DECISIONE (PESC) 2020/1127 DEL CONSIGLIO

del 30 luglio 2020

che modifica la decisione (PESC) 2019/797, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato dell'Unione europea, in particolare l'articolo 29,

vista la proposta dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza,

considerando quanto segue:

(1) Il 17 maggio 2019 il Consiglio ha adottato la decisione (PESC) 2019/797 ([1]).

(2) Le misure restrittive mirate contro gli attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri fanno parte delle misure previste nel quadro dell'Unione relativo a una risposta diplomatica comune alle attività informatiche dolose (pacchetto di strumenti della diplomazia informatica) e sono uno strumento fondamentale per scoraggiare e contrastare tali attività. Le misure restrittive possono altresì essere applicate in risposta ad attacchi informatici con effetti significativi nei confronti di Stati terzi o organizzazioni internazionali, ove ritenuto necessario ai fini del conseguimento degli obiettivi della politica estera e di sicurezza comune enunciati nelle pertinenti disposizioni dell'articolo 21 del trattato sull'Unione europea.

(3) Il 16 aprile 2018 il Consiglio ha adottato conclusioni in cui condanna fermamente l'uso illecito di tecnologie dell'informazione e della comunicazione, inclusi gli attacchi informatici pubblicamente noti come «WannaCry» e «NotPetya», che hanno causato danni significativi e perdite economiche nell'Unione e nel resto del mondo. Il 4 ottobre 2018 i presidenti del Consiglio europeo e della Commissione europea e l'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza («alto rappresentante») hanno espresso serie preoccupazioni in una dichiarazione congiunta relativa a un tentativo di attacco informatico inteso a compromettere l'integrità dell'Organizzazione per la proibizione delle armi chimiche (OPCW) nei Paesi Bassi, un atto aggressivo che costituisce un oltraggio nei confronti del solenne obiettivo dell'OPCW. In una dichiarazione rilasciata a nome dell'Unione il 12 aprile 2019, l'alto rappresentante ha esortato i soggetti interessati a cessare di intraprendere attività informatiche dolose volte a compromettere l'integrità, la sicurezza e la competitività economica dell'Unione, ivi compreso il furto di proprietà intellettuale favorito dall'informatica. I furti favoriti dall'informatica comprendono quelli effettuati dal soggetto pubblicamente noto come «APT10» («*Advanced Persistent Threat* 10»).

(4) In tale contesto e al fine di prevenire, scoraggiare e contrastare il persistere e l'aumento del comportamento doloso nel ciberspazio, sei persone fisiche e tre entità o organismi dovrebbero essere inseriti nell'elenco delle persone fisiche e giuridiche, delle entità e degli organismi soggetti a misure restrittive che figura nell'allegato della decisione (PESC) 2019/797. Tali persone ed entità o organismi sono responsabili di attacchi informatici o tentati attacchi informatici, hanno fornito sostegno a tali attacchi, vi erano coinvolti o li hanno agevolati, compresi il tentativo di attacco informatico contro l'OPCW, gli attacchi informatici pubblicamente noti come «WannaCry» e «NotPetya», nonché la campagna «*Operation Cloud Hopper*».

(5) È opportuno pertanto modificare di conseguenza la decisione (PESC) 2019/797,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

L'allegato della decisione (PESC) 2019/797 è modificato conformemente all'allegato della presente decisione.

([1]) Decisione (PESC) 2019/797 del Consiglio, del 17 maggio 2019, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri (GU L 129I del 17.5.2019, pag. 13).

Articolo 2

La presente decisione entra in vigore il giorno della pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Fatto a Bruxelles, il 30 luglio 2020

Per il Consiglio
Il presidente
M. ROTH

ALLEGATO

Le persone e le entità o gli organismi seguenti sono aggiunti all'elenco delle persone fisiche e giuridiche, delle entità e degli organismi riportato nell'allegato della decisione (PESC) 2019/797:

