Consejo de la Unión Europea

Bruselas, 7 de julio de 2026
(OR. en)

8643/26

LIMITE

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

ACTOS LEGISLATIVOS Y OTROS INSTRUMENTOS

Asunto:	DECISIÓN DEL CONSEJO por la que se modifica la Decisión (PESC) 2019/797 relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros

DECISIÓN (UE) 2026/…DEL CONSEJO

de …

por la que se modifica la Decisión (PESC) 2019/797 relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros

EL CONSEJO DE LA UNIÓN EUROPEA,

Visto el Tratado de la Unión Europea, y en particular su artículo 29,

Vista la propuesta de la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad,

Considerando lo siguiente:

(1) El 17 de mayo de 2019, el Consejo adoptó la Decisión (PESC) 2019/797[1].

(2) Como parte de la actuación continua, específica y coordinada de la Unión frente a los agentes de ciberamenazas persistentes, procede añadir a ocho personas físicas y cuatro entidades en la lista de personas físicas o jurídicas, entidades y organismos sujetos a medidas restrictivas que figura en el anexo de la Decisión (PESC) 2019/797. Dichas personas y entidades son responsables de ciberataques con un efecto significativo que constituyen una amenaza externa para la Unión o sus Estados miembros, o los apoyan o están implicadas en ellos.

(3) Por lo tanto, procede modificar la Decisión (PESC) 2019/797 en consecuencia.

HA ADOPTADO LA PRESENTE DECISIÓN:

[1] Decisión (PESC) 2019/797 del Consejo, de 17 de mayo de 2019, relativa a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros (DO L 129 I de 17.5.2019, p. 13, ELI: http://data.europa.eu/eli/dec/2019/797/oj).

Artículo 1

El anexo de la Decisión (PESC) 2019/797 se modifica de conformidad con lo dispuesto en el anexo de la presente Decisión.

Artículo 2

La presente Decisión entrará en vigor el día de su publicación en el *Diario Oficial de la Unión Europea*.

Hecho en …, el

Por el Consejo
La Presidenta / El Presidente

ANEXO

El anexo de la Decisión (PESC) 2019/797 se modifica como sigue:

1) Bajo el epígrafe «A. Personas físicas», se añaden las entradas siguientes:

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
«20.	Vitaly Nikolayevich KOVALEV	Виталий Николаевич КОВАЛЕВ Aliases:“Bentley”, “Bergen”, “Alex Konor”, “Benny”, “Ben”, “Stern” Fecha de nacimiento: 23.6.1988 Dirección: Serebristy Bulvar 34 (Serebristyy Bul’var); krp 1; flt 528; 197341; San Petersburgo, Federación de Rusia Nacionalidad: rusa Sexo: masculino Entidades asociadas: TrickBot, Wizard Spider, Conti	Vitaly Kovalev es un alto responsable de los programas maliciosos “Trickbot” y “Conti”. Asimismo, es conocido por los alias en línea “Bentley”, “Bergen”, “Alex Konor”, “Benny”, “Ben” y “Stern”. Conti y Trickbot fueron originalmente creados y desarrollados por Wizard Spider. Wizard Spider ha efectuado campañas de programas de secuestro contra diversos sectores, en particular servicios esenciales como los sistemas sanitario o bancario, ha infectado ordenadores de todo el mundo y ha desarrollado sus programas maliciosos hasta convertirlos en un paquete malicioso altamente modular. Las campañas de Wizard Spider, que utilizan programas maliciosos como Conti y TrickBot, han causado importantes perjuicios económicos en la Unión Europea. Por consiguiente, Vitaly Kovalev es responsable de ciberataques con un efecto significativo que constituyen una amenaza externa para la Unión y sus Estados miembros y está implicado en ellos.	+

+ DO: insértese la fecha de publicación de la presente Decisión.

