2026/1714

2026 7 13

TARYBOS ĮGYVENDINIMO REGLAMENTAS (ES) 2026/1714

2026 m. liepos 13 d.

kuriuo įgyvendinamas Reglamentas (ES) 2019/796 dėl ribojamųjų priemonių, skirtų kovai su kibernetiniais išpuoliais, keliančiais grėsmę Sąjungai arba jos valstybėms narėms

EUROPOS SĄJUNGOS TARYBA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2019 m. gegužės 17 d. Tarybos reglamentą (ES) 2019/796 dėl ribojamųjų priemonių, skirtų kovai su kibernetiniais išpuoliais, keliančiais grėsmę Sąjungai arba jos valstybėms narėms ([1]), ypač į jo 13 straipsnio 1 dalį,

atsižvelgdama į Sąjungos vyriausiojo įgaliotinio užsienio reikalams ir saugumo politikai pasiūlymą,

kadangi:

(1) 2019 m. gegužės 17 d. Taryba priėmė Reglamentą (ES) 2019/796;

(2) vykdant ilgalaikius, pritaikytus ir koordinuojamus Sąjungos veiksmus prieš tęstinių kibernetinių grėsmių subjektus, į Reglamento (ES) 2019/796 I priede pateiktą fizinių ir juridinių asmenų, subjektų ir organizacijų, kuriems taikomos ribojamosios priemonės, sąrašą turėtų būti įtraukti aštuoni fiziniai asmenys ir keturi subjektai. Tie asmenys ir subjektai yra atsakingi už reikšmingo poveikio kibernetinius išpuolius, keliančius išorės grėsmę Sąjungai ar jos valstybėms narėms, arba dalyvauja juos vykdant;

(3) todėl Reglamento (ES) 2019/796 I priedas turėtų būti atitinkamai iš dalies pakeistas,

PRIĖMĖ ŠĮ REGLAMENTĄ:

1 straipsnis

Reglamento (ES) 2019/796 I priedas iš dalies keičiamas pagal šio reglamento priedą.

2 straipsnis

Šis reglamentas įsigalioja jo paskelbimo *Europos Sąjungos oficialiajame leidinyje* dieną.

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje 2026 m. liepos 13 d.

Tarybos vardu

Pirmininkė

K. KALLAS

([1]) OL L 129 I, 2019 5 17, p. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj.

PRIEDAS

Reglamento (ES) 2019/796 I priedas iš dalies keičiamas taip:

1) antraštinė dalis „A. Fiziniai asmenys“ papildoma šiais įrašais:

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
„20.	Vitaly Nikolayevich KOVALEV	Виталий Николаевич КОВАЛЕВ Dar žinomas kaip: „Bentley“, „Bergen“, „Alex Konor“, „Benny“, „Ben“, „Stern“ Gimimo data: 1988 6 23 Adresas: Serebristy Bulvar 34 (Serebristyy Bul'var); krp 1; flt 528; 197341; St Petersburg, Russian Federation Pilietybė: Rusijos Lytis: vyras Susiję subjektai: TrickBot, Wizard Spider, Conti	Vitaly Kovalev yra vyresniąsias pareigas einantis asmuo, kiek tai susiję su kenkimo programine įranga „Trickbot“ ir „Conti“. Jis taip pat žinomas internetiniais slapyvardžiais „Bentley“, „Bergen“, „Alex Konor“, „Benny“, „Ben“ ir „Stern“. Iš pradžių kenkimo programinę įrangą „Conti“ ir „Trickbot“ kūrė ir plėtojo „Wizard Spider“. „Wizard Spider“ vykdė išpirkos reikalavimo programinės įrangos kampanijas įvairiuose sektoriuose, įskaitant esmines paslaugas, pavyzdžiui, sveikatos ir bankininkystės, užkrėtė kompiuterius visame pasaulyje, o jų kenkimo programinė įranga buvo išplėtota iki itin modulinio pobūdžio kenkimo programinės įrangos rinkinio. Kampanijos „Wizard Spider“, vykdomos naudojant tokią kenkimo programinę įrangą kaip „Conti“ ir „TrickBot“, daro esminę ekonominę žalą Europos Sąjungoje. Taigi, Vitaly Kovalev yra atsakingas už reikšmingo poveikio kibernetinius išpuolius, keliančius išorės grėsmę Sąjungai arba jos valstybėms narėms, ir dalyvauja juos vykdant.	2026 7 13

