2026/1713

13.7.2026.

ODLUKA VIJEĆA (ZVSP) 2026/1713

od 13. srpnja 2026.

o izmjeni Odluke (ZVSP) 2019/797 o mjerama ograničavanja protiv kibernapada koji predstavljaju prijetnju Uniji ili njezinim državama članicama

VIJEĆE EUROPSKE UNIJE,

uzimajući u obzir Ugovor o Europskoj uniji, a posebno njegov članak 29.,

uzimajući u obzir prijedlog Visokog predstavnika Unije za vanjske poslove i sigurnosnu politiku,

budući da:

(1) Vijeće je 17. svibnja 2019. donijelo Odluku (ZVSP) 2019/797 ([1]).

(2) U okviru trajnog, prilagođenog i koordiniranog djelovanja Unije protiv aktera koji predstavljaju stalnu kibernetičku prijetnju osam fizičkih osoba i četiri subjekta trebalo bi dodati na popis fizičkih i pravnih osoba, subjekata i tijela koji podliježu mjerama ograničavanja naveden u Prilogu Odluci (ZVSP) 2019/797. Te su osobe i subjekti odgovorni za kibernetičke napade sa znatnim učinkom koji predstavljaju vanjsku prijetnju Uniji ili njezinim državama članicama, podržavaju ih ili su u njih uključeni.

(3) Odluku (ZVSP) 2019/797 trebalo bi stoga na odgovarajući način izmijeniti,

DONIJELO JE OVU ODLUKU:

Članak 1.

Prilog Odluci (ZVSP) 2019/797 mijenja se u skladu s Prilogom ovoj Odluci.

Članak 2.

Ova Odluka stupa na snagu na dan objave u *Službenom listu Europske unije*.

Sastavljeno u Bruxellesu 13. srpnja 2026.

Za Vijeće

Predsjednica

K. KALLAS

([1]) Odluka Vijeća (ZVSP) 2019/797 od 17. svibnja 2019. o mjerama ograničavanja protiv kibernapada koji predstavljaju prijetnju Uniji ili njezinim državama članicama (SL L 129 I, 17.5.2019., str. 13., ELI: http://data.europa.eu/eli/dec/2019/797/oj).

PRILOG

Prilog Odluci (ZVSP) 2019/797 mijenja se kako slijedi:

1. sljedeći unosi dodaju se pod naslovom „A. Fizičke osobe”:

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
„20.	Vitaly Nikolayevich KOVALEV	Виталий Николаевич КОВАЛЕВ također poznat kao: ‚Bentley', ‚Bergen', ‚Alex Konor', ‚Benny', ‚Ben', ‚Stern' Datum rođenja: 23.6.1988. Adresa: Serebristy Bulvar 34 (Serebristyy Bul'var); krp 1; flt 528; 197341; St Petersburg (Sankt Peterburg), Ruska Federacija Državljanstvo: rusko Spol: muški Povezani subjekti: TrickBot, Wizard Spider, Conti	Vitaly Kovalev vodeća je osoba za programe zlonamjernog softvera ‚Trickbot' i ‚Conti'. Poznat je i po internetskim nadimcima ‚Bentley', ‚Bergen', ‚Alex Konor', ‚Benny', ‚Ben' i ‚Stern'. Programe zlonamjernih softvera ‚Conti' i ‚Trickbot' izvorno je izradila i razvila skupina Wizard Spider. Skupina Wizard Spider provodila je širenje ucjenjivačkog softvera u raznim sektorima, uključujući ključne službe kao što su zdravstvo i bankarstvo, zarazila je računala u cijelom svijetu, a njezin zlonamjerni softver razvijen je u vrlo modularni paket zlonamjernih softvera. Aktivnosti skupine Wizard Spider u kojima su se upotrebljavali zlonamjerni softveri kao što su ‚Conti' i ‚TrickBot' uzrokovale su znatnu gospodarsku štetu u Europskoj uniji. Vitaly Kovalev stoga je odgovoran za kibernetičke napade sa znatnim učinkom koji predstavljaju vanjsku prijetnju Uniji i njenim državama članicama i u njih je uključen.	13.7.2026.

