Europeiska unionens råd

Bryssel den 7 juli 2026
(OR. en)

8645/26

LIMITE

CORLX 390
CFSP/PESC 586
RELEX 561
CYBER 194
JAI 507
FIN 594

LAGSTIFTNINGSAKTER OCH ANDRA INSTRUMENT

Ärende:	RÅDETS GENOMFÖRANDEFÖRORDNING om genomförande av förordning (EU) 2019/796 om restriktiva åtgärder mot cyberattacker som hotar unionen eller dess medlemsstater

RÅDETS GENOMFÖRANDEFÖRORDNING (EU) 2026/…

av den …

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 13.1,

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

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

av följande skäl:

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

(2) Som en del i de kontinuerliga, skräddarsydda och samordnade unionsinsatserna mot aktörer som utgör ett ihållande cyberhot bör åtta fysiska personer och fyra enheter läggas till i förteckningen över fysiska och juridiska personer, enheter och organ som är föremål för restriktiva åtgärder i bilaga I till förordning (EU) 2019/796. Dessa personer och enheter är ansvariga för eller inblandade i cyberattacker med en betydande effekt som utgör ett externt hot för unionen eller dess medlemsstater.

(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 samma dag som den offentliggörs i *Europeiska unionens officiella tidning*.

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

Utfärdad i … den …

På rådets vägnar
[…]
Ordförande

BILAGA

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

1. Följande poster ska läggas till under rubriken ”A. Fysiska personer”:

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
”20.	Vitaly Nikolayevich KOVALEV	Виталий Николаевич КОВАЛЕВ Alias: ”Bentley”, ”Bergen”, ”Alex Konor”, ”Benny”, ”Ben”, ”Stern” Födelsedatum: 23.6.1988 Adress: Serebristy Bulvar 34 (Serebristyy Bul’var); krp 1; flt 528; 197341; St Petersburg, Russian Federation Nationalitet: rysk Kön: man Associerade enheter: TrickBot, Wizard Spider, Conti	Vitaly Kovalev är en ledande person i samband med sabotageprogrammen ”Trickbot” och ”Conti”. Han är också känd under internetmonikerna ”Bentley”, ”Bergen”, ”Alex Konor”, ”Benny”, ”Ben” och ”Stern”. Conti och Trickbot skapades och utvecklades ursprungligen av Wizard Spider. Wizard Spider har genomfört kampanjer med utpressningsprogram inom en rad olika sektorer, däribland samhällsviktiga tjänster som hälso- och sjukvård och bankverksamhet, och 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 och TrickBot orsakar betydande ekonomiska skador i Europeiska unionen. Vitaly Kovalev är därför ansvarig för och inblandad i cyberattacker med en betydande effekt som utgör ett externt hot för unionen eller dess medlemsstater.	+

+ EUT: vänligen för in datum för offentliggörande av denna förordning.

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
21.	Alexander Alexandrovich VOLOSOVIK	Александр Александрович ВОЛОСОВИК Födelsedatum: 30.1.1983 Födelseort: Sovjetunionen Nationalitet: rysk Passnummer: 762988138 Kön: man Associerade enheter: Yalishanda, LARVA-34, podzemniyl, Ohyeahhellno, Stas_vl, downlow	Alexander Volosovik är ägare till Media Land LLC. Sedan 2016 har Bullet Proof Hosting service Media Land LLC underlättat ett brett spektrum av attacker med sabotageprogram mot både unionen och globalt genom att erbjuda värdtjänster som döljer användaridentiteter och motverkar brottsbekämpande myndigheters avlägsnande. Media Land LLC möjliggjorde storskaliga operationer med utpressningsprogram, ledningstjänster, och nätfiskeoperationer som riktar sig mot kritisk infrastruktur och samhällsviktiga tjänster i medlemsstaterna, vilket ledde till betydande ekonomiska förluster. Till de operationer som Media Land LLC underlättat hör bland annat LockBit, EvilCorp och BlackBasta. Media Land LLC är därför inblandat i cyberattacker med en betydande effekt som utgör ett externt hot för unionen eller dess medlemsstater. I egenskap av ägare till Media Land LLC är Alexander Volosovik ansvarig för och inblandad i dessa cyberattacker. Han har också samröre med Media Land LLC.	+

+ EUT: vänligen för in datum för offentliggörande av denna förordning.