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
21.	Alexander Alexandrovich VOLOSOVIK	Александр Александрович ВОЛОСОВИК Gimimo data: 1983 1 30 Gimimo vieta: TSRS Pilietybė: Rusijos Paso numeris: 762988138 Lytis: vyras Susiję subjektai: Yalishanda, LARVA-34, podzemniyl, Ohyeahhellno, Stas_vl, downlow	Alexander Volosovik yra „Media Land LLC“ savininkas. Nuo 2016 m. nepramušamos prieglobos paslaugų teikėja „Media Land LLC“ sudaro palankesnes sąlygas įvairiems kenkimo programinės įrangos išpuoliams tiek Sąjungai, tiek visame pasaulyje, teikdama prieglobos paslaugas, kuriomis slepiamos naudotojų tapatybės ir priešinamasi teisėsaugos institucijų vykdomam turinio šalinimui. „Media Land LLC“ sudarė galimybes didelio masto išpirkos reikalavimo programinės įrangos operacijoms, vadovavimo ir kontrolės paslaugoms ir duomenų viliojimo operacijoms, nukreiptoms į ypatingos svarbos infrastruktūrą ir esmines paslaugas valstybėse narėse, – dėl to patirta reikšmingų finansinių nuostolių. Operacijos, kurioms „Media Land LLC“ sudarė palankesnes sąlygas, yra, *inter alia*, „LockBit“, „EvilCorp“ ir „BlackBasta“. Taigi, „Media Land LLC“ dalyvauja reikšmingą poveikį darančiuose kibernetiniuose išpuoliuose, kurie kelia išorės grėsmę Sąjungai arba jos valstybėms narėms. Kaip „Media Land LLC“ savininkas, Alexander Volosovik yra atsakingas už tuos kibernetinius išpuolius ir dalyvauja juos vykdant. Jis taip pat yra susijęs su „Media Land LLC“.	2026 7 13

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
22.	Denis Olegovich DEGTYARENKO	Денис Олегович ДЕГТЯРЕНКО Dar žinomas kaip: „Dena“ Gimimo data: 1989 10 9 Gimimo vieta: TSRS Pilietybė: Rusijos Lytis: vyras Adresas: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation	Denis Degtyarenko, dar žinomas kaip Dena, yra įsilaužėlis iš Rusijos, atstovaujantis CARR („Cyber Army of Russia Reborn“). CARR yra atsakinga už kibernetinius išpuolius prieš paslaugas, kurios būtinos esminei ekonominei veiklai ir ypatingos svarbos valstybės funkcijoms valstybėse narėse palaikyti, taip pat prieš infrastruktūrą Ukrainoje ir kitose trečiosiose valstybėse. CARR yra susijusi su Rusijos Federacijos ginkluotųjų pajėgų generalinio štabo vyriausiosios valdybos (GRU) Pagrindiniu specialiųjų technologijų centru (GTsST). GTsST toliau aktyviai vykdo kibernetinius išpuolius prieš Sąjungą ar jos valstybes nares. CARR taikiniai, be kita ko, yra vyriausybinės agentūros, finansų įstaigos, žiniasklaidos priemonės ir ypatingos svarbos infrastruktūra valstybėse narėse bei Jungtinėse Amerikos Valstijose. CARR vykdė paskirstytas paslaugos trikdymo (distributed denial-of-service, DDoS) atakas Ukrainoje ir prieš vyriausybes bei įmones, įsikūrusias šalyse, kurios rėmė Ukrainą. Taigi, Denis Degtyarenko, pagrindinis CARR įsilaužėlis, dalyvauja vykdant reikšmingo poveikio kibernetinius išpuolius, įskaitant pasikėsinimus įvykdyti potencialiai reikšmingo poveikio kibernetinius išpuolius, kurie kelia išorės grėsmę valstybėms narėms, taip pat trečiosioms valstybėms. Kaip CARR narys, jis taip pat yra susijęs su GTsST.	2026 7 13