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
21.	Alexander Alexandrovich VOLOSOVIK	Александр Александрович ВОЛОСОВИК Datum rođenja: 30.1.1983. Mjesto rođenja: SSSR Državljanstvo: rusko Broj putovnice: 762988138 Spol: muški Povezani subjekti: Yalishanda, LARVA-34, podzemniyl, Ohyeahhellno, Stas_vl, downlow	Alexander Volosovik vlasnik je društva Media Land LLC. To društvo koje pruža uslugama smještaja na poslužiteljima bez kontrole sadržaja (engl. bulletproof hosting) od 2016. olakšava širok niz napada zlonamjernim softverom protiv Unije i širom svijeta tako što nudi usluge smještaja na poslužiteljima kojima se prikrivaju korisnički identiteti i odupire mjerama tijela za izvršavanje zakonodavstva. Društvo Media Land LLC omogućilo je operacije s ucjenjivačkim programima velikih razmjera, usluge za zapovijedanje i kontrolu te operacije phishinga usmjerene na ključnu infrastrukturu i službe u državama članicama, što je dovelo do znatnih financijskih gubitaka. Operacije koje je olakšalo društvo Media Land LLC uključuju, među ostalim, skupine LockBit, EvilCorp i BlackBasta. Stoga je društvo Media Land LLC uključeno u kibernetičke napade sa znatnim učinkom koji predstavljaju vanjsku prijetnju Uniji ili njenim državama članicama. Kao vlasnik društva Media Land LLC Alexander Volosovik odgovoran je za te kibernetičke napade i sudjeluje u njima. Također je povezan s društvom Media Land LLC.	13.7.2026.

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
22.	Denis Olegovich DEGTYARENKO	Денис Олегович ДЕГТЯРЕНКО također poznat kao: ‚Dena' Datum rođenja: 9.10.1989. Mjesto rođenja: SSSR Državljanstvo: rusko Spol: muški Adresa: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Ruska Federacija	Denis Degtyarenko također poznat kao Dena ruski je haker za skupinu CARR (Cyber Army of Russia Reborn). Skupina CARR odgovorna je za kibernetičke napade na službe nužne za održavanje ključnih gospodarskih aktivnosti i ključnih državnih funkcija u državama članicama, kao i na infrastrukturu u Ukrajini i drugim trećim zemljama. Skupina CARR povezana je s Glavnim centrom za posebne tehnologije (GTsST) glavne uprave glavnog stožera oružanih snaga Ruske Federacije (GRU). GTsST i dalje aktivno provodi kibernetičke napade na Uniju ili njezine države članice. Mete skupine CARR uključuju vladine agencije, financijske institucije, medijske kuće i kritičnu infrastrukturu u državama članicama i Sjedinjenim Američkim Državama. Skupina CARR izvodila je distribuirane napade uskraćivanjem usluga u Ukrajini te napade na vlade i poduzeća u zemljama koje podupiru Ukrajinu. Stoga je Denis Degtyarenko, glavni haker skupine CARR, uključen u kibernetičke napade sa znatnim učinkom, uključujući pokušaje kibernetičkih napada s potencijalno znatnim učinkom, koji predstavljaju vanjsku prijetnju državama članicama, kao i trećim zemljama. Kao član skupine CARR povezan je i s centrom GTsST.	13.7.2026.

