Rådet for
Den Europæiske Union

Bruxelles, den 5. maj 2026
(OR. en)

7281/26

LIMITE

CORLX 271
CFSP/PESC 388
CYBER 113
JAI 338
FIN 406

LOVGIVNINGSMÆSSIGE RETSAKTER OG ANDRE INSTRUMENTER

Vedr.:	RÅDETS AFGØRELSE om ændring af afgørelse (FUSP) 2019/797 om restriktive foranstaltninger til bekæmpelse af cyberangreb, der truer Unionen eller dens medlemsstater

RÅDETS AFGØRELSE (FUSP) 2026/…

af …

om ændring af afgørelse (FUSP) 2019/797 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 Union, særlig artikel 29,

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

ud fra følgende betragtninger:

(1) Rådet vedtog den 17. maj 2019 afgørelse (FUSP) 2019/797[1].

(2) Afgørelse (FUSP) 2019/797 finder anvendelse indtil den 18. maj 2028.

(3) På grundlag af en fornyet gennemgang af bilaget til afgørelse (FUSP) 2019/797 bør anvendelsen af foranstaltningerne i nævnte afgørelses artikel 4 og 5 på de fysiske og juridiske personer, enheder og organer, der er opført på listen i nævnte bilag, forlænges indtil den 18. maj 2027. Desuden bør begrundelserne for opførelsen af fire personer og én enhed på listen over fysiske og juridiske personer, enheder og organer, der er omfattet af restriktive foranstaltninger, ajourføres.

(4) Afgørelse (FUSP) 2019/797 bør derfor ændres i overensstemmelse hermed —

VEDTAGET DENNE AFGØRELSE:

[1] Rådets afgørelse (FUSP) 2019/797 af 17. maj 2019 om restriktive foranstaltninger til bekæmpelse af cyberangreb, der truer Unionen eller dens medlemsstater (EUT L 129I af 17.5.2019, s. 13, ELI: http://data.europa.eu/eli/dec/2019/797/oj).

Artikel 1

I afgørelse (FUSP) 2019/797 foretages følgende ændringer:

1) Artikel 10 affattes således:

"Artikel 10

Denne afgørelse finder anvendelse indtil den 18. maj 2028 og overvåges løbende. Foranstaltningerne fastsat i artikel 4 og 5 finder anvendelse på de fysiske og juridiske personer, enheder og organer, der er opført på listen i bilaget, indtil den 18. maj 2027."

2) Bilaget ændres som angivet i bilaget til nærværende afgørelse.

Artikel 2

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

Udfærdiget i …, den …

På Rådets vegne
Formand

BILAG

I bilaget til afgørelse (FUSP) 2019/797 foretages følgende ændringer:

1) Under overskriften "A. Fysiske personer" affattes punkt 1, 2, 13 og 14 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 knyttet til paraplyorganisationen "APT10" ("Advanced Persistent Threat 10") (alias "Red Apollo", "CVNX", "Stone Panda", "MenuPass" og "Potassium") og har været 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. GAO Qiang er tilknyttet APT10's kommando- og kontrolinfrastruktur. Desuden har Gao Qiang været ansat i Huaying Haitai, et selskab, som anvendes af APT10, og som er opført på listen for at have ydet støtte til og lettet "Operation Cloud Hopper". Han har også forbindelser til Zhang Shilong, som er knyttet til APT10, og som også har været ansat i Huaying Haitai.	30.7.2020

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
2.	ZHANG Shilong	Fødselsdato: 10. september 1981 Fødested: Kina Adresse: Hedong, Yuyang Road No 121, Tianjin, China Nationalitet: kinesisk Køn: mand	Zhang Shilong er knyttet til paraplyorganisationen "APT10" ("Advanced Persistent Threat 10") (alias "Red Apollo", "CVNX", "Stone Panda", "MenuPass" og "Potassium") og har været 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. Zhang Shilong er tilknyttet APT10, herunder via den malware, han har udviklet og testet i forbindelse med de cyberangreb, der er blevet udført af APT10. Desuden har Zhang Shilong været ansat i Huaying Haitai, et selskab, som anvendes af APT10, og som er opført på listen for at have ydet støtte til og lettet "Operation Cloud Hopper". Han har forbindelser til Gao Qiang, som er knyttet til APT10, og som også har været ansat i Huaying Haitai.	30.7.2020

