2026/1078

12.5.2026

RÅDETS GENOMFÖRANDEFÖRORDNING (EU) 2026/1078

av den 11 maj 2026

om genomförande av förordning (EU) 2019/796 om restriktiva åtgärder mot cyberattacker som 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,

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) Rådet har sett över förteckningen över fysiska och juridiska personer, enheter och organ i bilaga I till förordning (EU) 2019/796. På grundval av denna översyn bör skälen till att fyra personer och en enhet förts upp på förteckningen över fysiska och juridiska personer, enheter och organ som är föremål för restriktiva åtgärder uppdateras.

(3) Bilaga I till 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 11 maj 2026.

På rådets vägnar

K. KALLAS

Ordförande

[1] EUT L 129 I, 17.5.2019, s. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj.

BILAGA

Bilaga I till förordning (EU) 2019/796 ska ändras på följande sätt:

1. Under rubriken ”A. Fysiska personer” ska posterna 1, 2, 13 och 14 ersättas med följande motsvarande poster:

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
”1.	GAO Qiang	Födelsedatum: 4 oktober 1983 Födelseort: Provinsen Shandong, Kina Adress: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Nationalitet: kinesisk Kön: man	Gao Qiang är kopplad till *APT10* (*Advanced Persistent Threat 10*) (alias *Red Apollo*, *CVNX*, *Stone Panda*, *MenuPass* och *Potassium*) och har varit 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. Gao Qiang har samröre med APT10:s ledningsinfrastruktur. Dessutom har Gao Qiang varit anställd av Huaying Haitai, ett företag som använts av APT10 och som förts upp på förteckningen för att ha gett stöd till och underlättat *Operation Cloud Hopper*. Han har också samröre med Zhang Shilong, som är kopplad till APT10 och som också har varit anställd av Huaying Haitai.	30.7.2020

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
2.	ZHANG Shilong	Födelsedatum: 10 september 1981 Födelseort: Kina Adress: Hedong, Yuyang Road No 121, Tianjin, China Nationalitet: kinesisk Kön: man	Zhang Shilong är kopplad till *APT10* (*Advanced Persistent Threat 10*) (alias *Red Apollo*, *CVNX*, *Stone Panda*, *MenuPass* och *Potassium*) och har varit 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. Zhang Shilong har samröre med 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, ett företag som använts av APT10 och som förts upp på förteckningen för att ha gett stöd till och underlättat *Operation Cloud Hopper*. Han har samröre med Gao Qiang, som är kopplad till APT10 och som också har varit anställd av Huaying Haitai.	30.7.2020

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
13.	Mikhail Mikhailovich TSAREV	Михаил Михайлович ЦАРЕВ Födelsedatum: 20.4.1989 Födelseort: Serpuchov, Ryska federationen Nationalitet: rysk Adress: Serpuchov Kön: man	Mikhail Mikhailovich TSAREV var inblandad i cyberattacker med en betydande effekt som utgör ett externt hot mot EU:s medlemsstater. Mikhail Mikhailovich TSAREV, som också är känd under internetmonikerna 'Mango', 'Alexander Grachev', 'Super Misha', 'Ivanov Mixail', 'Misha Krutysha' och 'Nikita Andrejevitj Tsarev' är en viktig aktör i användningen av sabotageprogrammen 'Conti' och Trickbot och är inblandad i den Rysslandsbaserade hotgruppen 'Wizard Spider'. Wizard Spider fortsätter att utveckla och intensifiera sin verksamhet. Sabotageprogrammen Conti och Trickbot skapades och utvecklades av Wizard Spider. Wizard Spider har genomfört kampanjer med utpressningsprogram inom en rad olika sektorer, däribland grundläggande tjänster som hälso- och sjukvård och bankverksamhet. Gruppen har infekterat datorer i hela världen och dess skadliga programvaror har utvecklats till ett mycket modulärt sabotageprogram. Kampanjer som genomförs av Wizard Spider med hjälp av skadliga programvaror som Conti, 'Ruyk', TrickBot och Black Basta orsakar betydande ekonomiska skador i Europeiska unionen. Mikhail Mikhailovich TSAREV är därför inblandad i cyberattacker med en betydande effekt som utgör ett externt hot mot unionen eller dess medlemsstater.	24.6.2024

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
14.	Maksim Sergeevich GALOCHKIN	Максим Сергеевич ГАЛОЧКИН Födelsedatum: 19.5.1982 Födelseort: Abakan, Ryska federationen Nationalitet: rysk Kön: man	Maksim Galochkin var inblandad i cyberattacker med en betydande effekt som utgör ett externt hot mot EU:s medlemsstater. Maksim Galochkin är också känd under webbmonikerna 'Benalen', 'Bentley', 'Volhvb', 'volhvb', 'manuel', 'Max17' och 'Crypt'. Galochkin är en viktig aktör i användningen av sabotageprogrammen 'Conti' och 'Trickbot' och är inblandad i den Rysslandsbaserade hotgruppen 'Wizard Spider'. Han har lett en grupp testare med ansvar för utveckling, övervakning och genomförande av tester för sabotageprogrammet TrickBot, som skapats och satts in av Wizard Spider. Wizard Spider fortsätter att utveckla och intensifiera sin verksamhet. Wizard Spider har genomfört kampanjer med utpressningsprogram inom en rad olika sektorer, däribland grundläggande tjänster som hälso- och sjukvård och bankverksamhet. Gruppen har infekterat datorer i hela världen och dess skadliga programvaror har utvecklats till ett mycket modulärt sabotageprogram. Kampanjer som genomförs av Wizard Spider med hjälp av skadliga programvaror som Conti, 'Ruyk', TrickBot och Black Basta orsakar betydande ekonomiska skador i Europeiska unionen. Maksim Galochkin är därför inblandad i cyberattacker med en betydande effekt som utgör ett externt hot mot unionen eller dess medlemsstater.	24.6.2024”.

2. Under rubriken ”B. Juridiska personer, enheter och organ” ska post 1 ersättas med följande:

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
”1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	alias Haitai Technology Development Co. Ltd Plats: Tianjin, Kina	Huaying Haitai tillhandahöll finansiellt, tekniskt eller materiellt stöd till och underlättade *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*) (alias *Red Apollo*, *CVNX*, *Stone Panda*, *MenuPass* och *Potassium*) genomförde *Operation Cloud Hopper*. Huaying Haitai kan kopplas till APT10. Dessutom har Gao Qiang och Zhang Shilong, som båda har förts upp på förteckningen i samband med *Operation Cloud Hopper*, varit anställda av Huaying Haitai. Huaying Haitai har därför även samröre med Gao Qiang och Zhang Shilong.	30.7.2020”.