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
21.	Alexander Alexandrovich VOLOSOVIK	Александр Александрович ВОЛОСОВИК Fecha de nacimiento: 30.1.1983 Lugar de nacimiento: URSS Nacionalidad: rusa Número de pasaporte: 762988138 Sexo: masculino Entidades asociadas: Yalishanda, LARVA-34, podzemniyl, Ohyeahhellno, Stas_vl, downlow	Alexander Volosovik es el propietario de Media Land LLC. Desde 2016, Bullet Proof Hosting service Media Land LLC ha estado permitiendo una amplia gama de ataques de programas maliciosos contra la Unión y en el resto del mundo, al ofrecer servicios de alojamiento de datos que ocultan las identidades de los usuarios y resisten las retiradas por parte de las autoridades policiales. Media Land LLC permitió operaciones a gran escala de programas de secuestro, servicios de mando y control y ataques por suplantación de identidad contra infraestructuras críticas y servicios esenciales en los Estados miembros, lo que ha dado lugar a importantes pérdidas económicas. Entre las operaciones a las que ha contribuido Media Land LLC se encuentran LockBit, EvilCorp y BlackBasta. Por consiguiente, Media Land LLC participa en ciberataques con un efecto significativo que constituyen una amenaza externa para la Unión o sus Estados miembros. Alexander Volosovik es propietario de Media Land LLC y, como tal, es responsable de estos ciberataques y está implicado en ellos. Asimismo, está asociado a Media Land LLC.	+

+ DO: insértese la fecha de publicación de la presente Decisión.

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
22.	Denis Olegovich DEGTYARENKO	Денис Олегович ДЕГТЯРЕНКО Alias: “Dena” Fecha de nacimiento: 9.10.1989 Lugar de nacimiento: URSS Nacionalidad: rusa Sexo: masculino Dirección: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, región de Orenburgo, Federación de Rusia	Denis Degtyarenko, alias Dena, es un pirata informático en el CARR (Cyber Army of Russia Reborn, Ciberejército de Rusia Renacida). CARR ha sido responsable de ciberataques contra servicios necesarios para el mantenimiento de actividades económicas esenciales y funciones estatales vitales en los Estados miembros, así como contra infraestructuras en Ucrania y en otros terceros países. CARR está vinculado con el Centro Principal de Tecnologías Especiales (GTsST) del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GRU) [Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU)]. El GTsST sigue perpetrando ciberataques contra la Unión o sus Estados miembros. Entre los objetivos de CARR se encuentran organismos gubernamentales, entidades financieras, medios de comunicación e infraestructuras críticas en los Estados miembros y en los Estados Unidos. CARR ha llevado ataques distribuidos de denegación de servicio en Ucrania y contra gobiernos y empresas situados en países que han apoyado a Ucrania. Por consiguiente, Denis Degtyarenko, uno de los principales piratas informáticos de CARR, participa en ciberataques con un efecto significativo, así como en intentos de ciberataques con un posible efecto significativo, que constituyen una amenaza externa para los Estados miembros y para terceros países. Como miembro de CARR, también está asociado con el GTsST.	+

+ DO: insértese la fecha de publicación de la presente Decisión.

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
23.	Yuliya Vladimirovna PANKRATOVA	Юлия Владимировна ПАНКРАТОВА Alias: “YUliYA” Fecha de nacimiento: 6.4.1984 Lugar de nacimiento: URSS Nacionalidad: rusa Sexo: femenino Dirección: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, región de Orenburgo, Federación de Rusia	Yuliya Pankratova es una pirata informática que ha trabajado para CARR (Cyber Army of Russia Reborn, Ciberejército de Rusia Renacida) y luego fundó Z-Pentest, para quien sigue trabajando. CARR ha sido responsable de ciberataques contra servicios necesarios para el mantenimiento de actividades económicas esenciales y funciones estatales vitales en los Estados miembros, así como contra infraestructuras en Ucrania y en otros terceros países. CARR está vinculado con el Centro Principal de Tecnologías Especiales (GTsST) del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GRU) [Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU)]. El GTsST sigue perpetrando ciberataques contra la Unión o sus Estados miembros. Entre los objetivos de CARR se encuentran organismos gubernamentales, entidades financieras, medios de comunicación e infraestructuras críticas en Estados miembros y en los Estados Unidos. CARR ha llevado ataques distribuidos de denegación de servicio en Ucrania y contra gobiernos y empresas situados en países que han apoyado a Ucrania.	+

+ DO: insértese la fecha de publicación de la presente Decisión.

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
			Z-Pentest es responsable de ciberataques con un efecto significativo contra servicios necesarios para el mantenimiento de actividades esenciales en los Estados miembros, entre otros. Por consiguiente, Yuliya Pankratova, una de los principales piratas informáticos de CARR y de Z-Pentest, participa en ciberataques con un efecto significativo, así como en intentos de ciberataques con un posible efecto significativo, que constituyen una amenaza externa para los Estados miembros y para terceros países. Asimismo, está asociada con Z-Pentest.	