«A. Persone fisiche

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
1.	GAO Qiang	Luogo di nascita: Shandong Province, Cina Indirizzo: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, Cina Cittadinanza: cinese Sesso: maschile	Gao Qiang è coinvolto nella campagna "Operation Cloud Hopper", una serie di attacchi informatici con effetti significativi che proviene dall'esterno dell'Unione e costituisce una minaccia esterna per l'Unione o i suoi Stati membri e di attacchi informatici con effetti significativi nei confronti di Stati terzi. La campagna "Operation Cloud Hopper" ha preso di mira i sistemi di informazione di imprese multinazionali in sei continenti, tra cui imprese situate nell'Unione, e ha ottenuto l'accesso non autorizzato a dati sensibili sotto il profilo commerciale, causando perdite economiche significative. Il soggetto noto pubblicamente come "APT10" ("Advanced Persistent Threat 10") (alias "Red Apollo", "CVNX", "Stone Panda", "MenuPass" e "Potassium") ha condotto la campagna "Operation Cloud Hopper". Gao Qiang può essere collegato all'APT10, anche attraverso la sua associazione con l'infrastruttura di comando e controllo di APT10. Inoltre, Huaying Haitai, un'entità designata per il fatto di fornire sostegno e agevolare la campagna "Operation Cloud Hopper", ha impiegato Gao Qiang. Quest'ultimo ha legami con Zhang Shilong, la cui designazione è altresì connessa alla campagna "Operation Cloud Hopper". Gao Qiang è pertanto associato sia a Huaying Haitai che a Zhang Shilong.	30.7.2020
2.	ZHANG Shilong	Indirizzo: Hedong, Yuyang Road No 121, Tianjin, Cina Cittadinanza: cinese Sesso: maschile	Zhang Shilong è coinvolto nella campagna "Operation Cloud Hopper", una serie di attacchi informatici con effetti significativi che proviene dall'esterno dell'Unione e costituisce una minaccia esterna per l'Unione o i suoi Stati membri e di attacchi informatici con effetti significativi nei confronti di Stati terzi. La campagna "Operation Cloud Hopper" ha preso di mira i sistemi di informazione di imprese multinazionali in sei continenti, tra cui imprese situate nell'Unione, e ha ottenuto l'accesso non autorizzato a dati sensibili sotto il profilo commerciale, causando perdite economiche significative. Il soggetto noto pubblicamente come "APT10" ("Advanced Persistent Threat 10") (alias "Red Apollo", "CVNX", "Stone Panda", "MenuPass" e "Potassium") ha condotto la campagna "Operation Cloud Hopper".	30.7.2020

			Zhang Shilong può essere collegato all'APT10, anche attraverso il malware che ha sviluppato e testato in relazione agli attacchi informatici condotti dall'APT10. Inoltre, Huaying Haitai, un'entità designata per il fatto di fornire sostegno e agevolare la campagna "Operation Cloud Hopper", ha impiegato Zhang Shilong. Quest'ultimo ha legami con Gao Qiang, la cui designazione è altresì connessa alla campagna "Operation Cloud Hopper". Zhang Shilong è pertanto associato sia a Huaying Haitai che a Gao Qiang.	
3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Data di nascita: 27 maggio 1972 Luogo di nascita: Perm Oblast, RSFS russa (ora Federazione russa) Passaporto n.: 120017582 Rilasciato da: ministero degli Affari esteri della Federazione russa Validità: dal 17 aprile 2017 al 17 aprile 2022 Luogo: Mosca, Federazione russa Cittadinanza: russa Sesso: maschile	Alexey Minin ha partecipato a un tentativo di attacco informatico con effetti potenzialmente significativi contro l'Organizzazione per la proibizione delle armi chimiche (OPCW) nei Paesi Bassi. In qualità di agente di supporto dell'intelligence della direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU), Alexey Minin faceva parte di una squadra di quattro agenti dell'intelligence militare russa che hanno cercato di ottenere un accesso non autorizzato alla rete Wi-Fi dell'OPCW all'Aia (Paesi Bassi) nell'aprile 2018. Il tentativo di attacco informatico era finalizzato a ottenere un accesso abusivo alla rete Wi-Fi dell'OPCW, che, in caso di successo, avrebbe compromesso la sicurezza della rete e i lavori di indagine dell'OPCW in corso. Il Servizio di intelligence e sicurezza militare dei Paesi Bassi (*Militaire Inlichtingen- en Veiligheidsdienst* — MIVD) ha sventato il tentativo di attacco informatico, impedendo in tal modo gravi danni all'OPCW.	30.7.2020
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Data di nascita: 31 luglio 1977 Luogo di nascita: Murmanskaya Oblast, RSFS russa (ora Federazione russa) Passaporto n.: 100135556 Rrilasciato da: ministero degli Affari esteri della Federazione russa Validità: dal 17 aprile 2017 al 17 aprile 2022 Luogo: Mosca, Federazione russa Cittadinanza: russa Sesso: maschile	Aleksei Morenets ha partecipato a un tentativo di attacco informatico con effetti potenzialmente significativi contro l'Organizzazione per la proibizione delle armi chimiche (OPCW) nei Paesi Bassi. In qualità di operatore informatico della direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU), Aleksei Morenets faceva parte di una squadra di quattro agenti dell'intelligence militare russa che hanno cercato di ottenere un accesso non autorizzato alla rete Wi-Fi dell'OPCW all'Aia (Paesi Bassi) nell'aprile 2018. Il tentativo di attacco informatico era finalizzato a ottenere un accesso abusivo alla rete Wi-Fi dell'OPCW, che, in caso di successo, avrebbe compromesso la sicurezza della rete e i lavori di indagine dell'OPCW in corso. Il Servizio di intelligence e sicurezza militare dei Paesi Bassi (*Militaire Inlichtingen- en Veiligheidsdienst* — MIVD) ha sventato il tentativo di attacco informatico, impedendo in tal modo gravi danni all'OPCW.	30.7.2020

