Rådet for
Den Europæiske Union

Bruxelles, den 7. juli 2026
(OR. en)

8643/26

LIMITE

CORLX 388
CFSP/PESC 584
CYBER 192
JAI 505
FIN 592

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

(2) Som led i den fortsatte skræddersyede og koordinerede EU-indsats over for persistente cybertrusselsaktører bør otte fysiske personer og fire enheder tilføjes til listen over fysiske og juridiske personer, enheder og organer, der er omfattet af restriktive foranstaltninger, i bilaget til afgørelse (FUSP) 2019/797. Disse personer og enheder er ansvarlige for, støtter eller er involveret i cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater.

(3) 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

Bilaget til afgørelse (FUSP) 2019/797 ændres som angivet i bilaget til nærværende afgørelse.

Artikel 2

Denne afgørelse træder i kraft på dagen for 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) Følgende punkter tilføjes under overskriften "A. Fysiske personer":

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
"20.	Vitaly Nikolayevich KOVALEV	Виталий Николаевич КОВАЛЕВ Aliasser: "Bentley", "Bergen", "Alex Konor", "Benny", "Ben", "Stern" Fødselsdato: 23.6.1988 Adresse: Serebristy Bulvar 34 (Serebristyy Bul'var); krp 1; flt 528; 197341; St Petersburg, Russian Federation Nationalitet: russisk Køn: mand Tilknyttede enheder: TrickBot, Wizard Spider, Conti	Vitaly Kovalev er en fremtrædende figur i malwareprogrammerne "Trickbot" og "Conti". Han er også kendt under internettilnavnene "Bentley", "Bergen", "Alex Konor", "Benny", "Ben" og "Stern". Conti og Trickbot blev oprindeligt oprettet og udviklet af Wizard Spider. Wizard Spider har gennemført ransomwarekampagner i en række sektorer, herunder vigtige tjenester såsom sundhed og bankvæsen, og har inficeret computere verden over, og deres malware er blevet udviklet til en meget modulær malwarepakke. De kampagner, der gennemføres af Wizard Spider, som bruger malware såsom Conti og TrickBot, er skyld i omfattende økonomisk skade i Den Europæiske Union. Vitaly Kovalev er derfor ansvarlig for og er involveret i cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater.	+

+ EUT: Indsæt venligst datoen for offentliggørelsen af denne afgørelse.

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
21.	Alexander Alexandrovich VOLOSOVIK	Александр Александрович ВОЛОСОВИК Fødselsdato: 30.1.1983 Fødested: USSR Nationalitet: russisk Pasnummer: 762988138 Køn: mand Tilknyttede enheder: Yalishanda, LARVA-34, podzemniyl, Ohyeahhellno, Stas_vl, downlow	Alexander Volosovik er ejer af Media Land LLC. Siden 2016 har Bullet Proof Hosting Service Media Land LLC faciliteret en bred vifte af malwareangreb mod både Unionen og globalt ved at tilbyde hostingtjenester, der skjuler brugeridentiteter og modsætter sig retshåndhævende myndigheders fjernelse heraf. Media Land LLC muliggjorde storstilede ransomwareoperationer, kommando- og kontroltjenester og phishingoperationer, der er rettet mod kritisk infrastruktur og vigtige tjenester blandt medlemsstaterne, hvilket førte til betydelige finansielle tab. De operationer, der faciliteres af Media Land LLC, omfatter bl.a. LockBit, EvilCorp og BlackBasta. Media Land LLC er derfor involveret i cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod Unionen eller dens medlemsstater. Som ejer af Media Land LLC er Alexander Volosovik ansvarlig for og involveret i disse cyberangreb. Han har også tilknytning til Media Land LLC.	+

+ EUT: Indsæt venligst datoen for offentliggørelsen af denne afgørelse.

