



2024/1779

24.6.2024.

PADOMES LĒMUMS (KĀDP) 2024/1779

(2024. gada 24. jūnijs),

**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 Augstā pārstāvja ārlietās un drošības politikas jautājumos priekšlikumu,

tā kā:

- (1) Padome 2019. gada 17. maijā pieņēma Lēmumu (KĀDP) 2019/797 par ierobežojošiem pasākumiem pret kiberuzbrukumiem, kuri apdraud Savienību vai tās dalībvalstis ⁽¹⁾.
- (2) Mērķtiecīgi ierobežojoši pasākumi pret kiberuzbrukumiem ar būtisku ietekmi, kuri ir ārējs apdraudējums Savienībai vai tās dalībvalstīm, ir viens no pasākumiem, kas iekļauti Savienības satvarā vienotai diplomātiskajai reakcijai uz ļaunprātīgām kiberdarbībām (kiberdiplomātijas rīkkopa), un ir vitāli svarīgs instruments, lai novērstu un nepieļautu šādas darbības, no tām atturētu un reaģētu uz tām.
- (3) Ļaunprātīgas kiberdarbības pret kritisko infrastruktūru vai pamatpakalpojumiem, tostarp izmantojot izspiedējprogrammatūru un dzēšanas ļaunprogrammatūru (*wipers*), vēršanās pret piegādes ķēdēm un kiberspiegošana, tostarp intelektuālā īpašuma zādzības, šobrīd pieaug skaita, biežuma un sarežģītības ziņā. Šīs darbības ar savu graužošu un destruktīvo ietekmi rada sistēmiskus draudus Savienības drošībai, ekonomikai, demokrātijai un sabiedrībai kopumā.
- (4) Tādu kiberoperāciju izmantošana, kas ir ļāvušas īstenot neprovocēto un nepamatoto Krievijas agresijas karu pret Ukrainu un kas ir norisinājušās līdztekus tam, ietekmē globālo stabilitāti un drošību, ir nozīmīgs eskalācijas risks un vēl vairāk papildina jau tā nopietno pēdējos gados vērojamo ļaunprātīgu kiberdarbību skaita pieaugumu ārpus bruņota konflikta. Pieaugošie kiberdrošības riski un kopumā sarežģītā kiberdraudu aina, kurā pastāv nepārprotams risks, ka kiberincidenti varētu strauji izplatīties no vienas dalībvalsts uz citām un no trešām valstīm uz Savienību, ir vēl viens iemesls īstenot ierobežojošus pasākumus saskaņā ar Lēmumu (KĀDP) 2019/797.
- (5) Kā daļu no noturīgas, pielāgotas un koordinētas Savienības darbības pret pastāvīgiem kiberdraudu aktoriem Lēmuma (KĀDP) 2019/797 pielikumā ietvertajā to fizisko un juridisko personu, vienību un struktūru sarakstā, kurām piemēro ierobežojošus pasākumus, būtu jāiekļauj sešas fiziskas personas. Minētās personas ir atbildīgas vai bija iesaistītas kiberuzbrukumos ar būtisku ietekmi, kas rada ārējus draudus Savienībai vai tās dalībvalstīm.
- (6) Tādēļ Lēmums (KĀDP) 2019/797 būtu attiecīgi jāgroza,

IR PIEŅĒMUSI ŠO LĒMUMU.

1. pants

Lēmuma (KĀDP) 2019/797 pielikumu groza tā, kā noteikts šā lēmuma pielikumā.

2. pants

Šis lēmums stājas spēkā dienā, kad to publicē *Eiropas Savienības Oficiālajā Vēstnesī*.

Luksemburgā, 2024. gada 24. jūnijā

Padomes vārdā –

priekšsēdētājs

J. BORRELL FONTELLES

⁽¹⁾ Padomes Lēmums (KĀDP) 2019/797 (2019. gada 17. maijs) par ierobežojošiem pasākumiem pret kiberuzbrukumiem, kuri apdraud Savienību vai tās dalībvalstis (OV L 129 I, 17.5.2019., 13. lpp.).

