2025/887

13.5.2025

# DECISIONE (PESC) 2025/887 DEL CONSIGLIO

## del 12 maggio 2025

## 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 sull'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) La decisione (PESC) 2019/797 si applica fino al 18 maggio 2025. In esito a un riesame di tale decisione, il Consiglio ritiene che sia opportuno prorogarne l'applicazione fino al 18 maggio 2028.

(3) Sulla base del riesame dell'allegato della decisione (PESC) 2019/797 risulta opportuno prorogare fino al 18 maggio 2026 l'applicazione delle misure di cui agli articoli 4 e 5 di tale decisione in relazione alle persone fisiche e giuridiche, alle entità e agli organismi elencati in tale allegato. È opportuno inoltre aggiornare le motivazioni per l'inclusione di sei persone nell'elenco di persone fisiche e giuridiche, delle entità e degli organismi oggetto di misure restrittive.

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

HA ADOTTATO LA PRESENTE DECISIONE:

*Articolo 1*

La decisione (PESC) 2019/797 è così modificata:

1) L'articolo 10 è sostituito dal seguente:

«*Articolo 10*

La presente decisione si applica fino al 18 maggio 2028 ed è costantemente riesaminata. Le misure di cui agli articoli 4 e 5 si applicano nei confronti delle persone fisiche e giuridiche, delle entità e degli organismi elencati nell'allegato fino al 18 maggio 2026»;

2) L'allegato è modificato conformemente all'allegato della presente decisione.

*Articolo 2*

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

Fatto a Bruxelles, il 12 maggio 2025

*Per il Consiglio*

*Il presidente*

B. NOWACKA

[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 129 I del 17.5.2019, pag. 13, ELI: http://data.europa.eu/eli/dec/2019/797/oj).

*ALLEGATO*

Nell'allegato della decisione (PESC) 2019/797, nella sottorubrica «A. Persone fisiche», le voci da 3 a 8 sono sostituite dalle seguenti:

| | Nome | Informazioni identificative | Motivi | Data di inserimento nell'elenco |
|---|---|---|---|---|
| «3. | Alexey Valeryevich MININ | Алексей Валерьевич МИНИН<br>Data di nascita: 27.5.1972<br>Luogo di nascita: oblast di Perm, RSFS russa (ora Federazione russa)<br>N. di passaporto: 120017582<br>Rilasciato da: ministero degli Affari esteri della Federazione russa<br>Validità: dal 17.4.2017 al 17.4.2022<br>Luogo: Mosca, Federazione russa<br>Cittadinanza: russa<br>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 e ad attacchi informatici con effetti significativi contro Stati terzi.<br>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) ha sventato il tentativo di attacco informatico, impedendo in tal modo gravi danni all'OPCW.<br>Un grand jury nel distretto occidentale della Pennsylvania (Stati Uniti d'America) ha accusato Alexey Minin, in quanto agente del GRU russo, di pirateria informatica, frode telematica, furto aggravato d'identità e riciclaggio.<br>Il GRU continua a condurre attacchi informatici contro l'Unione o i suoi Stati membri. In qualità di membro del GRU, Alexey Minin è pertanto coinvolto in attacchi informatici con effetti significativi, inclusi i tentati attacchi informatici con effetti potenzialmente significativi, che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri. | 30.7.2020 |

| | Nome | Informazioni identificative | Motivi | Data di inserimento nell'elenco |
|---|---|---|---|---|
| 4. | Aleksei Sergeyvich MORENETS | Алексей Сергеевич МОРЕНЕЦ<br>Data di nascita: 31.7.1977<br>Luogo di nascita: oblast di Murmanskaya, RSFS russa (ora Federazione russa)<br>N. di passaporto: 100135556<br>Rilasciato da: ministero degli Affari esteri della Federazione russa<br>Validità: dal 17.4.2017 al 17.4.2022<br>Luogo: Mosca, Federazione russa<br>Cittadinanza: russa<br>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 e ad attacchi informatici con effetti significativi contro Stati terzi.<br>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) ha sventato il tentativo di attacco informatico, impedendo in tal modo gravi danni all'OPCW.<br>Un grand jury nel distretto occidentale della Pennsylvania (Stati Uniti d'America) ha accusato Aleksei Morenets, in quanto assegnato all'unità militare 26165, di pirateria informatica, frode telematica, furto aggravato d'identità e riciclaggio.<br>Il GRU continua a condurre attacchi informatici contro l'Unione o i suoi Stati membri. In qualità di membro del GRU, Aleksei Morenets è pertanto coinvolto in attacchi informatici con effetti significativi, inclusi i tentati attacchi informatici con effetti potenzialmente significativi, che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri. | 30.7.2020 |