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
22.	Denis Olegovich DEGTYARENKO	Денис Олегович ДЕГТЯРЕНКО Alias: "Dena" Fødselsdato: 9.10.1989 Fødested: USSR Nationalitet: russisk Køn: mand Adresse: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation	Denis Degtyarenko alias Dena er en russisk hacker for CARR (Cyber Army of Russia Reborn). CARR har været ansvarlig for cyberangreb mod tjenester, der er nødvendige for opretholdelsen af væsentlige økonomiske aktiviteter og kritiske statslige funktioner i medlemsstaterne, samt mod infrastruktur i Ukraine og andre tredjelande. CARR har tilknytning til hovedcentret for særlige teknologier (Main Centre for Special Technologies (GTsST)) i hoveddirektoratet for Den Russiske Føderations væbnede styrkers generalstab (Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU)). GTsST udfører fortsat aktivt cyberangreb mod Unionen eller dens medlemsstater. CARR's mål omfatter statslige agenturer, finansielle institutioner, medieforetagender og kritisk infrastruktur i medlemsstaterne og USA. CARR har udført distributed denial of service-angreb (DDoS-angreb) i Ukraine og mod regeringer og virksomheder i lande, der har støttet Ukraine. Derfor er Denis Degtyarenko, som er en primær hacker for CARR, involveret i cyberangreb med betydelige konsekvenser, herunder forsøg på cyberangreb med potentielt betydelige konsekvenser, som udgør en ekstern trussel mod medlemsstaterne samt mod tredjelande. Som medlem af CARR har han også tilknytning til GTsST.	+

+ EUT: Indsæt venligst datoen for offentliggørelsen af denne afgørelse.

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
23.	Yuliya Vladimirovna PANKRATOVA	Юлия Владимировна ПАНКРАТОВА Alias: "YUliYA" Fødselsdato: 6.4.1984 Fødested: USSR Nationalitet: russisk Køn: kvinde Adresse: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation	Yuliya Pankratova er en russisk hacker, der har arbejdet for CARR (Cyber Army of Russia Reborn) og har grundlagt, og arbejder fortsat for, Z-Pentest. CARR har været ansvarlig for cyberangreb mod tjenester, der er nødvendige for opretholdelsen af væsentlige økonomiske aktiviteter og kritiske statslige funktioner i medlemsstaterne, samt mod infrastruktur i Ukraine og andre tredjelande. CARR har tilknytning til hovedcentret for særlige teknologier (Main Centre for Special Technologies (GTsST)) i hoveddirektoratet for Den Russiske Føderations væbnede styrkers generalstab (Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU)). GTsST udfører fortsat aktivt cyberangreb mod Unionen eller dens medlemsstater. CARR's mål omfatter statslige agenturer, finansielle institutioner, medieforetagender og kritisk infrastruktur i medlemsstaterne og USA. CARR har udført distributed denial of service-angreb (DDoS-angreb) i Ukraine og mod regeringer og virksomheder i lande, der har støttet Ukraine.	+

+ EUT: Indsæt venligst datoen for offentliggørelsen af denne afgørelse.

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
			Z-Pentest er ansvarlig for cyberangreb med betydelige konsekvenser for bl.a. tjenester, der er nødvendige for opretholdelsen af væsentlige aktiviteter i medlemsstaterne. Derfor er Yuliya Pankratova, som er en primær hacker for CARR og for Z-Pentest, involveret i cyberangreb med betydelige konsekvenser, herunder forsøg på cyberangreb med potentielt betydelige konsekvenser, som udgør en ekstern trussel mod medlemsstaterne samt mod tredjelande. Hun har også tilknytning til Z-Pentest.	

