Europos Sąjungos
Taryba

Briuselis, 2026 m. kovo 10 d.
(OR. en)

5134/26

LIMITE

CORLX 10
CFSP/PESC 17
CYBER 4
JAI 21
FIN 8

TEISĖS AKTAI IR KITI DOKUMENTAI

Dalykas:	TARYBOS SPRENDIMAS, kuriuo iš dalies keičiamas Sprendimas (BUSP) 2019/797 dėl ribojamųjų priemonių, skirtų kovai su Sąjungai ar jos valstybėms narėms gresiančiais kibernetiniais išpuoliais

TARYBOS SPRENDIMAS (BUSP) 2026/…

… m. … … d.

kuriuo iš dalies keičiamas Sprendimas (BUSP) 2019/797 dėl ribojamųjų priemonių, skirtų kovai su Sąjungai ar jos valstybėms narėms gresiančiais kibernetiniais išpuoliais

EUROPOS SĄJUNGOS TARYBA,

atsižvelgdama į Europos Sąjungos sutartį, ypač į jos 29 straipsnį,

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

kadangi:

(1) 2019 m. gegužės 17 d. Taryba priėmė Sprendimą (BUSP) 2019/797[1];

(2) vykdant ilgalaikius, pritaikytus ir koordinuojamus Sąjungos veiksmus prieš tęstinių kibernetinių grėsmių subjektus, į Sprendimo (BUSP) 2019/797 priede pateikiamą fizinių ir juridinių asmenų, subjektų ir organizacijų, kuriems taikomos ribojamosios priemonės, sąrašą turėtų būti įtraukti du fiziniai asmenys ir trys subjektai. Tie fiziniai asmenys ir subjektai yra atsakingi už didelio poveikio kibernetinius išpuolius, keliančius išorės grėsmę Sąjungai ar jos valstybėms narėms, arba dalyvauja juos vykdant;

(3) todėl Sprendimas (BUSP) 2019/797 turėtų būti atitinkamai iš dalies pakeistas,

PRIĖMĖ ŠĮ SPRENDIMĄ:

[1] 2019 m. gegužės 17 d. Tarybos sprendimas (BUSP) 2019/797 dėl ribojamųjų priemonių, skirtų kovai su Sąjungai ar jos valstybėms narėms gresiančiais kibernetiniais išpuoliais, (OL L 129I, 2019 5 17, p. 13, ELI: http://data.europa.eu/eli/dec/2019/797/oj).

1 straipsnis

Sprendimo (BUSP) 2019/797 priedas iš dalies keičiamas pagal šio sprendimo priedą.

2 straipsnis

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

Priimta … …

Tarybos vardu

Pirmininkas / Pirmininkė

PRIEDAS

Sprendimo (BUSP) 2019/797 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
„18.	CHEN Cheng	陈诚 (rašyba kinų k.) Kiti vardai (*alias*): Jesse Chen lengmo l3n6m0 Gimimo data: 1984 10 20 Gimimo vieta: Jančengas (Yancheng), Dziangsu (Jiangsu), Kinija (China) Pilietybė: Kinijos Lytis: vyras	Chen Cheng yra Kinijos verslininkas, vienas iš bendrovės „Anxun Information Technology Co. Ltd.“ steigėjų ir vienas iš jos generalinių direktorių (generalinis administracijos direktorius). Jis taip pat yra tos bendrovės Sičuano padalinio teisinis atstovas. Bendrovė „Anxun Information Technology Co. Ltd.“, dar žinoma kaip „i-Soon“, yra Kinijos Liaudies Respublikoje (KLR) įsikūrusi bendrovė, teikianti įsilaužimo paslaugas už atlygį. „Anxun Information Technology Co. Ltd.“ vykdė veiklą, nukreiptą prieš valstybių narių ypatingos svarbos infrastruktūrą ir ypatingos svarbos valstybės funkcijas, taip pat gavo ir pardavė įslaptintą informaciją. Be to, „Anxun Information Technology Co. Ltd.“ vykdė išpuolius prieš įvairių trečiųjų valstybių vyriausybes, taip keldama grėsmę Sąjungos bendros užsienio ir saugumo politikos (BUSP) tikslams, kaip išdėstyta Europos Sąjungos sutarties 21 straipsnio 2 dalies a–c punktuose. „Anxun Information Technology Co. Ltd.“ iš teikiamų paslaugų gauna didelę ekonominę naudą.	+

+ OL: prašom įrašyti šio sprendimo įsigaliojimo datą.

