Publicatieblad
van de Europese Unie

NL
L-serie

2024/1778

24.6.2024

UITVOERINGSVERORDENING (EU) 2024/1778 VAN DE RAAD

van 24 juni 2024

tot uitvoering van Verordening (EU) 2019/796 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen

DE RAAD VAN DE EUROPESE UNIE,

Gezien het Verdrag betreffende de werking van de Europese Unie,

Gezien Verordening (EU) 2019/796 van de Raad van 17 mei 2019 betreffende beperkende maatregelen tegen cyberaanvallen die de Unie of haar lidstaten bedreigen ([1]), en met name artikel 13, lid 1,

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 Verordening (EU) 2019/796 vastgesteld.

(2) Gerichte beperkende maatregelen tegen cyberaanvallen met aanzienlijke gevolgen, die een externe bedreiging vormen voor de Unie of haar lidstaten, vallen onder de maatregelen binnen het Uniekader voor een gezamenlijke diplomatieke respons op kwaadwillige cyberactiviteiten (het instrumentarium voor cyberdiplomatie) en zijn een cruciaal instrument om dergelijke activiteiten te voorkomen, te beletten, te ontmoedigen en te beantwoorden.

(3) Kwaadwillige cyberactiviteiten tegen kritieke infrastructuur of essentiële diensten, onder meer door het gebruik van ransomware en wipers, aanvallen op toeleveringsketens en cyberspionage, met inbegrip van diefstal van intellectuele eigendom, nemen toe in aantal, frequentie en complexiteit. Door hun ontwrichtende en destructieve effecten vormen deze activiteiten een systemische bedreiging voor de veiligheid, de economie, de democratie en voor de samenleving in het algemeen van de Unie.

(4) De cyberoperaties die Ruslands niet-uitgelokte en ongerechtvaardigde aanvalsoorlog tegen Oekraïne mogelijk hebben gemaakt en deze daarna hebben begeleid, hebben gevolgen voor de mondiale stabiliteit en veiligheid, vormen een belangrijk risico op escalatie en werken de reeds aanzienlijke toename van kwaadwillige cyberactiviteiten buiten de context van gewapende conflicten van de afgelopen jaren in de hand. De toenemende cyberbeveiligingsrisico's en een algemeen complex cyberdreigingslandschap, met een duidelijk risico dat cyberincidenten snel overslaan van de ene lidstaat naar de andere en van derde landen naar de Unie, versterken de roep om beperkende maatregelen uit hoofde van Verordening (EU) 2019/796.

(5) In het kader van het volgehouden, op maat gesneden en gecoördineerde optreden van de Unie tegen actoren die aanhoudend voor cyberdreigingen zorgen, moeten zes natuurlijke personen worden toegevoegd aan de in bijlage I bij Verordening (EU) 2019/796 opgenomen lijst van natuurlijke personen en rechtspersonen, entiteiten en lichamen die aan beperkende maatregelen onderworpen zijn. Die personen zijn verantwoordelijk voor of waren betrokken bij cyberaanvallen met aanzienlijke gevolgen, die een externe bedreiging vormen voor de Unie of haar lidstaten.

(6) Bijlage I bij Verordening (EU) 2019/796 moet derhalve dienovereenkomstig worden gewijzigd,

HEEFT DE VOLGENDE VERORDENING VASTGESTELD:

Artikel 1

Bijlage I bij Verordening (EU) 2019/796 wordt gewijzigd overeenkomstig de bijlage bij deze verordening.

([1]) PB L 129 I van 17.5.2019, blz. 1.

Artikel 2

Deze verordening treedt in werking op de datum van de bekendmaking ervan in het *Publicatieblad van de Europese Unie*.

Deze verordening is verbindend in al haar onderdelen en is rechtstreeks toepasselijk in elke lidstaat.

Gedaan te Luxemburg, 24 juni 2024.

Voor de Raad

De voorzitter

J. BORRELL FONTELLES

BIJLAGE

De volgende vermeldingen worden toegevoegd aan rubriek A “Natuurlijke personen” in bijlage I bij Verordening (EU) 2019/796:

