Council of the European Union

Brussels, 7 July 2026
(OR. en)

8645/26

LIMITE

CORLX 390
CFSP/PESC 586
RELEX 561
CYBER 194
JAI 507
FIN 594

LEGISLATIVE ACTS AND OTHER INSTRUMENTS

Subject:	COUNCIL IMPLEMENTING REGULATION implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States

COUNCIL IMPLEMENTING REGULATION (EU) 2026/…

of …

implementing Regulation (EU) 2019/796 concerning restrictive measures against cyber-attacks threatening the Union or its Member States

THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to Council Regulation (EU) 2019/796 of 17 May 2019 concerning restrictive measures against cyber-attacks threatening the Union or its Member States[1], and in particular Article 13(1) thereof,

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

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

Whereas:

(1) On 17 May 2019, the Council adopted Regulation (EU) 2019/796.

(2) As part of the sustained, tailored and coordinated Union action against persistent cyber threat actors, eight natural persons and four entities should be added to the list of natural and legal persons, entities and bodies subject to restrictive measures set out in Annex I to Regulation (EU) 2019/796. Those persons and entities are responsible for, or involved in, cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States.

(3) Annex I to Regulation (EU) 2019/796 should therefore be amended accordingly,

HAS ADOPTED THIS REGULATION:

Article 1

Annex I to Regulation (EU) 2019/796 is amended in accordance with the Annex to this Regulation.

Article 2

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

This Regulation shall be binding in its entirety and directly applicable in all Member States.

Done at …, …

For the Council
The President

ANNEX

Annex I to Regulation (EU) 2019/796 is amended as follows:

(1) the following entries are added under the heading ‘A. Natural persons’:

	Name	Identifying information	Reasons	Date of listing
‘20.	Vitaly Nikolayevich KOVALEV	Виталий Николаевич КОВАЛЕВ Aliases: “Bentley”, “Bergen”, “Alex Konor”, “Benny”, “Ben”, “Stern” DOB: 23.6.1988 Address: Serebristy Bulvar 34 (Serebristyy Bul’var); krp 1; flt 528; 197341; St Petersburg, Russian Federation Nationality: Russian Gender: male Associated entities: TrickBot, Wizard Spider, Conti	Vitaly Kovalev is a senior figure in the malware programs “Trickbot” and “Conti”. He is also known by the online monikers “Bentley”, “Bergen”, “Alex Konor”, “Benny”, “Ben” and “Stern”. Conti and Trickbot were originally 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, 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, and TrickBot, are responsible for substantial economic damage in the European Union. Vitaly Kovalev is therefore responsible for, and involved in, cyber-attacks with a significant effect which constitute an external threat to the Union or its Member States.	+

+ OJ: please insert the date of publication of this Regulation.

	Name	Identifying information	Reasons	Date of listing
21.	Alexander Alexandrovich VOLOSOVIK	Александр Александрович ВОЛОСОВИК DOB: 30.1.1983 POB: USSR Nationality: Russian Passport number: 762988138 Gender: male Associated entities: Yalishanda, LARVA-34, podzemniyl, Ohyeahhellno, Stas_vl, downlow	Alexander Volosovik is the owner of Media Land LLC. Since 2016, Bullet Proof Hosting service Media Land LLC has been facilitating a wide array of malware attacks against both the Union and globally, by offering hosting services that hide user identities and resist takedowns by law enforcement. Media Land LLC enabled large-scale ransomware operations, command-and-control services, and phishing operations that target critical infrastructure and essential services in the Member States, leading to significant financial losses. Operations facilitated by Media Land LLC include, inter alia, LockBit, EvilCorp and BlackBasta. Therefore, Media Land LLC is involved in cyber-attacks with significant effect which constitute an external threat to the Union or its Member States. As owner of Media Land LLC, Alexander Volosovik is responsible for, and involved in, these cyber-attacks. He is also associated to Media Land LLC.	+

+ OJ: please insert the date of publication of this Regulation.