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
22.	Denis Olegovich DEGTYARENKO	Денис Олегович ДЕГТЯРЕНКО Alias: ”Dena” Födelsedatum: 9.10.1989 Födelseort: Sovjetunionen Nationalitet: rysk Kön: man Adress: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation	Denis Degtyarenko alias Dena är en rysk hackare för CARR (Cyber Army of Russia Reborn). CARR har varit ansvarigt för cyberattacker mot tjänster som är nödvändiga för att upprätthålla väsentliga ekonomiska verksamheter och kritiska statliga funktioner i medlemsstaterna, samt mot infrastruktur i Ukraina och andra tredjeländer. CARR har anknytning till Main Centre for Special Technologies (GTsST) (huvudcentrum för specialteknik) vid huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt (GRU). GTsST fortsätter att aktivt utföra cyberattacker mot unionen eller dess medlemsstater. CARR:s mål inbegriper statliga myndigheter, finansinstitut, medieföretag och kritisk infrastruktur i medlemsstaterna och Förenta staterna. CARR har utfört samordnade överbelastningsattacker (DDoS) i Ukraina och mot regeringar och företag i länder som har stött Ukraina. Denis Degtyarenko, en viktig hackare för CARR, är därför inblandad i cyberattacker med en betydande effekt, inbegripet försök till cyberattacker med en potentiellt betydande effekt, som utgör ett externt hot för medlemsstaterna och för tredjeländer. I egenskap av medlem i CARR har han också samröre med GTsST.	+

+ EUT: vänligen för in datum för offentliggörande av denna förordning.

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
23.	Yuliya Vladimirovna PANKRATOVA	Юлия Владимировна ПАНКРАТОВА Alias: ”YUliYA” Födelsedatum: 6.4.1984 Födelseort: Sovjetunionen Nationalitet: rysk Kön: kvinna Adress: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation	Yuliya Pankratova är en rysk hackare som har arbetat för CARR (Cyber Army of Russia Reborn) och som har grundat Z-Pentest, som hon fortfarande arbetar för. CARR har varit ansvarigt för cyberattacker mot tjänster som är nödvändiga för att upprätthålla väsentliga ekonomiska verksamheter och kritiska statliga funktioner i medlemsstaterna, samt mot infrastruktur i Ukraina och andra tredjeländer. CARR har anknytning till Main Centre for Special Technologies (GTsST) (huvudcentrum för specialteknik) vid huvuddirektoratet vid generalstaben inom Ryska federationens försvarsmakt (GRU). GTsST fortsätter att aktivt utföra cyberattacker mot unionen eller dess medlemsstater. CARR:s mål inbegriper statliga myndigheter, finansinstitut, medieföretag och kritisk infrastruktur i medlemsstaterna och Förenta staterna. CARR har utfört samordnade överbelastningsattacker (DDoS) i Ukraina och mot regeringar och företag i länder som har stött Ukraina.	+

+ EUT: vänligen för in datum för offentliggörande av denna förordning.

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
			Z-Pentest är ansvarigt för cyberattacker med en betydande effekt mot bland annat tjänster som är nödvändiga för att upprätthålla väsentliga ekonomiska verksamheter i medlemsstaterna. Yuliya Pankratova, en viktig hackare för CARR och för Z-Pentest, är därför inblandad i cyberattacker med en betydande effekt, inbegripet försök till cyberattacker med en potentiellt betydande effekt, som utgör ett externt hot för medlemsstaterna och för tredjeländer. Hon har också samröre med Z-Pentest.	

