



Bruselas, 5 de mayo de 2026
(OR. en)

7281/26

LIMITE

CORLX 271
CFSP/PESC 388
CYBER 113
JAI 338
FIN 406

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 (PESC) 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) 2019/797¹.
- (2) La Decisión (PESC) 2019/797 es aplicable hasta el 18 de mayo de 2028.
- (3) Sobre la base de la revisión del anexo de la Decisión (PESC) 2019/797, debe prorrogarse hasta el 18 de mayo de 2027 la aplicación de las medidas establecidas en sus artículos 4 y 5 a las personas físicas y jurídicas, entidades y organismos enumerados en dicho anexo. Además, deben actualizarse los motivos de inclusión de cuatro personas y una entidad en la lista de personas físicas y jurídicas, entidades y organismos sujetos a medidas restrictivas.
- (4) 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

La Decisión (PESC) 2019/797 se modifica como sigue:

- (1) El artículo 10 se sustituye por el texto siguiente:

«Artículo 10

La presente Decisión será aplicable hasta el 18 de mayo de 2028 y estará sujeta a revisión continua. Las medidas establecidas en los artículos 4 y 5 se aplicarán hasta el 18 de mayo de 2027 a las personas físicas y jurídicas, entidades y organismos enumerados en el anexo.».

- (2) El anexo se modifica de conformidad con el anexo de la presente Decisión.

Artículo 2

La presente Decisión entrará en vigor el día siguiente al 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», las entradas 1,2,13 y 14 se sustituyen por las entradas correspondientes que figuran a continuación:

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
«1.	GAO Qiang	Fecha de nacimiento: 4 de octubre de 1983 Lugar de nacimiento: provincia de Shandong, China Dirección: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Nacionalidad: china Sexo: masculino	<p>Gao Qiang está vinculado al grupo matriz “APT10” (“Advanced Persistent Threat 10”) (alias “Red Apollo”, “CVNX”, “Stone Panda”, “MenuPass” y “Potassium”) y ha participado en la operación “Cloud Hopper”, una serie de ciberataques con efecto significativo realizados desde fuera de la Unión, constitutivos de una amenaza externa para la Unión o sus Estados miembros y de ciberataques con un efecto significativo contra terceros Estados.</p> <p>La operación “Cloud Hopper” se dirigía contra los sistemas de información de empresas multinacionales de seis continentes, entre ellas empresas ubicadas en la Unión, y consiguió acceso no autorizado a datos sensibles a efectos comerciales, lo que dio lugar a importantes pérdidas económicas.</p> <p>Gao Qiang está asociado a la infraestructura de mando y control APT10. Además, Gao Qiang estuvo empleado en Huaying Haitai, una empresa utilizada por APT10 e incluida en la lista por facilitar y prestar apoyo a la operación “Cloud Hopper”. También se le asocia a Zhang Shilong, que está vinculado a APT10 y también ha sido empleado de Huaying Haitai.</p>	30.7.2020

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
2.	ZHANG Shilong	<p>Fecha de nacimiento: 10 de septiembre de 1981</p> <p>Lugar de nacimiento: China</p> <p>Dirección: Hedong, Yuyang Road No 121, Tianjin, China</p> <p>Nacionalidad: china</p> <p>Sexo: masculino</p>	<p>Zhang Shilong está vinculado al grupo matriz “APT10” (“Advanced Persistent Threat 10”) (alias “Red Apollo”, “CVNX”, “Stone Panda”, “MenuPass” y “Potassium”) y ha participado en la operación “Cloud Hopper”, una serie de ciberataques con efecto significativo realizados desde fuera de la Unión, constitutivos de una amenaza externa para la Unión o sus Estados miembros y de ciberataques con un efecto significativo contra terceros Estados.</p> <p>La operación “Cloud Hopper” se dirigía contra los sistemas de información de empresas multinacionales de seis continentes, entre ellas empresas ubicadas en la Unión, y consiguió acceso no autorizado a datos sensibles a efectos comerciales, lo que dio lugar a importantes pérdidas económicas.</p> <p>Zhang Shilong está asociado a APT10, entre otras cosas por el programa malicioso que desarrolló y probó en relación con los ciberataques llevados a cabo por APT10.</p> <p>Además, Zhang Shilong estuvo empleado en Huaying Haitai, una empresa utilizada por APT10 e incluida en la lista por facilitar y prestar apoyo a la operación “Cloud Hopper”.</p> <p>También se le asocia a Gao Qiang, que está vinculado a APT10 y también ha sido empleado de Huaying Haitai.</p>	30.7.2020