ELI: http://data.europa.eu/eli/dec/2026/1713/oj

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
23.	Yuliya Vladimirovna PANKRATOVA	Юлия Владимировна ПАНКРАТОВА također poznata kao: ‚YUliYA' Datum rođenja: 6.4.1984. Mjesto rođenja: SSSR Državljanstvo: rusko Spol: ženski Adresa: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Ruska Federacija	Yuliya Pankratova ruska je hakerica koja radi za skupinu CARR (Cyber Army of Russia Reborn) i koja je osnovala skupinu Z-Pentest i nastavila raditi za skupinu Z-Pentest. Skupina CARR odgovorna je za kibernetičke napade na službe nužne za održavanje ključnih gospodarskih aktivnosti i ključnih državnih funkcija u državama članicama , kao i na infrastrukturu u Ukrajini i drugim trećim zemljama. Skupina CARR povezana je s Glavnim centrom za posebne tehnologije (GTsST) glavne uprave glavnog stožera oružanih snaga Ruske Federacije (GRU). GTsST i dalje aktivno provodi kibernetičke napade na Uniju ili njezine države članice. Mete skupine CARR uključuju vladine agencije, financijske institucije, medijske kuće i kritičnu infrastrukturu u državama članicama i Sjedinjenim Američkim Državama. Skupina CARR izvodila je distribuirane napade uskraćivanjem usluga u Ukrajini te napade na vlade i poduzeća u zemljama koje podupiru Ukrajinu. Skupina Z-Pentest odgovorna je za kibernetičke napade sa znatnim učinkom na, među ostalim, službe nužne za održavanje ključnih aktivnosti u državama članicama. Stoga je Yuliya Pankratova, glavna hakerica za skupine CARR i Z-Pentest, uključena u kibernetičke napade sa znatnim učinkom, uključujući pokušaje kibernetičkog napada s potencijalno znatnim učinkom, koji predstavljaju vanjsku prijetnju državama članicama, kao i trećim zemljama. Također je povezana sa skupinom Z-Pentest.	13.7.2026.

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
24.	Maksim Evgenevich VORONIN	Максим Евгеньевич ВОРОНИН također poznat kao: ‚Daugn0' Državljanstvo: rusko Spol: muški	Maksim Voronin također poznat kao Daugn0 uključen je u razvoj, distribuciju i prodaju zlonamjernog softvera za krađu informacija LummaC2 (također poznat kao Lumma Infostealer, Lumma Stealer). LummaC2 je platforma u obliku zlonamjernog softvera kao usluge (engl. Malware-as-a-Service, MaaS) koja se upotrebljava za krađu osjetljivih osobnih podataka iz preglednika, novčanika za kriptoimovinu ili informacija o sustavu, za uvođenje dodatnog zlonamjernog softvera na zaražene uređaje, krađu kriptovaluta i kampanje špijunaže. Kibernetički napadi koji uključuju zlonamjerni softver LummaC2 upotrebljavaju i financijski motivirani akteri koji predstavljaju kibernetički prijetnju kao što su Storm-113, Storm-1607, Storm-1674, Octo Tempest i drugi. Zlonamjerni softver LummaC2 upotrebljava se za kibernetičke napade na ključne državne funkcije i službe nužne za održavanje ključnih društvenih i gospodarskih aktivnosti država članica. Softver LummaC2 2024. i 2025. bio je jedan od najčešće korištenih alata za krađu informacija u svijetu. Stoga je Maksim Voronin kao programer, distributer i prodavač softvera LummaC2 uključen u kibernetičke napade sa znatnim učinkom, koji predstavljaju vanjsku prijetnju državama članicama, te ih olakšava.	13.7.2026.

ELI: http://data.europa.eu/eli/dec/2026/1713/oj

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
25.	Maksim Aleksandrovich GORDIENKO također poznat kao: Maxim Alexandrovich GORDIENKO	Максим Александрович ГОРДИЕНКО također poznat kao: ‚Lummaseller' Državljanstvo: rusko Spol: muški	Maksim Gordienko također poznat kao Lummaseller uključen je u razvoj i distribuciju zlonamjernog softvera za krađu informacija LummaC2 (također poznat kao Lumma Infostealer, Lumma Stealer). LummaC2 je platforma u obliku zlonamjernog softvera kao usluge (engl. Malware-as-a-Service, MaaS) koja se upotrebljava za krađu osjetljivih osobnih podataka iz preglednika, novčanika za kriptoimovinu ili informacija o sustavu, za uvođenje dodatnog zlonamjernog softvera na zaražene uređaje, krađu kriptovaluta i kampanje špijunaže. Kibernetički napadi koji uključuju zlonamjerni softver LummaC2 upotrebljavaju i financijski motivirani akteri koji predstavljaju kibernetički prijetnju kao što su Storm-113, Storm-1607, Storm-1674, Octo Tempest i drugi. Zlonamjerni softver LummaC2 upotrebljava se za kibernetičke napade na ključne državne funkcije i službe nužne za održavanje ključnih društvenih i gospodarskih aktivnosti država članica. Softver LummaC2 2024. i 2025. bio je jedan od najčešće korištenih alata za krađu informacija u svijetu. Stoga je Maksim Gordienko kao programer, distributer i prodavatelj softvera LummaC2 uključen u kibernetičke napade sa znatnim učinkom, koji predstavljaju vanjsku prijetnju državama članicama, te ih olakšava.	13.7.2026.