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
			Taigi, „Anxun Information Technology Co. Ltd.“ yra atsakinga už reikšmingo poveikio kibernetinius išpuolius, keliančius išorės grėsmę Sąjungai bei jos valstybėms narėms, taip pat išpuolius prieš trečiąsias valstybes. Eidamas šias pareigas Chen Cheng yra atsakingas už ir dalyvauja vykdant reikšmingo poveikio kibernetinius išpuolius, keliančius išorės grėsmę valstybėms narėms, taip pat už reikšmingo poveikio kibernetinius išpuolius prieš trečiąsias valstybes ir dalyvauja juos vykdant.	

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
19.	WU Haibo	**吴海波** (rašyba kinų k.) Kiti vardai (*alias*): shutdown shutd0wn Gimimo vieta: Kinija Pilietybė: Kinijos Lytis: vyras	Wu Haibo yra Kinijos verslininkas, vienas iš bendrovės „Anxun Information Technology Co. Ltd.“ steigėjų ir vienas iš jos generalinių direktorių (generalinis direktorius). Jis taip pat yra „Anxun Information Technology Co. Ltd.“ Šanchajaus padalinio (patronuojančiosios įmonės) teisinis atstovas, valdybos pirmininkas ir generalinis direktorius. Be to, jis veikia kaip tos bendrovės Sičuano padalinio teisinis atstovas. Bendrovė „Anxun Information Technology Co. Ltd.“, dar žinoma kaip „i-Soon“, yra Kinijos Liaudies Respublikoje (KLR) įsikūrusi bendrovė, teikianti įsilaužimo paslaugas už atlygį. „Anxun Information Technology Co. Ltd.“ vykdė veiklą, nukreiptą prieš valstybių narių ypatingos svarbos infrastruktūrą ir ypatingos svarbos valstybės funkcijas, ir gavo bei pardavė įslaptintą informaciją. Be to, „Anxun Information Technology Co. Ltd.“ vykdė išpuolius prieš įvairių trečiųjų valstybių vyriausybes, taip keldama grėsmę Sąjungos bendros užsienio ir saugumo politikos (BUSP) tikslams, kaip išdėstyta Europos Sąjungos sutarties 21 straipsnio 2 dalies a–c punktuose. „Anxun Information Technology Co. Ltd.“ iš teikiamų paslaugų gauna didelę ekonominę naudą.	[+]“;

[+] OL: prašom įrašyti šio sprendimo įsigaliojimo datą.

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
			Taigi, „Anxun Information Technology Co. Ltd.“ yra atsakinga už reikšmingo poveikio kibernetinius išpuolius, keliančius išorės grėsmę valstybėms narėms, taip pat išpuolius prieš trečiąsias valstybes. Wu Haibo dalyvavo vadovaujant mėginimams įvykdyti kibernetinius išpuolius, darančius reikšmingą poveikį valstybėms narėms, ir juos skatinant. Eidamas šias pareigas jis yra atsakingas už ir dalyvauja vykdant reikšmingo poveikio kibernetinius išpuolius, keliančius išorės grėsmę valstybėms narėms, taip pat už reikšmingo poveikio kibernetinius išpuolius prieš trečiąsias valstybes ir dalyvauja juos vykdant.	

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

	Pavadinimas	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
„5.	Integrity Technology Group	永信至诚科技集团股份有限公司 (rašyba kinų k.) *Alias*: Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited Adresas: Fenghao East Road, Room 103, Building 6, No. 9, Beijing Haidian District, China	„Integrity Technology Group“ yra Kinijos Liaudies Respublikoje (KLR) įsikūrusi kibernetinio saugumo įmonė, kuri sudarė palankesnes sąlygas kibernetiniams išpuoliams, siejamiems su aukšto lygio tęstinės grėsmės (toliau – APT) subjektu „Flax Typhoon“. Tas APT subjektas panaudojo įmonės „Integrity Technology Group“ produktus ir technologijas savo kompiuterių tinklo išnaudojimo veiklai parengti. Nuo to laiko „Integrity Technology Group“ produktai buvo naudojami siekiant įsilaužti į daiktų interneto įrenginius ir gauti prieigą prie jų valstybėse narėse, taip pat valstybėse visoje Europoje ir visame pasaulyje.2022–2023 m. „Flax Typhoon“, naudodamasis „Integrity Technology Group“ produktais, šešiose valstybėse narėse įgijo prieigą prie bent 65 600 daiktų interneto įrenginių. Taigi, „Integrity Technology Group“ komerciniai produktai ir infrastruktūra buvo reguliariai naudojami vykdant kibernetinius išpuolius prieš valstybes nares ir trečiąsias valstybes. Dėl to, darydama poveikį su skaitmenine infrastruktūra susijusioms informacinėms sistemoms, „Integrity Technology Group“ teikia techninę ir materialinę paramą reikšmingą poveikį darantiems kibernetiniams išpuoliams, keliantiems išorės grėsmę valstybėms narėms ir trečiosioms valstybėms.	[+]

[+] OL: prašom įrašyti šio sprendimo įsigaliojimo datą.

