “Ivanov Mixail”, “Misha Krutysha”, and “Nikita Andreevich Tsarev” is a key-player in the deployment of the “Conti” and “Trickbot” malware programs and is involved in the Russia-based threat group “Wizard Spider”. The Conti and Trickbot malware programs were created and developed by Wizard Spider. Wizard Spider has conducted ransomware campaigns in a variety of sectors, including essential services such as health and banking. The group has infected computers worldwide and their malware has been developed into a highly modular malware suite. Campaigns by Wizard Spider, using malware such as Conti, “Ryuk” and TrickBot, are responsible for substantial economic damage in the European Union. Mikhail Mikhailovich Tsarev is therefore involved in cyberattacks with a significant effect, which constitute an external threat to the Union or its Member States.	24.6.2024

ELI: http://data.europa.eu/eli/dec/2024/1779/oj

	Name	Identifying information	Reasons	Date of listing
14.	Maksim Sergeevich GALOCHKIN	Максим Сергеевич ГАЛОЧКИН Date of birth: 19.5.1982 Place of birth: Abakan, Russian Federation Nationality: Russian Gender: male	Maksim Galochkin took part in cyberattacks with a significant effect, which constitute an external threat to EU Member States. Maksim Galochkin is also known by the online monikers “Benalen”, “Bentley”, “Volhvb”, “volhvb”, “manuel”, “Max17” and “Crypt”. Galochkin is a key player in the deployment of the “Conti” and “Trickbot” malware programs and is involved in the Russia-based threat group “Wizard Spider”. He has led a group of testers, with responsibilities for the development, supervision, and implementation of tests for the TrickBot malware program, created and deployed by Wizard Spider. Wizard Spider has conducted ransomware campaigns in a variety of sectors, including essential services such as health and banking. The group has infected computers worldwide and their malware has been developed into a highly modular malware suite. Campaigns by Wizard Spider, using malware such as Conti, “Ryuk” and TrickBot, are responsible for substantial economic damage in the European Union. Maksim Galochkin is therefore involved in cyberattacks with a significant effect, which constitute an external threat to the Union or its Member States.	24.6.2024’