II

(Icke-lagstiftningsakter)

FÖRORDNINGAR

RÅDETS GENOMFÖRANDEFÖRORDNING (EU) 2020/1744

av den 20 november 2020

om genomförande av förordning (EU) 2019/796om restriktiva åtgärder mot cyberattackersom hotar unionen eller dess medlemsstater

EUROPEISKA UNIONENS RÅD HAR ANTAGIT DENNA FÖRORDNING

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av rådets förordning (EU) 2019/796 av den 17 maj 2019 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater ([1]), särskilt artikel 13.1,

med beaktande av förslaget från unionens höga representant för utrikes frågor och säkerhetspolitik, och

av följande skäl:

(1) Den 17 maj 2019 antog rådet förordning (EU) 2019/796.

(2) Den 30 juli 2020 antog rådet genomförandeförordning (EU) 2020/1125 ([2]) varigenom sex fysiska personer och tre enheter eller organ lades till på förteckningen över fysiska och juridiska personer, enheter och organ som är föremål för restriktiva åtgärder i bilaga I till beslut (EU) 2019/796.

(3) Uppdaterad information har mottagits avseende två poster i förteckningen över fysiska personer.

(4) Förordning (EU) 2019/796 bör därför ändras i enlighet med detta.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

Artikel 1

Bilaga I till förordning (EU) 2019/796 ska ändras i enlighet med bilagan till den här förordningen.

Artikel 2

Denna förordning träder i kraft dagen efter det att den har offentliggjorts i *Europeiska unionens officiella tidning*.

Denna förordning är till alla delar bindande och direkt tillämplig i alla medlemsstater.

Utfärdad i Bryssel den 20 november 2020.

På rådets vägnar
M. Roth
Ordförande

([1]) EUT L 129I, 17.5.2019, s. 1.
([2]) Rådets genomförandeförordning (EU) 2020/1125 av den 30 juli 2020 om genomförande av förordning (EU) 2019/796 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater (EUT L 246, 30.7.2020, s. 4).

BILAGA

I bilaga I till förordning (EU) 2019/796 under underrubriken ”A. Fysiska personer” ska posterna 1 och 2 ersättas med följande poster:

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
”1.	GAO Qiang	Födelsedatum: 4 oktober 1983 Födelseort: Shandong Province, China (provinsen Shandong, Kina) Adress: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Nationalitet: kinesisk Kön: man	Gao Qiang är involverad i *Operation Cloud Hopper*, en rad cyberattacker med betydande effekt och med ursprung utanför unionen, som utgör ett externt hot mot unionen eller dess medlemsstater, och cyberattacker som har en betydande effekt på tredjeländer. *Operation Cloud Hopper* har varit inriktad på multinationella företags informationssystem på sex kontinenter, inbegripet företag belägna i unionen, och har skaffat sig otillåten tillgång till kommersiellt känsliga uppgifter, vilket har medfört betydande ekonomiska förluster. Den aktör som är allmänt känd som *APT10* (*Advanced Persistent Threat 10*) (även kallad *Red Apollo*, *CVNX*, *Stone Panda*, *MenuPass* och *Potassium*) genomförde *Operation Cloud Hopper*. Gao Qiang kan kopplas till APT10, bl.a. genom sin koppling till APT10:s ledningsinfrastruktur. Dessutom har Gao Qiang varit anställd av Huaying Haitai, en enhet som förts upp på förteckningen för att ha gett stöd till och underlättat *Operation Cloud Hopper*. Han har kopplingar till Zhang Shilong, som också har förts upp på förteckningen i samband med *Operation Cloud Hopper*. Gao Qiang har därför kopplingar till både Huaying Haitai och Zhang Shilong.	30.7.2020
2.	ZHANG Shilong	Födelsedatum: 10 september 1981 Födelseort: China (Kina) Adress: Hedong, Yuyang Road No 121, Tianjin, China Nationalitet: kinesisk Kön: man	Zhang Shilong är involverad i *Operation Cloud Hopper*, en rad cyberattacker med betydande effekt och med ursprung utanför unionen, som utgör ett externt hot mot unionen eller dess medlemsstater, och cyberattacker som har en betydande effekt på tredjeländer. *Operation Cloud Hopper* har varit inriktad på multinationella företags informationssystem på sex kontinenter, inbegripet företag belägna i unionen, och har skaffat sig otillåten tillgång till kommersiellt känsliga uppgifter, vilket har medfört betydande ekonomiska förluster. Den aktör som är allmänt känd som *APT10* (*Advanced Persistent Threat 10*) (även kallad *Red Apollo*, *CVNX*, *Stone Panda*, *MenuPass* och *Potassium*) genomförde *Operation Cloud Hopper*. Zhang Shilong kan kopplas till APT10, bl.a. genom sabotageprogram som han utvecklade och testade i samband med de cyberattacker som genomfördes av APT10. Dessutom har Zhang Shilong varit anställd av Huaying Haitai, en enhet som förts upp på förteckningen för att ha gett stöd till och underlättat *Operation Cloud Hopper*. Han har kopplingar till Gao Qiang, som också har förts upp på förteckningen i samband med *Operation Cloud Hopper*. Zhang Shilong har därför kopplingar till både Huaying Haitai och Gao Qiang.	30.7.2020”