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
24.	Maksim Evgenevich VORONIN	Максим Евгеньевич ВОРОНИН Alias: “Daugn0” Nacionalidad: presuntamente rusa Sexo: masculino	Maksim Voronin, alias Daugn0, participa en el desarrollo, la distribución y la comercialización del programa malicioso LummaC2 (alias Lumma Infostealer, Lumma Stealer) para robar información. LummaC2 es una plataforma de “*malware* como servicio” (MaaS, por sus siglas en inglés), empleada para robar credenciales sensibles de navegadores, criptomonederos o información del sistema, para desplegar programas maliciosos adicionales en dispositivos infectados, para el robo de criptomonedas y para campañas de espionaje. Los ciberataques con el programa malicioso LummaC2 también son empleados por agentes de riesgo con motivaciones económicas, como Storm-113, Storm-1607, Storm-1674 y Octo Tempest, entre otros. El programa malicioso LummaC2 ha sido empleado para ciberataques contra funciones y servicios estatales vitales necesarios para el mantenimiento de actividades sociales y económicas esenciales de los Estados miembros. En 2024 y 2025, LummaC2 fue una de las herramientas más utilizadas para el robo de información en todo el mundo. Por consiguiente, Maksim Voronin, en calidad de desarrollador, distribuidor y comercializador de LummaC2, está implicado en ciberataques con un efecto significativo constitutivos de una amenaza externa para los Estados miembros, y permite dichos ciberataques.	+

+ DO: insértese la fecha de publicación de la presente Decisión.

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
25.	Maksim Aleksandrovich GORDIENKO alias: Maxim Alexandrovich GORDIENKO	Максим Александрович ГОРДИЕНКО Alias: “Lummaseller” Nacionalidad: presuntamente rusa Sexo: masculino	Maksim Gordienko, alias Lummaseller, participa en el desarrollo y la distribución del programa malicioso LummaC2 (alias Lumma Infostealer, Lumma Stealer) para robar información. LummaC2 es una plataforma de “*malware* como servicio” (MaaS, por sus siglas en inglés), empleada para robar credenciales sensibles de navegadores, criptomonederos o información del sistema, para desplegar programas maliciosos adicionales en dispositivos infectados, para el robo de criptomonedas y para campañas de espionaje. Los ciberataques con el programa malicioso LummaC2 también son empleados por agentes de riesgo con motivaciones económicas, como Storm-113, Storm-1607, Storm-1674 y Octo Tempest, entre otros. El programa malicioso LummaC2 ha sido empleado para ciberataques contra funciones y servicios estatales vitales necesarios para el mantenimiento de actividades sociales y económicas esenciales de los Estados miembros. En 2024 y 2025, LummaC2 fue una de las herramientas más utilizadas para el robo de información en todo el mundo. Por consiguiente, Maksim Gordienko, en calidad de desarrollador, distribuidor y comercializador de LummaC2, está implicado en ciberataques con un efecto significativo constitutivos de una amenaza externa para los Estados miembros, y permite dichos ciberataques.	+

+ DO: insértese la fecha de publicación de la presente Decisión.

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
26.	Evgeniy Viktorovich BASHEV	Евгений Викторович БАШЕВ Fecha de nacimiento: 25.1.1980 Lugar de nacimiento: URSS Nacionalidad: rusa Sexo: masculino Personas asociadas: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin Entidades asociadas: unidad 29155 del GRU, “Impuls” LLC	Evgeniy Bashev es miembro de la unidad 29155 de la Agencia de Inteligencia Militar rusa (Russian Military Intelligence Agency, GRU). Dentro de la unidad, apoya y permite ciberataques con un efecto significativo contra los Estados miembros, entre otros mediante el control del servidor “Aegon”, empleado para actividades de piratería informática. En concreto, presta apoyo técnico y material a los ciberataques de la unidad 29155 del GRU a través de su empresa “Impuls” LLC, que permitió la cobertura operativa, la infraestructura y los pagos, y gestionó los activos técnicos, entre ellos los servidores, empleados para los ciberataques. Además, coordinó la cooperación entre las estructuras del GRU y redes externas de piratas informáticos. Los ciberataques que permitió iban dirigidos a funciones, sistemas y servicios estatales vitales necesarios para el mantenimiento de actividades sociales o económicas esenciales de los Estados miembros, especialmente en el sector del transporte. La unidad 29155 del GRU también atacó infraestructuras críticas de Ucrania mediante su campaña WhisperGate.	+

+ DO: insértese la fecha de publicación de la presente Decisión.

