DECISIÓN (PESC) 2020/1127 DEL CONSEJO

de 30 de julio de 2020

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 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 la Decisión (PESC) 2019/797 ([1]).

(2) Las medidas restrictivas selectivas contra los ciberataques con un efecto significativo que constituyen una amenaza externa para la Unión o sus Estados miembros forman parte de las medidas previstas en el marco de la Unión para una respuesta diplomática conjunta a las actividades informáticas malintencionadas («conjunto de instrumentos de ciberdiplomacia») y son un instrumento crucial de disuasión y de respuesta a tales actividades. También pueden adoptarse medidas restrictivas en respuesta a ciberataques con un efecto significativo contra terceros Estados u organizaciones internacionales, cuando se estimen necesarias para la consecución de los objetivos de la política exterior y de seguridad común establecidos en las disposiciones pertinentes del artículo 21 del Tratado de la Unión Europea

(3) El 16 de abril de 2018, el Consejo adoptó unas conclusiones en las que condenaba firmemente el uso malintencionado de las tecnologías de la información y la comunicación, incluidos los ataques cibernéticos conocidos como «WannaCry» y «NotPetya», que han causado perjuicios y pérdidas económicas importantes dentro y fuera de la Unión. El 4 de octubre de 2018, los presidentes del Consejo Europeo y de la Comisión Europea y la Alta Representante de la Unión para Asuntos Exteriores y Política de Seguridad («la Alta Representante») expresaron en una declaración conjunta su grave preocupación por una tentativa de ciberataque para socavar la integridad de la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos, un acto de agresión que supuso una demostración de desprecio hacia la alta misión de la OPAQ. En una declaración en nombre de la Unión de 12 de abril de 2019, la Alta Representante instó a que se dejaran de emprender actividades informáticas malintencionadas con la finalidad de menoscabar la integridad, la seguridad y la competitividad económica de la Unión, incluidos los actos de ciberrobo de propiedad intelectual. Entre dichos ciberrobos figuran los perpetrados por el grupo conocido como «APT10» («Advanced Persistent Threat 10»).

(4) En este contexto, y con el fin de evitar, desalentar e impedir los comportamientos malintencionados en el ciberespacio, constantes y en aumento, y de reaccionar ante tales comportamientos, procede incluir a seis personas físicas y tres entidades u organismos en la lista de personas físicas o jurídicas, entidades y organismos sujetos a medidas restrictivas que figuran en el anexo de la Decisión (PESC) 2019/797. Dichas personas y entidades u organismos son responsables de diversos ciberataques o tentativas de ciberataque, prestaron apoyo para su realización, participaron en ellos o los facilitaron, entre los que se incluyen la tentativa de ciberataque contra la OPAQ y los ciberataques conocidos como «WannaCry» y «NotPetya», así como la operación «Cloud Hopper».

(5) Procede, por tanto, modificar la Decisión (PESC) 2019/797 en consecuencia.

HA ADOPTADO LA PRESENTE DECISIÓN:

Artículo 1

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

Artículo 2

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

Hecho en Bruselas, el 30 de julio de 2020.

Por el Consejo
El Presidente
M. ROTH

ANEXO

Las siguientes personas y entidades u organismos se añaden a la lista de personas físicas o jurídicas, entidades y organismos que figura en el anexo de la Decisión (PESC) 2019/797:

«A. Personas físicas

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
1.	GAO Qiang	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". 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	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".	30.7.2020

			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". 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.	
3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Fecha de nacimiento: 27 de mayo de 1972 Lugar de nacimiento: Oblast Perm, República Socialista Federativa Soviética de Rusia (ahora Federación de Rusia) Número de pasaporte: 120017582, Expedido por: Ministerio de Asuntos Exteriores de la Federación de Rusia Validez: del 17 de abril de 2017 al 17 de abril de 2022 Lugar: Moscú, Federación de Rusia Nacionalidad: rusa Sexo: masculino	Alexey Minin participó en una tentativa de ciberataque, con un efecto potencialmente significativo, contra la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos. Como agente auxiliar de inteligencia humana del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU), Alexey Minin formó parte de un equipo de cuatro agentes rusos de inteligencia militar que trataron de obtener acceso no autorizado a la red wifi de la OPAQ en La Haya (Países Bajos) en abril de 2018. La tentativa de ciberataque tenía por objeto piratear la red wifi de la OPAQ, lo que, de haberse conseguido, habría puesto en peligro la seguridad de la red y las investigaciones en curso de la OPAQ. El Servicio de Inteligencia y Seguridad de la Defensa de los Países Bajos (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) frustró la tentativa de ciberataque, impidiendo así un perjuicio grave a la OPAQ.	30.7.2020
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Fecha de nacimiento: 31 de julio de 1977 Lugar de nacimiento: Oblast Murmanskaya, República Socialista Federativa Soviética de Rusia (ahora Federación de Rusia) Número de pasaporte: 100135556 Expedido por: Ministerio de Asuntos Exteriores de la Federación de Rusia Validez: del 17 de abril de 2017 al 17 de abril de 2022 Lugar: Moscú, Federación de Rusia Nacionalidad: rusa Sexo: masculino	Aleksei Morenets participó en una tentativa de ciberataque, con un efecto potencialmente significativo, contra la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos. Como informático especializado en ciberseguridad del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU), Aleksei Morenets formó parte de un equipo de cuatro agentes rusos de inteligencia militar que trataron de obtener acceso no autorizado a la red wifi de la OPAQ en La Haya (Países Bajos) en abril de 2018. La tentativa de ciberataque tenía por objeto piratear la red wifi de la OPAQ, lo que, de haberse conseguido, habría puesto en peligro la seguridad de la red y las investigaciones en curso de la OPAQ. El Servicio de Inteligencia y Seguridad de la Defensa de los Países Bajos (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) frustró la tentativa de ciberataque, impidiendo así un perjuicio grave a la OPAQ.	30.7.2020