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
23.	Yuliya Vladimirovna PANKRATOVA	Юлия Владимировна ПАНКРАТОВА Dar žinoma kaip: „YUliYA“ Gimimo data: 1984 4 6 Gimimo vieta: TSRS Pilietybė: Rusijos Lytis: moteris Adresas: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation	Yuliya Pankratova yra įsilaužėlė iš Rusijos, dirbusi CARR („Cyber Army of Russia Reborn“), įsteigė „Z-Pentest“ ir toliau ten dirba. CARR yra atsakinga už kibernetinius išpuolius prieš paslaugas, kurios būtinos esminei ekonominei veiklai ir ypatingos svarbos valstybės funkcijoms valstybėse narėse palaikyti, taip pat prieš infrastruktūrą Ukrainoje ir kitose trečiosiose valstybėse. CARR yra susijusi su Rusijos Federacijos ginkluotųjų pajėgų generalinio štabo vyriausiosios valdybos (GRU) Pagrindiniu specialiųjų technologijų centru (GTsST). GTsST toliau aktyviai vykdo kibernetinius išpuolius prieš Sąjungą ar jos valstybes nares. CARR taikiniai, be kita ko, yra vyriausybinės agentūros, finansų įstaigos, žiniasklaidos priemonės ir ypatingos svarbos infrastruktūra valstybėse narėse ir Jungtinėse Amerikos Valstijose. CARR vykdė paskirstytas paslaugos trikdymo (distributed denial-of-service, DDoS) atakas Ukrainoje ir prieš vyriausybes bei įmones, įsikūrusias šalyse, kurios rėmė Ukrainą. „Z-Pentest“ yra atsakinga už kibernetinius išpuolius, darančius reikšmingą poveikį, *inter alia*, paslaugoms, būtinoms esminei veiklai valstybėse narėse palaikyti. Taigi, Yuliya Pankratova, pagrindinė įsilaužėlė CARR ir „Z-Pentest“, dalyvauja vykdant reikšmingo poveikio kibernetinius išpuolius, įskaitant pasikėsinimus įvykdyti potencialiai reikšmingo poveikio kibernetinius išpuolius, kurie kelia išorės grėsmę valstybėms narėms, taip pat trečiosioms valstybėms. Ji taip pat yra susijusi su „Z-Pentest“.	2026 7 13

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
24.	Maksim Evgenevich VORONIN	Максим Евгеньевич ВОРОНИН Dar žinomas kaip: „Daugn0“ Pilietybė: įtariama, Rusijos Lytis: vyras	Maksim Voronin, dar žinomas kaip „Daugn0“, dalyvauja kuriant, platinant ir parduodant informaciją vagiančią kenkimo programinę įrangą „LummaC2“ (dar žinomą kaip „Lumma Infostealer“, „Lumma Stealer“). „LummaC2“ yra paslauginės kenkimo programinės įrangos (MaaS) platforma, naudojama neskelbtiniems duomenims, naršyklės prisijungimo duomenims, kriptovaliutų piniginėms ar sistemos informacijai pavogti, papildomai kenkimo programinei įrangai įdiegti užkrėstuose įrenginiuose, kriptovaliutų vagystėms ir šnipinėjimo kampanijoms. Kibernetinius išpuolius, kuriuose naudojama kenkimo programinė įranga „LummaC2“, vykdo ir finansiškai motyvuoti kibernetines grėsmes keliantys subjektai, pavyzdžiui, „Storm-113“, „Storm-1607“, „Storm-1674“, „Octo Tempest“ ir kiti. Kenkimo programinė įranga „LummaC2“ buvo naudojama kibernetiniams išpuoliams prieš ypatingos svarbos valstybės funkcijas ir paslaugas, būtinas esminei valstybių narių socialinei ir ekonominei veiklai palaikyti. 2024 m. ir 2025 m. „LummaC2“ buvo viena iš dažniausiai naudojamų informacijos vagystės priemonių visame pasaulyje. Taigi, Maksim Voronin, kaip „LummaC2“ kūrėjas, platintojas ir pardavėjas, dalyvauja reikšmingą poveikį darančiuose kibernetiniuose išpuoliuose, kurie kelia išorės grėsmę valstybėms narėms, ir padeda juos vykdyti.	2026 7 13

