Raad van de
Europese Unie

Brussel, 5 mei 2026
(OR. en)

7281/26

LIMITE

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

WETGEVINGSBESLUITEN EN ANDERE INSTRUMENTEN

Betreft:	BESLUIT VAN DE RAAD tot wijziging van Besluit (GBVB) 2019/797 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen

BESLUIT (GBVB) 2026/… VAN DE RAAD

van …

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

(2) Besluit (GBVB) 2019/797 is van toepassing tot en met 18 mei 2028.

(3) Op basis van een evaluatie van de bijlage bij Besluit (GBVB) 2019/797 moet de toepassing van de in de artikelen 4 en 5 van dat besluit opgenomen maatregelen ten aanzien van de in die bijlage vermelde natuurlijke personen en rechtspersonen, entiteiten en lichamen worden verlengd tot en met 18 mei 2027. Voorts moet de motivering voor het opnemen van vier personen en één entiteit in de lijst van aan beperkende maatregelen onderworpen natuurlijke personen en rechtspersonen, entiteiten en lichamen, worden geactualiseerd.

(4) Besluit (GBVB) 2019/797 moet daarom dienovereenkomstig worden gewijzigd,

HEEFT HET VOLGENDE BESLUIT VASTGESTELD:

[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 129I van 17.5.2019, blz. 13, ELI: http://data.europa.eu/eli/dec/2019/797/oj).

Artikel 1

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

1) artikel 10 wordt vervangen door:

"*Artikel 10*

Dit besluit is van toepassing tot en met 18 mei 2028 en wordt voortdurend geëvalueerd. De in de artikelen 4 en 5 opgenomen maatregelen zijn tot en met 18 mei 2027 van toepassing ten aanzien van de in de bijlage vermelde natuurlijke personen en rechtspersonen, entiteiten en lichamen.";

2) de bijlage wordt gewijzigd overeenkomstig de bijlage bij dit besluit.

Artikel 2

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

Gedaan te …, …

Voor de Raad
De voorzitter

BIJLAGE

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

1) onder de rubriek “A. Natuurlijke personen” worden de vermeldingen 1, 2, 13 en 14 vervangen door de volgende overeenkomstige vermeldingen:

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
“1.	GAO Qiang	Geboortedatum: 4 oktober 1983 Geboorteplaats: provincie Shandong, China Adres: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Nationaliteit: Chinees Geslacht: man	Gao Qiang is verbonden met de “APT10”-koepel (“Advanced Persistent Threat 10”, ook bekend als “Red Apollo”, “CVNX”, “Stone Panda”, “MenuPass” en “Potassium”) en is betrokken geweest bij “Operation Cloud Hopper”, een reeks cyberaanvallen afkomstig van buiten de Unie die aanzienlijke gevolgen hebben en een externe bedreiging vormen voor de Unie of haar lidstaten, en die aanzienlijke gevolgen voor derde landen hebben. “Operation Cloud Hopper” was gericht op informatiesystemen van multinationale ondernemingen op zes continenten, waaronder in de Unie gevestigde ondernemingen, en heeft het mogelijk gemaakt ongeautoriseerde toegang te verkrijgen tot commercieel gevoelige gegevens, wat tot significante economische verliezen heeft geleid. Gao Qiang heeft banden met de commando- en controle-infrastructuur van APT10. Bovendien was Gao Qiang in dienst bij Huaying Haitai, een door APT10 gebruikt bedrijf dat op de lijst is geplaatst voor het ondersteunen en faciliteren van “Operation Cloud Hopper”. Hij heeft ook banden met Zhang Shilong, die verbonden is met APT10 en die ook in dienst is geweest bij Huaying Haitai.	30.7.2020

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
2.	ZHANG Shilong	Geboortedatum: 10 september 1981 Geboorteplaats: China Adres: Hedong, Yuang Road nr. 121, Tianjin, China Nationaliteit: Chinees Geslacht: man	Zhang Shilong is verbonden met de “APT10”-koepel (“Advanced Persistent Threat 10”, ook bekend als “Red Apollo”, “CVNX”, “Stone Panda”, “MenuPass” en “Potassium”) en is betrokken geweest bij “Operation Cloud Hopper”, een reeks cyberaanvallen afkomstig van buiten de Unie die aanzienlijke gevolgen hebben en een externe bedreiging vormen voor de Unie of haar lidstaten, en die aanzienlijke gevolgen voor derde landen hebben. “Operation Cloud Hopper” was gericht op informatiesystemen van multinationale ondernemingen op zes continenten, waaronder in de Unie gevestigde ondernemingen, en heeft het mogelijk gemaakt ongeautoriseerde toegang te verkrijgen tot commercieel gevoelige gegevens, wat tot significante economische verliezen heeft geleid. Zhang Shilong heeft banden met APT10, onder meer door de malware die hij heeft ontwikkeld en getest in verband met de door APT10 uitgevoerde cyberaanvallen. Bovendien was Zhang Shilong in dienst bij Huaying Haitai, een door APT10 gebruikt bedrijf dat op de lijst is geplaatst voor het ondersteunen en faciliteren van “Operation Cloud Hopper”. Hij heeft ook banden met Gao Qiang, die verbonden is met APT10 en die ook in dienst is geweest bij Huaying Haitai.	30.7.2020

