Svet
Evropske unije

Bruselj, 7. julij 2026
(OR. en)

8645/26

LIMITE

CORLX 390
CFSP/PESC 586
RELEX 561
CYBER 194
JAI 507
FIN 594

ZAKONODAJNI AKTI IN DRUGI INSTRUMENTI

Zadeva:	IZVEDBENA UREDBA SVETA o izvajanju Uredbe (EU) 2019/796 o omejevalnih ukrepih proti kibernetskim napadom, ki ogrožajo Unijo ali njene države članice

IZVEDBENA UREDBA SVETA (EU) 2026/…

z dne …

o izvajanju Uredbe (EU) 2019/796 o omejevalnih ukrepih proti kibernetskim napadom, ki ogrožajo Unijo ali njene države članice

SVET EVROPSKE UNIJE JE –

ob upoštevanju Pogodbe o delovanju Evropske unije,

ob upoštevanju Uredbe Sveta (EU) 2019/796 z dne 17. maja 2019 o omejevalnih ukrepih proti kibernetskim napadom, ki ogrožajo Unijo ali njene države članice[1], in zlasti člena 13(1) Uredbe,

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

[1] UL L 129I, 17.5.2019, str. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj.

ob upoštevanju naslednjega:

(1) Svet je 17. maja 2019 sprejel Uredbo (EU) 2019/796.

(2) V okviru stalnega, prilagojenega in usklajenega ukrepanja Unije proti vztrajnim akterjem na področju kibernetskih groženj bi bilo treba na seznam fizičnih in pravnih oseb, subjektov in organov, za katere veljajo omejevalni ukrepi iz Priloge I k Uredbi (EU) 2019/796, dodati osem fizičnih oseb in štiri subjekte. Te osebe in subjekti so odgovorni za ali vpleteni v kibernetske napade s pomembnim učinkom, ki pomenijo zunanjo grožnjo Uniji ali njenim državam članicam.

(3) Prilogo I k Uredbi (EU) 2019/796 bi bilo zato treba ustrezno spremeniti –

SPREJEL NASLEDNJO UREDBO:

Člen 1

Priloga I k Uredbi (EU) 2019/796 se spremeni v skladu s Prilogo k tej uredbi.

Člen 2

Ta uredba začne veljati na dan objave v *Uradnem listu Evropske unije.*

Ta uredba je v celoti zavezujoča in se neposredno uporablja v vseh državah članicah.

V…,

Za Svet
predsednik/predsednica

PRILOGA

Priloga I k Uredbi (EU) 2019/796 se spremeni:

(1) pod naslovom „A. Fizične osebe“ se dodajo naslednji vnosi:

	Ime	Podatki o istovetnosti	Utemeljitev	Datum uvrstitve na seznam
„20.	Vitaly Nikolayevich KOVALEV	Виталий Николаевич КОВАЛЕВ tudi:“Bentley”, “Bergen”, “Alex Konor”, “Benny”, “Ben”, “Stern” Datum rojstva: 23.6.1988 Naslov: Serebristy Bulvar 34 (Serebristyy Bul’var); krp 1; flt 528; 197341; St Petersburg, Russian Federation Državljanstvo: rusko Spol: moški Povezani subjekti: TrickBot, Wizard Spider, Conti	Vitaly Kovalev je vodilna osebnost pri programih zlonamerne programske opreme “Trickbot“ in “Conti“. Znan je tudi po spletnih vzdevkih “Bentley”, “Bergen”, “Alex Konor”, “Benny”, “Ben” in “Stern”. Programa Conti in Trickbot je zasnovala 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, in okužila računalnike po vsem svetu, njihova zlonamerna programska oprema pa se je razvila v izjemno modularno zbirko zlonamerne programske opreme. Kampanje skupine Wizard Spider, v katerih se uporablja zlonamerna programska oprema, kot sta Conti in TrickBot, so v Evropski uniji povzročile veliko gospodarsko škodo. Vitaly Kovalev je torej odgovoren za in vpleten v kibernetske napade s pomembnim učinkom, ki pomenijo zunanjo grožnjo Uniji ali njenim državam članicam.	[+]

[+] UL: prosimo, da vstavite datum objave te uredbe.