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
24.	Maksim Evgenevich VORONIN	Максим Евгеньевич ВОРОНИН Alias: ”Daugn0” Nationalitet: påstått rysk Kön: man	Maksim Voronin alias Daugn0 är inblandad i utveckling, distribution och försäljning av sabotageprogrammet LummaC2 (alias Lumma Infostealer, Lumma Stealer), som används för att stjäla information. LummaC2 är en plattform av typen ”Malware-as-a-Service” (MaaS), som används för att stjäla känsliga uppgifter, åtkomstuppgifter till webbläsare, kryptoplånböcker eller systeminformation, för att installera ytterligare sabotageprogram på infekterade enheter, för stöld av kryptovalutor och för spionagekampanjer. Cyberattacker med sabotageprogrammet LummaC2 används också av ekonomiskt motiverade aktörer som utgör ett cyberhot som Storm-113, Storm-1607, Storm-1674, Octo Tempest med flera. Sabotageprogrammet LummaC2 har använts för cyberattacker mot kritiska statliga funktioner och tjänster som är nödvändiga för att upprätthålla väsentliga sociala och ekonomiska verksamheter i medlemsstaterna. Under 2024 och 2025 var LummaC2 ett av världens mest använda verktyg för informationsstöld. I egenskap av utvecklare, distributör och försäljare av LummaC2 är Maksim Voronin därför inblandad i och underlättar cyberattacker med en betydande effekt, som utgör ett externt hot för medlemsstaterna.	[+]

[+] EUT: vänligen för in datum för offentliggörande av denna förordning.

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
25.	Maksim Aleksandrovich GORDIENKO alias Maxim Alexandrovich GORDIENKO	Максим Александрович ГОРДИЕНКО Alias: ”Lummaseller” Nationalitet: påstått rysk Kön: man	Maksim Gordienko alias Lummaseller är inblandad i utveckling och distribution av sabotageprogrammet LummaC2 (alias Lumma Infostealer, Lumma Stealer), som används för att stjäla information. LummaC2 är en plattform av typen ”Malware-as-a-Service” (MaaS), som används för att stjäla känsliga uppgifter, åtkomstuppgifter till webbläsare, kryptoplånböcker eller systeminformation, för att installera ytterligare sabotageprogram på infekterade enheter, för stöld av kryptovalutor och för spionagekampanjer. Cyberattacker med sabotageprogrammet LummaC2 används också av ekonomiskt motiverade aktörer som utgör ett cyberhot som Storm-113, Storm-1607, Storm-1674, Octo Tempest med flera. Sabotageprogrammet LummaC2 har använts för cyberattacker mot kritiska statliga funktioner och tjänster som är nödvändiga för att upprätthålla väsentliga sociala och ekonomiska verksamheter i medlemsstaterna. Under 2024 och 2025 var LummaC2 ett av världens mest använda verktyg för informationsstöld. I egenskap av utvecklare, distributör och försäljare av LummaC2 är Maksim Gordienko därför inblandad i och underlättar cyberattacker med en betydande effekt, som utgör ett externt hot för medlemsstaterna.	[+]

[+] EUT: vänligen för in datum för offentliggörande av denna förordning.

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
26.	Evgeniy Viktorovich BASHEV	Евгений Викторович БАШЕВ Födelsedatum: 25.1.1980 Födelseort: Sovjetunionen Nationalitet: rysk Kön: man Associerade personer: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin Associerade enheter: GRU Unit 29155 (GRU-enhet 29155), ”Impuls” LLC	Evgeniy Bashev är medlem av den ryska militära underrättelsetjänsten GRU, enhet 29155. Inom enheten stöder och underlättar han cyberattacker med en betydande effekt mot medlemsstaterna, bland annat genom att kontrollera servern ”Aegon”, som används för hackningsoperationer. Han tillhandahåller särskilt tekniskt och materiellt stöd till cyberattackerna vid GRU-enheten 29155 genom sitt företag ”Impuls” LLC, som underlättade operativ täckning, infrastruktur och betalningar och förvaltade tekniska tillgångar, inbegripet servrar, som används för cyberattackerna. Han samordnade också samarbetet mellan GRU-strukturer och externa hackernätverk. De cyberattacker han underlättade riktade in sig på kritiska statliga funktioner, system och tjänster som är nödvändiga för att upprätthålla väsentliga sociala eller ekonomiska verksamheter i medlemsstaterna, särskilt inom transportsektorn. Genom WhisperGate-kampanjen riktade GRU-enhet 29155 också in sig på kritisk infrastruktur i Ukraina.	+

+ EUT: vänligen för in datum för offentliggörande av denna förordning.