PIELIKUMS

Lēmuma (KĀDP) 2019/797 pielikuma iedaļā "A. Fiziskas personas" pievieno šādus ierakstus:

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
"9.	Ruslan Aleksandrovich PERETYATKO	Руслан Александрович ПЕРЕТЯТЬКО Dzimšanas datums: 3.8.1985. Valstspiederība: Krievijas Dzimums: vīrietis	<i>Ruslan PERETYATKO</i> piedalījās kiberuzbrukumos ar būtiskām sekām, kas rada ārējus draudus Savienībai vai tās dalībvalstīm. <i>Ruslan PERETYATKO</i> ir dalībnieks Krievijas militārās izlūkošanas virsnieku grupā "Callisto", kas veic kiberoperācijas pret ES dalībvalstīm un trešām valstīm. "Callisto" grupa (jeb "Seaborgium", "Star Blizzard", "ColdRiver", "TA446") ir sākusi daudzgadējas pikšķerēšanas kampaņas, ko izmanto, lai zagtu kontu informāciju un datus. Turklāt "Callisto" grupa ir atbildīga par kampaņām, kas vērstas pret indivīdiem un kritiski svarīgām valsts funkcijām, tostarp aizsardzības un ārējo attiecību jomā. Tāpēc <i>Ruslan PERETYATKO</i> ir iesaistīts kiberuzbrukumos ar būtiskām sekām, kas rada ārējus draudus Savienībai vai tās dalībvalstīm.	24.6.2024.
10.	Andrey Stanislavovich KORINETS	Андрей Станиславович КОРИНЕЦ Dzimšanas datums: 18.5.1987. Dzimšanas vieta: Сыктывкар, Krievija Valstspiederība: Krievijas Dzimums: vīrietis	<i>Andrey Stanislavovich KORINETS</i> piedalījās kiberuzbrukumos ar būtiskām sekām, kas rada ārējus draudus Savienībai vai tās dalībvalstīm. <i>Andrey Stanislavovich KORINETS</i> ir Krievijas Federācijas Federālā drošības dienesta (FSB) "18. centra" virsnieks. <i>Andrey Stanislavovich KORINETS</i> ir dalībnieks Krievijas militārās izlūkošanas virsnieku grupā "Callisto", kas veic kiberoperācijas pret ES dalībvalstīm un trešām valstīm. "Callisto" grupa (jeb "Seaborgium", "Star Blizzard", "ColdRiver", "TA446") ir sākusi daudzgadējas pikšķerēšanas kampaņas, ko izmanto, lai zagtu kontu informāciju un datus. Turklāt "Callisto" grupa ir atbildīga par kampaņām, kas vērstas pret indivīdiem un kritiski svarīgām valsts funkcijām, tostarp aizsardzības un ārējo attiecību jomā. Tāpēc <i>Andrey Stanislavovich KORINETS</i> ir iesaistīts kiberuzbrukumos ar būtiskām sekām, kas rada ārējus draudus Savienībai vai tās dalībvalstīm.	24.6.2024.

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
11.	Oleksandr SKLIANKO	Александр СКЛЯНКО (rakstība krievu valodā) Олександр СКЛЯНКО (rakstība ukraiņu valodā) Dzimšanas datums: 5.8.1973. Pase: EC 867868, izdota 27.11.1998. (Ukraina) Dzimums: vīrietis	<i>Oleksandr SKLIANKO</i> piedalījās kiberuzbrukumos ar būtisku ietekmi uz ES dalībvalstīm, kā arī kiberuzbrukumos ar būtisku ietekmi uz trešām valstīm. <i>Oleksandr SKLIANKO</i> ir dalībnieks hakeru grupā “ <i>Armageddon</i> ”, kuru atbalsta Krievijas Federācijas Federālais drošības dienests (FSB) un kura veica dažādus kiberuzbrukumus ar būtisku ietekmi uz Ukrainas valdību, ES dalībvalstīm un to valdības amatpersonām, tostarp, izmantojot pikšķerēšanas e-pastus un ļaunatūras kampaņas. Tāpēc <i>Oleksandr SKLIANKO</i> ir iesaistīts kiberuzbrukumos ar būtisku ietekmi pret trešām valstīm, kā arī kiberuzbrukumos ar būtisku ietekmi, kas rada ārējus draudus Savienībai vai tās dalībvalstīm.	24.6.2024.
12.	Микола CHERNYKH	Николай ЧЕРНЫХ (rakstība krievu valodā) Микола ЧЕРНИХ (rakstība ukraiņu valodā) Dzimšanas datums: 12.10.1978. Pase: EC 922162, izdota 20.1.1999. (Ukraina) Dzimums: vīrietis	<i>Микола CHERNYKH</i> piedalījās kiberuzbrukumos ar būtisku ietekmi uz ES dalībvalstīm, kā arī kiberuzbrukumos ar būtisku ietekmi uz trešām valstīm. <i>Микола CHERNYKH</i> ir dalībnieks hakeru grupā “ <i>Armageddon</i> ”, kuru atbalsta Krievijas Federācijas Federālais drošības dienests (FSB) un kura veica dažādus kiberuzbrukumus ar būtisku ietekmi uz Ukrainas valdību, ES dalībvalstīm un to valdības amatpersonām, tostarp, izmantojot pikšķerēšanas e-pastus un ļaunatūras kampaņas. Būdam bijušais Ukrainas Drošības dienesta darbinieks, viņš Ukrainā ir apsūdzēts par nodevību un neatļautu iejaukšanos elektronisko datu nodošanas iekārtu un automatizēto sistēmu darbībā. Tāpēc <i>Микола CHERNYKH</i> ir iesaistīts kiberuzbrukumos ar būtiskām sekām, kas rada ārējus draudus Savienībai vai tās dalībvalstīm.	24.6.2024.

