Consejo de la Unión Europea

Bruselas, 13 de mayo de 2024
(OR. en)

8500/24

LIMITE

CORLX 354
CFSP/PESC 510
CYBER 108
JAI 570
FIN 339

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) 2024/… 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 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) La Decisión (PESC) 2019/797 es aplicable hasta el 18 de mayo de 2025. Sobre la base de una revisión de dicha Decisión, la validez de las medidas restrictivas establecidas en ella debe prorrogarse hasta esa fecha.

(3) Ante la persistencia y el aumento de los comportamientos malintencionados en el ciberespacio, entre ellos los dirigidos contra terceros Estados, deben actualizarse los motivos para incluir a seis personas y dos 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.

(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).

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 2025 y estará sujeta a revisión continua.».

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 («Lista de personas físicas o jurídicas, entidades y organismos a que se refieren los artículos 4 y 5») se modifica como sigue:

1) En la lista «A. Personas físicas», las entradas 3 a 8 se sustituyen por el texto siguiente:

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
«3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Fecha de nacimiento: 27.5.1972 Lugar de nacimiento: provincia de 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 17.4.2017 al 17.4.2022 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, así como en ciberataques con un efecto significativo contra terceros Estados. 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) frustró la tentativa de ciberataque, impidiendo así un perjuicio grave a la OPAQ. Un jurado de acusación del Distrito Oeste de Pensilvania (Estados Unidos de América) ha acusado a Alexey Minin, como agente de la Dirección Central de Inteligencia de Rusia (GRU), de piratería informática, fraude electrónico, usurpación de identidad agravada y blanqueo de capitales.	30.7.2020

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Fecha de nacimiento: 31.7.1977 Lugar de nacimiento: provincia de 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 17.4.2017 al 17.4.2022 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, así como en ciberataques con un efecto significativo contra terceros Estados. Como operador informático 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) frustró la tentativa de ciberataque, impidiendo así un perjuicio grave a la OPAQ. Un jurado de acusación del Distrito Oeste de Pensilvania (Estados Unidos de América) ha acusado a Aleksei Morenets, como miembro de la unidad militar 26165, de piratería informática, fraude electrónico, usurpación de identidad agravada y blanqueo de capitales.	30.7.2020

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Fecha de nacimiento: 26.7.1981 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 17.4.2017 al 17.4.2022 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, así como en ciberataques con un efecto significativo contra terceros Estados. Como operador informático 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) frustró la tentativa de ciberataque, impidiendo así un perjuicio grave a la OPAQ. Desde la primavera de 2022, Evgenii Serebriakov dirige «Sandworm» (alias: «Sandworm Team», «BlackEnergy Group», «Voodoo Bear», «Quedagh», «Olympic Destroyer» y «Telebots»), agente y grupo de piratas informáticos vinculado a la unidad 74455 de la Dirección Central de Inteligencia de Rusia. «Sandworm» ha llevado a cabo ciberataques contra Ucrania, incluidos organismos gubernamentales ucranianos, tras la guerra de agresión de Rusia contra Ucrania.	30.7.2020

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Fecha de nacimiento: 24.8.1972 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 17.4.2017 al 17.4.2022 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, así como en ciberataques con un efecto significativo contra terceros Estados. 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) frustró la tentativa de ciberataque, impidiendo así un perjuicio grave a la OPAQ. Un jurado de acusación del Distrito Oeste de Pensilvania ha acusado a Oleg Sotnikov, como agente de la Dirección Central de Inteligencia de Rusia (GRU), de piratería informática, fraude electrónico, usurpación de identidad agravada y blanqueo de capitales.	30.7.2020