	Ime	Podatki o istovetnosti	Utemeljitev	Datum uvrstitve na seznam
21.	Alexander Alexandrovich VOLOSOVIK	Александр Александрович ВОЛОСОВИК Datum rojstva: 30.1.1983 Kraj rojstva: ZSSR Državljanstvo: rusko Številka potnega lista: 762988138 Spol: moški Povezani subjekti: Yalishanda, LARVA-34, podzemniyl, Ohyeahhellno, Stas_vl, downlow	Alexander Volosovik je lastnik družbe Media Land LLC. Ta je od leta 2016 omogočila že celo vrsto napadov z zlonamerno programsko opremo tako v Uniji kot drugod po svetu, saj nudi storitve gostovanja, ki skrivajo uporabniško identiteto in se zoperstavljajo odstranitvam te opreme s strani organov kazenskega pregona. Omogoča tudi obsežne operacije z izsiljevalskim programjem, storitve upravljanja in kontrole ter operacije ribarjenja (phishing), ki so usmerjene v kritično infrastrukturo in bistvene storitve v državah članicah, kar slednjim povzroča znatne finančne izgube. Med operacijami, ki jih družba omogoča, so med drugim LockBit, EvilCorp in BlackBasta. Media Land LLC je torej vpletena v kibernetske napade s pomembnim učinkom, ki pomenijo zunanjo grožnjo Uniji ali njenim državam članicam. Alexander Volosovik je kot lastnik te družbe odgovoren za in vpleten v te kibernetske napade. S to družbo je tudi povezan.	+

+ UL: prosimo, da vstavite datum objave te uredbe.

	Ime	Podatki o istovetnosti	Utemeljitev	Datum uvrstitve na seznam
22.	Denis Olegovich DEGTYARENKO	Денис Олегович ДЕГТЯРЕНКО tudi: “Dena” Datum rojstva: 9.10.1989 Kraj rojstva: ZSSR Državljanstvo: rusko Spol: moški Naslov: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation	Denis Degtyarenko oziroma Dena je ruski heker za hekersko aktivistično skupino CARR (Cyber Army of Russia Reborn). Skupina CARR je odgovorna za kibernetske napade na storitve, ki so nujne za ohranjanje bistvenih gospodarskih dejavnosti in kritičnih državnih funkcij v državah članicah, ter na infrastrukturo v Ukrajini in drugih tretjih državah. Povezana je z Main Centre for Special Technologies (GTsST), ki deluje v okviru Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). GTsST je še naprej dejaven pri izvajanju kibernetskih napadov na Unijo ali njene države članice. Med tarče skupine CARR spadajo vladne agencije, finančne institucije, medijske hiše in kritična infrastruktura v državah članicah in v Združenih državah Amerike. Porazdeljene napade za zavrnitev storitve izvaja v Ukrajini ter na vlade in na podjetja v državah, ki podpirajo Ukrajino. Denis Degtyarenko je torej glavni heker za skupino CARR, vpleten v kibernetske napade s pomembnim učinkom, vključno s poskusi kibernetskih napadov s potencialno pomembnim učinkom, ki pomenijo zunanjo grožnjo državam članicam in tretjim državam. Kot član skupine CARR je povezan tudi z GTsST.	+

+ UL: prosimo, da vstavite datum objave te uredbe.

