II

(Actos no legislativos)

REGLAMENTOS

REGLAMENTO DE EJECUCIÓN (UE) 2020/1744 DEL CONSEJO

de 20 de noviembre de 2020

por el que se aplica el Reglamento (UE) 2019/796 relativo 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 Funcionamiento de la Unión Europea,

Visto el Reglamento (UE) 2019/796 del Consejo, de 17 de mayo de 2019, relativo a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros ([1]), y en particular su artículo 13, apartado 1,

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

Considerando lo siguiente:

(1) El 17 de mayo de 2019, el Consejo adoptó el Reglamento (UE) 2019/796.

(2) El 30 de julio de 2020, el Consejo adoptó el Reglamento de Ejecución (UE) 2020/1125 ([2]), que añadía seis personas físicas y tres entidades u organismos a la lista de personas físicas y jurídicas, entidades y organismos sujetos a medidas restrictivas que figura en el anexo I del Reglamento (UE) 2019/796.

(3) Se ha recibido información actualizada en relación con dos personas físicas incluidas en la lista.

(4) Por lo tanto, procede modificar el Reglamento (UE) 2019/796 en consecuencia.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Artículo 1

El anexo I del Reglamento (UE) 2019/796 se modifica de conformidad con el anexo del presente Reglamento.

Artículo 2

El presente Reglamento entrará en vigor el día siguiente al de su publicación en el *Diario Oficial de la Unión Europea*.

El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en cada Estado miembro.

Hecho en Bruselas, el 20 de noviembre de 2020.

Por el Consejo
El Presidente
M. ROTH

([1]) DO L 129 I de 17.5.2019, p. 1.
([2]) Reglamento de Ejecución (UE) 2020/1125 del Consejo, de 30 de julio de 2020, por el que se aplica el Reglamento (UE) 2019/796 relativo a medidas restrictivas contra los ciberataques que amenacen a la Unión o a sus Estados miembros (DO L 246 de 30.7.2020, p. 4).

ANEXO

En el anexo I del Reglamento (UE) 2019/796, bajo el epígrafe «A. Personas físicas», las entradas 1 y 2 se sustituyen por las entradas siguientes:

	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	Gao Qiang está implicado en 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. 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. 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". Puede relacionarse a Gao Qiang con el APT10, entre otras cosas por su relación con la infraestructura de mando y control del grupo. Además, Gao Qiang estuvo empleado en Huaying Haitai, entidad incluida en la lista por facilitar y prestar apoyo a la operación "Cloud Hopper". Gao Qiang tiene vínculos con Zhang Shilong, que también ha sido incluido en la lista en relación con la operación "Cloud Hopper". Por lo tanto, Gao Qiang está relacionado tanto con Huaying Haitai como con Zhang Shilong.	30.7.2020
2.	ZHANG Shilong	Fecha de nacimiento: 10 de septiembre de 1981 Lugar de nacimiento: China Dirección: Hedong, Yuyang Road No 121, Tianjin, China Nacionalidad: china Sexo: masculino	Zhang Shilong está implicado en 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. 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. 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". Puede relacionarse a Zhang Shilong con APT10, entre otras cosas por el software malicioso que desarrolló y probó en relación con los ciberataques llevados a cabo por APT10. Además, Zhang Shilong estuvo empleado en Huaying Haitai, entidad incluida en la lista por facilitar y prestar apoyo a la operación "Cloud Hopper". Zhang Shilong tiene vínculos con Gao Qiang, que también ha sido incluido en la lista en relación con la operación "Cloud Hopper". Por lo tanto, Zhang Shilong está relacionado tanto con Huaying Haitai como con Gao Qiang.	30.7.2020»