	Pavadinimas	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
		Registracijos vieta: Pekinas (Beijing), Kinija (China) Registracijos data: 2010 9 2 Bendras socialinių kreditų sistemos kodas: 91110108562135265P		

	Pavadinimas	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
6.	Emennet Pasargad	*Alias*: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten Registracijos vieta: Teheranas (Tehran), Iranas (Iran) Registracijos numeris: 554267 Pagrindinė veiklos vykdymo vieta: Teheranas (Tehran), Iranas (Iran)	„Emennet Pasargad“ yra Irano kibernetinis subjektas (įmonė), nusitaikęs į daugelį subjektų, visų pirma, į subjektus valstybėse narėse ir Jungtinėse Amerikos Valstijose (JAV). „Emennet Pasargad“, veikdamas kaip „Anzu Team“, buvo nusitaikęs į skaitmeninę infrastruktūrą Švedijoje ir pakenkė Švedijos SMS paslaugai, o tai padarė poveikį daugeliui žmonių. Be to, veikdamas kaip „Holy Souls“, subjektas įsilaužė į Prancūzijos satyrinio leidinio „Charlie Hebdo“ abonentų duomenų bazę ir „juodajame tinkle“ paskelbė, kad duomenų bazė parduodama. „Emennet Pasargad“ Paryžiaus olimpinių žaidynių metu įsilaužė į reklaminius lauko ekranus ir per juos transliavo dezinformacijos kampanijas. „Emennet Pasargad“ taip pat bandė kištis į 2020 m. JAV prezidento rinkimus, keldamas grėsmę demokratijai ir teisinei valstybei – rinko konfidencialią JAV rinkėjų informaciją ir įgijo neteisėtą prieigą prie JAV žiniasklaidos bendrovės kompiuterių tinklo. Taigi, „Emennet Pasargad“ yra atsakingas už reikšmingo poveikio kibernetinius išpuolius, keliančius išorės grėsmę valstybėms narėms, ir už reikšmingo poveikio kibernetinius išpuolius prieš trečiąją valstybę.	+

+ OL: prašom įrašyti šio sprendimo įsigaliojimo datą.

	Pavadinimas	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
7.	Anxun Information Technology Co. Ltd.	**安洵信息技**术有限公司 (rašyba kinų k.) *Alias*: i-Soon Adresas: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Shanghai Bendras socialinių kreditų sistemos kodas: 91510105332025597A (Sičuano filialas) Bendras socialinių kreditų sistemos kodas: 91310116561906136G (Šanchajaus filialas)	„Anxun Information Technology Co. Ltd.“ yra Kinijos Liaudies Respublikoje įsikūrusi bendrovė, teikianti įsilaužimo paslaugas už atlygį. Ji vykdė veiklą, nukreiptą prieš valstybių narių ypatingos svarbos infrastruktūrą ir ypatingos svarbos valstybės funkcijas, ir gavo bei pardavė įslaptintą informaciją. Be to, „Anxun Information Technology Co. Ltd.“ vykdė išpuolius prieš įvairių trečiųjų valstybių vyriausybes, taip keldama grėsmę Sąjungos bendros užsienio ir saugumo politikos (BUSP) tikslams, kaip išdėstyta Europos Sąjungos sutarties 21 straipsnio 2 dalies a–c punktuose. „Anxun Information Technology Co. Ltd.“ iš teikiamų paslaugų gauna didelę ekonominę naudą. Taigi, „Anxun Information Technology Co. Ltd.“ yra atsakinga už reikšmingo poveikio kibernetinius išpuolius, keliančius išorės grėsmę valstybėms narėms, taip pat už reikšmingo poveikio kibernetinius išpuolius prieš trečiąsias valstybes.	[+]“.

[+] OL: prašom įrašyti šio sprendimo įsigaliojimo datą.

	Pavadinimas	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
		Interneto svetainės: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win Telefono numeriai: +862161119992, +8605645893417, +8613761671735, +864000665915 El. paštas: shutdown@163.com, isoon2015@126.com, tao_tingting@i-soon.net li_ping@i-soon.net		