Eiropas Savienības
Padome

Briselē, 2026. gada 5. maijā
(OR. en)

7281/26

LIMITE

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

LEĢISLATĪVIE AKTI UN CITI DOKUMENTI

Temats:	PADOMES LĒMUMS, ar ko groza Lēmumu (KĀDP) 2019/797 par ierobežojošiem pasākumiem pret kiberuzbrukumiem, kuri apdraud Savienību vai tās dalībvalstis

PADOMES LĒMUMS (KĀDP) 2026/...

(... gada ...),

ar ko groza Lēmumu (KĀDP) 2019/797 par ierobežojošiem pasākumiem pret kiberuzbrukumiem, kuri apdraud Savienību vai tās dalībvalstis

EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienību un jo īpaši tā 29. pantu,

ņemot vērā Savienības Augstās pārstāves ārlietās un drošības politikas jautājumos priekšlikumu,

tā kā:

(1) Padome 2019. gada 17. maijā pieņēma Lēmumu (KĀDP) 2019/797[1].

(2) Lēmumu (KĀDP) 2019/797 piemēro līdz 2028. gada 18. maijam.

(3) Pamatojoties uz Lēmuma (KĀDP) 2019/797 pielikuma pārskatīšanu, minētā lēmuma 4. un 5. pantā noteikto pasākumu piemērošana minētajā pielikumā uzskaitītajām fiziskajām un juridiskajām personām, vienībām un struktūrām būtu jāpagarina līdz 2027. gada 18. maijam. Turklāt būtu jāatjaunina pamatojumi četru personu un vienas vienības iekļaušanai fizisku un juridisku personu, vienību un struktūru sarakstā, kurām piemēro ierobežojošus pasākumus.

(4) Tādēļ Lēmums (KĀDP) 2019/797 būtu attiecīgi jāgroza,

IR PIEŅĒMUSI ŠO LĒMUMU.

[1] Padomes Lēmums (KĀDP) 2019/797 (2019. gada 17. maijs) par ierobežojošiem pasākumiem pret kiberuzbrukumiem, kuri apdraud Savienību vai tās dalībvalstis (OV L 129I, 17.5.2019., 13. lpp., ELI: http://data.europa.eu/eli/dec/2019/797/oj).

1. pants

Lēmumu (KĀDP) 2019/797 groza šādi:

1) lēmuma 10. pantu aizstāj ar šādu:

"*10. pants*

Šo lēmumu piemēro līdz 2028. gada 18. maijam un pastāvīgi pārskata. Šā lēmuma 4. un 5. pantā noteiktos pasākumus attiecībā uz pielikumā uzskaitītajām fiziskajām un juridiskajām personām, vienībām un struktūrām piemēro līdz 2027. gada 18. maijam.";

2) pielikumu groza saskaņā ar šā lēmuma pielikumu.

2. pants

Šis lēmums stājas spēkā nākamajā dienā pēc tā publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

..., ...

Padomes vārdā –
priekšsēdētājs / priekšsēdētāja

PIELIKUMS

Lēmuma (KĀDP) 2019/797 pielikumu groza šādi:

1) sadaļā "A. Fiziskas personas" 1., 2., 13. un 14. ierakstu aizstāj ar šādiem attiecīgiem ierakstiem:

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
"1.	GAO Qiang	Dzimšanas datums: 1983. gada 4. oktobris Dzimšanas vieta: *Shandong* province, Ķīna Adrese: *Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin,* Ķīna Valstspiederība: Ķīnas Dzimums: vīrietis	*GAO Qiang* ir saistīts ar "*APT10*" ("*Advanced Persistent Threat 10*") jumta grupējumu (jeb "*Red Apollo*", "*CVNX*", "*Stone Panda*", "*MenuPass*" un "*Potassium*"), un viņš ir bijis iesaistīts "*Operation Cloud Hopper*" – virknē kiberuzbrukumu ar būtisku ietekmi, kuru izcelsme ir ārpus Savienības un kuri rada ārēju apdraudējumu Savienībai vai tās dalībvalstīm, un virknē kiberuzbrukumu ar būtisku ietekmi uz trešām valstīm. "*Operation Cloud Hopper*" bija vērsta pret daudznacionālu uzņēmumu informācijas sistēmām, kuri atrodas sešos kontinentos, tostarp to uzņēmumu informācijas sistēmām, kuri atrodas Savienībā, un tās ietvaros neatļauti piekļuva komerciāli sensitīviem datiem, tādējādi radot ievērojamus ekonomiskus zaudējumus. *Gao Qiang* ir saistīts ar *APT10* vadības un kontroles infrastruktūru. Turklāt *Gao Qiang* bija nodarbināts *Huaying Haitai* – uzņēmumā, kuru izmantoja *ATP10* un kurš iekļauts sarakstā, jo sniedza atbalstu "*Operation Cloud Hopper*" un sekmēja to. Viņš ir arī saistīts ar *Zhang Shilong*, kuram ir saiknes ar *APT10* un kuru arī nodarbināja *Huaying Haitai*.	30.7.2020.

