Publicatieblad
van de Europese Unie

NL
L-serie

2026/1713

13.7.2026

BESLUIT (GBVB) 2026/1713 VAN DE RAAD

van 13 juli 2026

tot wijziging van Besluit (GBVB) 2019/797 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen

DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de Europese Unie, en met name artikel 29,

Gezien het voorstel van de hoge vertegenwoordiger van de Unie voor buitenlandse zaken en veiligheidsbeleid,

Overwegende hetgeen volgt:

(1) Op 17 mei 2019 heeft de Raad Besluit (GBVB) 2019/797 ([1]) vastgesteld.

(2) In het kader van het volgehouden, op maat gesneden en gecoördineerde optreden van de Unie tegen actoren die aanhoudend voor cyberdreigingen zorgen, moeten acht natuurlijke personen en vier entiteiten worden toegevoegd aan de in de bijlage bij Besluit (GBVB) 2019/797 opgenomen lijst van natuurlijke personen en rechtspersonen, entiteiten en lichamen die aan beperkende maatregelen onderworpen zijn. Die personen en entiteiten zijn verantwoordelijk voor, bieden steun aan of zijn betrokken bij cyberaanvallen met aanzienlijke gevolgen die een externe bedreiging vormen voor de Unie of haar lidstaten.

(3) Besluit (GBVB) 2019/797 moet derhalve dienovereenkomstig worden gewijzigd,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

Artikel 1

De bijlage bij Besluit (GBVB) 2019/797 wordt gewijzigd overeenkomstig de bijlage bij dit besluit.

Artikel 2

Dit besluit treedt in werking op de datum van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Gedaan te Brussel, 13 juli 2026.

Voor de Raad

De voorzitter

K. KALLAS

([1]) Besluit (GBVB) 2019/797 van de Raad van 17 mei 2019 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen (PB L 129 I van 17.5.2019, blz. 13, ELI: http://data.europa.eu/eli/dec/2019/797/oj).

BIJLAGE

De bijlage bij Besluit (GBVB) 2019/797 wordt als volgt gewijzigd:

1) de volgende vermeldingen worden toegevoegd aan rubriek A “Natuurlijke personen”:

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
“20.	Vitaly Nikolayevich KOVALEV	Виталий Николаевич КОВАЛЕВ Alias: “Bentley”, “Bergen”, “Alex Konor”, “Benny”, “Ben”, “Stern” Geboortedatum: 23.6.1988 Adres: Serebristy Bulvar 34 (Serebristyy Bul’var); krp 1; flt 528; 197341; St Petersburg, Russian Federation (Sint-Petersburg, Russische Federatie) Nationaliteit: Russisch Geslacht: mannelijk Geassocieerde entiteiten: TrickBot, Wizard Spider, Conti	Vitaly Kovalev is een spilfiguur achter de malwareprogramma’s “Trickbot” en “Conti”. Hij staat online ook bekend onder de bijnamen “Bentley”, “Bergen”, “Alex Konor”, “Benny”, “Ben” en “Stern”. Conti en TrickBot werden aanvankelijk gecreëerd en ontwikkeld door Wizard Spider. Wizard Spider heeft ransomwarecampagnes gevoerd in verschillende sectoren, waaronder essentiële diensten zoals gezondheidszorg en banken, en wereldwijd computers besmet, en de malware is ontwikkeld tot een zeer modulair malwarepakket. Campagnes van Wizard Spider waarbij malware zoals Conti en TrickBot wordt gebruikt, hebben aanzienlijke economische schade aangericht in de Europese Unie. Vitaly Kovalev is derhalve verantwoordelijk voor en betrokken bij cyberaanvallen met aanzienlijke gevolgen die een externe bedreiging vormen voor de Unie of haar lidstaten.	13.7.2026

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
21.	Alexander Alexandrovich VOLOSOVIK	Александр Александрович ВОЛОСОВИК Geboortedatum: 30.1.1983 Geboorteplaats: USSR Nationaliteit: Russisch Paspoortnummer: 762988138 Geslacht: mannelijk Geassocieerde entiteiten: Yalishanda, LARVA-34, podzemniyl, Ohyeahhellno, Stas_vl, downlow	Alexander Volosovik is eigenaar van Media Land LLC. Bullet Proof Hosting service Media Land LLC faciliteert al sinds 2016 een breed scala aan malware-aanvallen, zowel tegen de Unie als wereldwijd, door hostingdiensten aan te bieden waarbij de identiteit van gebruikers wordt verborgen en verwijdering van inhoud door rechtshandhavingsinstanties wordt tegengegaan. Media Land LLC heeft grootschalige ransomware-operaties, command-and-controldiensten en phishingactiviteiten mogelijk gemaakt die gericht zijn tegen kritieke infrastructuur en essentiële diensten in de lidstaten, met aanzienlijke financiële verliezen tot gevolg. De door Media Land LLC gefaciliteerde activiteiten hebben onder meer betrekking op LockBit, EvilCorp en BlackBasta. Media Land LLC is derhalve betrokken bij cyberaanvallen met aanzienlijke gevolgen die een externe bedreiging vormen voor de Unie of haar lidstaten. Als eigenaar van Media Land LLC is Alexander Volosovik verantwoordelijk voor en betrokken bij deze cyberaanvallen. Hij is ook geassocieerd met Media Land LLC.	13.7.2026

