



Briuselis, 2026 m. gegužės 5 d.  
(OR. en)

7281/26

LIMITE

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

#### 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 SAJUNGOS TARYBA,

atsižvelgdama 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<sup>1</sup>;
- (2) Sprendimas (BUSP) 2019/797 taikomas iki 2028 m. gegužės 18 d.;
- (3) remiantis Sprendimo (BUSP) 2019/797 priedo peržiūros rezultatais, to sprendimo 4 ir 5 straipsniuose išdėstytų priemonių taikymas tame priede išvardytų fizinių ir juridinių asmenų, subjektų ir organizacijų atžvilgiu turėtų būti pratęstas iki 2027 m. gegužės 18 d. Be to, turėtų būti atnaujintos priemonės, dėl kurių į fizinių ir juridinių asmenų, subjektų ir organizacijų, kuriems taikomos ribojamosios priemonės, sąrašą įtraukti keturi asmenys ir vienas subjektas;
- (4) todėl Sprendimas (BUSP) 2019/797 turėtų būti atitinkamai iš dalies pakeistas,

**PRIĖMĖ ŠĮ SPRENDIMĄ:**

---

<sup>1</sup> 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*

Sprendimas (BUSP) 2019/797 iš dalies keičiamas taip:

(1) 10 straipsnis pakeičiamas taip:

*„10 straipsnis*

Šis sprendimas taikomas iki 2028 m. gegužės 18 d. ir nuolat peržiūrimas. 4 ir 5 straipsniuose išdėstytos priemonės priede išvardytų fizinių ir juridinių asmenų, subjektų ir organizacijų atžvilgiu taikomos iki 2027 m. gegužės 18 d.“;

(2) priedas iš dalies keičiamas pagal šio sprendimo priedą.

*2 straipsnis*

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

Primta ... ..

*Tarybos vardu*

*Pirmininkas / Pirmininkė*

**PRIEDAS**

Sprendimo (BUSP) 2019/797 priedas iš dalies keičiamas taip:

- 1) antraštės „A. Fiziniai asmenys“ 1, 2, 13 ir 14 įrašai pakeičiami atitinkamai šiais įrašais:

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
„1.	GAO Qiang	Gimimo data: 1983 m. spalio 4 d. Gimimo vieta: Šandong provincija (Shandong Province), Kinija Adresas: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Pilietybė: Kinijos Lytis: vyras	Gao Qiang yra susijęs su grupės „APT10“ („Advanced Persistent Threat 10“) (dar žinomos kaip „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ ir „Potassium“) tinklu ir dalyvavo operacijoje „Operation Cloud Hopper“ – už Sąjungos ribų vykdant kibernetinius išpuolius, kurie turi didelį poveikį ir kelia išorės grėsmę Sąjungai ar jos valstybėms narėms, taip pat kibernetinius išpuolius, kurie turi didelį poveikį trečiosioms valstybėms.  „Operation Cloud Hopper“ buvo nukreipta prieš tarptautinių bendrovių šešiuose žemynuose, įskaitant Sąjungoje esančias bendroves, informacines sistemas ir ją įvykdžius buvo įgyta neteisėta prieiga prie neskelbtinų komercinių duomenų ir dėl to buvo padaryti dideli ekonominiai nuostoliai.  Gao Qiang yra susijęs su „APT10“ vadovavimo ir kontrolės infrastruktūra. Be to, Gao Qiang buvo įdarbintas „Huaying Haitai“, „APT10“ naudojamos bendrovės, kuri yra įtraukta į sąrašą už paramos teikimą ir palankesnių sąlygų sudarymą operacijai „Operation Cloud Hopper“. Jis taip pat siejamas su Zhang Shilong, kuris yra susijęs su „APT10“ ir kuris taip pat dirba „Huaying Haitai“.	2020 7 30

