2026/1078

12.5.2026.

PADOMES ĪSTENOŠANAS REGULA (ES) 2026/1078

(2026. gada 11. maijs),

ar ko īsteno Regulu (ES) 2019/796 par ierobežojošiem pasākumiem pret kiberuzbrukumiem, kuri apdraud Savienību vai tās dalībvalstis

EIROPAS SAVIENĪBAS PADOME,

ņemot vērā Līgumu par Eiropas Savienības darbību,

ņemot vērā Padomes Regulu (ES) 2019/796 (2019. gada 17. maijs) par ierobežojošiem pasākumiem pret kiberuzbrukumiem, kuri apdraud Savienību vai tās dalībvalstis [1], un jo īpaši tās 13. pantu,

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

tā kā:

(1) Padome 2019. gada 17. maijā pieņēma Regulu (ES) 2019/796.

(2) Padome ir pārskatījusi Regulas (ES) 2019/796 I pielikumā iekļauto fizisko un juridisko personu, vienību un struktūru sarakstu. Pamatojoties uz minēto pārskatīšanu, būtu jāatjaunina pamatojumi četru personu un vienas vienības iekļaušanai fizisku un juridisku personu, vienību un struktūru sarakstā, kurām piemēro ierobežojošus pasākumus.

(3) Tādēļ Regulas (ES) 2019/796 I pielikums būtu attiecīgi jāgroza,

IR PIEŅĒMUSI ŠO REGULU.

1. pants

Regulas (ES) 2019/796 I pielikumu groza saskaņā ar šīs regulas pielikumu.

2. pants

Šī regula stājas spēkā nākamajā dienā pēc tās publicēšanas *Eiropas Savienības Oficiālajā Vēstnesī*.

Šī regula uzliek saistības kopumā un ir tieši piemērojama visās dalībvalstīs.

Briselē, 2026. gada 11. maijā

Padomes vārdā –

priekšsēdētāja

K. KALLAS

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

PIELIKUMS

Regulas (ES) 2019/796 I 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.

ELI: http://data.europa.eu/eli/reg_impl/2026/1078/oj

	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.”