| | Nome | Informazioni identificative | Motivi | Data di inserimento nell'elenco |
|---|---|---|---|---|
| 5. | Evgenii Mikhaylovich SEREBRIAKOV | Евгений Михайлович СЕРЕБРЯКОВ<br>Data di nascita: 26.7.1981<br>Luogo di nascita: Kursk, RSFS russa (ora Federazione russa)<br>N. di passaporto: 100135555<br>Rilasciato da: ministero degli Affari esteri della Federazione russa<br>Validità: dal 17.4.2017 al 17.4.2022<br>Luogo: Mosca, Federazione russa<br>Cittadinanza: russa<br>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 e ad attacchi informatici con effetti significativi contro Stati terzi.<br>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) ha sventato il tentativo di attacco informatico, impedendo in tal modo gravi danni all'OPCW.<br>Dalla primavera del 2022 Evgenii Serebriakov guida "Sandworm" (alias "Sandworm Team", "BlackEnergy Group", "Voodoo Bear", "Quedagh", "Olympic Destroyer" e "Telebots"), un soggetto e un gruppo di pirateria informatica affiliato all'unità 74455 della direzione principale dell'intelligence russa. Sandworm ha sferrato attacchi informatici contro l'Ucraina, compresi organismi pubblici ucraini, a seguito della guerra di aggressione della Russia nei confronti dell'Ucraina.<br>Il GRU continua a condurre attacchi informatici contro l'Unione o i suoi Stati membri. In qualità di membro del GRU, Evgenii Serebriakov è pertanto coinvolto in attacchi informatici con effetti significativi, inclusi i tentati attacchi informatici con effetti potenzialmente significativi, che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri. | 30.7.2020 |

| | Nome | Informazioni identificative | Motivi | Data di inserimento nell'elenco |
|---|---|---|---|---|
| 6. | Oleg Mikhaylovich SOTNIKOV | Олег Михайлович СОТНИКОВ<br>Data di nascita: 24.8.1972<br>Luogo di nascita: Ulyanovsk, RSFS russa (ora Federazione russa)<br>N. di passaporto: 120018866<br>Rilasciato da: ministero degli Affari esteri della Federazione russa<br>Validità: dal 17.4.2017 al 17.4.2022<br>Luogo: Mosca, Federazione russa<br>Cittadinanza: russa<br>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 e ad attacchi informatici con effetti significativi contro Stati terzi.<br>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) ha sventato il tentativo di attacco informatico, impedendo in tal modo gravi danni all'OPCW.<br>Un grand jury nel distretto occidentale della Pennsylvania (Stati Uniti d'America) ha accusato Oleg Sotnikov, in quanto agente del GRU russo, di pirateria informatica, frode telematica, furto aggravato d'identità e riciclaggio.<br>Il GRU continua a condurre attacchi informatici contro l'Unione o i suoi Stati membri. In qualità di membro del GRU, Oleg Sotnikov è pertanto coinvolto in attacchi informatici con effetti significativi, inclusi i tentati attacchi informatici con effetti potenzialmente significativi, che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri. | 30.7.2020 |

| | Nome | Informazioni identificative | Motivi | Data di inserimento nell'elenco |
|---|---|---|---|---|
| 7. | Dmitry Sergeyevich BADIN | Дмитрий Сергеевич БАДИН<br>Data di nascita: 15.11.1990<br>Luogo di nascita: Kursk, RSFS russa (ora Federazione russa)<br>Cittadinanza: russa<br>Sesso: maschile | Dmitry Badin ha partecipato a un attacco informatico con effetti significativi contro il parlamento federale tedesco (Deutscher Bundestag) e ad attacchi informatici con effetti significativi contro Stati terzi.<br>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 contro il parlamento federale tedesco 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 dell'ex cancelliera Angela Merkel.<br>Un grand jury nel distretto occidentale della Pennsylvania (Stati Uniti d'America) ha accusato Dmitry Badin, in quanto assegnato all'unità militare 26165, di pirateria informatica, frode telematica, furto aggravato d'identità e riciclaggio.<br>Il GRU continua a condurre attacchi informatici contro l'Unione o i suoi Stati membri. In qualità di membro del GRU, Dmitry Badin è pertanto coinvolto in attacchi informatici con effetti significativi, inclusi i tentati attacchi informatici con effetti potenzialmente significativi, che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri. | 22.10.2020 |

| | Nome | Informazioni identificative | Motivi | Data di inserimento nell'elenco |
|---|---|---|---|---|
| 8. | Igor Olegovich KOSTYUKOV | Игорь Олегович КОСТЮКОВ<br>Data di nascita: 21.2.1961<br>Cittadinanza: russa<br>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 vicecapo. Tra le unità sotto il suo comando vi è l'85° Centro principale per i servizi speciali (GTsSS), (alias "unità militare 26165", "APT28", "Fancy Bear", "Sofacy Group", "Pawn Storm", "Strontium").<br>In tale veste, Igor Kostyukov è responsabile degli attacchi informatici condotti dal GTsSS, tra cui quelli con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.<br>In particolare, agenti dell'intelligence militare del GTsSS hanno partecipato all'attacco informatico contro il 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.<br>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 dell'ex cancelliera Angela Merkel.<br>Il GRU continua a condurre attacchi informatici contro l'Unione o i suoi Stati membri. In qualità di membro del GRU, Igor Kostyukov è pertanto coinvolto in attacchi informatici con effetti significativi, inclusi i tentati attacchi informatici con effetti potenzialmente significativi, che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri. | 22.10.2020» |