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
2.	ZHANG Shilong	Gimimo data: 1981 m. rugsėjo 10 d. Gimimo vieta: Kinija Adresas: Hedong, Yuyang Road No 121, Tianjin, China Pilietybė: Kinijos Lytis: vyras	<p>Zhang Shilong yra susijęs su grupės „APT10“ („Advanced Persistent Threat 10“) (dar žinomas kaip „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ ir „Potassium“) tinklu ir dalyvavo operacijoje „Operation Cloud Hopper“ – už Sąjungos ribų vykdant kibernetinius išpuolius, kurie turi didelį poveikį ir kelia išorės grėsmę Sąjungai ar jos valstybėms narėms, taip pat kibernetinius išpuolius, kurie turi didelį poveikį trečiosioms valstybėms.</p> <p>„Operation Cloud Hopper“ buvo nukreipta prieš tarptautinių bendrovių šešiuose žemynuose, įskaitant Sąjungoje esančias bendroves, informacines sistemas ir ją įvykdžius buvo įgyta neteisėta prieiga prie neskelbtinų komercinių duomenų ir dėl to buvo padaryti dideli ekonominiai nuostoliai.</p> <p>Zhang Shilong yra susijęs su „APT10“, be kita ko, dėl kenkimo programinės įrangos, kurią jis sukūrė ir testavo „APT10“ vykdant kibernetinius išpuolius.</p> <p>Be to, Zhang Shilong buvo įdarbintas „Huaying Haitai“, „APT10“ naudojamos bendrovės, kuri yra įtraukta į sąrašą už paramos teikimą ir palankesnių sąlygų sudarymą operacijai „Operation Cloud Hopper“.</p> <p>Jis taip pat siejamas su Gao Qiang, kuris yra susijęs su „APT10“ ir taip pat dirba „Huaying Haitai“.</p>	2020 7 30

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
13.	Mikhail Mikhailovich TSAREV	<p>Михаил Михайлович ЦАРЕВ</p> <p>Gimimo data: 1989 4 20</p> <p>Gimimo vieta: Serpuchovas (Serpukhov), Rusijos Federacija</p> <p>Pilietybė: Rusijos</p> <p>Adresas: Serpukhov</p> <p>Lytis: vyras</p>	<p>Mikhail Mikhailovich Tsarev dalyvavo vykdant didelio poveikio kibernetinius išpuolius, keliančius išorės grėsmę ES valstybėms narėms.</p> <p>Mikhail Mikhailovich Tsarev, dar žinomas internetiniais slapyvardžiais „Mango“, „Alexander Grachev“, „Super Misha“, „Ivanov Mixail“, „Misha Krutysha“ ir „Nikita Andreevich Tsarev“, yra vienas pagrindinių „Conti“ ir „Trickbot“ kenkimo programinės įrangos diegimo specialistų ir dalyvauja Rusijoje veikiančioje grėsmę keliančioje grupėje „Wizard Spider“. „Wizard Spider“ toliau vystosi ir intensyvina savo operacijas.</p> <p>„Conti“ ir „Trickbot“ kenkimo programinė įranga buvo sukurta ir išplėta „Wizard Spider“. „Wizard Spider“ vykdo kampanijas naudodama išpirkos reikalavimo programinę įrangą įvairiuose sektoriuose, įskaitant tokias esmines paslaugas kaip sveikatos priežiūra ir bankininkystė.</p> <p>Grupė užkrečia kompiuterius įvairiose pasaulio dalyse, o jų kenkimo programinė įranga buvo išplėta į aukšto lygio kenkimo modulinę programinę įrangą. „Wizard Spider“ kampanijos, vykdomos naudojant tokią kenkimo programinę įrangą kaip „Conti“, „Ryuk“, „Trickbot“ ar „Black Basta“, daro didelę ekonominę žalą Europos Sąjungoje.</p> <p>Taigi, Mikhail Mikhailovich Tsarev dalyvauja vykdant didelio poveikio kibernetinius išpuolius, keliančius išorės grėsmę Sąjungai arba jos valstybėms narėms.</p>	2024 6 24