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
25.	Maksim Aleksandrovich GORDIENKO Dar žinomas kaip: Maxim Alexandrovich GORDIENKO	Максим Александрович ГОРДИЕНКО Dar žinomas kaip: „Lummaseller“ Pilietybė: įtariama, Rusijos Lytis: vyras	Maksim Gordienko, dar žinomas kaip „Lummaseller“, dalyvauja kuriant ir platinant informaciją vagiančią kenkimo programinę įrangą „LummaC2“ (dar žinomą kaip „Lumma Infostealer“, „Lumma Stealer“). „LummaC2“ yra paslauginės kenkimo programinės įrangos (MaaS) platforma, naudojama neskelbtiniems duomenims, naršyklės prisijungimo duomenims, kriptovaliutų piniginėms ar sistemos informacijai pavogti, papildomai kenkimo programinei įrangai įdiegti užkrėstuose įrenginiuose, kriptovaliutų vagystėms ir šnipinėjimo kampanijoms. Kibernetinius išpuolius, kuriuose naudojama kenkimo programinė įranga „LummaC2“, vykdo ir finansiškai motyvuoti kibernetines grėsmes keliantys subjektai, pavyzdžiui, „Storm-113“, „Storm-1607“, „Storm-1674“, „Octo Tempest“ ir kiti. Kenkimo programinė įranga „LummaC2“ buvo naudojama kibernetiniams išpuoliams prieš ypatingos svarbos valstybės funkcijas ir paslaugas, būtinas esminei valstybių narių socialinei ir ekonominei veiklai palaikyti. 2024 m. ir 2025 m. „LummaC2“ buvo viena iš dažniausiai naudojamų informacijos vagystės priemonių visame pasaulyje. Taigi, Maksim Gordienko, kaip „LummaC2“ kūrėjas, platintojas ir pardavėjas, dalyvauja reikšmingą poveikį darančiuose kibernetiniuose išpuoliuose, kurie kelia išorės grėsmę valstybėms narėms, ir padeda juos vykdyti.	2026 7 13

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
26.	Evgeniy Viktorovich BASHEV	Евгений Викторович БАШЕВ Gimimo data: 1980 1 25 Gimimo vieta: TSRS Pilietybė: Rusijos Lytis: vyras Susiję asmenys: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin Susiję subjektai: GRU padalinys Nr. 29155, „Impuls“ LLC	Evgeniy Bashev yra Rusijos karinės žvalgybos agentūros GRU padalinio Nr. 29155 narys. Šiame padalinyje jis remia ir palengvina kibernetinius išpuolius, darančius reikšmingą poveikį valstybėms narėms, *inter alia*, kontroliuodamas įsilaužimo operacijoms naudojamą serverį „Aegon“. Visų pirma jis teikia techninę ir materialinę paramą GRU padalinio Nr. 29155 kibernetiniams išpuoliams per savo bendrovę „Impuls“ LLC, kuri sudarė palankesnes sąlygas operacinei priedangai, infrastruktūrai ir mokėjimams, taip pat jis valdė techninius išteklius, įskaitant serverius, kurie naudojami kibernetiniams išpuoliams. Be to, jis koordinavo GRU struktūrų ir įsilaužėlių iš išorės tinklų bendradarbiavimą. Kibernetiniai išpuoliai, kurių vykdymą jis palengvino, buvo nukreipti į ypatingos svarbos valstybės funkcijų sistemas ir paslaugas, būtinas esminei socialinei ar ekonominei veiklai valstybėse narėse, visų pirma transporto sektoriuje, palaikyti. Per kampaniją „WhisperGate“ GRU padalinys Nr. 29155 taip pat taikėsi į Ukrainos ypatingos svarbos infrastruktūrą. Taigi, Evgeniy Bashev teikia techninę ir materialinę paramą reikšmingą poveikį turintiems kibernetiniams išpuoliams, įskaitant pasikėsinimus įvykdyti reikšmingą poveikį galinčius turėti kibernetinius išpuolius, keliančius išorės grėsmę valstybėms narėms, taip pat reikšmingą poveikį trečiajai valstybei darantiems kibernetiniams išpuoliams, arba kitaip dalyvauja juos vykdant. Kaip savininkas ir generalinis direktorius jis yra susijęs su bendrove „Impuls“ LLC. Kaip GRU padalinio Nr. 29155 narys, jis taip pat yra susijęs su šiuo subjektu.	2026 7 13