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
			Por consiguiente, Evgeniy Bashev presta ayuda técnica y material o está implicado de alguna otra forma en ciberataques con un efecto significativo, incluidas las tentativas de ciberataque con un efecto potencialmente significativo, que constituyen una amenaza externa para los Estados miembros, así como en ciberataques con un efecto significativo contra un tercer país. En calidad de propietario y director general, está asociado con la empresa "Impuls" LLC. Como miembro de la unidad 29155 del GRU, también está asociado con dicha entidad.	

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
27.	Roman Alexandrovich PUNTUS	Роман Александрович ПУНТУС Lugar de nacimiento: Federación de Rusia Nacionalidad: rusa Sexo: masculino Personas asociadas: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin, Evgeniy Viktorovich Bashev Entidades asociadas: unidad 29155 del GRU	Roman Puntus es miembro de la unidad 29155 de la Agencia de Inteligencia Militar rusa (Russian Military Intelligence Agency, GRU). En dicha unidad, desempeña un importante papel en la organización y coordinación de ciberataques con efecto significativo contra los Estados miembros. Además, apoya el desarrollo de las cibercapacidades internas de la unidad, entre las que se encuentran el reclutamiento y la supervisión de personal, como piratas informáticos y programadores. Al crear la sociedad fantasma “Aegeon-Impulse”, facilitó los aspectos logísticos y financieros de las operaciones cibernéticas. Bajo su coordinación, la unidad perpetró ciberataques dirigidos a funciones y servicios estatales vitales necesarios para el mantenimiento de actividades sociales o económicas esenciales de los Estados miembros, especialmente en el sector del transporte. La unidad 29155 del GRU también atacó infraestructuras críticas de Ucrania mediante su campaña WhisperGate.	[+]».

[+] DO: insértese la fecha de publicación de la presente Decisión.

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
			Por consiguiente, Roman Puntus es responsable de ciberataques con un efecto significativo, incluidas las tentativas de ciberataque con un efecto potencialmente significativo que constituyen una amenaza externa para los Estados miembros, así como de ciberataques con un efecto significativo contra un tercer país, o está implicado de alguna otra forma en ellos. Como miembro de la unidad 29155 del GRU, también está asociado con dicha entidad.	

(2) Bajo el epígrafe «B. Personas jurídicas, entidades y organismos», se añaden las entradas siguientes:

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
«8.	Media Land LLC	Dirección: Tsvetnochnaya st., 16 Litera P, Room 27 distrito municipal de Moskovskaya Zastava San Petersburgo, 196006, Federación de Rusia Tipo de entidad: sociedad de responsabilidad limitada (*limited liability company*) Lugar de registro: San Petersburgo Fecha de registro: 19.10.2015 Número de registro: 1152536009900 Lugar principal de actividad: San Petersburgo, Federación de Rusia Entidad asociada: ML.Cloud	Desde 2016, Bullet Proof Hosting service Media Land LLC ha estado permitiendo una amplia gama de ataques de programas maliciosos contra los Estados miembros y en el resto del mundo, al ofrecer servicios de alojamiento de datos que ocultan las identidades de los usuarios y resisten las retiradas por parte de las autoridades policiales, lo que ha dado lugar a importantes pérdidas económicas. Media Land LLC permitió operaciones a gran escala de programas de secuestro, servicios de mando y control y ataques por suplantación de identidad contra infraestructuras críticas y servicios esenciales en los Estados miembros. Entre las operaciones a las que ha contribuido Media Land LLC se encuentran LockBit, EvilCorp y BlackBasta. Por consiguiente, Media Land LLC participa en ciberataques con un efecto significativo que constituyen una amenaza externa para los Estados miembros.	+

+ DO: insértese la fecha de publicación de la presente Decisión.