	Name	Identifying information	Reasons	Date of listing
22.	Denis Olegovich DEGTYARENKO	Денис Олегович ДЕГТЯРЕНКО Alias: “Dena” DOB: 9.10.1989 POB: USSR Nationality: Russian Gender: male Address: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation	Denis Degtyarenko aka Dena is a Russian hacker for CARR (Cyber Army of Russia Reborn). CARR has been responsible for cyber-attacks against services necessary for the maintenance of essential economic activities and critical state functions in the Member States, as well as against infrastructure in Ukraine and other third countries. CARR is linked to the Main Centre for Special Technologies (GTsST) within the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). The GTsST remains active in carrying out cyber-attacks against the Union or its Member States. CARR’s targets include government agencies, financial institutions, media outlets, and critical infrastructure in the Member States and the United States. CARR has conducted distributed denial-of-service (DDoS) attacks in Ukraine and against governments and companies located in countries that have supported Ukraine. Therefore, Denis Degtyarenko, a primary hacker for CARR, is involved in cyber-attacks with a significant effect, including attempted cyber-attacks with a potentially significant effect, which constitute an external threat to the Member States, as well as against third states. As a member of CARR, he is also associated to GTsST.	+

+ OJ: please insert the date of publication of this Regulation.

	Name	Identifying information	Reasons	Date of listing
23.	Yuliya Vladimirovna PANKRATOVA	Юлия Владимировна ПАНКРАТОВА Alias: “YUliYA” DOB: 6.4.1984 POB: USSR Nationality: Russian Gender: female Address: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation	Yuliya Pankratova is a Russian hacker who has been working for CARR (Cyber Army of Russia Reborn) and has founded, and continues to work for Z-Pentest. CARR has been responsible for cyber attacks against services necessary for the maintenance of essential economic activities and critical state functions in the Member States, as well as against infrastructure in Ukraine and other third countries. CARR is linked to the Main Centre for Special Technologies (GTsST) within the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). The GTsST remains active in carrying out cyber-attacks against the Union or its Member States. CARR’s targets include government agencies, financial institutions, media outlets, and critical infrastructure in Member States and the United States. CARR has conducted distributed denial-of-service (DDoS) attacks in Ukraine and against governments and companies located in countries that have supported Ukraine.	+

+ OJ: please insert the date of publication of this Regulation.

	Name	Identifying information	Reasons	Date of listing
			Z-Pentest is responsible for cyber-attacks with a significant effect against inter alia services necessary for the maintenance of essential activities in the Member States. Therefore, Yuliya Pankratova, a primary hacker for CARR and for Z-Pentest, is involved in cyber-attacks with a significant effect, including attempted cyber-attacks with a potentially significant effect, which constitute an external threat to the Member States, as well as against third states. She is also associated to Z-Pentest.	

	Name	Identifying information	Reasons	Date of listing
24.	Maksim Evgenevich VORONIN	Максим Евгеньевич ВОРОНИН Alias: “Daugn0” Nationality: allegedly Russian Gender: male	Maksim Voronin aka Daugn0 is involved in the development, distribution and selling of the information stealing malware LummaC2 (aka Lumma Infostealer, Lumma Stealer). LummaC2 is a Malware-as-a-Service (MaaS) platform, used to steal sensitive data, browser credentials, crypto wallets, or system info, to deploy additional malware on infected devices, for cryptocurrency theft and for espionage campaigns. Cyberattacks involving LummaC2 malware are used also by financially motivated cyber threat actors like Storm-113, Storm-1607, Storm-1674, Octo Tempest and others. LummaC2 malware has been used for cyber-attacks against critical state functions and services necessary for the maintenance of essential social and economic activities of the Members States. In 2024 and 2025, LummaC2 was one of the most used tools for stealing information worldwide. Therefore, Maksim Voronin as developer, distributor and seller of LummaC2 is involved in and facilitates cyberattacks with a significant effect, which constitute an external threat to the Member States.	[+]

[+] OJ: please insert the date of publication of this Regulation.

	Name	Identifying information	Reasons	Date of listing
25.	Maksim Aleksandrovich GORDIENKO a.k.a. Maxim Alexandrovich GORDIENKO	Максим Александрович ГОРДИЕНКО Alias: “Lummaseller” Nationality: allegedly Russian Gender: male	Maksim Gordienko aka Lummaseller is involved in the development and distribution of the information stealing malware LummaC2 (aka Lumma Infostealer, Lumma Stealer). LummaC2 is a Malware-as-a-Service (MaaS) platform, used to steal sensitive data, browser credentials, crypto wallets or system info, to deploy additional malware on infected devices, for cryptocurrency theft and for espionage campaigns. Cyberattacks involving LummaC2 malware are used also by financially motivated cyber threat actors like Storm-113, Storm-1607, Storm-1674, Octo Tempest and others. LummaC2 malware has been used for cyber-attacks against critical state functions and services necessary for the maintenance of essential social and economic activities of the Member States. In 2024 and 2025 LummaC2 was one of the most used tools for stealing information worldwide. Therefore, Maksim Gordienko as developer, distributor and seller of LummaC2 is involved in and facilitates cyberattacks with a significant effect, which constitute an external threat to the Member States.	+

+ OJ: please insert the date of publication of this Regulation.