5.	Evgenii Mikhaylovich MORENETS	Евгений Михайлович СЕРЕБРЯКОВ Data di nascita: 26 luglio 1981 Luogo di nascita: Kursk, RSFS russa (ora Federazione russa) Passaporto n.: 100135555 R ilasciato dal ministero degli Affari esteri della Federazione russa Validità: dal 17 aprile 2017 al 17 aprile 2022 Luogo: Mosca, Federazione russa Cittadinanza: russa Sesso: maschile	Evgenii Serebriakov ha partecipato a un tentativo di attacco informatico con effetti potenzialmente significativi contro l'Organizzazione per la proibizione delle armi chimiche (OPCW) nei Paesi Bassi. In qualità di operatore informatico della direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU), Evgenii Serebriakov faceva parte di una squadra di quattro agenti dell'intelligence militare russa che hanno cercato di ottenere un accesso non autorizzato alla rete Wi-Fi dell'OPCW all'Aia (Paesi Bassi) nell'aprile 2018. Il tentativo di attacco informatico era finalizzato a ottenere un accesso abusivo alla rete Wi-Fi dell'OPCW, che, in caso di successo, avrebbe compromesso la sicurezza della rete e i lavori di indagine dell'OPCW in corso. Il Servizio di intelligence e sicurezza militare dei Paesi Bassi (*Militaire Inlichtingen- en Veiligheidsdienst* — MIVD) ha sventato il tentativo di attacco informatico, impedendo in tal modo gravi danni all'OPCW.	30.7.2020
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Data di nascita: 24 agosto 1972 Luogo di nascita: Ulyanovsk, RSFS russa (ora Federazione russa) Passaporto n.: 120018866 Rilasciato dal ministero degli Affari esteri della Federazione russa Validità: dal 17 aprile 2017 al 17 aprile 2022 Luogo: Mosca, Federazione russa Cittadinanza: russa Sesso: maschile	Oleg Sotnikov ha partecipato a un tentativo di attacco informatico con effetti potenzialmente significativi contro l'Organizzazione per la proibizione delle armi chimiche (OPCW) nei Paesi Bassi. In qualità di agente di supporto dell'intelligence della direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU), Oleg Sotnikov faceva parte di una squadra di quattro agenti dell'intelligence militare russa che hanno cercato di ottenere un accesso non autorizzato alla rete Wi-Fi dell'OPCW all'Aia (Paesi Bassi) nell'aprile 2018. Il tentativo di attacco informatico era finalizzato a ottenere un accesso abusivo alla rete Wi-Fi dell'OPCW, che, in caso di successo, avrebbe compromesso la sicurezza della rete e i lavori di indagine dell'OPCW in corso. Il Servizio di intelligence e sicurezza militare dei Paesi Bassi (*Militaire Inlichtingen- en Veiligheidsdienst* — MIVD) ha sventato il tentativo di attacco informatico, impedendo in tal modo gravi danni all'OPCW.	30.7.2020

