Europos Sąjungos Taryba

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

7283/26

LIMITE

CORLX 273
CFSP/PESC 390
RELEX 352
CYBER 115
JAI 340
FIN 408

TEISĖS AKTAI IR KITI DOKUMENTAI

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

TARYBOS ĮGYVENDINIMO REGLAMENTAS (ES) 2026/…

… m. ... … 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 straipsnį,

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

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

kadangi:

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

(2) Taryba peržiūrėjo Reglamento (ES) 2019/796 I priede pateiktą fizinių ir juridinių asmenų, subjektų ir organizacijų sąrašą. Remiantis tos peržiūros rezultatais, turėtų būti atnaujintos priežastys, dėl kurių į fizinių ir juridinių asmenų, subjektų ir organizacijų, kuriems taikomos ribojamosios priemonės, sąrašą įtraukti keturi asmenys ir vienas subjektas;

(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 kitą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta …

Tarybos vardu
Pirmininkas / Pirmininkė

PRIEDAS

Reglamento (ES) 2019/796 I 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: Šandongo 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	Zhang Shilong 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. Zhang Shilong yra susijęs su „APT10“, be kita ko, dėl kenkimo programinės įrangos, kurią jis sukūrė ir testavo „APT10“ vykdant kibernetinius išpuolius. 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“. Jis taip pat siejamas su Gao Qiang, kuris yra susijęs su „APT10“ ir taip pat dirba „Huaying Haitai“.	2020 7 30

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
13.	Mikhail Mikhailovich TSAREV	Михаил Михайлович ЦАРЕВ Gimimo data: 1989 4 20 Gimimo vieta: Serpuchovas (Serpukhov), Rusijos Federacija Pilietybė: Rusijos Adresas: Serpukhov Lytis: vyras	Mikhail Mikhailovich Tsarev dalyvavo vykdant didelio poveikio kibernetinius išpuolius, keliančius išorės grėsmę ES valstybėms narėms. 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. „Conti“ ir „Trickbot“ kenkimo programinė įranga buvo sukurta ir išplėtota „Wizard Spider“. „Wizard Spider“ vykdo kampanijas naudodama išpirkos reikalavimo programinę įrangą įvairiuose sektoriuose, įskaitant tokias esmines paslaugas kaip sveikatos priežiūra ir bankininkystė. Grupė užkrečia kompiuterius įvairiose pasaulio dalyse, o jų kenkimo programinė įranga buvo išplėtota 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. Taigi, Mikhail Mikhailovich Tsarev dalyvauja vykdant didelio poveikio kibernetinius išpuolius, keliančius išorės grėsmę Sąjungai arba jos valstybėms narėms.	2024 6 24

	Vardas, pavardė	Identifikuojamoji informacija	Įtraukimo į sąrašą priežastys	Įtraukimo į sąrašą data
14.	Maksim Sergeevich GALOCHKIN	Максим Сергеевич ГАЛОЧКИН Gimimo data: 1982 5 19 Gimimo vieta: Abakanas (Abakan), Rusijos Federacija Pilietybė: Rusijos Lytis: vyras	Maksim Galochkin dalyvavo vykdant didelio poveikio kibernetinius išpuolius, keliančius išorės grėsmę ES valstybėms narėms. Maksim Galochkin dar žinomas internetiniais slapyvardžiais „Benalen“, „Bentley“, „Volhvb“, „volhvb“, „manuel“, „Max17“ ir „Crypt“. 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. „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. „Wizard Spider“ kampanijos, vykdomos naudojant tokią kenkimo programinę įrangą kaip „Conti“, „Ryuk“, „TrickBot“ ar „Black Basta“, daro didelę ekonominę žalą Europos Sąjungoje. Taigi, Maksim Galochkin dalyvauja vykdant didelio poveikio kibernetinius išpuolius, keliančius išorės grėsmę Sąjungai arba jos valstybėms narėms.	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	„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. „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. „Operation Cloud Hopper“ įvykdė subjektas, viešai žinomas kaip „APT10“ („Advanced Persistent Threat 10“) (dar žinomas kaip „Red Apollo“, CVNX, „Stone Panda“, „MenuPass“ ir „Potassium“). „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.	2020 7 30“.