Svet
Evropske unije

Bruselj, 5. maj 2026
(OR. en)

7281/26

LIMITE

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

ZAKONODAJNI AKTI IN DRUGI INSTRUMENTI

Zadeva:	SKLEP SVETA o spremembi Sklepa (SZVP) 2019/797 o omejevalnih ukrepih proti kibernetskim napadom, ki ogrožajo Unijo ali njene države članice

SKLEP SVETA (SZVP) 2026/…

z dne …

o spremembi Sklepa (SZVP) 2019/797 o omejevalnih ukrepih proti kibernetskim napadom, ki ogrožajo Unijo ali njene države članice

SVET EVROPSKE UNIJE JE –

ob upoštevanju Pogodbe o Evropski uniji in zlasti člena 29 Pogodbe,

ob upoštevanju predloga visokega predstavnika Unije za zunanje zadeve in varnostno politiko,

ob upoštevanju naslednjega:

(1) Svet je 17. maja 2019 sprejel Sklep (SZVP) 2019/797[1].

(2) Sklep (SZVP) 2019/797 se uporablja do 18. maja 2028.

(3) Na podlagi pregleda Priloge k Sklepu (SZVP) 2019/797 bi bilo treba uporabo ukrepov iz členov 4 in 5 navedenega sklepa v zvezi s fizičnimi in pravnimi osebami, subjekti in organi iz navedene priloge podaljšati do 18. maja 2027. Poleg tega bi bilo treba posodobiti razloge za uvrstitev štirih oseb in enega subjekta na seznam fizičnih in pravnih oseb, subjektov in organov, za katere veljajo omejevalni ukrepi.

(4) Sklep (SZVP) 2019/797 bi bilo zato treba ustrezno spremeniti –

SPREJEL NASLEDNJI SKLEP:

[1] Sklep Sveta (SZVP) 2019/797 z dne 17. maja 2019 o omejevalnih ukrepih proti kibernetskim napadom, ki ogrožajo Unijo ali njene države članice (UL L 129 I, 17.5.2019, str. 13, ELI: http://data.europa.eu/eli/dec/2019/797/oj.

Člen 1

Sklep (SZVP) 2019/797 se spremeni:

(1) Člen 10 se nadomesti z naslednjim:

„*Člen 10*

Ta sklep se uporablja do 18. maja 2028 in se redno pregleduje. Ukrepi iz členov 4 in 5 se za fizične in pravne osebe, subjekte in organe s seznama v Prilogi uporabljajo do 18. maja 2027.“;

(2) Priloga se spremeni v skladu s Prilogo k temu sklepu.

Člen 2

Ta sklep začne veljati dan po objavi v *Uradnem listu Evropske unije*.

V…, …

Za Svet
predsednik/predsednica

PRILOGA

Priloga k Sklepu (SZVP) 2019/797 se spremeni:

(1) pod naslovom „A. Fizične osebe“ se vnosi 1, 2, 13 in 14 nadomestijo z naslednjimi vnosi:

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
„1.	GAO Qiang	Datum rojstva: 4. oktober 1983 Kraj rojstva: provinca Shandong, Kitajska Naslov: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Državljanstvo: kitajsko Spol: moški	Povezan je z „APT10“ („Advanced Persistent Threat 10“) umbrella (tudi „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ in „Potassium“) in je bil vpleten v „Operation Cloud Hopper“, tj. vrsto kibernetskih napadov s pomembnim učinkom, ki izvirajo iz držav zunaj Unije in pomenijo zunanjo grožnjo Uniji ali njenim državam članicam, ter kibernetskih napadov s pomembnim učinkom, uperjenih zoper tretje države. Tarča „Operation Cloud Hopper“ so bili informacijski sistemi multinacionalnih družb na šestih celinah, vključno z družbami v Uniji, pri čemer je bil pridobljen nepooblaščen dostop do komercialno občutljivih podatkov, kar je povzročilo precejšnjo ekonomsko izgubo. Gao Qiang je povezan z infrastrukturo APT10 za poveljevanje in nadzor. Poleg tega je bil zaposlen pri podjetju Huaying Haitai, ki ga uporablja APT10 ter ki zagotavlja podporo in omogoča „Operation Cloud Hopper“. Povezan je tudi z Zhang Shilongom, ki je povezan z APT10 in je bil prav tako zaposlen pri Huaying Haitai.	30.7.2020

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
2.	ZHANG Shilong	Datum rojstva: 10. september 1981 Kraj rojstva: Kitajska Naslov: Hedong, Yuyang Road No 121, Tianjin, China Državljanstvo: kitajsko Spol: moški	Povezan je z „APT10“ („Advanced Persistent Threat 10“) umbrella (tudi „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ in „Potassium“) in je bil vpleten v „Operation Cloud Hopper“, tj. vrsto kibernetskih napadov s pomembnim učinkom, ki izvirajo iz držav zunaj Unije in pomenijo zunanjo grožnjo Uniji ali njenim državam članicam, ter kibernetskih napadov s pomembnim učinkom, uperjenih zoper tretje države. Tarča „Operation Cloud Hopper“ so bili informacijski sistemi multinacionalnih družb na šestih celinah, vključno z družbami v Uniji, pri čemer je bil pridobljen nepooblaščen dostop do komercialno občutljivih podatkov, kar je povzročilo precejšnjo ekonomsko izgubo. Zhang Shilonga je povezan z APT10, med drugim zaradi zlonamerne programske opreme, ki jo je razvil in testiral v povezavi s kibernetskimi napadi, ki jih je izvedel APT10. Poleg tega je bil zaposlen pri podjetju Huaying Haitai, ki ga uporablja APT10 ter ki zagotavlja podporo in omogoča „Operation Cloud Hopper“. Povezan je z Gao Qiangom, ki je povezan z APT10 in je bil prav tako zaposlen pri Huaying Haitai.	30.7.2020