B. Persone giuridiche, entità e organismi

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	Alias: Haitai Technology Development Co. Ltd Ubicazione: Tianjin, Cina	Huaying Haitai ha fornito sostegno finanziario, tecnico o materiale e ha agevolato la campagna "Operation Cloud Hopper", una serie di attacchi informatici con effetti significativi, che proviene dall'esterno dell'Unione e costituisce una minaccia esterna per l'Unione o i suoi Stati membri e di attacchi informatici con effetti significativi nei confronti di Stati terzi.	30.7.2020

			La campagna "Operation Cloud Hopper" ha preso di mira i sistemi di informazione di imprese multinazionali in sei continenti, tra cui imprese situate nell'Unione, e ha ottenuto l'accesso non autorizzato a dati sensibili sotto il profilo commerciale, causando perdite economiche significative. Il soggetto noto pubblicamente come "APT10" ("Advanced Persistent Threat 10") (alias "Red Apollo", "CVNX", "Stone Panda", "MenuPass" e "Potassium") ha condotto la campagna "Operation Cloud Hopper". Huaying Haitai può essere collegata all'APT10. Inoltre, Huaying Haitai impiegava Gao Qiang e Zhang Shilong, entrambi designati in relazione alla campagna "Operation Cloud Hopper". Huaying Haitai è pertanto associata sia a Gao Qiang che a Zhang Shilong.	
2.	Chosun Expo	Alias: Chosen Expo; Korea Export Joint Venture Ubicazione: RPDC	Chosun Expo ha fornito sostegno finanziario, tecnico o materiale e ha agevolato una serie di attacchi informatici con effetti significativi, che proviene dall'esterno dell'Unione e costituisce una minaccia esterna per l'Unione o i suoi Stati membri e di attacchi informatici con effetti significativi nei confronti di Stati terzi, compresi gli attacchi informatici pubblicamente noti come "WannaCry" e gli attacchi informatici contro l'autorità di vigilanza finanziaria polacca e Sony Pictures Entertainment, nonché il furto informatico alla Bangladesh Bank e il tentativo di furto informatico alla Vietnam Tien Phong Bank. "WannaCry" ha causato perturbazioni a sistemi informatici in diverse parti del mondo compromettendo i sistemi di informazione con ransomware e bloccando l'accesso ai dati. Ha colpito i sistemi di informazione di imprese nell'Unione, compresi quelli relativi ai servizi necessari per il mantenimento di servizi e attività economiche essenziali all'interno degli Stati membri. L'attacco "WannaCry" è stato effettuato dal soggetto noto pubblicamente come "APT38" ("Advanced Persistent Threat 38") o "Lazarus Group". Chosun Expo può essere collegata all'APT38/Lazarus Group, anche attraverso i conti utilizzati per gli attacchi informatici.	30.7.2020
3.	Centro principale per le tecnologie speciali (GTsST), direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU)	Indirizzo: 22 Kirova Street, Mosca, Federazione russa	Il Centro principale per le tecnologie speciali (GTsST), direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU), noto anche come unità 74455, è responsabile di attacchi informatici con effetti significativi che provengono dall'esterno dell'Unione e costituiscono una minaccia esterna per l'Unione o i suoi Stati membri e di attacchi informatici con effetti significativi nei confronti di Stati terzi, compresi gli attacchi informatici pubblicamente noti come "NotPetya" o "EternalPetya" nel giugno 2017 e gli attacchi informatici diretti a una rete elettrica ucraina nell'inverno del 2015 e del 2016.	30.7.2020»

			"NotPetya" o "EternalPetya" ha reso i dati inaccessibili a diverse imprese nell'Unione, in Europa in generale e nel resto del mondo, compromettendo i computer con ransomware e bloccando l'accesso ai dati e causando così, tra l'altro, perdite economiche significative. L'attacco informatico a una rete elettrica ucraina ha fatto sì che parti della stessa rimanessero spente durante l'inverno. Il soggetto pubblicamente noto come "Sandworm" (alias "Sandworm Team", "BlackEnergy Group", "Voodoo Bear", "Quedagh", "Olympic Destoyer" e Telebot), che è anche all'origine dell'attacco alla rete elettrica ucraina, è responsabile di "NotPetya" o "EternalPetya". Il Centro principale per le tecnologie speciali, direzione principale dello Stato maggiore delle forze armate della Federazione russa, ha un ruolo attivo nelle attività informatiche intraprese da Sandworm e può essere collegato a Sandworm.	