II

*(Atti non legislativi)*

# REGOLAMENTI

## REGOLAMENTO DI ESECUZIONE (UE) 2020/1744 DEL CONSIGLIO

**del 20 novembre 2020**

**che attua il regolamento (UE) 2019/796 concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri**

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) 2019/796 del Consiglio, del 17 maggio 2019, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri ([1]), in particolare l'articolo 13, paragrafo 1,

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 il regolamento (UE) 2019/796.

(2) Il 30 luglio 2020 il Consiglio ha adottato il regolamento di esecuzione (UE) 2020/1125 ([2]), con il quale sono state aggiunte sei persone fisiche e tre entità od organismi all'elenco delle persone fisiche e giuridiche, delle entità e degli organismi soggetti a misure restrittive che figura nell'allegato I del regolamento (UE) 2019/796.

(3) Sono state ricevute informazioni aggiornate per due voci dell'elenco delle persone fisiche.

(4) È opportuno pertanto modificare di conseguenza il regolamento (UE) 2019/796,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

*Articolo 1*

L'allegato I del regolamento (UE) 2019/796 è modificato conformemente all'allegato del presente regolamento.

*Articolo 2*

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

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il 20 novembre 2020

*Per il Consiglio*
*Il president*
M. ROTH

([1]) GU L 129I del 17.5.2019, pag. 1.
([2]) Regolamento di esecuzione (UE) 2020/1125 del Consiglio, del 30 luglio 2020, che attua il regolamento (UE) 2019/796, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri (GU L 246 del 30.7.2020, pag. 4).

*ALLEGATO*

Nell'allegato I del regolamento (UE) 2019/796, nella sottorubrica «A. Persone fisiche», le voci 1 e 2 sono sostituite dalle seguenti:

| | Nome | Informazioni identificative | Motivi | Data di inserimento nell'elenco |
|---|---|---|---|---|
| «1. | GAO Qiang | Data di nascita: 4 ottobre 1983<br>Luogo di nascita: Shandong Province, Cina<br>Indirizzo: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, Cina<br>Cittadinanza: cinese<br>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.<br>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.<br>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».<br>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 | Data di nascita: 10 settembre 1981<br>Luogo di nascita: Cina<br>Indirizzo: Hedong, Yuyang Road No 121, Tianjin, Cina<br>Cittadinanza: cinese<br>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.<br>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.<br>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».<br>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. | 30.7.2020». |