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
26.	Evgeniy Viktorovich BASHEV	Евгений Викторович БАШЕВ Datum rođenja: 25.1.1980. Mjesto rođenja: SSSR Državljanstvo: rusko Spol: muški Povezane osobe: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin Povezani subjekti: Jedinica 29155 GRU-a, ‚Impuls' LLC	Evgeniy Bashev član je jedinice 29155 ruske vojne obavještajne agencije GRU. U okviru te jedinice podupire i olakšava kibernetičke napade sa znatnim učinkom na države članice, među ostalim upravljanjem poslužiteljem ‚Aegon', koji se koristi za operacije hakiranja. Konkretno, pruža tehničku i materijalnu potporu za kibernetičke napade jedinice 29155 GRU-a putem svojeg društva ‚Impuls' LLC, koje je olakšalo operativnu pokrivenost i plaćanja te pružilo infrastrukturu i upravljanje tehničkom imovinom, među ostalim poslužiteljima, koja se upotrebljava za kibernetičke napade. Također je koordinirao suradnju između struktura GRU-a i vanjskih hakerskih mreža. Kibernetički napadi koje je olakšao bili su usmjereni na sustave i službe ključnih državnih funkcija nužne za održavanje ključnih društvenih ili gospodarskih aktivnosti u državama članicama , osobito u prometnom sektoru. U okviru kampanje sa softverom WhisperGate jedinica 29155 GRU-a bila je usmjerena i na ključnu infrastrukturu Ukrajine. Stoga Evgeniy Bashev pruža tehničku i materijalnu potporu za kibernetičke napade za znatnim učinkom ili je na drugi način uključen u takve kibernetičke napade, uključujući pokušaje kibernetičkih napada s potencijalno znatnim učinkom, koji predstavljaju vanjsku prijetnju državama članicama, kao i za kibernetičke napade sa znatnim učinkom protiv treće zemlje. Kao vlasnik i glavni direktor povezan je s društvom ‚Impuls' LLC. Kao član jedinice 29155 GRU-a također je povezan s tim subjektom.	13.7.2026.

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
27.	Roman Alexandrovich PUNTUS	Роман Александрович ПУНТУС Mjesto rođenja: Russian Federation (Ruska Federacija) Državljanstvo: rusko Spol: muški Povezane osobe: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin, Evgeniy Viktorovich Bashev Povezani subjekti: Jedinica 29155 GRU-a	Roman Puntus član je jedinice 29155 ruske vojne obavještajne agencije GRU. U okviru te jedinice ima vodeću ulogu u organizaciji i koordinaciji kibernetičkih napada sa znatnim učinkom na države članice. Također podupire razvoj unutarnjih kibernetičkih sposobnosti jedinice, uključujući zapošljavanje i nadzor osoblja kao što su hakeri i programeri. Osnivanjem fiktivnog društva ‚Aegeon-Impulse' olakšao je logističke i financijske aspekte kibernetičkih operacija. Pod njegovom je koordinacijom jedinica provela kibernetičke napade usmjerene na sustave i službe ključnih državnih funkcija nužne za održavanje ključnih društvenih ili gospodarskih aktivnosti u državama članicama, osobito u prometnom sektoru. U okviru kampanje sa softverom WhisperGate jedinica 29155 GRU-a bila je usmjerena i na ključnu infrastrukturu Ukrajine. Stoga je Roman Puntus odgovoran za kibernetičke napade za znatnim učinkom ili je na drugi način uključen u takve kibernetičke napade, uključujući pokušaje kibernetičkih napada s potencijalno znatnim učinkom, koji predstavljaju vanjsku prijetnju državama članicama, kao i za kibernetičke napade sa znatnim učinkom protiv treće zemlje. Kao član jedinice 29155 GRU-a također je povezan s tim subjektom.	13.7.2026.”

