REGLAMENTO DE EJECUCIÓN (UE) 2020/1125 DEL CONSEJO

de 30 de julio de 2020

por el que se aplica el Reglamento (UE) 2019/796 sobre medidas restrictivas contra los ciberataques que amenazan a la Unión o 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, sobre medidas restrictivas contra los ciberataques que amenazan a la Unión o sus Estados miembros ([1]) y, en particular, su artículo 13, apartado 1,

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

Mientras:

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

(2)Las medidas restrictivas dirigidas contra los ciberataques con un efecto significativo que constituyen una amenaza externa para la Unión o sus Estados miembros se encuentran entre las medidas incluidas en el marco de la Unión para una respuesta diplomática conjunta a las actividades cibernéticas maliciosas (la caja de herramientas de la diplomacia cibernética) y son un instrumento vital para disuadir y responder a tales actividades. Las medidas restrictivas también se pueden aplicar en respuesta a los ataques cibernéticos con un efecto significativo contra terceros Estados u organizaciones internacionales, cuando se considere necesario para lograr objetivos comunes de política exterior y de seguridad establecidos en las disposiciones pertinentes del artículo 21 del Tratado de la Unión Europea.

(3)El 16 de abril de 2018, el Consejo adoptó conclusiones en las que condenaba firmemente el uso malicioso de las tecnologías de la información y las comunicaciones, incluidos los ataques cibernéticos conocidos públicamente como 'WannaCry' y 'NotPetya', que causaron daños significativos y pérdidas económicas en la Unión y más allá. El 4 de octubre de 2018, los Presidentes del Consejo Europeo y de la Comisión Europea y el Alto Representante de la Unión para Asuntos Exteriores y Política de Seguridad (el 'Alto Representante') expresaron serias preocupaciones en una declaración conjunta sobre un intento de ataque cibernético para socavar La integridad de la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos, un acto agresivo que demostró desprecio por el solemne propósito de la OPAQ. En una declaración realizada en nombre de la Unión el 12 de abril de 2019, El Alto Representante instó a los actores a que dejen de emprender actividades cibernéticas maliciosas que pretendan socavar la integridad, la seguridad y la competitividad económica de la Unión, incluidos los actos de robo de propiedad intelectual habilitados por el cibernético. Tales robos cibernéticos incluyen los realizados por el actor conocido públicamente como 'APT10' ('Amenaza persistente avanzada 10').

(4)En este contexto, y para prevenir, desalentar, disuadir y responder al comportamiento malicioso continuo y creciente en el ciberespacio, seis personas físicas y tres entidades u organismos deben incluirse en la lista de personas físicas y jurídicas, entidades y organismos sujetos a las medidas restrictivas establecidas. en el anexo I del Reglamento (UE) 2019/796. Esas personas y entidades u organismos son responsables, brindaron apoyo o estuvieron involucrados en, o facilitaron ciberataques o intentos de ciberataques, incluido el intento de ciberataque contra la OPAQ y los ciberataques conocidos públicamente como 'WannaCry' y 'NotPetya', así como 'Operation Cloud Hopper'.

(5) El Reglamento (UE) 2019/796 debe modificarse en consecuencia.

HA ADOPTADO EL PRESENTE REGLAMENTO:

Articulo 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 en la fecha de su publicación en el *Diario Oficial de la Unión Europea* .
El presente Reglamento será obligatorio en todos sus elementos y directamente aplicable en todos los Estados miembros.

Hecho en Bruselas, el 30 de julio de 2020.

Por el Consejo
El presidente
M. ROTH

(1) DO L 129 I de 17.5.2019, p. 1 .