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Fecha de nacimiento: 15.11.1990 Lugar de nacimiento: Kursk, República Socialista Federativa Soviética de Rusia (ahora Federación de Rusia) Nacionalidad: rusa Sexo: masculino	Dmitry Badin participó en un ciberataque con un efecto significativo contra el Parlamento federal alemán (Deutscher Bundestag) y en ciberataques con un efecto significativo contra terceros Estados. Como agente de inteligencia militar del 85.º Centro Principal de Servicios Especiales (GTsSS) del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU), Dmitry Badin formó parte de un equipo de agentes rusos de inteligencia militar que perpetró un ciberataque contra el Parlamento federal alemán en abril y mayo de 2015. Ese ciberataque iba dirigido contra el sistema de información del Parlamento y afectó a su funcionamiento durante varios días. Se sustrajo una cantidad significativa de datos y se vieron afectadas las cuentas de correo electrónico de varios diputados así como la de la excanciller Angela Merkel. Un jurado de acusación del Distrito Oeste de Pensilvania (Estados Unidos de América) ha acusado a Dmitry Badin, como miembro de la unidad militar 26165, de piratería informática, fraude electrónico, usurpación de identidad agravada y blanqueo de capitales.	22.10.2020

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Fecha de nacimiento: 21.2.1961 Nacionalidad: rusa Sexo: masculino	Igor Kostyukov es el actual jefe del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU), después de haber sido primer jefe adjunto del mismo. Una de las unidades bajo su mando es el 85.º Centro Principal de Servicios Especiales (GTsSS) (alias «unidad militar 26165», «APT28», «Fancy Bear», «Sofacy Group», «Pawn Storm» y «Strontium»). Como tal, Igor Kostyukov es responsable de los ciberataques perpetrados por el GTsSS, entre ellos los ciberataques con un efecto significativo constitutivos de amenaza externa para la Unión o sus Estados miembros. En particular, agentes de inteligencia militar del GTsSS participaron en el ciberataque contra el Parlamento federal alemán (Deutscher Bundestag) en abril y mayo de 2015 y en la tentativa de ciberataque dirigido a piratear la red wifi de la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos en abril de 2018. El ciberataque contra el Parlamento federal alemán iba dirigido contra su sistema de información y afectó a su funcionamiento durante varios días. Se sustrajo una cantidad significativa de datos y se vieron afectadas las cuentas de correo electrónico de varios diputados así como la de la excanciller Angela Merkel.».	22.10.2020».

2) En la lista «B. Personas jurídicas, entidades y organismos», las entradas 3 y 4 se sustituyen por el texto siguiente:

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
«3	Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (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) [Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)], también conocido por el código 74455, está implicado en 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 en 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. «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.	30.7.2020

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
			«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. «Sandworm» ha llevado a cabo ciberataques contra Ucrania, incluidos organismos gubernamentales ucranianos e infraestructuras críticas ucranianas, tras la guerra de agresión de Rusia contra Ucrania. Dichos ciberataques incluyen campañas de phishing personalizado, programas maliciosos y ataques con programas de secuestro. 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 el mismo.	

	Nombre	Información identificativa	Motivos	Fecha de inclusión en la lista
4.	85th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)	Dirección: Komsomol'skiy Prospekt, 20, Moscú, 119146, Federación de Rusia	El 85.º Centro Principal de Servicios Especiales (GTsSS) del Mando Principal del Estado Mayor de la Defensa de las Fuerzas Armadas de la Federación de Rusia (GU/GRU) [85th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)] (alias «unidad militar 26165», «APT28», «Fancy Bear», «Sofacy Group», «Pawn Storm» y «Strontium») está implicado en ciberataques con un efecto significativo y constitutivos de amenaza externa para la Unión o sus Estados miembros, así como en ciberataques con un efecto significativo contra terceros Estados. En particular, agentes de inteligencia militar del GTsSS participaron en el ciberataque contra el Parlamento federal alemán (Deutscher Bundestag) en abril y mayo de 2015 y en la tentativa de ciberataque dirigido a piratear la red wifi de la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos en abril de 2018. El ciberataque contra el Parlamento federal alemán iba dirigido contra su sistema de información y afectó a su funcionamiento durante varios días. Se sustrajo una cantidad significativa de datos y se vieron afectadas las cuentas de correo electrónico de varios diputados así como la de la excanciller Angela Merkel. Tras la guerra de agresión de Rusia contra Ucrania, se perpetraron los ciberataques del GTsSS (ataques de phishing personalizado y ataques con programas maliciosos) contra Ucrania.	22.10.2020».