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
22.	Denis Olegovich DEGTYARENKO	Денис Олегович ДЕГТЯРЕНКО Alias: “Dena” Geboortedatum: 9.10.1989 Geboorteplaats: USSR Nationaliteit: Russisch Geslacht: mannelijk Adres: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation (Orsk, Russische Federatie)	Denis Degtyarenko, ook bekend als Dena, is een Russische hacker binnen de groep CARR (Cyber Army of Russia Reborn). CARR is verantwoordelijk voor cyberaanvallen tegen diensten die nodig zijn om essentiële economische activiteiten en kritieke functies van de staat in de lidstaten in stand te houden, alsook tegen infrastructuur in Oekraïne en andere derde landen. CARR heeft banden met het hoofdcentrum voor speciale technologieën (GTsST) van het hoofddirectoraat van de generale staf van de strijdkrachten van de Russische Federatie (GRU). De GTsST blijft actief cyberaanvallen uitvoeren tegen de Unie of haar lidstaten. De doelwitten van CARR zijn onder meer overheidsinstanties, financiële instellingen, mediakanalen en kritieke infrastructuur in de lidstaten en de Verenigde Staten. CARR heeft DDoS-aanvallen (distributed denial-of-service) uitgevoerd in Oekraïne en tegen regeringen en bedrijven in landen die Oekraïne hebben gesteund. Denis Degtyarenko, een van de belangrijkste hackers binnen CARR, is derhalve betrokken bij cyberaanvallen met aanzienlijke gevolgen, met inbegrip van pogingen tot cyberaanvallen met potentieel aanzienlijke gevolgen die een externe bedreiging vormen voor de lidstaten, alsook tegen derde landen. Als lid van CARR is hij ook geassocieerd met GTsST.	13.7.2026

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
23.	Yuliya Vladimirovna PANKRATOVA	Юлия Владимировна ПАНКРАТОВА Alias: “YUliYA” Geboortedatum: 6.4.1984 Geboorteplaats: USSR Nationaliteit: Russisch Geslacht: vrouwelijk Adres: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation (Orsk, Russische Federatie)	Yuliya Pankratova is een Russische hacker die actief is geweest voor CARR (Cyber Army of Russia Reborn) en die Z-Pentest heeft opgericht, waarvoor zij nog steeds actief is. CARR is verantwoordelijk voor cyberaanvallen tegen diensten die nodig zijn om essentiële economische activiteiten en kritieke functies van de staat in de lidstaten in stand te houden, alsook tegen infrastructuur in Oekraïne en andere derde landen. CARR heeft banden met het hoofdcentrum voor speciale technologieën (GTsST) van het hoofddirectoraat van de generale staf van de strijdkrachten van de Russische Federatie (GRU). De GTsST blijft actief cyberaanvallen uitvoeren tegen de Unie of haar lidstaten. De doelwitten van CARR zijn onder meer overheidsinstanties, financiële instellingen, mediakanalen en kritieke infrastructuur in de lidstaten en de Verenigde Staten. CARR heeft DDoS-aanvallen (distributed denial-of-service) uitgevoerd in Oekraïne en tegen regeringen en bedrijven in landen die Oekraïne hebben gesteund. Z-Pentest is verantwoordelijk voor cyberaanvallen met aanzienlijke gevolgen tegen onder meer diensten die nodig zijn om essentiële activiteiten in de lidstaten in stand te houden. Yuliya Pankratova, een van de belangrijkste hackers van CARR en Z-Pentest, is derhalve betrokken bij cyberaanvallen met aanzienlijke gevolgen, met inbegrip van pogingen tot cyberaanvallen met potentieel aanzienlijke gevolgen, die een externe bedreiging vormen voor de lidstaten, alsook tegen derde landen. Zij is ook geassocieerd met Z-Pentest.	13.7.2026