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
13.	Mikhail Mikhailovich TSAREV	<p>Михаил Михайлович ЦАРЕВ</p> <p>Fecha de nacimiento: 20.4.1989</p> <p>Lugar de nacimiento: Serpukhov, Federación de Rusia</p> <p>Nacionalidad: rusa</p> <p>Dirección: Serpukhov</p> <p>Sexo: masculino</p>	<p>Mikhail Mikhailovich Tsarev participó en ciberataques con un efecto significativo constitutivos de una amenaza externa para los Estados miembros de la UE.</p> <p>Mikhail Mikhailovich Tsarev, también conocido por los alias en línea “Mango”, “Alexander Grachev”, “Super Misha”, “Ivanov Mixail”, “Misha Krutysha” y “Nikita Andreevich Tsarev”, es un actor fundamental en el despliegue de los programas maliciosos “Conti” y “Trickbot” y está implicado en el grupo de amenazas “Wizard Spider”, establecido en Rusia. Wizard Spider sigue evolucionando e intensificando sus operaciones.</p> <p>Los programas maliciosos Conti y Trickbot utilizan un programa espía troyano creado y desarrollado por “Wizard Spider”. Wizard Spider ha llevado a cabo campañas de programas de secuestro contra diversos sectores, en particular servicios esenciales como los sistemas sanitario o bancario.</p> <p>El grupo ha infectado ordenadores en 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, “Ryuk”, TrickBot o Black Basta han causado importantes perjuicios económicos en la Unión Europea.</p> <p>Por consiguiente, Mikhail Mikhailovich Tsarev está implicado en ciberataques con un efecto significativo constitutivos de una amenaza externa para la Unión o sus Estados miembros.</p>	24.6.2024

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
14.	Maksim Sergeevich GALOCHKIN	<p>Максим Сергеевич ГАЛОЧКИН</p> <p>Fecha de nacimiento: 19.5.1982</p> <p>Lugar de nacimiento: Abakan, Federación de Rusia</p> <p>Nacionalidad: rusa</p> <p>Sexo: masculino</p>	<p>Maksim Galochkin participó en ciberataques con un efecto significativo constitutivos de una amenaza externa para los Estados miembros de la UE.</p> <p>Maksim Galochkin también es conocido por los alias en línea “Benalen”, “Bentley”, “Volhvb”, “volhvb”, “manuel”, “Max17” y “Crypt”. Galochkin es un actor fundamental en el despliegue de los programas maliciosos “Conti” y “Trickbot” y está implicado en el grupo de amenazas “Wizard Spider”, establecido en Rusia. Ha dirigido un grupo de probadores, responsable del desarrollo, la supervisión y la realización de pruebas del programa malicioso TrickBot, que fue creado y puesto en funcionamiento por Wizard Spider. Wizard Spider sigue evolucionando e intensificando sus operaciones.</p> <p>Wizard Spider ha llevado a cabo campañas de programas de secuestro contra diversos sectores, en particular servicios esenciales como los sistemas sanitario o bancario. Desde entonces, el grupo ha infectado ordenadores de todo el mundo y ha desarrollado sus programas maliciosos hasta convertirlos en un paquete altamente modular. Las campañas de “Wizard Spider”, que utilizan programas maliciosos como Conti, “Ryuk”, TrickBot o Black Basta, han causado importantes perjuicios económicos en la Unión Europea.</p> <p>Por consiguiente, Maksim Galochkin está implicado en ciberataques con un efecto significativo constitutivos de una amenaza externa para la Unión o sus Estados miembros.</p>	24.6.2024».

2) Bajo el epígrafe «B. Personas jurídicas, entidades y organismos», la entrada 1 se sustituye por el texto siguiente:

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
«1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	Alias: Haitai Technology Development Co. Ltd Lugar: Tianjin, China	<p>Huaying Haitai prestó apoyo financiero, técnico o material para la operación “Cloud Hopper”, una serie de ciberataques con un efecto significativo, realizados desde fuera de la Unión, constitutivos de una amenaza externa para la Unión o sus Estados miembros, y de ciberataques con un efecto significativo contra terceros Estados, y facilitó dicha operación.</p> <p>La operación “Cloud Hopper” se dirigía contra los sistemas de información de empresas multinacionales de seis continentes, entre ellas empresas ubicadas en la Unión, y consiguió acceso no autorizado a datos sensibles a efectos comerciales, lo que dio lugar a importantes pérdidas económicas.</p> <p>El grupo conocido como “APT10” (“Advanced Persistent Threat 10”) (alias “Red Apollo”, “CVNX”, “Stone Panda”, “MenuPass” y “Potassium”) llevó a cabo la operación “Cloud Hopper”.</p> <p>Puede vincularse a Huaying Haitai con APT10. Además, Huaying Haitai tuvo en su nómina a Gao Qiang y a Zhang Shilong, ambos incluidos en la lista en relación con la operación “Cloud Hopper”. Por ello Huaying Haitai también está asociado a Gao Qiang y Zhang Shilong.</p>	30.7.2020».