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
13.	Mikhail Mikhailovich TSAREV	Михаил Михайлович ЦАРЕВ Datum rojstva: 20.4.1989 Kraj rojstva: Serpukhov, Ruska federacija Državljanstvo: rusko Naslov: Serpukhov Spol: moški	Sodeloval je v kibernetskih napadih s pomembnim učinkom, ki pomenijo zunanjo grožnjo državam članicam EU. Znan je tudi pod spletnimi vzdevki „Mango“, „Alexander Grachev“, „Super Misha“, „Ivanov Mixail“, „Misha Krutysha“ in „Nikita Andreevich Tsarev“ ter je ključni akter pri uvajanju zlonamerne programske opreme „Conti“ in „Trickbot“ ter je vključen v skupino za grožnje „Wizard Spider“, ki ima sedež v Rusiji. Skupina Wizard Spider se še vedno razvija in krepi svoje delovanje. Zlonamerno programsko opremo Conti in Trickbot je oblikovala in razvila skupina Wizard Spider. Skupina Wizard Spider je izvedla kampanje z izsiljevalskim programjem v različnih sektorjih, vključno z bistvenimi storitvami, kot sta zdravstvo in bančništvo. Skupina je okužila računalnike po vsem svetu, njihova zlonamerna programska oprema pa se je razvila v izjemno modularno zbirko zlonamerne programske opreme. Kampanje skupine Wizard Spider, ki uporabljajo zlonamerno programsko opremo, kot so Conti, „Ryuk“ TrickBot ali Black Basta, so odgovorne za veliko gospodarsko škodo v Evropski uniji. Zato je vpleten v kibernetske napade s pomembnim učinkom, ki pomenijo zunanjo grožnjo Uniji ali njenim državam članicam.	24.6.2024

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
14.	Maksim Sergeevich GALOCHKIN	Максим Сергеевич ГАЛОЧКИН Datum rojstva: 19.5.1982 Kraj rojstva: Abakan, Ruska federacija Državljanstvo: rusko Spol: moški	Sodeloval je v kibernetskih napadih s pomembnim učinkom, ki pomenijo zunanjo grožnjo državam članicam EU. Znan je tudi pod spletnimi vzdevki „Benalen“, „Bentley“, „Volhvb“, „volhvb“, „manuel“, „Max17“ in „Crypt“. Je ključni akter pri uvajanju zlonamerne programske opreme „Conti“ in „Trickbot“ ter je vključen v skupino za grožnje „Wizard Spider“, ki ima sedež v Rusiji. Vodil je skupino preskuševalcev, ki so odgovorni za razvoj, nadzor in izvajanje testov za program zlonamerne programske opreme TrickBot, ki jo je oblikovala in razvila skupina „Wizard Spider“. Skupina Wizard Spider se še vedno razvija in krepi svoje delovanje. Skupina Wizard Spider je izvedla kampanje z izsiljevalskim programjem v različnih sektorjih, vključno z bistvenimi storitvami, kot sta zdravstvo in bančništvo. Skupina je okužila računalnike po vsem svetu, njihova zlonamerna programska oprema pa se je razvila v izjemno modularno zbirko zlonamerne programske opreme. Kampanje skupine Wizard Spider, ki uporabljajo zlonamerno programsko opremo, kot so Conti, „Ryuk“ TrickBot ali Black Basta, so odgovorne za veliko gospodarsko škodo v Evropski uniji. Zato je vpleten v kibernetske napade s pomembnim učinkom, ki pomenijo zunanjo grožnjo Uniji ali njenim državam članicam.	24.6.2024“;

(2) pod naslovom „B. Pravne osebe, subjekti in organi“ se vnos 1 nadomesti z naslednjim:

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
„1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	tudi: Haitai Technology Development Co. Ltd Lokacija: Tianjin, Kitajska	Huaying Haitai je zagotovil finančno, tehnično ali materialno podporo in omogočil „Operation Cloud Hopper“, tj. vrsto kibernetskih napadov s pomembnim učinkom, ki izvirajo iz držav zunaj Unije in pomenijo zunanjo grožnjo Uniji ali njenim državam članicam, ter kibernetskih napadov s pomembnim učinkom, uperjenih zoper tretje države. Tarča „Operation Cloud Hopper“ so bili informacijski sistemi multinacionalnih družb na šestih celinah, vključno z družbami v Uniji, pri čemer je bil pridobljen nepooblaščen dostop do komercialno občutljivih podatkov, kar je povzročilo precejšnjo ekonomsko izgubo. „Operation Cloud Hopper“ je izvedel akter, v javnosti znan kot „APT10“ („Advanced Persistent Threat 10“) (tudi „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ in „Potassium“). Huaying Haitai je mogoče povezati z APT10. Poleg tega sta bila pri Huaying Haitai zaposlena Gao Qiang in Zhang Shilong, ki sta oba uvrščena na seznam v povezavi z „Operation Cloud Hopper“. Huaying Haitai je torej povezan tudi z Gao Qiangom in Zhang Shilongom.	30.7.2020“.