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
24.	Maksim Evgenevich VORONIN	Максим Евгеньевич ВОРОНИН Alias: “Daugn0” Nationaliteit: naar verluidt Russisch Geslacht: mannelijk	Maksim Voronin, ook bekend als Daugn0, is betrokken bij de ontwikkeling, verspreiding en verkoop van de malware LummaC2 (ook bekend als Lumma Infostealer, Lumma Stealer), die wordt gebruikt om informatie te stelen. LummaC2 is een platform voor Malware-as-a-Service (MaaS) dat wordt gebruikt om gevoelige gegevens, inloggegevens voor browsers, cryptowallets of systeeminformatie te stelen, en om nog meer malware te installeren op al besmette apparaten, alsook om cryptovaluta te stelen en spionagecampagnes uit te voeren. Cyberaanvallen met LummaC2-malware worden ook voor financieel gewin gebruikt door actoren die voor cyberdreigingen zorgen, zoals Storm-113, Storm-1607, Storm-1674, Octo Tempest en andere. LummaC2-malware is gebruikt voor cyberaanvallen tegen kritieke functies van de staat en diensten die nodig zijn om essentiële sociale en economische activiteiten van de lidstaten in stand te houden. In 2024 en 2025 was LummaC2 wereldwijd een van de meest gebruikte instrumenten om informatie te stelen. Als ontwikkelaar, verspreider en verkoper van LummaC2 is Maksim Voronin derhalve betrokken bij en faciliteert hij cyberaanvallen met aanzienlijke gevolgen die een externe bedreiging vormen voor de lidstaten.	13.7.2026

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
25.	Maksim Aleksandrovich GORDIENKO ook bekend als Maxim Alexandrovich GORDIENKO	Максим Александрович ГОРДИЕНКО Alias: “Lummaseller” Nationaliteit: naar verluidt Russisch Geslacht: mannelijk	Maksim Gordienko, ook bekend als Lummaseller, is betrokken bij de ontwikkeling en verspreiding van de malware LummaC2 (ook bekend als Lumma Infostealer, Lumma Stealer), die wordt gebruikt om informatie te stelen. LummaC2 is een platform voor Malware-as-a-Service (MaaS) dat wordt gebruikt om gevoelige gegevens, inloggegevens voor browsers, cryptowallets of systeeminformatie te stelen, en om nog meer malware te installeren op al besmette apparaten, alsook om cryptovaluta te stelen en spionagecampagnes uit te voeren. Cyberaanvallen met LummaC2-malware worden ook voor financieel gewin gebruikt door actoren die voor cyberdreigingen zorgen, zoals Storm-113, Storm-1607, Storm-1674, Octo Tempest en andere. LummaC2-malware is gebruikt voor cyberaanvallen tegen kritieke functies van de staat en diensten die nodig zijn om essentiële sociale en economische activiteiten van de lidstaten in stand te houden. In 2024 en 2025 was LummaC2 wereldwijd een van de meest gebruikte instrumenten om informatie te stelen. Als ontwikkelaar, verspreider en verkoper van LummaC2 is Maksim Gordienko derhalve betrokken bij en faciliteert hij cyberaanvallen met aanzienlijke gevolgen die een externe bedreiging vormen voor de lidstaten.	13.7.2026

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
26.	Evgeniy Viktorovich BASHEV	Евгений Викторович БАШЕВ Geboortedatum: 25.1.1980 Geboorteplaats: USSR Nationaliteit: Russisch Geslacht: mannelijk Geassocieerde personen: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin Geassocieerde entiteiten: GRU-eenheid 29155, “Impuls” LLC	Evgeniy Bashev is lid van de Russische militaire inlichtingendienst GRU, eenheid 29155. Binnen de eenheid ondersteunt en faciliteert hij cyberaanvallen tegen de lidstaten met aanzienlijke gevolgen, onder meer door de “Aegon”-server te beheren, die wordt gebruikt voor hackingactiviteiten. Hij verleent met name technische en materiële steun voor de cyberaanvallen van GRU-eenheid 29155 via zijn bedrijf “Impuls” LLC, dat het verlenen van een operationele dekmantel, infrastructuur en betalingen faciliteerde, en technische activa beheerde, waaronder servers, die worden gebruikt voor de cyberaanvallen. Hij coördineerde ook de samenwerking tussen GRU-structuren en externe netwerken van hackers. De door hem gefaciliteerde cyberaanvallen waren gericht tegen systemen voor kritieke functies van de staat en diensten die nodig zijn om essentiële sociale of economische activiteiten in de lidstaten in stand te houden, met name in de vervoerssector. Via de WhisperGate-campagne heeft GRU-eenheid 29155 ook kritieke infrastructuur in Oekraïne aangevallen. Evgeniy Bashev verleent derhalve technische en materiële steun voor of is anderszins betrokken bij cyberaanvallen met aanzienlijke gevolgen, met inbegrip van pogingen tot cyberaanvallen met potentieel aanzienlijke gevolgen die een externe bedreiging vormen voor de lidstaten, alsook cyberaanvallen met aanzienlijke gevolgen tegen een derde land. Als eigenaar en algemeen directeur is hij geassocieerd met het bedrijf “Impuls” LLC. Als lid van GRU-eenheid 29155 is hij ook geassocieerd met die entiteit.	13.7.2026