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
24.	Maksim Evgenevich VORONIN	Максим Евгеньевич ВОРОНИН Alias: "Daugn0" Nationalitet: angiveligt russisk Køn: mand	Maksim Voronin alias Daugn0 er involveret i udvikling, distribution og salg af malwaren, der stjæler oplysninger: LummaC2 (alias Lumma infostealer, Lumma Stealer). LummaC2 er en Malware-as-a-Service-platform, der anvendes til at stjæle følsomme databrowseroplysninger, kryptotegnebøger eller systemoplysninger, til at udbrede yderligere malware på inficerede enheder, til tyveri af kryptovaluta og til spionagekampagner. Cyberangreb, der involverer malwaren LummaC2, anvendes også af økonomisk motiverede cybertrusselsaktører som Storm-113, Storm-1607, Storm-1674, Octo Tempest m.fl. Malwaren LummaC2 er blevet anvendt til cyberangreb mod kritiske statslige funktioner og tjenester, der er nødvendige for opretholdelsen af medlemsstaternes væsentlige sociale og økonomiske aktiviteter. I 2024 og 2025 var LummaC2 et af de mest anvendte værktøjer til at stjæle oplysninger verden over. Derfor er Maksim Voronin som udvikler, distributør og sælger af LummaC2 involveret i og fremmer cyberangreb med betydelige konsekvenser, som udgør en ekstern trussel mod medlemsstaterne.	+

+ EUT: Indsæt venligst datoen for offentliggørelsen af denne afgørelse.

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
25.	Maksim Aleksandrovich GORDIENKO alias Maxim Alexandrovich GORDIENKO	Максим Александрович ГОРДИЕНКО Alias: "Lummaseller" Nationalitet: angiveligt russisk Køn: mand	Maksim Gordienko alias Lummaseller er involveret i udvikling og distribution af malwaren, der stjæler oplysninger: LummaC2 (alias Lumma infostealer, Lumma Stealer). LummaC2 er en Malware-as-a-Service-platform, der anvendes til at stjæle følsomme databrowseroplysninger, kryptotegnebøger eller systemoplysninger, til at udbrede yderligere malware på inficerede enheder, til tyveri af kryptovaluta og til spionagekampagner. Cyberangreb, der involverer malwaren LummaC2, anvendes også af økonomisk motiverede cybertrusselsaktører som Storm-113, Storm-1607, Storm-1674, Octo Tempest m.fl. Malwaren LummaC2 er blevet anvendt til cyberangreb mod kritiske statslige funktioner og tjenester, der er nødvendige for opretholdelsen af medlemsstaternes væsentlige sociale og økonomiske aktiviteter. I 2024 og 2025 var LummaC2 et af de mest anvendte værktøjer til at stjæle oplysninger verden over. Derfor er Maksim Gordienko som udvikler, distributør og sælger af LummaC2 involveret i og fremmer cyberangreb med betydelige konsekvenser, som udgør en ekstern trussel mod medlemsstaterne.	+

+ EUT: Indsæt venligst datoen for offentliggørelsen af denne afgørelse.

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
26.	Evgeniy Viktorovich BASHEV	Евгений Викторович БАШЕВ Fødselsdato: 25.1.1980 Fødested: USSR Nationalitet: russisk Køn: mand Tilknyttede personer: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin Tilknyttede enheder: GRU-enhed 29155, "Impuls" LLC	Evgeniy Bashev er medlem af den russiske militære efterretningstjeneste GRU, enhed 29155. I enheden støtter og fremmer han cyberangreb med betydelige konsekvenser for medlemsstaterne, bl.a. ved at kontrollere serveren "Aegon", der anvendes til hackingoperationer. Han yder navnlig teknisk og materiel støtte til cyberangrebene i GRU-enhed 29155 gennem sin virksomhed "Impuls" LLC, som lettede operationel dækning, infrastruktur og betalinger og forvaltede tekniske aktiver, herunder servere, der anvendes til cyberangrebene. Han koordinerede også samarbejdet mellem GRU-strukturer og eksterne hackernetværk. De cyberangreb, som han faciliterede, var rettet mod systemer og tjenester med kritiske statslige funktioner, der er nødvendige for opretholdelsen af væsentlige sociale eller økonomiske aktiviteter i medlemsstaterne, navnlig i transportsektoren. Via WhisperGate-kampagnen havde GRU-enhed 29155 også kritisk infrastruktur i Ukraine som mål.	+

+ EUT: Indsæt venligst datoen for offentliggørelsen af denne afgørelse.