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
13.	Mikhail Mikhailovich TSAREV	Михаил Михайлович ЦАРЕВ Geboortedatum: 20.4.1989 Geboorteplaats: Serpoechov, Russische Federatie Nationaliteit: Russisch Adres: Serpoechov Geslacht: man	Mikhail Mikhailovich Tsarev nam deel aan cyberaanvallen met aanzienlijke gevolgen, die een externe bedreiging vormen voor de EU-lidstaten. Mikhail Mikhailovich Tsarev, ook bekend onder de online bijnamen “Mango”, “Alexander Grachev”, “Super Misha”, “Ivanov Mixail”, “Misha Krutysha” en “Nikita Andreevich Tsarev”, is een belangrijke speler bij de uitrol van de malwareprogramma’s “Conti” en “TrickBot”, en is betrokken bij de in Rusland gevestigde dreigingsgroep “Wizard Spider”. Wizard Spider blijft zich ontwikkelen en zijn activiteiten intensiveren. De malwareprogramma’s “Conti” en “TrickBot” zijn opgezet en ontwikkeld door “Wizard Spider”. Wizard Spider heeft ransomwarecampagnes gevoerd in verschillende sectoren, waaronder essentiële diensten zoals gezondheidszorg en banken. De groep heeft wereldwijd computers besmet en de malware is ontwikkeld tot een zeer modulair malwarepakket. Campagnes van Wizard Spider waarbij malware zoals Conti, “Ryuk”, TrickBot of Black Basta wordt gebruikt, hebben aanzienlijke economische schade aangericht in de Europese Unie. Mikhail Mikhailovich Tsarev is derhalve betrokken bij cyberaanvallen met aanzienlijke gevolgen die een externe bedreiging vormen voor de Unie of haar lidstaten.	24.6.2024

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
14.	Maksim Sergeevich GALOCHKIN	Максим Сергеевич ГАЛОЧКИН Geboortedatum: 19.5.1982 Geboorteplaats: Abakan, Russische Federatie Nationaliteit: Russisch Geslacht: man	Maksim Galochkin nam deel aan cyberaanvallen met aanzienlijke gevolgen, die een externe bedreiging vormen voor de EU-lidstaten. Maksim Galochkin staat ook bekend onder de online bijnamen “Benalen”, “Bentley”, “Volhvb”, “volhvb”, “manuel”, “Max17” en “Crypt”. Galochkin is een belangrijke speler bij de uitrol van de malwareprogramma’s “Conti” en “TrickBot”, en is betrokken bij de in Rusland gevestigde dreigingsgroep “Wizard Spider”. Hij heeft een groep testers geleid en is belast met taken inzake de ontwikkeling van, het toezicht op en de uitvoering van tests voor het malwareprogramma TrickBot, opgezet en ontwikkeld door “Wizard Spider”. Wizard Spider blijft zich ontwikkelen en zijn activiteiten intensiveren. Wizard Spider heeft ransomwarecampagnes gevoerd in verschillende sectoren, waaronder essentiële diensten zoals gezondheidszorg en banken. De groep heeft wereldwijd computers besmet en de malware is ontwikkeld tot een zeer modulair malwarepakket. Campagnes van Wizard Spider waarbij malware zoals Conti, “Ryuk”, TrickBot of Black Basta wordt gebruikt, hebben aanzienlijke economische schade aangericht in de Europese Unie. Maksim Galochkin is derhalve betrokken bij cyberaanvallen met aanzienlijke gevolgen die een externe bedreiging vormen voor de Unie of haar lidstaten.	24.6.2024”;

2) onder de rubriek “B. Rechtspersonen, entiteiten en lichamen” wordt vermelding 1 vervangen door:

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
“1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	Ook bekend als: Haitai Technology Development Co. Ltd. Locatie: Tianjin, China	Huaying Haitai heeft financiële, technische of materiële steun verleend voor “Operation Cloud Hopper”, een reeks cyberaanvallen afkomstig van buiten de Unie die aanzienlijke gevolgen hebben en een externe bedreiging vormen voor de Unie of haar lidstaten, en een reeks cyberaanvallen die aanzienlijke gevolgen voor derde landen hebben, en heeft die operatie gefaciliteerd. “Operation Cloud Hopper” was gericht op informatiesystemen van multinationale ondernemingen op zes continenten, waaronder in de Unie gevestigde ondernemingen, en heeft het mogelijk gemaakt ongeautoriseerde toegang te verkrijgen tot commercieel gevoelige gegevens, wat tot significante economische verliezen heeft geleid. De actor bekend als “APT10” (“Advanced Persistent Threat 10”) (ook bekend als “Red Apollo”, “CVNX”, “Stone Panda”, “MenuPass” en “Potassium”) voerde “Operation Cloud Hopper” uit. Huaying Haitai kan worden gelinkt aan APT10. Bovendien was Huaying Haitai de werkgever van Gao Qiang en Zhang Shilong. die beiden op de lijst zijn geplaatst in verband met “Operation Cloud Hopper”. Huaying Haitai heeft derhalve ook banden met Gao Qiang en Zhang Shilong.	30.7.2020”.