	Naam	Identificatiegegevens	Motivering	Datum van plaatsing op de lijst
“9.	Ruslan Aleksandrovich PERETYATKO	Руслан Александрович ПЕРЕТЯТЬКО Geboortedatum: 3.8.1985 Nationaliteit: Russisch Geslacht: mannelijk	Ruslan Peretyatko nam deel aan cyberaanvallen met aanzienlijke gevolgen die een externe bedreiging vormen voor de Unie of haar lidstaten. Ruslan Peretyatko maakt deel uit van de “Callisto-groep” van Russische militaire-inlichtingenofficieren die cyberoperaties uitvoeren tegen EU-lidstaten en derde landen. De Callisto-groep (ook bekend als “Seaborgium”, “Star Blizzard”, “ColdRiver”, “TA446”) heeft meerjarige phishingcampagnes opgezet om accountgegevens en data te stelen. Voorts is de Callisto-groep verantwoordelijk voor campagnes tegen personen en tegen kritieke staatsfuncties, onder meer op het gebied van defensie en externe betrekkingen. Ruslan Peretyatko is derhalve betrokken bij cyberaanvallen met aanzienlijke gevolgen die een externe bedreiging vormen voor de Unie of haar lidstaten.	24.6.2024
10.	Andrey Stanislavovich KORINETS	Андрей Станиславович КОРИНЕЦ Geboortedatum: 18.5.1987 Geboorteplaats: de stad Syktyvkar, Rusland Nationaliteit: Russisch Geslacht: mannelijk	Andrey Stanislavovich Korinets nam deel aan cyberaanvallen met aanzienlijke gevolgen, die een externe bedreiging vormen voor de Unie of haar lidstaten. Andrey Stanislavovich Korinets is officier bij “Center 18” van de Federale Veiligheidsdienst (FSB) van de Russische Federatie. Andrey Stanislavovich Korinets maakt deel uit van de “Callisto-groep” van Russische militaire-inlichtingenofficieren die cyberoperaties uitvoeren tegen EU-lidstaten en derde landen. De Callisto-groep (ook bekend als “Seaborgium”, “Star Blizzard”, “ColdRiver”, “TA446”) heeft meerjarige phishingcampagnes opgezet om accountgegevens en data te stelen. Voorts is de Callisto-groep verantwoordelijk voor campagnes tegen personen en tegen kritieke staatsfuncties, onder meer op het gebied van defensie en externe betrekkingen. Andrey Stanislavovich Korinets 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
11.	Oleksandr SKLIANKO	Александр СКЛЯНКО (Russische spelling) Олександр СКЛЯНКО (Oekraïense spelling) Geboortedatum: 5.8.1973 Paspoort: EC 867868, afgegeven op 27.11.1998 (Oekraïne) Geslacht: man	Oleksandr Sklianko nam deel aan cyberaanvallen met aanzienlijke gevolgen tegen EU-lidstaten en derde landen. Oleksandr Sklianko maakt deel uit van de hackergroep “Armageddon”, die wordt gesteund door de Federale Veiligheidsdienst (FSB) van de Russische Federatie en die verschillende cyberaanvallen met aanzienlijke gevolgen heeft uitgevoerd tegen de regering van Oekraïne en tegen EU-lidstaten en hun regeringsfunctionarissen, onder meer via phishingmails en malwarecampagnes. Oleksandr Sklianko is derhalve betrokken bij cyberaanvallen met aanzienlijke gevolgen tegen derde landen en bij cyberaanvallen met aanzienlijke gevolgen die een externe bedreiging vormen voor de Unie of haar lidstaten.	24.6.2024
12.	Mykola CHERNYKH	Николай ЧЕРНЫХ (Russische spelling) Микола ЧЕРНИХ (Oekraïense spelling) Geboortedatum: 12.10.1978 Paspoort: EC 922162, afgegeven op 20.1.1999 (Oekraïne) Geslacht: man	Mykola Chernykh nam deel aan cyberaanvallen met aanzienlijke gevolgen tegen EU-lidstaten en derde landen. Mykola Chernykh maakt deel uit van de hackergroep “Armageddon”, die wordt gesteund door de Federale Veiligheidsdienst (FSB) van de Russische Federatie en die verschillende cyberaanvallen met aanzienlijke gevolgen heeft uitgevoerd tegen de regering van Oekraïne en tegen EU-lidstaten en hun regeringsfunctionarissen, onder meer via phishingmails en malwarecampagnes. Als voormalig werknemer van de Oekraïense veiligheidsdienst wordt hij in Oekraïne beschuldigd van verraad en ongeoorloofde inmenging in de exploitatie van elektronische computers en geautomatiseerde systemen. Mykola Chernykh is derhalve betrokken bij cyberaanvallen met aanzienlijke gevolgen, die een externe bedreiging vormen voor de Unie of haar lidstaten.	24.6.2024

ELI: http://data.europa.eu/eli/reg_impl/2024/1778/oj

	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”. 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” en TrickBot 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 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” en TrickBot 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”