ANEXO

Las siguientes personas y entidades u organismos se añaden a la lista de personas físicas y jurídicas, entidades y organismos que figuran en el anexo I del Reglamento (UE) 2019/796:

'UNA. Personas naturales

	Nombre	**Información identificativa**	**Razones**	**Fecha de listado**
1)	GAO Qiang	Lugar de nacimiento: provincia de Shandong, China Dirección: Habitación 1102, Mansión Guanfu, 46 Xinkai Road, Distrito Hedong, Tianjin, China Nacionalidad: china Género masculino	Gao Qiang participa en la "Operación Cloud Hopper", una serie de ciberataques con un efecto significativo que se origina desde fuera de la Unión y que constituye 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 centró en los sistemas de información de empresas multinacionales en seis continentes, incluidas las empresas ubicadas en la Unión, y obtuvo acceso no autorizado a datos sensibles desde el punto de vista comercial, lo que resultó en una pérdida económica significativa.	30.7.2020
			El actor conocido públicamente como "APT10" ("Advanced Persistent Threat 10") (también conocido como "Red Apollo", "CVNX", "Stone Panda", "MenuPass" y "Potassium") llevó a cabo "Operation Cloud Hopper". Gao Qiang puede vincularse a APT10, incluso a través de su asociación con la infraestructura de	

			control y comando APT10. Además, Huaying Haitai, una entidad designada para brindar apoyo y facilitar la "Operación Cloud Hopper", empleó a Gao Qiang. Tiene vínculos con Zhang Shilong, quien también está designado en relación con la "Operación Cloud Hopper". Gao Qiang está asociado con Huaying Haitai y Zhang Shilong.	
2)	ZHANG Shilong	Dirección: Hedong, Yuyang Road No 121, Tianjin, China Nacionalidad: china Género masculino	Zhang Shilong participa en la "Operación Cloud Hopper", una serie de ciberataques con un efecto significativo que se origina desde fuera de la Unión y que constituye 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 ha dirigido a los sistemas de información de empresas multinacionales en seis continentes, incluidas las empresas ubicadas en la Unión, y ha obtenido acceso no autorizado a datos sensibles desde el punto de vista comercial, lo que ha resultado en una importante pérdida económica. El actor conocido públicamente como "APT10" ("Advanced Persistent Threat 10") (también conocido como "Red Apollo", "CVNX", "Stone Panda", "MenuPass" y "Potassium") llevó a cabo "Operation Cloud Hopper".	30.7.2020
			Zhang Shilong se puede vincular a APT10, incluso a través del malware que desarrolló y probó en relación con los ataques cibernéticos llevados a cabo por APT10. Además, Huaying Haitai, una entidad designada para brindar apoyo y facilitar la "Operación Cloud Hopper", empleó a Zhang Shilong. Él tiene vínculos con Gao Qiang, quien también es designado en relación con "Operation Cloud Hopper". Por lo tanto, Zhang Shilong está asociado con Huaying Haitai y Gao Qiang.	
3)	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Fecha de nacimiento: 27 de mayo de 1972 Lugar de nacimiento: Óblast de Perm, SFSR ruso (ahora Federación de Rusia) Número de pasaporte: 120017582 Emitido por: Ministerio de Asuntos Exteriores de la Federación de Rusia Validez: desde el 17 de abril de 2017 hasta el 17 de abril de 2022 Ubicación: Moscú, Federación Rusa	Alexey Minin participó en un intento de ciberataque con un efecto potencialmente significativo contra la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos. Como oficial de apoyo de inteligencia humana de la Dirección Principal del Estado Mayor de las Fuerzas Armadas de la Federación de Rusia (GU / GRU), Alexey Minin era parte de un equipo de cuatro oficiales de inteligencia militar rusos que intentaron obtener acceso no autorizado a Wi -Fi red de la OPAQ en La Haya, Países Bajos, en abril de 2018. El intento de ciberataque tuvo como objetivo piratear la red Wi-Fi de la OPAQ, lo que, de haber tenido éxito, habría comprometido la seguridad de la red y El trabajo de investigación en curso de la OPAQ. El Servicio de Inteligencia y Seguridad de Defensa de los Países Bajos (DISS)	30.7.2020