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
14.	Maksim Sergeevich GALOCHKIN	<p>Максим Сергеевич ГАЛОЧКИН</p> <p>Gimimo data: 1982 5 19</p> <p>Gimimo vieta: Abakanas (Abakan), Rusijos Federacija</p> <p>Pilietybė: Rusijos</p> <p>Lytis: vyras</p>	<p>Maksim Galochkin dalyvavo vykdant didelio poveikio kibernetinius išpuolius, keliančius išorės grėsmę ES valstybėms narėms.</p> <p>Maksim Galochkin dar žinomas internetiniais slapyvardžiais „Benalen“, „Bentley“, „Volhvb“, „volhvb“, „manuel“, „Max17“ ir „Crypt“.</p> <p>M. Galochkin yra vienas pagrindinių „Conti“ ir „Trickbot“ kenkimo programinės įrangos diegimo specialistų ir dalyvauja Rusijoje veikiančioje grėsmę keliančioje grupėje „Wizard Spider“. Jis vadovavo grupei testuotojų, atsakingų už šnipinėjimo programos „TrickBot“, kurią sukūrė ir įdiegė grėsmę kelianti grupė „Wizard Spider“, testų kūrimą, priežiūrą ir įgyvendinimą. „Wizard Spider“ toliau vystosi ir intensyvina savo operacijas.</p> <p>„Wizard Spider“ vykdo kampanijas naudodama išpirkos reikalavimo programinę įrangą įvairiuose sektoriuose, įskaitant tokias esmines paslaugas kaip sveikatos priežiūra ir bankininkystė. Ši grupė užkrečia kompiuterius įvairiose pasaulio dalyse, o jų kenkimo programinė įranga buvo išplėtota į aukšto lygio kenkimo modulinę programinę įrangą.</p> <p>„Wizard Spider“ kampanijos, vykdomos naudojant tokią kenkimo programinę įrangą kaip „Conti“, „Ryuk“, „TrickBot“ ar „Black Basta“, daro didelę ekonominę žalą Europos Sąjungoje.</p> <p>Taigi, Maksim Galochkin dalyvauja vykdant didelio poveikio kibernetinius išpuolius, keliančius išorės grėsmę Sąjungai arba jos valstybėms narėms.</p>	2024 6 24“;

2) antraštės „B. Juridiniai asmenys, subjektai ir organizacijos“ 1 įrašas pakeičiamas šiuo įrašu:

	Pavadinimas	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
„1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai),	dar žinomas kaip: Haitai Technology Development Co. Ltd Vieta: Tiandžinas (Tianjin), Kinija	<p>„Huaying Haitai“ teikė finansinę, techninę arba materialinę paramą ir sudarė palankias sąlygas operacijai „Operation Cloud Hopper“ – už Sąjungos ribų vykdant kibernetinius išpuolius, kurie turi didelį poveikį ir kelia išorės grėsmę Sąjungai ar jos valstybėms narėms, taip pat kibernetinius išpuolius, kurie turi didelį poveikį trečiosioms valstybėms.</p> <p>„Operation Cloud Hopper“ buvo nukreipta prieš tarptautinių bendrovių šešiuose žemynuose, įskaitant Sąjungoje esančias bendroves, informacines sistemas ir ją įvykdžius buvo įgyta neteisėta prieiga prie neskelbtinų komercinių duomenų ir dėl to buvo padaryti dideli ekonominiai nuostoliai.</p> <p>„Operation Cloud Hopper“ įvykdė subjektas, viešai žinomas kaip „APT10“ („Advanced Persistent Threat 10“) (dar žinomas kaip „Red Apollo“, CVNX, „Stone Panda“, „MenuPass“ ir „Potassium“).</p> <p>„Huaying Haitai“ gali būti siejamas su „APT10“. Be to, subjekte „Huaying Haitai“ buvo įdarbinti Gao Qiang ir Zhang Shilong, kurie abu yra įtraukti į sąrašą dėl sąsajų su „Operation Cloud Hopper“. Todėl „Huaying Haitai“ taip pat siejamas su Gao Qiang ir Zhang Shilong.</p>	2020 7 30“.