DECISIONI

DECISIONE (PESC) 2020/1537 DEL CONSIGLIO

del 22 ottobre 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 nell'ambito 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.

(3) Al fine di prevenire, scoraggiare e contrastare il persistere e l'aumento di comportamenti dolosi nel ciberspazio, due persone fisiche e un organismo 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 e tale organismo sono responsabili di attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri, o vi sono stati coinvolti, in particolare l'attacco informatico ai danni del parlamento federale tedesco (Deutscher Bundestag) avvenuto tra aprile e maggio 2015.

(4) 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.

Articolo 2

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

Fatto a Bruxelles, il 22 ottobre 2020

Per il Consiglio
Il presidente
M. ROTH

([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).

ALLEGATO

Le seguenti voci sono aggiunte 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
«7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Data di nascita: 15 novembre 1990 Luogo di nascita: Kursk, RSFS russa (ora Federazione russa) Cittadinanza: russa Sesso: maschile	Dmitry Badin ha partecipato a un attacco informatico con effetti significativi ai danni del parlamento federale tedesco (Deutscher Bundestag). In qualità di agente dell'intelligence militare dell'85° Centro principale per i servizi speciali (GTsSS), direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU), Dmitry Badin faceva parte di una squadra di agenti dell'intelligence militare russa che ha condotto un attacco informatico ai danni del parlamento federale tedesco (Deutscher Bundestag) tra aprile e maggio 2015. Tale attacco ha colpito il sistema informatico del parlamento, compromettendone il funzionamento per diversi giorni. È stato sottratto un ingente volume di dati e sono stati violati gli account di posta elettronica di diversi parlamentari, nonché quello della Cancelliera Angela Merkel.	22.10.2020
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Data di nascita: 21 febbraio 1961 Cittadinanza: russa Sesso: maschile	Igor Kostyukov è l'attuale capo della direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU), presso cui ha precedentemente svolto le funzioni di primo vice capo. Tra le unità sotto il suo comando vi è l'85° Centro principale per i servizi speciali (GTsSS), noto anche come unità militare 26165 (alias: APT28, Fancy Bear, Sofacy Group, Pawn Storm, Strontium). In tale veste, Igor Kostyukov è responsabile degli attacchi informatici condotti dall'85° Centro principale per i servizi speciali (GTsSS), tra cui quelli con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri. In particolare, agenti dell'intelligence militare dell'85° Centro principale per i servizi speciali (GTsSS) hanno partecipato all'attacco informatico ai danni del parlamento federale tedesco (Deutscher Bundestag) tra aprile e maggio 2015, nonché al tentativo di attacco informatico finalizzato a ottenere un accesso abusivo alla rete Wi-Fi dell'Organizzazione per la proibizione delle armi chimiche (OPCW) nei Paesi Bassi nell'aprile 2018. L'attacco informatico ai danni del parlamento federale tedesco ha colpito il sistema informatico del parlamento, compromettendone il funzionamento per diversi giorni. È stato sottratto un ingente volume di dati e sono stati violati gli account di posta elettronica di diversi parlamentari, nonché quello della Cancelliera Angela Merkel.	22.10.2020»

B. Persone giuridiche, entità e organismi

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
«4.	85° Centro principale per i servizi speciali (GTsSS), direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU)	Indirizzo: Komsomol'skiy Prospekt, 20, Mosca, 119146, Federazione russa	L'85° Centro principale per i servizi speciali (GTsSS), direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU), noto anche come unità militare 26165 (alias: APT28, Fancy Bear, Sofacy Group, Pawn Storm, Strontium), è responsabile di attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri. In particolare, agenti dell'intelligence militare dell'85° Centro principale per i servizi speciali (GTsSS) hanno partecipato all'attacco informatico ai danni del parlamento federale tedesco (Deutscher Bundestag) tra aprile e maggio 2015, nonché al tentativo di attacco informatico finalizzato a ottenere un accesso abusivo alla rete Wi-Fi dell'Organizzazione per la proibizione delle armi chimiche (OPCW) nei Paesi Bassi nell'aprile 2018. L'attacco informatico ai danni del parlamento federale tedesco ha colpito il sistema informatico del parlamento, compromettendone il funzionamento per diversi giorni. È stato sottratto un ingente volume di dati e sono stati violati gli account di posta elettronica di diversi parlamentari, nonché quello della Cancelliera Angela Merkel.	22.10.2020»