	Ime	Podatki o istovetnosti	Utemeljitev	Datum uvrstitve na seznam
23.	Yuliya Vladimirovna PANKRATOVA	Юлия Владимировна ПАНКРАТОВА tudi: “YUliYA” Datum rojstva: 6.4.1984 Kraj rojstva: ZSSR Državljanstvo: rusko Spol: ženski Naslov: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation	Yuliya Pankratova je ruska hekerka, ki je delala za hekersko aktivistično skupino CARR (Cyber Army of Russia Reborn) in je ustanovila hekersko aktivistično skupino Z-Pentest, za katero še naprej dela. Skupina CARR je odgovorna za kibernetske napade na storitve, ki so nujne za ohranjanje bistvenih gospodarskih dejavnosti in kritičnih državnih funkcij v državah članicah, ter na infrastrukturo v Ukrajini in drugih tretjih državah. Povezana je z Main Centre for Special Technologies (GTsST), ki deluje v okviru Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GRU). GTsST je še naprej dejaven pri izvajanju kibernetskih napadov na Unijo ali njene države članice. Med tarče skupine CARR spadajo vladne agencije, finančne institucije, medijske hiše in kritična infrastruktura v državah članicah in v Združenih državah Amerike. Porazdeljene napade za zavrnitev storitve izvaja v Ukrajini ter na vlade in na podjetja v državah, ki podpirajo Ukrajino.	+

+ UL: prosimo, da vstavite datum objave te uredbe.

	Ime	Podatki o istovetnosti	Utemeljitev	Datum uvrstitve na seznam
			Skupina Z-Pentest je odgovorna za kibernetske napade s pomembnim učinkom, in sicer med drugim na storitve, ki so nujne za ohranjanje bistvenih dejavnosti v državah članicah. Yuliya Pankratova je torej glavna hekerka za skupini CARR in Z-Pentest, vpletena v kibernetske napade s pomembnim učinkom, vključno s poskusi kibernetskih napadov s potencialno pomembnim učinkom, ki pomenijo zunanjo grožnjo državam članicam in tretjim državam. Povezana je tudi s skupino Z-Pentest.	

	Ime	Podatki o istovetnosti	Utemeljitev	Datum uvrstitve na seznam
24.	Maksim Evgenevich VORONIN	Максим Евгеньевич ВОРОНИН tudi: “Daugn0” Državljanstvo: domnevno rusko Spol: moški	Maksim Voronin, znan tudi kot Daugn0, sodeluje pri razvoju, distribuciji in prodaji zlonamerne programske opreme za krajo informacij LummaC2 (tudi Lumma Infostealer, Lumma Stealer). LummaC2 je zlonamerna programska oprema kot storitev (MaaS oz. Malware-as-a-Service), ki se uporablja za krajo občutljivih poverilnic podatkovnega brskalnika, kriptodenarnic ali sistemskih informacij, za namestitev dodatne zlonamerne programske opreme na okužene naprave, za krajo kriptovalut in za kampanje vohunjenja. Kibernetske napade z zlonamerno programsko opremo LummaC2 uporabljajo tudi finančno motivirani akterji na področju kibernetskih groženj, kot so Storm-113, Storm-1607, Storm-1674, Octo Tempest in drugi. LummaC2 se uporablja za kibernetske napade na kritične državne funkcije in storitve, ki so nujne za ohranjanje bistvenih družbenih in gospodarskih dejavnosti držav članic. V letih 2024 in 2025 je bila LummaC2 eno od najpogosteje uporabljenih orodij za krajo informacij po celem svetu. Maksim Voronin torej kot razvijalec, distributer in prodajalec zlonamerne programske opreme LummaC2 sodeluje v kibernetskih napadih s pomembnim učinkom, ki pomenijo zunanjo grožnjo državam članicam, in jih omogoča.	[+]

[+] UL: prosimo, da vstavite datum objave te uredbe.