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
			Evgeniy Bashev tillhandahåller därför tekniskt och materiellt stöd till eller är på annat sätt inblandad i cyberattacker med en betydande effekt, inbegripet försök till cyberattacker med en potentiellt betydande effekt, som utgör ett externt hot för medlemsstaterna, samt cyberattacker med en betydande effekt mot ett tredjeland. I egenskap av ägare och generaldirektör har han samröre med företaget ”Impuls” LLC. I egenskap av medlem i GRU-enhet 29155 har han också samröre med denna enhet.	

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
27.	Roman Alexandrovich PUNTUS	Роман Александрович ПУНТУС Födelseort: Ryska federationen Nationalitet: rysk Kön: man Associerade personer: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin, Evgeniy Viktorovich Bashev Associerade enheter: GRU Unit 29155 (GRU-enhet 29155)	Roman Puntus är medlem av den ryska militära underrättelsetjänsten GRU, enhet 29155. Inom enheten har han en ledande roll när det gäller att organisera och samordna cyberattacker med en betydande effekt mot medlemsstaterna. Han stöder också utvecklingen av enhetens interna cyberkapacitet, inbegripet rekrytering av och tillsyn över personal såsom hackare och programmerare. Genom bildandet av bulvanföretaget ”Aegeon-Impulse” underlättade han logistiska och ekonomiska aspekter av cyberoperationer. Under hans samordning genomförde enheten cyberattacker som riktade in sig på kritiska statliga funktioner, system och tjänster som är nödvändiga för att upprätthålla väsentliga sociala eller ekonomiska verksamheter i medlemsstaterna, särskilt inom transportsektorn. Genom WhisperGate-kampanjen riktade GRU-enhet 29155 också in sig på kritisk infrastruktur i Ukraina.	[+]”.

[+] EUT: vänligen för in datum för offentliggörande av denna förordning.

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
			Roman Puntus är därför ansvarig för eller på annat sätt inblandad i cyberattacker med en betydande effekt, inbegripet försök till cyberattacker med en potentiellt betydande effekt, som utgör ett externt hot för medlemsstaterna, samt cyberattacker med en betydande effekt mot ett tredjeland. I egenskap av medlem i GRU-enhet 29155 har han också samröre med denna enhet.	

2. Följande poster ska läggas till under rubriken ”B. Juridiska personer, enheter och organ”:

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
”8.	Media Land LLC	Adress: Tsvetnochnaya st., 16 Litera P, Room 27, Moskovskaya Zastava Municipal District St Petersburg, 196006, Russian Federation Typ av enhet: Limited Liability Company (bolag med begränsat ansvar) Registreringsort: Sankt Petersburg Registreringsdatum: 19.10.2015 Registreringsnummer: 1152536009900 Huvudsakligt verksamhetsställe: Sankt Petersburg, Ryska federationen Associerad enhet: ML.Cloud	Sedan 2016 har Bullet Proof Hosting service Media Land LLC underlättat ett brett spektrum av attacker med sabotageprogram mot medlemsstaterna och globalt genom att erbjuda värdtjänster som döljer användaridentiteter och motverkar brottsbekämpande myndigheters avlägsnande av innehåll, vilket lett till betydande ekonomiska förluster. Media Land LLC möjliggjorde storskaliga operationer med utpressningsprogram, ledningstjänster, och nätfiskeoperationer som riktar sig mot kritisk infrastruktur och samhällsviktiga tjänster i medlemsstaterna. Till de operationer som Media Land LLC underlättat hör bland annat LockBit, EvilCorp och BlackBasta. Media Land LLC är därför inblandat i cyberattacker med en betydande effekt, som utgör ett externt hot för medlemsstaterna.	+

+ EUT: vänligen för in datum för offentliggörande av denna förordning.