		Nacionalidad: rusa Género masculino	(Militaire Inlichtingen- en Veiligheidsdienst - MIVD) interrumpió el intento de ciberataque, evitando así daños graves a la OPAQ.	
4)	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Fecha de nacimiento: 31 de julio de 1977. Lugar de nacimiento: Murmanskaya Oblast, Rusia SFSR (ahora Federación de Rusia) Número de pasaporte: 100135556 Emitido por: Ministerio de Asuntos Exteriores de la Federación de Rusia Validez: desde el 17 de abril de 2017 hasta el 17 de abril de 2022 Ubicación: Moscú, Federación Rusa Nacionalidad: rusa Género masculino	Aleksei Morenets participó en un intento de ciberataque con un efecto potencialmente significativo contra la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos. Como operador cibernético de la Dirección Principal del Estado Mayor General de las Fuerzas Armadas de la Federación de Rusia (GU / GRU), Aleksei Morenets formó parte de un equipo de cuatro oficiales de inteligencia militar rusos que intentaron obtener acceso no autorizado a Wi- Red Fi de la OPAQ en La Haya, Países Bajos, en abril de 2018. El intento de ciberataque tuvo como objetivo piratear la red Wi-Fi de la OPAQ, que, de haber tenido éxito, habría comprometido la seguridad de la red y el El trabajo de investigación en curso de la OPAQ. El Servicio de Inteligencia y Seguridad de Defensa de los Países Bajos (DISS) (Militaire Inlichtingen- en Veiligheidsdienst - MIVD) interrumpió el intento de ciberataque, evitando así daños graves 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, Rusia SFSR (ahora Federación de Rusia) Número de pasaporte: 100135555 Emitido por: Ministerio de Asuntos Exteriores de la Federación de Rusia Validez: desde el 17 de abril de 2017 hasta el 17 de abril de 2022 Ubicación: Moscú, Federación Rusa Nacionalidad: rusa Género masculino	Evgenii Serebriakov participó en un intento de ciberataque con un efecto potencialmente significativo contra la Organización para la Prohibición de las Armas Químicas (OPAQ) en los Países Bajos. Como operador cibernético de la Dirección Principal del Estado Mayor General de las Fuerzas Armadas de la Federación Rusa (GU / GRU), Evgenii Serebriakov formó parte de un equipo de cuatro oficiales de inteligencia militar rusos que intentaron obtener acceso no autorizado a Wi- Red Fi de la OPAQ en La Haya, Países Bajos, en abril de 2018. El intento de ciberataque tuvo como objetivo piratear la red Wi-Fi de la OPAQ, que, de haber tenido éxito, habría comprometido la seguridad de la red y el El trabajo de investigación en curso de la OPAQ. El Servicio de Inteligencia y Seguridad de Defensa de los Países Bajos (DISS) (Militaire Inlichtingen- en Veiligheidsdienst - MIVD) interrumpió el intento de ciberataque, evitando así daños graves 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, Rusia SFSR	Oleg Sotnikov participó en un intento de ciberataque con un efecto potencialmente significativo contra la Organización para la Prohibición de las Armas Químicas (OPAQ), en los Países Bajos. Como oficial de apoyo de inteligencia humana de la Dirección Principal del Estado Mayor de las Fuerzas Armadas de la Federación de Rusia	30.7.2020

		(ahora Federación de Rusia) Número de pasaporte: 120018866 Emitido por: Ministerio de Asuntos Exteriores de la Federación de Rusia Validez: desde el 17 de abril de 2017 hasta el 17 de abril de 2022 Ubicación: Moscú, Federación Rusa Nacionalidad: rusa Género masculino	(GU / GRU), Oleg Sotnikov formó parte de un equipo de cuatro oficiales de inteligencia militar rusos que intentaron obtener acceso no autorizado a Wi - Red de la OPCW en La Haya, Países Bajos, en abril de 2018. El intento de ciberataque tuvo como objetivo piratear la red Wi-Fi de la OPCW, que, de haber tenido éxito, habría comprometido la seguridad de la red y El trabajo de investigación en curso de la OPAQ. El Servicio de Inteligencia y Seguridad de Defensa de los Países Bajos (DISS) (Militaire Inlichtingen- en Veiligheidsdienst - MIVD) interrumpió el intento de ciberataque, evitando así daños graves a la OPAQ.	