	Ime	Podatki o istovetnosti	Utemeljitev	Datum uvrstitve na seznam
25.	Maksim Aleksandrovich GORDIENKO tudi Maxim Alexandrovich GORDIENKO	Максим Александрович ГОРДИЕНКО tudi: “Lummaseller” Državljanstvo: domnevno rusko Spol: moški	Maksim Gordienko, znan tudi kot Lummaseller, sodeluje pri razvoju in distribuciji zlonamerne programske opreme za krajo informacij LummaC2 (tudi Lumma Infostealer, Lumma Stealer). LummaC2 je zlonamerna programska oprema kot storitev (MaaS oz. Malware-as-a-Service), ki se uporablja za krajo občutljivih poverilnic podatkovnega brskalnika, kriptodenarnic ali sistemskih informacij, za namestitev dodatne zlonamerne programske opreme na okužene naprave, za krajo kriptovalut in za kampanje vohunjenja. Kibernetske napade z zlonamerno programsko opremo LummaC2 uporabljajo tudi finančno motivirani akterji na področju kibernetskih groženj, kot so Storm-113, Storm-1607, Storm-1674, Octo Tempest in drugi. LummaC2 se uporablja za kibernetske napade na kritične državne funkcije in storitve, ki so nujne za ohranjanje bistvenih družbenih in gospodarskih dejavnosti držav članic. V letih 2024 in 2025 je bila LummaC2 eno od najpogosteje uporabljenih orodij za krajo informacij po celem svetu. Maksim Gordienko torej kot razvijalec, distributer in prodajalec zlonamerne programske opreme LummaC2 sodeluje v kibernetskih napadih s pomembnim učinkom, ki pomenijo zunanjo grožnjo državam članicam, in jih omogoča.	[+]

[+] UL: prosimo, da vstavite datum objave te uredbe.

	Ime	Podatki o istovetnosti	Utemeljitev	Datum uvrstitve na seznam
26.	Evgeniy Viktorovich BASHEV	Евгений Викторович БАШЕВ Datum rojstva: 25.1.1980 Kraj rojstva: ZSSR Državljanstvo: rusko Spol: moški Povezani posamezniki: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin Povezana subjekta: GRU Unit 29155, „Impuls“ LLC	Evgeniy Bashev je član ruske vojaške obveščevalne agencije Russian Military Intelligence Agency GRU, Unit 29155 (Enota GRU 29155). V enoti podpira in omogoča kibernetske napade s pomembnim učinkom na države članice, med drugim z nadzorom strežnika „Aegon“, ki se uporablja za operacije vdora. Zlasti Enoti GRU 29155 zagotavlja tehnično in materialno podporo za kibernetske napade prek svojega podjetja „Impuls“ LLC, ki je zagotavljalo operativno kritje, infrastrukturo in plačila, ter upravljalo tehnična sredstva, vključno s strežniki, uporabljenimi za kibernetske napade. Usklajeval je tudi sodelovanje med strukturami GRU in zunanjimi hekerskimi mrežami. Kibernetski napadi, ki jih je omogočil, so bili usmerjeni v kritične državne funkcionalne sisteme in storitve, potrebne za ohranjanje bistvenih družbenih ali gospodarskih dejavnosti v državah članicah, zlasti v prometnem sektorju. Prek kampanje WhisperGate je bila tarča Enote GRU 29155 tudi kritična infrastruktura Ukrajine.	[+]

[+] UL: prosimo, da vstavite datum objave te uredbe.

	Ime	Podatki o istovetnosti	Utemeljitev	Datum uvrstitve na seznam
			Evgeniy Bashev torej zagotavlja tehnično in materialno podporo za kibernetske napade s pomembnim učinkom, tudi poskuse kibernetskih napadov z morebitnim pomembnim učinkom, ki pomenijo zunanjo grožnjo državam članicam, ter kibernetske napade s pomembnim učinkom, uperjene proti tretji državi, ali je kako drugače vpleten vanje. Kot lastnik in generalni direktor je povezan s podjetjem LLC „Impuls“ LLC. Kot član Enote GRU 29155 je prav tako povezan s tem subjektom.	