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
			Evgeniy Bashev yder derfor teknisk og materiel støtte til eller er på anden måde involveret i cyberangreb med betydelige konsekvenser, herunder forsøg på cyberangreb med potentielt betydelige konsekvenser, der udgør en ekstern trussel mod medlemsstaterne, samt cyberangreb med betydelige konsekvenser for et tredjeland. Som ejer og generaldirektør er han tilknyttet virksomheden "Impuls" LLC. Som medlem af GRU-enhed 29155 har han også tilknytning til denne enhed.	

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
27.	Roman Alexandrovich PUNTUS	Роман Александрович ПУНТУС Fødested: Den Russiske Føderation Nationalitet: russisk Køn: mand Tilknyttede personer: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin, Evgeniy Viktorovich Bashev Tilknyttede enheder: GRU-enhed 29155	Roman Puntus er medlem af den russiske militære efterretningstjeneste GRU, enhed 29155. I enheden har han en ledende rolle i tilrettelæggelsen og koordineringen af cyberangreb med betydelige konsekvenser for medlemsstaterne. Han støtter også udviklingen af enhedens interne cyberkapacitet, herunder rekruttering af og tilsyn med personale såsom hackere og programmører. Ved at oprette skuffeselskabet "Aegeon-Impulse" lettede han de logistiske og finansielle aspekter af cyberoperationer. Under hans koordinering foretog enheden cyberangreb mod systemer og tjenester med kritiske statslige funktioner, der er nødvendige for opretholdelsen af væsentlige sociale eller økonomiske aktiviteter i medlemsstaterne, navnlig i transportsektoren. Via WhisperGate-kampagnen havde GRU-enhed 29155 også kritisk infrastruktur i Ukraine som mål.	[+]".

[+] EUT: Indsæt venligst datoen for offentliggørelsen af denne afgørelse.

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
			Roman Puntus er derfor ansvarlig for eller er på anden måde involveret i cyberangreb med betydelige konsekvenser, herunder forsøg på cyberangreb med potentielt betydelige konsekvenser, der udgør en ekstern trussel mod medlemsstaterne, samt cyberangreb med betydelige konsekvenser for et tredjeland. Som medlem af GRU-enhed 29155 har han også tilknytning til denne enhed.	

2) Følgende punkter tilføjes under overskriften "B. Juridiske personer, enheder og organer":

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
"8.	Media Land LLC	Adresse: Tsvetnochnaya st., 16 Litera P, Room 27, Moskovskaya Zastava Municipal District St Petersburg, 196006, Russian Federation Type enhed: anpartsselskab Registreringssted: Skt. Petersborg Registreringsdato: 19.10.2015 Registreringsnummer: 1152536009900 Hovedforretningssted: Skt. Petersborg, Den Russiske Føderation Tilknyttet enhed: ML.Cloud	Siden 2016 har Bullet Proof Hosting Service Media Land LLC faciliteret en bred vifte af malwareangreb mod medlemsstaterne og globalt ved at tilbyde hostingtjenester, der skjuler brugeridentiteter og modsætter sig retshåndhævende myndigheders fjernelse heraf, hvilket har ført til betydelige finansielle tab. Media Land LLC muliggjorde storstilede ransomwareoperationer, kommando- og kontroltjenester og phishingoperationer, der er rettet mod kritisk infrastruktur og vigtige tjenester blandt medlemsstaterne. De operationer, der fremmes af Media Land LLC, omfatter bl.a. LockBit, EvilCorp og BlackBasta. Media Land LLC er derfor involveret i cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod medlemsstaterne.	[+]

[+] EUT: Indsæt venligst datoen for offentliggørelsen af denne afgørelse.