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
2.	ZHANG Shilong	Dzimšanas datums: 1981. gada 10. septembris Dzimšanas vieta: Ķīna Adrese: *Hedong, Yuyang Road No 121, Tianjin,* Ķīna Valstspiederība: Ķīnas Dzimums: vīrietis	*Zhang Shilong* ir saistīts ar "*APT10*" ("*Advanced Persistent Threat 10*") jumta grupējumu (jeb "*Red Apollo*", "*CVNX*", "*Stone Panda*", "*MenuPass*" un "*Potassium*"), un viņš ir bijis iesaistīts "*Operation Cloud Hopper*" – virknē kiberuzbrukumu ar būtisku ietekmi, kuru izcelsme ir ārpus Savienības un kuri rada ārēju apdraudējumu Savienībai vai tās dalībvalstīm, un virknē kiberuzbrukumu ar būtisku ietekmi uz trešām valstīm. "*Operation Cloud Hopper*" bija vērsta pret daudznacionālu uzņēmumu informācijas sistēmām, kuri atrodas sešos kontinentos, tostarp to uzņēmumu informācijas sistēmām, kuri atrodas Savienībā, un tās ietvaros neatļauti piekļuva komerciāli sensitīviem datiem, tādējādi radot ievērojamus ekonomiskus zaudējumus. *Zhang Shilong* ir saistīts ar *APT10*, tostarp saistībā ar ļaunprogrammatūru, ko viņš izstrādāja un testēja saistībā ar *APT10* veiktajiem kiberuzbrukumiem. Turklāt *Zhang Shilong* bija nodarbināts *Huaying Haitai* – uzņēmumā, kuru izmantoja *ATP10* un kurš iekļauts sarakstā, jo sniedza atbalstu "*Operation Cloud Hopper*" un sekmēja to. Viņš ir saistīts ar *Gao Qiang*, kuram ir saiknes ar *APT10* un kuru arī nodarbināja *Huaying Haitai*.	30.7.2020.

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
13.	Mikhail Mikhailovich TSAREV	Михаил Михайлович ЦАРЕВ Dzimšanas datums: 20.4.1989. Dzimšanas vieta: *Serpukhov*, Krievijas Federācija Valstspiederība: Krievijas Adrese: *Serpukhov* Dzimums: vīrietis	*Mikhail Mikhailovich TSAREV* piedalījās kiberuzbrukumos ar būtiskām sekām, kas rada ārējus draudus ES dalībvalstīm. *Mikhail Mikhailovich TSAREV*, kurš pazīstams arī ar tiešsaistes iesaukām "*Mango*", "*Alexander Grachev*", "*Super Misha*", "*Ivanov Mixail*", "*Misha Krutysha*" un "*Nikita Andreevich Tsarev*", ir svarīgs dalībnieks ļaunprogrammatūru "*Conti*" un "*Trickbot*" izvēršanā un ir iesaistīts Krievijā bāzētajā apdraudējumu grupējumā "*Wizard Spider*". *Wizard Spider* turpina attīstīties un pastiprināt savas darbības. Ļaunprogrammatūras "*Conti*" un "*Trickbot*" radīja un attīstīja "*Wizard Spider*". "*Wizard Spider*" ir rīkojis izspiedējprogrammatūras kampaņas dažādās nozarēs, tostarp tādos pamatpakalpojumos kā veselības aprūpe un banku joma. Grupa ir inficējusi datorus visā pasaulē, un tās ļaunprogrammatūra ir attīstījusies par augstā mērā modulāru ļaunprogrammatūras kopumu. "*Wizard Spider*" kampaņas, kurās izmanto tādas ļaunprogrammatūras kā, piemēram, "*Conti*", "*Ryuk*", "*TrickBot*" vai "*Black Basta*", ir atbildīgas par būtisku ekonomisko kaitējumu Eiropas Savienībā. Tāpēc *Mikhail Mikhailovich TSAREV* ir iesaistīts kiberuzbrukumos ar būtiskām sekām, kas rada ārējus draudus Savienībai vai tās dalībvalstīm.	24.6.2024.