	Ime	Podatki o istovetnosti	Utemeljitev	Datum uvrstitve na seznam
27.	Roman Alexandrovich PUNTUS	Роман Александрович ПУНТУС Kraj rojstva: Ruska federacija Državljanstvo: rusko Spol: moški Povezani posamezniki: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin, Evgeniy Viktorovich Bashev Povezan subjekt: GRU Unit 29155	Roman Puntus je član ruske vojaške obveščevalne agencije GRU, Unit 29155 (Enota GRU 29155). Znotraj enote ima vodilno vlogo pri organizaciji in usklajevanju kibernetskih napadov, ki pomembno vplivajo na države članice. Podpira tudi razvoj notranjih kibernetskih zmogljivosti enote, tudi z zaposlovanjem in nadzorom osebja, kot so hekerji in programerji. Z ustanovitvijo slamnate družbe „Aegeon-Impulse“ je pomagal pri logističnih in finančnih vidikih kibernetskih operacij. Enota je pod njegovim vodstvom izvajala kibernetske napade, usmerjene v kritične državne funkcionalne sisteme in storitve, potrebne za ohranjanje bistvenih družbenih ali gospodarskih dejavnosti v državah članicah, zlasti v prometnem sektorju. Prek kampanje WhisperGate je bila tarča Enote GRU 29155 tudi kritična infrastruktura Ukrajine.	[+]“

[+] UL: prosimo, da vstavite datum objave te uredbe.

	Ime	Podatki o istovetnosti	Utemeljitev	Datum uvrstitve na seznam
			Roman Puntus je torej odgovoren za kibernetske napade, tudi poskuse kibernetskih napadov z morebitnim pomembnim učinkom, ki pomenijo zunanjo grožnjo državam članicam, ter kibernetske napade s pomembnim učinkom, uperjene proti tretji državi, ali je kako drugače vpleten vanje. Kot član Enote GRU 29155 je prav tako povezan s tem subjektom.	

(2) pod naslovom „B. Pravne osebe, subjekti in organi“ se dodajo naslednji vnosi:

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
„8.	Media Land LLC	Naslov: Tsvetnochnaya st., 16 Litera P, Room 27, Moskovskaya Zastava Municipal District St Petersburg, 196006, Russian Federation Vrsta subjekta: družba z omejeno odgovornostjo Kraj vpisa: Sankt Peterburg Datum vpisa: 19.10.2015 Številka vpisa: 1152536009900 Glavni kraj delovanja: Sankt Peterburg, Ruska federacija Povezan subjekt: ML.Cloud	Media Land LLC je od leta 2016 omogočila že celo vrsto napadov z zlonamerno programsko opremo v državah članicah in po svetu, tako da nudi storitve gostovanja, ki skrivajo uporabniško identiteto in se zoperstavljajo odstranitvam te opreme s strani organov kazenskega pregona, kar povzroča znatne finančne izgube. Omogoča tudi obsežne operacije z izsiljevalskim programjem, storitve upravljanja in kontrole ter operacije ribarjenja (phishing), ki so usmerjene v kritično infrastrukturo in bistvene storitve med državami članicami. Med operacijami, ki jih družba omogoča, so med drugim LockBit, EvilCorp in BlackBasta. Media Land LLC je torej vpletena v kibernetske napade s pomembnim učinkom, ki pomenijo zunanjo grožnjo državam članicam.	+

+ UL: prosimo, da vstavite datum objave te uredbe.

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
9.	ML.Cloud	Naslov: Brivibas iela 52, Riga, LV-1011, Latvija;Russian Federation, Kazan, Peterburgskaya st. 52 Kraj vpisa: Riga Povezan posameznik: Alexander Volosovik Drugi povezani subjekti: Media Land LLC	ML.Cloud je sestrska družba družbe Media Land LLC in zagotavlja tehnično infrastrukturo za družbo Media Land LLC. Od leta 2016 je omogočila že celo vrsto napadov z zlonamerno programsko opremo v državah članicah in po svetu, tako da nudi storitve gostovanja, ki skrivajo uporabniško identiteto in se zoperstavljajo odstranitvam te opreme s strani organov kazenskega pregona, kar povzroča znatne finančne izgube. Omogoča tudi obsežne operacije z izsiljevalskim programjem, storitve upravljanja in kontrole ter operacije ribarjenja (phishing), ki so usmerjene v kritično infrastrukturo in bistvene storitve med državami članicami. Med operacijami, ki jih družba omogoča, so med drugim LockBit, EvilCorp in BlackBasta. Media Land LLC je torej vpletena v kibernetske napade, ki pomenijo zunanjo grožnjo s pomembnim učinkom za države članice EU. ML. Cloud torej zagotavlja tehnično podporo za kibernetske napade s pomembnim učinkom, ki pomenijo zunanjo grožnjo državam članicam.	+

+ UL: prosimo, da vstavite datum objave te uredbe.