B. Personas jurídicas, entidades y organismos.

	Nombre	Información identificativa	Razones	Fecha de listado
1)	Tianjin Huaying Haitai Ciencia y Tecnología Development Co. Ltd (Huaying Haitai)	alias: Haitai Technology Development Co. Ltd Ubicación: Tianjin, China	Huaying Haitai brindó apoyo financiero, técnico o material y facilitó la "Operación Cloud Hopper", una serie de ciberataques con un efecto significativo que se origina desde fuera de la Unión y que constituye 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 ha dirigido a los sistemas de información de empresas multinacionales en seis continentes, incluidas las empresas ubicadas en la Unión, y ha obtenido acceso no autorizado a datos sensibles desde el punto de vista comercial, lo que ha resultado en una importante pérdida económica. El actor conocido públicamente como "APT10" ("Advanced Persistent Threat 10") (también conocido como "Red Apollo", "CVNX", "Stone Panda", "MenuPass" y "Potassium") llevó a cabo "Operation Cloud Hopper". Huaying Haitai se puede vincular a APT10. Además, Huaying Haitai empleó a Gao Qiang y Zhang Shilong, ambos designados en relación con la "Operación Nube Tolva". Por lo tanto, Huaying Haitai está asociado con Gao Qiang y Zhang Shilong.	30.7.2020
2)	Expo Chosun	alias: Expo elegida; Empresa conjunta de exportación de Corea Ubicación: RPDC	Chosun Expo brindó apoyo financiero, técnico o material y facilitó una serie de ciberataques con un efecto significativo que se originó fuera de la Unión y que constituye una amenaza externa para la Unión o sus Estados miembros y de ciberataques con un efecto significativo contra terceros Estados, incluidos los ciberataques conocidos públicamente como	30.7.2020

			"WannaCry" y los ciberataques contra la Autoridad de Supervisión Financiera de Polonia y Sony Pictures Entertainment, así como el robo cibernético del Banco de Bangladesh y el intento de robo cibernético del Banco Vietnam Tien Phong. "WannaCry" interrumpió los sistemas de información en todo el mundo al atacar los sistemas de información con ransomware y bloquear el acceso a los datos. Afectó a los sistemas de información de las empresas de la Unión, incluidos los sistemas de información relacionados con los servicios necesarios para el mantenimiento de servicios esenciales y actividades económicas dentro de los Estados miembros. El actor conocido públicamente como "APT38" ("Amenaza persistente avanzada 38") o el "Grupo Lazarus" realizó "WannaCry". Chosun Expo se puede vincular a APT38 / The Lazarus Group, incluso a través de las cuentas utilizadas para los ciberataques.	
3)	Centro Principal de Tecnologías Especiales (GTsST) de la Dirección Principal del Estado Mayor de las Fuerzas Armadas de la Federación de Rusia (GU / GRU)	Dirección: calle Kirova 22, Moscú, Federación Rusa	El Centro Principal de Tecnologías Especiales (GTsST) de la Dirección Principal del Estado Mayor de las Fuerzas Armadas de la Federación de Rusia (GU / GRU), también conocido por su número de campo 74455, es responsable de los ataques cibernéticos con un efecto significativo. originarios de fuera de la Unión y que constituyen una amenaza externa para la Unión o sus Estados miembros y para los ciberataques con un efecto significativo contra terceros Estados, incluidos los ciberataques conocidos públicamente como "NotPetya" o "EternalPetya" en junio de 2017 y el ciberataques dirigidos a una red eléctrica ucraniana en el invierno de 2015 y 2016. "NotPetya" o "EternalPetya" hicieron que los datos fueran inaccesibles en varias empresas de la Unión, en toda Europa y en todo el mundo, al atacar computadoras con ransomware y bloquear el acceso a los datos, lo que resultó, entre otros, en una pérdida económica significativa. El ataque cibernético contra una red eléctrica ucraniana provocó la desconexión de partes durante el invierno.	30.7.2020
			El actor conocido públicamente como "Sandworm" (también conocido como "Sandworm Team", "BlackEnergy Group", "Voodoo Bear", "Quedagh", "Olympic Destroyer" y "Telebots"), que también está detrás del ataque a la red eléctrica de Ucrania. , realizado "NotPetya" o "EternalPetya". El Centro Principal de Tecnologías Especiales de la Dirección Principal del Estado Mayor de las Fuerzas Armadas de la Federación de Rusia tiene un papel activo en las actividades	

			cibernéticas realizadas por Sandworm y puede vincularse a Sandworm.	