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
27.	Roman Alexandrovich PUNTUS	Роман Александрович ПУНТУС Geboorteplaats: Russische Federatie Nationaliteit: Russisch Geslacht: mannelijk Geassocieerde personen: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin, Evgeniy Viktorovich Bashev Geassocieerde entiteiten: GRU-eenheid 29155	Roman Puntus is lid van de Russische militaire inlichtingendienst GRU, eenheid 29155. Binnen de eenheid heeft hij een leidende rol op het vlak van de organisatie en coördinatie van cyberaanvallen tegen de lidstaten met aanzienlijke gevolgen. Hij ondersteunt ook de ontwikkeling van de interne cybercapaciteit van de eenheid, met inbegrip van de aanwerving en aansturing van personeel zoals hackers en programmeurs. Door de oprichting van het dekmantelbedrijf “Aegeon-Impulse” faciliteerde hij de logistieke en financiële aspecten van cyberoperaties. Onder zijn coördinatie voerde de eenheid cyberaanvallen uit tegen systemen voor kritieke functies van de staat die nodig zijn om essentiële sociale of economische activiteiten in de lidstaten in stand te houden, met name in de vervoerssector. Via de WhisperGate-campagne heeft GRU-eenheid 29155 ook kritieke infrastructuur in Oekraïne aangevallen. Roman Puntus is derhalve verantwoordelijk voor of is anderszins betrokken bij cyberaanvallen met aanzienlijke gevolgen, met inbegrip van pogingen tot cyberaanvallen met potentieel aanzienlijke gevolgen die een externe bedreiging vormen voor de lidstaten, alsook cyberaanvallen met aanzienlijke gevolgen tegen een derde land. Als lid van GRU-eenheid 29155 is hij ook geassocieerd met die entiteit.	13.7.2026”

2) de volgende vermeldingen worden toegevoegd aan rubriek B “Rechtspersonen, entiteiten en lichamen”:

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
“8.	Media Land LLC	Adres: Tsvetnochnaya st., 16 Litera P, Room 27, Moskovskaya Zastava Municipal District, St Petersburg, 196006, Russian Federation (Sint-Petersburg, Russische Federatie) Soort entiteit: vennootschap met beperkte aansprakelijkheid Plaats van registratie: Sint-Petersburg Registratiedatum: 19.10.2015 Registratienummer: 1152536009900 Voornaamste plaats van bedrijvigheid: Sint-Petersburg, Russische Federatie Geassocieerde entiteit: ML.Cloud	Bullet Proof Hosting service Media Land LLC faciliteert sinds 2016 een breed scala aan malware-aanvallen, tegen de lidstaten en wereldwijd, door hostingdiensten aan te bieden waarbij de identiteit van gebruikers wordt verborgen en verwijdering van inhoud door rechtshandhavingsinstanties wordt tegengegaan, met aanzienlijke financiële verliezen tot gevolg. Media Land LLC heeft grootschalige ransomware-activiteiten, command-and-controldiensten en phishingactiviteiten mogelijk gemaakt die gericht zijn tegen kritieke infrastructuur en essentiële diensten in de lidstaten. De door Media Land LLC gefaciliteerde activiteiten hebben onder meer betrekking op LockBit, EvilCorp en BlackBasta. Media Land LLC is derhalve betrokken bij cyberaanvallen met aanzienlijke gevolgen, die een externe bedreiging vormen voor de lidstaten.	13.7.2026