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
9.	ML.Cloud	Dirección: Brivibas iela 52, Riga, LV-1011, Letonia; Federación de Rusia, Kazán, Peterburgskaya st. 52 Lugar de registro: Riga Persona asociada: Alexander Volosovik Otras entidades asociadas: Media Land LLC	ML.Cloud es una empresa afiliada de Media Land LLC y le proporciona la infraestructura técnica. Desde 2016, Bullet Proof Hosting service Media Land LLC ha estado permitiendo una amplia gama de ataques de programas maliciosos contra los Estados miembros y en el resto del mundo, al ofrecer servicios de alojamiento de datos que ocultan las identidades de los usuarios y resisten las retiradas por parte de las autoridades policiales, lo que ha dado lugar a importantes pérdidas económicas. Media Land LLC permitió operaciones a gran escala de programas de secuestro, servicios de mando y control y ataques por suplantación de identidad contra infraestructuras críticas y servicios esenciales en los Estados miembros. Entre las operaciones a las que ha contribuido Media Land LLC se encuentran LockBit, EvilCorp y BlackBasta. Por consiguiente, Media Land LLC participa en ciberataques con un efecto significativo que constituyen una amenaza externa para los Estados miembros de la UE. Por consiguiente, ML. Cloud presta apoyo técnico para ciberataques con un efecto significativo que constituyen una amenaza externa para los Estados miembros.	+

+ DO: insértese la fecha de publicación de la presente Decisión.

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
10.	“Impuls” LLC	Общество с ограниченной ответственностью «Импульс» Dirección: 344015, Federación de Rusia, región de Rostov, Rostov del Don, ul. Eremenko, d. 56, k. 6, apt. 88 Tipo de entidad: sociedad de responsabilidad limitada (*limited liability company*) Lugar de registro: Inspección Interdistrito del Servicio Tributario Federal n.º 26 para la región de Rostov, 344019, Rostov del Don, ul. Myasnikova, d. 52/32, Federación de Rusia Fecha de registro: 27.9.2010	“Impuls” LLC es una empresa rusa propiedad de Evgeniy Viktorovich Bashev, un miembro de la unidad 29155 de la Agencia de Inteligencia Militar (Russian Military Intelligence Agency, GRU). La empresa presta ayuda técnica y material a ciberataques o tentativas de ciberataques perpetrados por la unidad 29155 del GRU. En concreto, “Impuls” LLC sirve como intermediario operativo para permitir actividades relacionadas con la piratería informática que se realizan a través de una empresa sin relación formal con el Estado ruso. Ha proporcionado cobertura operativa, infraestructura y pagos para ciberataques, y estaba relacionada con activos técnicos, entre los que se encuentran servidores empleados en apoyo de actividades de piratería informática. En concreto, “Impuls” LLC permitió la cooperación entre las estructuras del GRU y las redes exterinas de piratas informáticos. Las operaciones cibernéticas facilitadas por “Impuls” LLC van dirigidas a funciones y servicios estatales vitales necesarios para el mantenimiento de actividades sociales y económicas esenciales en los Estados miembros, especialmente en el sector del transporte. La unidad 29155 del GRU también atacó infraestructuras críticas de Ucrania mediante su campaña WhisperGate.	+

+ DO: insértese la fecha de publicación de la presente Decisión.

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
		Número de registro: INN (ИНН): 6168033776; OGRN (ОГРН): 1106194004850 Lugar principal de actividad: Federación de Rusia Personas asociadas: Evgeniy Bashev Entidades asociadas: unidad 29155 del GRU	Por consiguiente, “Impuls” LLC presta ayuda técnica y material o está implicada de alguna otra forma en ciberataques con un efecto significativo, que constituyen una amenaza externa para los Estados miembros, así como en ciberataques con un efecto significativo contra un tercer país.	

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
11.	Z-Pentest	Alias: “Z-Pentest Alliance”, “Z-Alliance” Lugar principal de actividad: Federación de Rusia Personas asociadas: Yuliya Pankratova Entidades asociadas: Cyber Army of Russia/CARR Cuenta en X.com: ZPentest (cuenta suspendida) Cuenta en Telegram: Zpentestalliance	Z-Pentest es un grupo de hacktivistas rusos, formado por miembros de CARR (Cyber Army of Russia Reborn, Ciberejército de Rusia Renacida) y NoName057, que atacan infraestructuras críticas en todo el mundo, especialmente del sector energético e hidráulico. En concreto, el grupo atacó una empresa de servicios de agua danesa en diciembre de 2024. Por lo tanto, Z-Pentest es responsable de ciberataques con efectos significativos, que constituyen una amenaza externa para los Estados miembros.	[+]».

[+] DO: insértese la fecha de publicación de la presente Decisión.