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
13.	Mikhail Mikhailovich TSAREV	<p>Михаил Михайлович ЦАРЕВ</p> <p>Dzimšanas datums: 20.4.1989.</p> <p>Dzimšanas vieta: <i>Serpukhov</i>, Krievijas Federācija</p> <p>Valstspiederība: Krievijas</p> <p>Adrese: <i>Serpukhov</i></p> <p>Dzimums: vīrietis</p>	<p><i>Mikhail Mikhailovich TSAREV</i> piedalījās kiberuzbrukumos ar būtiskām sekām, kas rada ārējus draudus Savienībai vai tās dalībvalstīm.</p> <p><i>Mikhail Mikhailovich TSAREV</i>, kurš pazīstams arī ar tiešsaistes iesaukām “Mango”, “Alexander Grachev”, “Super Misha”, “Ivanov Mixail”, “Misha Krutysha” un “Nikita Andreevich Tsarev”, ir svarīgs dalībnieks ļaunprogrammatūras “Conti” un “Trickbot” izvēršanā un ir iesaistīts Krievijā bāzētajā apdraudējumu grupējumā “Wizard Spider”.</p> <p>Ļaunprogrammatūru “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 tādus ļaunprogrammatūras veidus kā “Conti”, “Ryuk” un “TrickBot”, ir atbildīgas par būtisku ekonomisko kaitējumu Eiropas Savienībā.</p> <p>Tāpēc <i>Mikhail Mikhailovich TSAREV</i> ir iesaistīts kiberuzbrukumos ar būtiskām sekām, kas rada ārējus draudus Savienībai vai tās dalībvalstīm.</p>	24.6.2024.

	Vārds	Identifikācijas informācija	Pamatojums	Sarakstā iekļaušanas datums
14.	Maksim Sergeevich GALOCHKIN	<p>Максим Сергеевич ГАЛОЧКИН</p> <p>Dzimšanas datums: 19.5.1982.</p> <p>Dzimšanas vieta: <i>Abakan</i>, Krievijas Federācija</p> <p>Valstspiederība: Krievijas</p> <p>Dzimums: vīrietis</p>	<p><i>Maksim Galochkin</i> piedalījās kiberuzbrukumos ar būtiskām sekām, kas rada ārējus draudus Savienībai vai tās dalībvalstīm.</p> <p><i>Maksim Galochkin</i> ir pazīstams arī ar tiešsaistes iesaukām “<i>Benalen</i>”, “<i>Bentley</i>”, “<i>Volhvb</i>”, “<i>volhvb</i>”, “<i>manuel</i>”, “<i>Max17</i>” un “<i>Crypt</i>”. <i>Galochkin</i> ir svarīgs dalībnieks ļaunprogrammatūras “<i>Conti</i>” un “<i>Trickbot</i>” izvēršanā un ir iesaistīts Krievijā bāzētajā apdraudējumu grupējumā “<i>Wizard Spider</i>”. Viņš ir vadījis testētāju grupu, būdams atbildīgs par “<i>Wizard Spider</i>” izstrādātās spieģprogrammatūras “<i>TrickBot</i>” testu izstrādi, uzraudzību un īstenošanu.</p> <p>“<i>Wizard Spider</i>” 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. “<i>Wizard Spider</i>” kampaņas, kurās izmanto tādas ļaunprogrammatūras veidus kā “<i>Conti</i>”, “<i>Ryuk</i>” un “<i>TrickBot</i>”, ir atbildīgas par būtisku ekonomisko kaitējumu Eiropas Savienībā.</p> <p>Tāpēc <i>Maksim Galochkin</i> ir iesaistīts kiberuzbrukumos ar būtiskām sekām, kas rada ārējus draudus Savienībai vai tās dalībvalstīm.</p>	24.6.2024.”