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
14.	Maksim Sergeevich GALOCHKIN	Максим Сергеевич ГАЛОЧКИН Dzimšanas datums: 19.5.1982. Dzimšanas vieta: *Abakan*, Krievijas Federācija Valstspiederība: Krievijas Dzimums: vīrietis	*Maksim Galochkin* piedalījās kiberuzbrukumos ar būtiskām sekām, kas rada ārējus draudus ES dalībvalstīm. *Maksim Galochkin* ir pazīstams arī ar tiešsaistes iesaukām "*Benalen*", "*Bentley*", "*Volhvb*", "*volhvb*", "*manuel*", "*Max17*" un "*Crypt*". *Galochkin* ir svarīgs dalībnieks ļaunprogrammatūru "*Conti*" un "*Trickbot*" izvēršanā un ir iesaistīts Krievijā bāzētajā apdraudējumu grupējumā "*Wizard Spider*". Viņš ir vadījis testētāju grupu, būdams atbildīgs par "*Wizard Spider*" izstrādātās un ieviestās ļaunprogrammatūras "*TrickBot*" testu izstrādi, uzraudzību un īstenošanu. *Wizard Spider* turpina attīstīties un pastiprināt savas darbības. "*Wizard Spider*" ir rīkojis izspiedējprogrammatūras kampaņas dažādās nozarēs, tostarp tādos pamatpakalpojumos kā veselības aprūpe un banku joma. Grupa ir inficējusi datorus visā pasaulē, un tās ļaunprogrammatūra ir attīstījusies par augstā mērā modulāru ļaunprogrammatūras kopumu. "*Wizard Spider*" kampaņas, kurās izmanto tādas ļaunprogrammatūras kā, piemēram, "*Conti*", "*Ryuk*", "*TrickBot*" vai "*Black Basta*", ir atbildīgas par būtisku ekonomisko kaitējumu Eiropas Savienībā. Tāpēc *Maksim Galochkin* ir iesaistīts kiberuzbrukumos ar būtiskām sekām, kas rada ārējus draudus Savienībai vai tās dalībvalstīm.	24.6.2024.”;

2) sadaļā “B. Juridiskas personas, vienības un struktūras” 1. ierakstu aizstāj ar šādu:

	Nosaukums	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
“1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	jeb: Haitai Technology Development Co. Ltd Vieta: *Tianjin*, Ķīna	*Huaying Haitai* sniedza finansiālu, tehnisku vai materiālu atbalstu “*Operation Cloud Hopper*” – virknei kiberuzbrukumu ar būtisku ietekmi, kuru izcelsme ir ārpus Savienības un kuri rada ārēju apdraudējumu Savienībai vai tās dalībvalstīm, un virknei kiberuzbrukumu ar būtisku ietekmi uz trešām valstīm – un sekmēja to. “*Operation Cloud Hopper*” bija vērsta pret daudznacionālu uzņēmumu informācijas sistēmām, kuri atrodas sešos kontinentos, tostarp to uzņēmumu informācijas sistēmām, kuri atrodas Savienībā, un tās ietvaros neatļauti piekļuva komerciāli sensitīviem datiem, tādējādi radot ievērojamus ekonomiskus zaudējumus. “*Operation Cloud Hopper*” veica aktors, kas publiski zināms kā “*APT10*” (“*Advanced Persistent Threat 10*”) (jeb “*Red Apollo*”, “*CVNX*”, “*Stone Panda*”, “*MenuPass*” un “*Potassium*”). *Huaying Haitai* var būt saistīts ar *APT10*. Turklāt *Huaying Haitai* nodarbināja *Gao Qiang* un *Zhang Shilong*, kuri abi ir iekļauti sarakstā saistībā ar “*Operation Cloud Hopper*”. Tāpēc *Huaying Haitai* ir arī saistīts ar *Gao Qiang* un *Zhang Shilong*.	30.7.2020.”.