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
9.	ML.Cloud	Adres: Brivibas iela 52, Riga, LV-1011, Latvija (Riga, Letland); Russian Federation, Kazan, Peterburgskaya st. 52 (Kazan, Russische Federatie) Plaats van registratie: Riga Geassocieerde persoon: Alexander Volosovik Andere geassocieerde entiteiten: Media Land LLC	ML.Cloud, een zusteronderneming van Media Land LLC, levert de technische infrastructuur voor Media Land LLC. Bullet Proof Hosting service Media Land LLC faciliteert sinds 2016 een breed scala aan malware-aanvallen, tegen de lidstaten en wereldwijd, door hostingdiensten aan te bieden waarbij de identiteit van gebruikers wordt verborgen en verwijdering van inhoud door rechtshandhavingsinstanties wordt tegengegaan, met aanzienlijke financiële verliezen tot gevolg. Media Land LLC heeft grootschalige ransomware-activiteiten, command-and-controldiensten en phishingactiviteiten mogelijk gemaakt die gericht zijn tegen kritieke infrastructuur en essentiële diensten in de lidstaten. De door Media Land LLC gefaciliteerde activiteiten hebben onder meer betrekking op LockBit, EvilCorp en BlackBasta. Media Land LLC is derhalve betrokken bij cyberaanvallen die een externe bedreiging vormen met aanzienlijke gevolgen voor de EU-lidstaten. ML.Cloud verleent derhalve technische ondersteuning voor cyberaanvallen met aanzienlijke gevolgen, die een externe bedreiging vormen voor de lidstaten.	13.7.2026

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
10.	“Impuls” LLC	Общество с ограниченной ответственностью “Импульс” Adres: 344015, Russian Federation, Rostov Region, Rostov-on-Don, ul. Eremenko, d. 56, k. 6, apt. 88 (Rostov aan de Don, Russische Federatie) Soort entiteit: vennootschap met beperkte aansprakelijkheid Plaats van registratie: Interdistrict Inspectorate of the Federal Tax Service No. 26 for the Rostov Region, 344019, Rostov-on-Don, ul. Myasnikova, d. 52/32, Russian Federation (Rostov aan de Don, Russische Federatie) Registratiedatum: 27.9.2010 Registratienummer: INN (ИНН): 6168033776; OGRN (ОГРН): 1106194004850 Voornaamste plaats van bedrijvigheid: Russische Federatie Geassocieerde personen: Evgeniy Bashev Geassocieerde entiteiten: GRU-eenheid 29155	“Impuls” LLC is een Russisch bedrijf dat eigendom is van Evgeniy Viktorovich Bashev, een lid van de Russische militaire inlichtingendienst GRU, eenheid 29155. Het bedrijf verleent technische en materiële steun voor cyberaanvallen en pogingen tot cyberaanvallen door GRU-eenheid 29155. “Impuls” LLC treedt met name op als operationele tussenpersoon die het mogelijk maakt hackingactiviteiten uit te voeren via een bedrijf dat officieel geen banden heeft met de Russische staat. Het faciliteerde een operationele dekmantel, infrastructuur en betalingen voor cyberaanvallen en was gelieerd aan technische activa, waaronder servers die worden gebruikt ter ondersteuning van hackingactiviteiten. “Impuls” LLC maakte met name samenwerking mogelijk tussen GRU-structuren en externe netwerken van hackers. De door “Impuls” LLC gefaciliteerde cyberoperaties zijn gericht tegen kritieke functies van de staat en diensten die nodig zijn om essentiële sociale en economische activiteiten in de lidstaten in stand te houden, met name in de vervoerssector. Via de WhisperGate-campagne heeft GRU-eenheid 29155 ook kritieke infrastructuur in Oekraïne aangevallen. “Impuls” LLC verleent derhalve technische en materiële steun voor of is anderszins betrokken bij cyberaanvallen met aanzienlijke gevolgen, die een externe bedreiging vormen voor de lidstaten, alsook cyberaanvallen met aanzienlijke gevolgen tegen een derde land.	13.7.2026

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
11.	Z-Pentest	Alias: “Z-Pentest Alliance”, “Z-Alliance” Voornaamste plaats van bedrijvigheid: Russische Federatie Geassocieerde personen: Yuliya Pankratova Geassocieerde entiteiten: Cyber Army of Russia/CARR X.com-account: ZPentest (account opgeschort) Telegramaccount: Zpentestalliance	Z-Pentest is een pro-Russische activistische hackersgroep, bestaande uit leden van CARR (Cyber Army of Russia Reborn) en NoName057, die wereldwijd kritieke infrastructuur aanvalt, voornamelijk in de energie- en watersector. De groep heeft met name in december 2024 een Deens waterbedrijf aangevallen. Z-Pentest is derhalve verantwoordelijk voor cyberaanvallen met aanzienlijke gevolgen, die een externe bedreiging voor de lidstaten vormen.	13.7.2026”