5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Fecha de nacimiento: 26 de julio de 1981 Lugar de nacimiento: Kursk, República Socialista Federativa Soviética de Rusia (ahora Federación de Rusia) Número de pasaporte: 100135555 Expedido por: Ministerio de Asuntos Exteriores de la Federación de Rusia Validez: del 17 de abril de 2017 al 17 de abril de 2022 Lugar: Moscú, Federación de Rusia Nacionalidad: rusa Sexo: masculino	Evgenii Serebriakov participó en una tentativa de ciberataque, con un efecto potencialmente significativo, contra la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos. Como informático especializado en ciberseguridad del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU), Evgenii Serebriakov formó parte de un equipo de cuatro agentes rusos de inteligencia militar que trataron de obtener acceso no autorizado a la red wifi de la OPAQ en La Haya (Países Bajos) en abril de 2018. La tentativa de ciberataque tenía por objeto piratear la red wifi de la OPAQ, lo que, de haberse conseguido, habría puesto en peligro la seguridad de la red y las investigaciones en curso de la OPAQ. El Servicio de Inteligencia y Seguridad de la Defensa de los Países Bajos (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) frustró la tentativa de ciberataque, impidiendo así un perjuicio grave a la OPAQ.	30.7.2020
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Fecha de nacimiento: 24 de agosto de 1972 Lugar de nacimiento: Ulyanovsk, República Socialista Federativa Soviética de Rusia (ahora Federación de Rusia) Número de pasaporte: 120018866 Expedido por: Ministerio de Asuntos Exteriores de la Federación de Rusia Validez: del 17 de abril de 2017 al 17 de abril de 2022 Lugar: Moscú, Federación de Rusia Nacionalidad: rusa Sexo: masculino	Oleg Sotnikov participó en una tentativa de ciberataque, con un efecto potencialmente significativo, contra la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos. Como agente auxiliar de inteligencia humana del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU), Oleg Sotnikov formó parte de un equipo de cuatro agentes rusos de inteligencia militar que trataron de obtener acceso no autorizado a la red wifi de la OPAQ en La Haya (Países Bajos) en abril de 2018. La tentativa de ciberataque tenía por objeto piratear la red wifi de la OPAQ, lo que, de haberse conseguido, habría puesto en peligro la seguridad de la red y las investigaciones en curso de la OPAQ. El Servicio de Inteligencia y Seguridad de la Defensa de los Países Bajos (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) frustró la tentativa de ciberataque, impidiendo así un perjuicio grave a la OPAQ.	30.7.2020

B. Personas jurídicas, entidades y organismos

	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	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.	30.7.2020

			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 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 se relaciona a Huaying Haitai con Gao Qiang y Zhang Shilong.	
2.	Chosun Expo	Alias: Chosen Expo; Korea Export Joint Venture Lugar: RPDC	Chosun Expo prestó apoyo financiero, técnico o material para 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 su realización; entre ellos se incluye el ciberataque conocido como “WannaCry” y varios ciberataques contra la Autoridad de Supervisión Financiera de Polonia y Sony Pictures Entertainment, así como el ciberrobo al Banco de Bangladesh y la tentativa de ciberrobo al Banco Tien Phong de Vietnam. “WannaCry” perturbó sistemas de información de todo el mundo mediante ataques con programas de secuestro y el bloqueo del acceso a los datos. Afectó a los sistemas de información de empresas de la Unión, entre ellos diversos sistemas de información relativos a servicios necesarios para el mantenimiento de servicios y actividades económicas esenciales en los Estados miembros. El ciberataque “WannaCry” fue llevado a cabo por el grupo conocido como “APT38” (“Advanced Persistent Threat 38”) o el “Grupo Lazarus”. Puede relacionarse a Chosun Expo con APT38/Grupo Lazarus, entre otras cosas a través de las cuentas utilizadas para los ciberataques.	30.7.2020
3.	Centro Principal de Tecnologías Especiales (GTsST) del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU)	Dirección: 22 Kirova Street, Moscú, Federación de Rusia	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 (GU/GRU), también conocido por el código 74455, es responsable de diversos ciberataques con un efecto significativo llevados a cabo 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; entre ellos se incluyen los ciberataques conocidos como “NotPetya” o “EternalPetya” en junio de 2017 y los ciberataques dirigidos contra una red eléctrica ucraniana en el invierno de 2015 y 2016.	30.7.2020»

			El ciberataque “NotPetya” o “EternalPetya” impidió el acceso a los datos en una serie de empresas de la Unión, de Europa en general y de todo el mundo, mediante ataques a ordenadores con programas de secuestro y el bloqueo del acceso a los datos, lo que causó, entre otros efectos, importantes pérdidas económicas. El ciberataque contra una red eléctrica ucraniana provocó el apagado de partes de dicha red durante el invierno. El ciberataque “NotPetya” o “EternalPetya” fue llevado a cabo por el grupo conocido como “Sandworm” (alias “Sandworm Team”, “BlackEnergy Group”, “Vodoo Bear”, “Quedagh”, “Olympic Destroyer” y “Telebots”), que también está detrás del ataque contra la red eléctrica ucraniana. El Centro Principal de Tecnologías Especiales del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia desempeña un papel activo en las actividades informáticas llevadas a cabo por Sandworm, por lo que es posible relacionarlo con dicho grupo.	