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
27.	Roman Alexandrovich PUNTUS	Роман Александрович ПУНТУС Gimimo vieta: Rusijos Federacija Pilietybė: Rusijos Lytis: vyras Susiję asmenys: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin, Evgeniy Viktorovich Bashev Susiję subjektai: GRU padalinys Nr. 29155	Roman Puntus yra Rusijos karinės žvalgybos agentūros GRU padalinio Nr. 29155 narys. Tame padalinyje jis atlieka vadovaujamą vaidmenį organizuojant ir koordinuojant kibernetinius išpuolius, darančius reikšmingą poveikį valstybėms narėms. Jis taip pat remia padalinio vidaus kibernetinių pajėgumų plėtojimą, įskaitant darbuotojų, pavyzdžiui, įsilaužėlių ir programuotojų, įdarbinimą ir priežiūrą. Įsteigdamas priedangos įmonę „Aegeon-Impulse“, jis sudarė palankesnes sąlygas kibernetinių operacijų logistiniams ir finansiniams aspektams. Padalinys, jam koordinuojant veiksmus, vykdė kibernetinius išpuolius, nukreiptus į ypatingos svarbos valstybės funkcijų sistemas ir paslaugas, būtinas esminei socialinei ar ekonominei veiklai valstybėse narėse, visų pirma transporto sektoriuje, palaikyti. Per kampaniją „WhisperGate“ GRU padalinys Nr. 29155 taip pat taikėsi į Ukrainos ypatingos svarbos infrastruktūrą. Taigi, Roman Puntus yra atsakingas už reikšmingą poveikį turinčius kibernetinius išpuolius, įskaitant pasikėsinimus įvykdyti reikšmingą poveikį galinčius turėti kibernetinius išpuolius, keliančius išorės grėsmę valstybėms narėms, taip pat reikšmingą poveikį trečiajai valstybei darančius kibernetinius išpuolius, arba kitaip dalyvauja juos vykdant. Kaip GRU padalinio Nr. 29155 narys, jis taip pat yra susijęs su šiuo subjektu.	2026 7 13“

2) antraštinė dalis „B. Juridiniai asmenys, subjektai ir organizacijos“ papildoma šiais įrašais:

	Pavadinimas	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
„8.	Media Land LLC	Adresas: Tsvetnochnaya st., 16 Litera P, Room 27, Moskovskaya Zastava Municipal District St Petersburg, 196006, Russian Federation Subjekto rūšis: ribotos atsakomybės bendrovė Registracijos vieta: Sankt Peterburgas Registracijos data: 2015 10 19 Registracijos numeris: 1152536009900 Pagrindinė veiklos vykdymo vieta: Sankt Peterburgas, Rusijos Federacija Susijęs subjektas: ML.Cloud	Nuo 2016 m. nepramušamos prieglobos paslaugų teikėja „Media Land LLC“ sudaro palankesnes sąlygas įvairiems kenkimo programinės įrangos išpuoliams tiek valstybėse narėse, tiek visame pasaulyje, teikdama prieglobos paslaugas, kuriomis slepiamos naudotojų tapatybės ir priešinamasi teisėsaugos institucijų vykdomam turinio šalinimui, todėl patiriama reikšmingų finansinių nuostolių. „Media Land LLC“ sudarė galimybes didelio masto išpirkos reikalavimo programinės įrangos operacijoms, vadovavimo ir kontrolės paslaugoms ir duomenų viliojimo operacijoms, nukreiptoms į ypatingos svarbos infrastruktūrą ir esmines paslaugas valstybėse narėse. Operacijos, kurioms „Media Land LLC“ sudarė palankesnes sąlygas, yra, *inter alia*, „LockBit“, „EvilCorp“ ir „BlackBasta“. Taigi, „Media Land LLC“ dalyvauja reikšmingą poveikį darančiuose kibernetiniuose išpuoliuose, kurie kelia išorės grėsmę valstybėms narėms.	2026 7 13

	Pavadinimas	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
9.	ML.Cloud	Adresas: Brivibas iela 52, Riga, LV-1011, Latvija; Russian Federation, Kazan, Peterburgskaya st. 52 Registracijos vieta: Ryga Susijęs asmuo: Alexander Volosovik Kiti susiję subjektai: Media Land LLC	„ML.Cloud“ yra su „Media Land LLC“ susijusi bendrovė, teikianti „Media Land LLC“ techninę infrastruktūrą. Nuo 2016 m. nepramušamos prieglobos paslaugų teikėja „Media Land LLC“ sudaro palankesnes sąlygas įvairiems kenkimo programinės įrangos išpuoliams tiek valstybėse narėse, tiek visame pasaulyje, teikdama prieglobos paslaugas, kuriomis slepiamos naudotojų tapatybės ir priešinamasi teisėsaugos institucijų vykdomam turinio šalinimui, todėl patiriama reikšmingų finansinių nuostolių. „Media Land LLC“ sudarė galimybes didelio masto išpirkos reikalavimo programinės įrangos operacijoms, vadovavimo ir kontrolės paslaugoms ir duomenų viliojimo operacijoms, nukreiptoms į ypatingos svarbos infrastruktūrą ir esmines paslaugas valstybėse narėse. Operacijos, kurioms „Media Land LLC“ sudarė palankesnes sąlygas, yra, *inter alia*, „LockBit“, „EvilCorp“ ir „BlackBasta“. Taigi, „Media Land LLC“ dalyvauja kibernetiniuose išpuoliuose, kurie kelia išorės grėsmę, darančią reikšmingą poveikį valstybėms narėms. Taigi, „ML Cloud“ teikia techninę paramą reikšmingą poveikį darantiems kibernetiniams išpuoliams, keliantiems išorės grėsmę valstybėms narėms.	2026 7 13