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
13.	Mikhail Mikhailovich TSAREV	Михаил Михайлович ЦАРЕВ Fødselsdato: 20.4.1989 Fødested: Serpukhov, Den Russiske Føderation Nationalitet: russisk Adresse: Serpukhov Køn: mand	Mikhail Mikhailovich Tsarev deltog i cyberangreb med betydelige konsekvenser, som udgør en ekstern trussel mod EU-medlemsstater. Mikhail Mikhailovich Tsarev, som også er kendt under internettilnavnene "Mango", "Alexander Grachev", "Super Misha", "Ivanov Mixail", "Misha Krutysha" og "Nikita Andreevich Tsarev", er en central aktør i deployeringen af malwareprogrammerne "Conti" og "Trickbot" og er involveret i den Ruslandbaserede trusselsgruppe "Wizard Spider". Wizard Spider fortsætter med at udvikle og intensivere sine operationer. De af Conyi og Trickbot anvendte malware programmer var oprettet og udviklet af Wizard Spider. Wizard Spider har gennemført ransomwarekampagner i en række sektorer, herunder vigtige tjenester såsom sundhed og bankvæsen. Gruppen har inficeret computere verden over, og dens malware er blevet udviklet til en meget modulær malwarepakke. De kampagner, der gennemføres af Wizard Spider, som bruger malware såsom Conti, "Ryuk", TrickBot eller Black Basta, er skyld i omfattende økonomisk skade i Den Europæiske Union. Mikhail Mikhailovich Tsarev er således involveret i cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater.	24.6.2024

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
14.	Maksim Sergeevich GALOCHKIN	Максим Сергеевич ГАЛОЧКИН Fødselsdato: 19.5.1982 Fødested: Abakan, Den Russiske Føderation Nationalitet: russisk Køn: mand	Maksim Galochkin deltog i cyberangreb med betydelige konsekvenser, som udgør en ekstern trussel mod EU-medlemsstater. Maksim Galochkin er også kendt under internettilnavnene "Benalen", "Bentley", "Volhvb", "volhvb", "manuel", "Max17" og "Crypt". Galochkin er en central aktør i deployeringen af malwareprogrammerne "Conti" og "Trickbot" og er involveret i den Ruslandbaserede trusselsgruppe "Wizard Spider". Han har stået i spidsen for en gruppe testere med ansvar for udviklingen af, tilsyn med og gennemførelse af test af TrickBot-spywareprogrammet, der er udviklet og anvendt af Wizard Spider. Wizard Spider fortsætter med at udvikle og intensivere sine operationer. Wizard Spider har gennemført ransomwarekampagner i en række sektorer, herunder vigtige tjenester såsom sundhed og bankvæsen. Gruppen har inficeret computere verden over, og dens malware er blevet udviklet til en meget modulær malwarepakke. De kampagner, der gennemføres af Wizard Spider, som bruger malware såsom Conti, "Ryuk", TrickBot eller Black Basta, er skyld i omfattende økonomisk skade i Den Europæiske Union. Maksim Galochkin er således involveret i cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater.	24.6.2024".

2) Under overskriften "B. Juridiske personer, enheder og organer" affattes punkt 1 således:

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
"1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	Alias: Haitai Technology Development Co. Ltd Sted: Tianjin, Kina	Huaying Haitai har ydet finansiel, teknisk eller materiel støtte til og lettet "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". Huaying Haitai kan sættes i forbindelse med APT10. Desuden har Gao Qiang og Zhang Shilong, som begge er opført på listen i forbindelse med "Operation Cloud Hopper", været ansat i Huaying Haitai. Huaying Haitai har således også tilknytning til Gao Qiang og Zhang Shilong.	30.7.2020".