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
10.	“Impuls” LLC	Общество с ограниченной ответственностью «Импульс» Naslov: 344015, Russian Federation, Rostov Region, Rostov-on-Don, ul. Eremenko, d. 56, k. 6, apt. 88 Vrsta subjekta: družba z omejeno odgovornostjo Kraj vpisa: Interdistrict Inspectorate of the Federal Tax Service No. 26 for the Rostov Region, 344019, Rostov-on-Don, ul. Myasnikova, d. 52/32, Russian Federation Datum vpisa: 27.9.2010	‚Impuls‘ LLC je rusko podjetje v lasti Evgeniya Viktorovicha Basheva, člana ruske vojaške obveščevalne agencije GRU, Unit 29155 (Enota GRU 29155). Podjetje zagotavlja tehnično in materialno podporo za kibernetske napade in poskuse kibernetskih napadov, ki jih izvaja Enota GRU 29155. Zlasti deluje kot operativni posrednik, ki omogoča izvajanje dejavnosti, povezanih s hekanjem, prek podjetja, ki formalno ni povezano z rusko državo. Omogočalo je operativno kritje, infrastrukturo in plačila za kibernetske napade ter je bilo povezano s tehničnimi sredstvi, vključno s strežniki, uporabljenimi v podporo hekerskim dejavnostim. Zlasti je omogočalo sodelovanje med strukturami GRU in zunanjimi hekerskimi mrežami. Kibernetske operacije, ki jih omogoča ‚Impuls‘ LLC, so usmerjene v kritične državne funkcionalne sisteme in storitve, potrebne za ohranjanje bistvenih socialnih in gospodarskih dejavnosti v državah članicah, zlasti v prometnem sektorju. Prek kampanje WhisperGate je bila tarča Enote GRU 29155 tudi kritična infrastruktura Ukrajine.	+

+ UL: prosimo, da vstavite datum objave te uredbe.

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
		Številka vpisa: INN (ИНН): 6168033776; OGRN (ОГРН): 1106194004850 Glavni kraj delovanja: Russian Federation Povezan posameznik: Evgeniy Bashev Povezan subjekt: GRU Unit 29155	‚Impuls' LLC torej zagotavlja tehnično in materialno podporo za kibernetske napade s pomembnim učinkom, ki pomenijo zunanjo grožnjo državam članicam, ter kibernetske napade s pomembnim učinkom, uperjene proti tretji državi, ali je kako drugače vpleteno vanje.	

	Ime	Podatki za identifikacijo	Razlogi za uvrstitev na seznam	Datum uvrstitve na seznam
11.	Z-Pentest	Vzdevki: „Z-Pentest Alliance“, „Z-Alliance“ Glavni kraj delovanja: Russian Federation Povezana posameznica: Yuliya Pankratova Povezan subjekt: Cyber Army of Russia/CARR Račun na X.com: ZPentest (račun začasno ukinjen) Račun na Telegramu: Zpentestalliance	Z-Pentest je proruska skupina hekerjev-aktivistov, sestavljena iz članov CARR (Cyber Army of Russia Reborn) in NoName057, ki je na svetovni ravni usmerjena v kritično infrastrukturo, zlasti v energetski in vodni sektor. Skupina je decembra 2024 napadla dansko komunalno podjetje za oskrbo z vodo. Skupina Z-Pentest je torej odgovorna za kibernetske napade s pomembnim učinkom, ki pomenijo zunanjo grožnjo državam članicam.	[+]“

[+] UL: prosimo, da vstavite datum objave te uredbe.