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
9.	ML.Cloud	Adress: Brivibas iela 52, Riga, LV-1011, Latvija; Russian Federation, Kazan, Peterburgskaya st. 52 Registreringsort: Riga Associerad person: Alexander Volosovik Andra associerade enheter: Media Land LLC	ML.Cloud är systerföretag till Media Land LLC och tillhandahåller teknisk infrastruktur för Media Land LLC. Sedan 2016 har Bullet Proof Hosting service Media Land LLC underlättat ett brett spektrum av attacker med sabotageprogram mot medlemsstaterna och globalt genom att erbjuda värdtjänster som döljer användaridentiteter och motverkar brottsbekämpande myndigheters avlägsnande av innehåll, vilket lett till betydande ekonomiska förluster. Media Land LLC möjliggjorde storskaliga operationer med utpressningsprogram, ledningstjänster, och nätfiskeoperationer som riktar sig mot kritisk infrastruktur och samhällsviktiga tjänster i medlemsstaterna. Till de operationer som Media Land LLC underlättat hör bland annat LockBit, EvilCorp och BlackBasta. Media Land LLC är därför inblandat i cyberattacker som utgör ett externt hot med en betydande effekt för EU:s medlemsstater. ML.Cloud tillhandahåller därför tekniskt stöd till cyberattacker med en betydande effekt, som utgör ett externt hot för medlemsstaterna.	+

+ EUT: vänligen för in datum för offentliggörande av denna förordning.

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
10.	”Impuls” LLC	Общество с ограниченной ответственностью ”Импульс” Adress: 344015, Russian Federation, Rostov Region, Rostov-on-Don, ul. Eremenko, d. 56, k. 6, apt. 88. Typ av enhet: Limited Liability Company (bolag med begränsat ansvar) Registreringsort: Interdistrict Inspectorate of the Federal Tax Service No. 26 for the Rostov Region, 344019, Rostov-on-Don, ul. Myasnikova, d. 52/32, Russian Federation Registreringsdatum: 27.9.2010	”Impuls” LLC är ett ryskt företag som ägs av Evgeniy Viktorovich Bashev, medlem av den ryska militära underrättelsetjänsten GRU, enhet 29155. Företaget tillhandahåller tekniskt och materiellt stöd till cyberattacker och försök till cyberattacker som genomförs av GRU-enhet 29155. ”Impuls” LLC fungerar särskilt som en operativ mellanhand som gör det möjligt att bedriva hackningsrelaterad verksamhet genom ett företag som formellt inte har någon koppling till den ryska staten. Det underlättade operativ täckning, infrastruktur och betalningar för cyberattacker och var kopplat till tekniska tillgångar, inbegripet servrar som används till stöd för hackningsverksamhet. ”Impuls” LLC möjliggjorde särskilt samarbete mellan GRU-strukturer och externa hackernätverk. De cyberoperationer som ”Impuls” LLC underlättade riktade in sig på kritiska statliga funktioner och tjänster som är nödvändiga för att upprätthålla väsentliga sociala och ekonomiska verksamheter i medlemsstaterna, särskilt inom transportsektorn. Genom WhisperGate-kampanjen riktade GRU-enhet 29155 också in sig på kritisk infrastruktur i Ukraina.	+

+ EUT: vänligen för in datum för offentliggörande av denna förordning.

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
		Registreringsnummer: INN (ИНН): 6168033776; OGRN (ОГРН): 1106194004850 Huvudsakligt verksamhetsställe: Ryska federationen Associerade personer: Evgeniy Bashev Associerade enheter: GRU Unit 29155 (GRU-enhet 29155)	”Impuls” LLC tillhandahåller därför tekniskt och materiellt stöd till eller är på annat sätt inblandad i cyberattacker med en betydande effekt, som utgör ett externt hot för medlemsstaterna, samt cyberattacker med en betydande effekt mot ett tredjeland.	

	Namn	Identifieringsuppgifter	Skäl	Datum för uppförande
11.	Z-Pentest	Alias: ”Z-Pentest Alliance”, ”Z-Alliance” Huvudsakligt verksamhetsställe: Ryska federationen Associerade personer: Yuliya Pankratova Associerade enheter: Cyber Army of Russia/CARR X.com-konto: ZPentest (tillfälligt avstängt konto) Telegramkonto: Zpentestalliance	Z-Pentest är en prorysk hacktivistgrupp som består av medlemmar från CARR (Cyber Army of Russia Reborn) och NoName057 och som globalt riktar in sig på kritisk infrastruktur, särskilt energi- och vattensektorn. Gruppen angrep i synnerhet ett danskt vattenverk i december 2024. Z-Pentest är därför ansvarigt för cyberattacker med en betydande effekt, som utgör ett externt hot för medlemsstaterna.	[+]”.

[+] EUT: vänligen för in datum för offentliggörande av denna förordning.