II

(Ikke-lovgivningsmæssige retsakter)

FORORDNINGER

RÅDETS GENNEMFØRELSESFORORDNING (EU) 2020/1744

af 20. november 2020

om gennemførelse af forordning (EU) 2019/796 om restriktive foranstaltninger til bekæmpelse af cyberangreb, der truer Unionen eller dens medlemsstater

RÅDET FOR DEN EUROPÆISKE UNION HAR —

under henvisning til traktaten om Den Europæiske Unions funktionsmåde,

under henvisning til Rådets forordning (EU) 2019/796 af 17. maj 2019 om restriktive foranstaltninger til bekæmpelse af cyberangreb, der truer Unionen eller dens medlemsstater ([1]), særlig artikel 13, stk. 1,

under henvisning til forslag fra Unionens højtstående repræsentant for udenrigsanliggender og sikkerhedspolitik, og

ud fra følgende betragtninger:

(1) Den 17. maj 2019 vedtog Rådet forordning (EU) 2019/796.

(2) Den 30. juli 2020 vedtog Rådet gennemførelsesforordning (EU) 2020/1125 ([2]), der tilføjede seks fysiske personer og tre enheder eller organer til den liste over fysiske og juridiske personer, enheder og organer, der er omfattet af restriktive foranstaltninger, som er fastsat i bilag I til forordning (EU) 2019/796.

(3) Der er modtaget ajourførte oplysninger for to opførelser af fysiske personer på listen.

(4) Forordning (EU) 2019/796 bør derfor ændres i overensstemmelse hermed —

VEDTAGET DENNE FORORDNING:

Artikel 1

Bilag I til forordning (EU) 2019/796 ændres som anført i bilaget til nærværende forordning.

Artikel 2

Denne forordning træder i kraft dagen efter offentliggørelsen i *Den Europæiske Unions Tidende*.

Denne forordning er bindende i alle enkeltheder og gælder umiddelbart i hver medlemsstat.

Udfærdiget i Bruxelles, den 20. november 2020.

På Rådets vegne
M. ROTH
Formand

([1]) EUT L 129 I af 17.5.2019, s. 1.
([2]) Rådets gennemførelsesforordning (EU) 2020/1125 af 30. juli 2020 om gennemførelse af forordning (EU) 2019/796 om restriktive foranstaltninger til bekæmpelse af cyberangreb, der truer Unionen eller dens medlemsstater (EUT L 246 af 30.7.2020, s. 4).

BILAG

I bilag I til forordning (EU) 2019/796 under underoverskriften »A. Fysiske personer« affattes punkt 1 og 2 således:

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
»1.	GAO Qiang	Fødselsdato: 4. oktober 1983 Fødested: Shandongprovinsen, Kina Adresse: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Nationalitet: kinesisk Køn: mand	Gao Qiang er involveret i »Operation Cloud Hopper«, en række cyberangreb med betydelige konsekvenser og med oprindelse uden for Unionen, som udgør en ekstern trussel mod Unionen eller dens medlemsstater, og i cyberangreb, som har betydelige konsekvenser for tredjelande. »Operation Cloud Hopper« har været rettet mod multinationale virksomheders informationssystemer på seks kontinenter, herunder virksomheder i Unionen, og har opnået uautoriseret adgang til kommercielt følsomme data, hvilket har medført et betydeligt økonomisk tab. Den aktør, der offentligt er kendt som »APT10« (»Advanced Persistent Threat 10«) (alias »Red Apollo«, »CVNX«, »Stone Panda«, »MenuPass« og »Potassium«), gennemførte »Operation Cloud Hopper«. Gao Qiang kan sættes i forbindelse med APT10, herunder gennem sin tilknytning til APT10's kommando- og kontrolinfrastruktur. Desuden ansatte Huaying Haitai, en enhed, der er opført på listen for at have ydet støtte til og lettet »Operation Cloud Hopper«, Gao Qiang. Han har forbindelser til Zhang Shilong, der også er opført på listen i forbindelse med »Operation Cloud Hopper«. Gao Qiang har således tilknytning til både Huaying Haitai og Zhang Shilong.	30.7.2020
2.	ZHANG Shilong	Fødselsdato: 10. september 1981 Fødested: Kina Adresse: Hehong, Yuyang Road nr. 121, Tianjin, Kina Nationalitet: kinesisk Køn: mand	Zhang Shilong er involveret i »Operation Cloud Hopper«, en række cyberangreb med betydelige konsekvenser og med oprindelse uden for Unionen, som udgør en ekstern trussel mod Unionen eller dens medlemsstater, og i cyberangreb, som har betydelige konsekvenser for tredjelande. »Operation Cloud Hopper« har været rettet mod multinationale virksomheders informationssystemer på seks kontinenter, herunder virksomheder i Unionen, og har opnået uautoriseret adgang til kommercielt følsomme data, hvilket har medført et betydeligt økonomisk tab. Den aktør, der offentligt er kendt som »APT10« (»Advanced Persistent Threat 10«) (alias »Red Apollo«, »CVNX«, »Stone Panda«, »MenuPass« og »Potassium«), gennemførte »Operation Cloud Hopper«. Zhang Shilong kan sættes i forbindelse med APT10, herunder via den malware, han har udviklet og testet i forbindelse med de cyberangreb, der er blevet udført af APT10. Desuden ansatte Huaying Haitai, en enhed, der er opført på listen for at have ydet støtte til og lettet »Operation Cloud Hopper«, Zhang Shilong Han har forbindelser til Gao Qiang, der også er opført på listen i forbindelse med »Operation Cloud Hopper«. Zhang Shilong har således tilknytning til både Huaying Haitai og Gao Qiang.	30.7.2020«.