	Name	Identifying information	Reasons	Date of listing
26.	Evgeniy Viktorovich BASHEV	Евгений Викторович БАШЕВ DOB: 25.1.1980 POB: USSR Nationality: Russian Gender: male Associated individuals: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin Associated entities: GRU Unit 29155, “Impuls” LLC	Evgeniy Bashev is a member of Russian Military Intelligence Agency GRU, Unit 29155. Within the unit he supports and facilitates cyber-attacks with a significant effect against the Member States, inter alia via controlling the server “Aegon”, used for hacking operations. In particular, he provides technical and material support to the cyber-attacks of the GRU Unit 29155 through his company “Impuls” LLC, which facilitated operational cover, infrastructure, and payments, and managed technical assets, including servers, that are used for the cyber-attacks. He also coordinated cooperation between GRU structures and external hacker networks. The cyber-attacks he facilitated targeted critical state functions systems and services necessary for the maintenance of essential social or economic activities in the Member States, notably in the transport sector. Via the WhisperGate campaign, GRU Unit 29155 also targeted critical infrastructure of Ukraine.	+

+ OJ: please insert the date of publication of this Regulation.

	Name	Identifying information	Reasons	Date of listing
			Therefore, Evgeniy Bashev provides technical and material support for, or is otherwise involved in, cyber-attacks with a significant effect, including attempted cyber-attacks with a potentially significant effect, which constitute an external threat to the Member States, as well as cyber-attacks with a significant effect against a third country. As owner and General Director, he is associated with the company "Impuls" LLC. As a Member of GRU Unit 29155, he is also associated with that entity.	

	Name	Identifying information	Reasons	Date of listing
27.	Roman Alexandrovich PUNTUS	Роман Александрович ПУНТУС POB: Russian Federation Nationality: Russian Gender: male Associated individuals: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin, Evgeniy Viktorovich Bashev Associated entities: GRU Unit 29155	Roman Puntus is a member of the Russian Military Intelligence Agency GRU, Unit 29155. Within the unit, he holds a leading role in the organisation and coordination of cyber-attacks with a significant effect against the Member States. He also supports the development of the unit's internal cyber capability, including the recruitment and supervision of personnel such as hackers and programmers. By establishing the front company "Aegeon-Impulse," he facilitated logistical and financial aspects of cyber operations. Under his coordination, the unit conducted cyber-attacks targeting critical state functions systems and services necessary for the maintenance of essential social or economic activities in the Member States, notably in the transport sector. Via the WhisperGate campaign, GRU Unit 29155 also targeted critical infrastructure of Ukraine.	[+]';

[+] OJ: please insert the date of publication of this Regulation.

	Name	Identifying information	Reasons	Date of listing
			Therefore, Roman Puntus is responsible for, or is otherwise involved in, cyber-attacks with a significant effect, including attempted cyber-attacks with a potentially significant effect, which constitute an external threat to the Member States, as well as cyber-attacks with a significant effect against a third country. As a Member of GRU Unit 29155, he is also associated with that entity.	

(2) the following entries are added under the heading ‘B. Legal persons, entities and bodies’:

	Name	Identifying information	Reasons	Date of listing
‘8.	Media Land LLC	Address: Tsvetnochnaya st., 16 Litera P, Room 27, Moskovskaya Zastava Municipal District St Petersburg, 196006, Russian Federation Type of entity: Limited Liability Company Place of registration: St Petersburg Date of registration: 19.10.2015 Registration number: 1152536009900 Principal place of business: St Petersburg, Russian Federation Associated entity: ML.Cloud	Since 2016, Bullet Proof Hosting service Media Land LLC has been facilitating a wide array of malware attacks against the Member States and globally, by offering hosting services that hide user identities and resist takedowns by law enforcement, leading to significant financial losses. Media Land LLC enabled large-scale ransomware operations, command-and-control services, and phishing operations that target critical infrastructure and essential services among the Member States. Operations facilitated by Media Land LLC include, inter alia, LockBit, EvilCorp and BlackBasta. Therefore, Media Land LLC is involved in cyber-attacks with a significant effect, which constitute an external threat to the Member States.	+

+ OJ: please insert the date of publication of this Regulation.