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
9.	ML.Cloud	Adresse: Brivibas iela 52, Riga, LV-1011, Latvija; Russian Federation, Kazan, Peterburgskaya st. 52 Registreringssted: Riga Tilknyttet person: Alexander Volosovik Andre tilknyttede enheder: Media Land LLC	ML.Cloud er søsterselskab til Media Land LLC og leverer den tekniske infrastruktur til Media Land LLC. Siden 2016 har Bullet Proof Hosting Service Media Land LLC faciliteret en bred vifte af malwareangreb mod medlemsstaterne og globalt ved at tilbyde hostingtjenester, der skjuler brugeridentiteter og modsætter sig retshåndhævende myndigheders fjernelse heraf, hvilket har ført til betydelige finansielle tab. Media Land LLC muliggjorde storstilede ransomwareoperationer, kommando- og kontroltjenester og phishingoperationer, der er rettet mod kritisk infrastruktur og vigtige tjenester blandt medlemsstaterne. De operationer, der fremmes af Media Land LLC, omfatter bl.a. LockBit, EvilCorp og BlackBasta. Media Land LLC er derfor involveret i cyberangreb, der udgør en ekstern trussel med betydelige konsekvenser for EU-medlemsstaterne. ML.Cloud yder derfor teknisk støtte til cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod medlemsstaterne.	[+]

[+] EUT: Indsæt venligst datoen for offentliggørelsen af denne afgørelse.

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
10.	"Impuls" LLC	Общество с ограниченной ответственностью "Импульс" Adresse: 344015, Russian Federation, Rostov Region, Rostov-on-Don, ul. Eremenko, d. 56, k. 6, apt. 88 Type enhed: anpartsselskab Registreringssted: Interdistrict Inspectorate of the Federal Tax Service No. 26 for the Rostov Region, 344019, Rostov-on-Don, ul. Myasnikova, d. 52/32, Den Russiske Føderation Registreringsdato: 27.9.2010	"Impuls" LLC er en russisk virksomhed, der ejes af Evgeniy Viktorovich Bashev, medlem af den russiske militære efterretningstjeneste GRU, enhed 29155. Virksomheden yder teknisk og materiel støtte til cyberangreb og forsøg på cyberangreb, der udføres af GRU-enhed 29155. "Impuls" LLC fungerer navnlig som en operationel formidler, der gør det muligt at udføre hackingrelaterede aktiviteter gennem en virksomhed, der formelt ikke er forbundet med den russiske stat. Den lettede operationel dækning, infrastruktur og betalinger for cyberangreb og var forbundet med tekniske aktiver, herunder servere, der anvendes til støtte for hackingaktiviteter. "Impuls" LLC muliggjorde navnlig samarbejde mellem GRU-strukturer og eksterne hackernet. De cyberoperationer, der lettes af "Impuls" LLC, er rettet mod kritiske statslige funktioner og tjenester, der er nødvendige for opretholdelsen af væsentlige sociale og økonomiske aktiviteter i medlemsstaterne, navnlig i transportsektoren. Via WhisperGate-kampagnen havde GRU-enhed 29155 også kritisk infrastruktur i Ukraine som mål.	+

+ EUT: Indsæt venligst datoen for offentliggørelsen af denne afgørelse.

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
		Registreringsnummer: INN (ИНН): 6168033776; OGRN (ОГРН): 1106194004850 Hovedforretningssted: Den Russiske Føderation Tilknyttede personer: Evgeniy Bashev Tilknyttede enheder: GRU-enhed 29155	"Impuls" LLC yder derfor teknisk og materiel støtte til eller er på anden måde involveret i cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod medlemsstaterne, samt cyberangreb med betydelige konsekvenser for et tredjeland.	

	Navn	Identificerende oplysninger	Begrundelse	Dato for opførelse
11.	Z-Pentest	Aliasser: "Z-Pentest Alliance", "Z-Alliance" Hovedforretningssted: Den Russiske Føderation Tilknyttede personer: Yuliya Pankratova Tilknyttede enheder: Cyber Army of Russia/CARR X.com-konto: ZPentest (konto suspenderet) Telegramkonto: Zpentestalliance	Z-Pentest er en prorussisk hacktivistgruppe bestående af medlemmer af CARR (Cyber Army of Russia Reborn) og NoName057, der på globalt plan har kritisk infrastruktur, navnlig energi- og vandsektoren, som mål. Gruppen angreb navnlig et dansk vandværk i december 2024. Z-Pentest er derfor ansvarlig for cyberangreb med betydelige konsekvenser, der udgør en ekstern trussel mod medlemsstaterne.	[+]".

[+] EUT: Indsæt venligst datoen for offentliggørelsen af denne afgørelse.