	Pavadinimas	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
10.	„Impuls“ LLC	Общество с ограниченной ответственностью „Импульс“ Adresas: 344015, Russian Federation, Rostov Region, Rostov-on-Don, ul. Eremenko, d. 56, k. 6, apt. 88 Subjekto rūšis: ribotos atsakomybės bendrovė Registracijos vieta: Interdistrict Inspectorate of the Federal Tax Service No. 26 for the Rostov Region, 344019, Rostov-on-Don, ul. Myasnikova, d. 52/32, Russian Federation Registracijos data: 2010 9 27 Registracijos numeris: INN (ИНН): 6168033776; OGRN (ОГРН): 1106194004850 Pagrindinė veiklos vykdymo vieta: Rusijos Federacija Susiję asmenys: Evgeniy Bashev Susiję subjektai: GRU padalinys Nr. 29155	„Impuls“ LLC yra Rusijos bendrovė, nuosavybės teise priklausanti Evgeniy Viktorovich Bashev, Rusijos karinės žvalgybos agentūros GRU padalinio Nr. 29155 nariui. Bendrovė teikia techninę ir materialinę paramą GRU padalinio Nr. 29155 vykdomiems kibernetiniams išpuoliams ir pasikėsinimams įvykdyti kibernetinius išpuolius. Visų pirma, „Impuls“ LLC veikia kaip veiklos tarpininkė, sudaranti sąlygas su įsilaužimu susijusią veiklą vykdyti per bendrovę, oficialiai nesusijusią su Rusijos valstybe. Ji sudarė palankesnes sąlygas operacinei priedangai, infrastruktūrai ir mokėjimams už kibernetinius išpuolius ir buvo susieta su techniniais ištekliais, įskaitant serverius, naudojamus įsilaužimo veiklai remti. Visų pirma, „Impuls“ LLC sudarė sąlygas GRU struktūrų ir išorės įsilaužėlių tinklų bendradarbiavimui. Kibernetinės operacijos, kurioms „Impuls“ LLC sudarė palankesnes sąlygas, yra nukreiptos į ypatingos svarbos valstybės funkcijas ir paslaugas, būtinas esminei socialinei ir ekonominei veiklai valstybėse narėse, visų pirma transporto sektoriuje, palaikyti. Per kampaniją „WhisperGate“ GRU padalinys Nr. 29155 taip pat taikėsi į Ukrainos ypatingos svarbos infrastruktūrą. Taigi, „Impuls“ LLC teikia techninę ir materialinę paramą reikšmingą poveikį darantiems kibernetiniams išpuoliams, keliantiems išorės grėsmę valstybėms narėms, taip pat reikšmingą poveikį trečiajai valstybei darantiems kibernetiniams išpuoliams, arba kitaip dalyvauja juos vykdant.	2026 7 13

	Pavadinimas	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
11.	Z-Pentest	Dar žinoma kaip: „Z-Pentest Alliance“, „Z-Alliance“ Pagrindinė veiklos vykdymo vieta: Rusijos Federacija Susiję asmenys: Yuliya Pankratova Susiję subjektai: Cyber Army of Russia Reborn/CARR X.com paskyra: ZPentest (paskyra sustabdyta) Telegram paskyra: Zpentestalliance	„Z-Pentest“ yra prorusiška įsilaužėlių grupuotė, kurią sudaro CARR („Cyber Army of Russia Reborn“) ir „NoName057“ nariai ir kuri visame pasaulyje taikosi į ypatingos svarbos infrastruktūrą, visų pirma energetikos ir vandens sektorių. Visų pirma, 2024 m. gruodžio mėn. grupuotė atakavo Danijos vandens tiekimo įmonę. Taigi, „Z-Pentest“ yra atsakinga už reikšmingą poveikį darančius kibernetinius išpuolius, keliančius išorės grėsmę valstybėms narėms.	2026 7 13“