	Name	Identifying information	Reasons	Date of listing
9.	ML.Cloud	Address: Brivibas iela 52, Riga, LV-1011, Latvija; Russian Federation, Kazan, Peterburgskaya st. 52 Place of registration: Riga Associated individual: Alexander Volosovik Other associated entities: Media Land LLC	ML.Cloud is the sister company of Media Land LLC, and provides the technical infrastructure for Media Land LLC. Since 2016, Bullet Proof Hosting service Media Land LLC has been facilitating a wide array of malware attacks against the Member States and globally, by offering hosting services that hide user identities and resist takedowns by law enforcement, leading to significant financial losses. Media Land LLC enabled large-scale ransomware operations, command-and-control services, and phishing operations that target critical infrastructure and essential services among the Member States. Operations facilitated by Media Land LLC include, inter alia, LockBit, EvilCorp and BlackBasta. Therefore, Media Land LLC is involved in cyber- attacks that constitute an external threat with significant effect to EU Member States. Therefore, ML. Cloud provides technical support for cyber-attacks with a significant effect, which constitute an external threat to the Member States.	+

+ OJ: please insert the date of publication of this Regulation.

	Name	Identifying information	Reasons	Date of listing
10.	“Impuls” LLC	Общество с ограниченной ответственностью “Импульс” Address: 344015, Russian Federation, Rostov Region, Rostov-on-Don, ul. Eremenko, d. 56, k. 6, apt. 88 Type of entity: Limited Liability Company Place of registration: Interdistrict Inspectorate of the Federal Tax Service No. 26 for the Rostov Region, 344019, Rostov-on-Don, ul. Myasnikova, d. 52/32, Russian Federation Date of registration: 27.9.2010	“Impuls” LLC is a Russian company owned by Evgeniy Viktorovich Bashev, a member of Russian Military Intelligence Agency GRU, Unit 29155. The company provides technical and material support to cyber-attacks and attempted cyber-attacks conducted by GRU Unit 29155. In particular, “Impuls” LLC serves as an operational intermediary enabling hacking-related activities to be carried out through a company formally unconnected to the Russian State. It facilitated operational cover, infrastructure and payments for cyber-attacks, and was connected to technical assets, including servers used in support of hacking activities. In particular, “Impuls” LLC enabled cooperation between GRU structures and external hacker networks. The cyber operations facilitated by “Impuls” LLC target critical state functions and services necessary for the maintenance of essential social and economic activities in the Member States, notably in the transport sector. Via the WhisperGate campaign, GRU Unit 29155 also targeted critical infrastructure of Ukraine.	+

+ OJ: please insert the date of publication of this Regulation.

	Name	Identifying information	Reasons	Date of listing
		Registration number: INN (ИНН): 6168033776; OGRN (ОГРН): 1106194004850 Principal place of business: Russian Federation Associated individuals: Evgeniy Bashev Associated entities: GRU Unit 29155	Therefore, “Impuls” LLC provides technical and material support for, or is otherwise involved in, cyber-attacks with a significant effect, which constitute an external threat to the Member States, as well as cyber-attacks with a significant effect against a third country.	

	Name	Identifying information	Reasons	Date of listing
11.	Z-Pentest	Aliases: “Z-Pentest Alliance”, “Z-Alliance” Principal place of business: Russian Federation Associated individuals: Yuliya Pankratova Associated entities: Cyber Army of Russia/CARR X.com account: ZPentest (Account suspended) Telegram account: Zpentestalliance	Z-Pentest is a pro-Russia hacktivist group, composed of members from CARR (Cyber Army of Russia Reborn) and NoName057, globally targeting critical infrastructure, especially the energy and water sector. Notably, the group attacked a Danish water utility in December 2024. Therefore, Z-Pentest is responsible for cyber-attacks with a significant effect, which constitute an external threat to the Member States.	[+]’.

[+] OJ: please insert the date of publication of this Regulation.