2. sljedeći unosi dodaju se pod naslovom „B. Pravne osobe, subjekti i tijela”:

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
„8.	Media Land LLC	Adresa: Tsvetnochnaya st., 16 Litera P, Room 27 Moskovskaya Zastava Municipal District St Petersburg (Sankt Peterburg), 196006, Ruska Federacija Vrsta subjekta: društvo s ograničenom odgovornošću Mjesto registracije: Sankt Peterburg Datum registracije: 19.10.2015. Registracijski broj: 1152536009900 Glavno sjedište: Sankt Peterburg, Ruska Federacija Povezani subjekti: ML.Cloud	Društvo Media Land LLC koje pruža uslugama smještaja na poslužiteljima bez kontrole sadržaja (engl. bulletproof hosting) od 2016. olakšava širok niz napada zlonamjernim softverom i na države članice i širom svijeta tako što nudi usluge smještaja na poslužiteljima kojima se prikrivaju korisnički identiteti i odupire mjerama tijela za izvršavanje zakonodavstva, što je dovelo do znatnih financijskih gubitaka. Društvo Media Land LLC omogućilo je operacije s ucjenjivačkim programima velikih razmjera, usluge za zapovijedanje i kontrolu te operacije phishinga usmjerene na ključnu infrastrukturu i službe među državama članicama. Operacije koje je olakšalo društvo Media Land LLC uključuju, među ostalim, skupine LockBit, EvilCorp i BlackBasta. Stoga je društvo Media Land LLC uključeno u kibernetičke napade sa znatnim učinkom koji predstavljaju vanjsku prijetnju državama članicama.	13.7.2026.

ELI: http://data.europa.eu/eli/dec/2026/1713/oj

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
9.	ML.Cloud	Adresa: Brivibas iela 52, Riga, LV-1011, Latvija; Russian Federation (Ruska Federacija), Kazan, Peterburgskaya st. 52 Mjesto registracije: Riga Povezane osobe: Alexander Volosovik Ostali povezani subjekti: Media Land LLC	ML.Cloud sestrinsko je društvo društva Media Land LLC kojemu osigurava tehničku infrastrukturu. Društvo Media Land LLC koje pruža uslugama smještaja na poslužiteljima bez kontrole sadržaja (engl. bulletproof hosting) od 2016. olakšava širok niz napada zlonamjernim softverom i na države članice i širom svijeta tako što nudi usluge smještaja na poslužiteljima kojima se prikrivaju korisnički identiteti i odupire mjerama tijela za izvršavanje zakonodavstva, što je dovelo do znatnih financijskih gubitaka. Društvo Media Land LLC omogućilo je operacije s ucjenjivačkim programima velikih razmjera, usluge za zapovijedanje i kontrolu te operacije phishinga usmjerene na ključnu infrastrukturu i službe među državama članicama. Operacije koje je olakšalo društvo Media Land LLC uključuju, među ostalim, skupine LockBit, EvilCorp i BlackBasta. Stoga je društvo Media Land LLC uključeno u kibernetičke napade koji predstavljaju vanjsku prijetnju sa znatnim učinkom za države članice EU-a. Stoga društvo ML.Cloud pruža tehnički potporu za kibernetičke napade sa znatnim učinkom koji predstavljaju vanjsku prijetnju državama članicama.	13.7.2026.

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
10.	‚Impuls' LLC	Общество с ограниченной ответственностью ‚Импульс' Adresa: 344015, Ruska Federacija, Rostov Region, Rostov-on-Don, ul. Eremenko, d. 56, k. 6, apt. 88 Vrsta subjekta: društvo s ograničenom odgovornošću Mjesto registracije: Interdistrict Inspectorate of the Federal Tax Service No. 26 for the Rostov Region, 344019, Rostov-on-Don, ul. Myasnikova, d. 52/32, Ruska Federacija Datum registracije: 27.9.2010. Registracijski broj: Ruski porezni identifikacijski broj (INN) (ИНН): 6168033776, Primarni nacionalni identifikacijski broj (OGRN) (ОГРН): 1106194004850 Glavno sjedište: Ruska Federacija Povezane osobe: Evgeniy Bashev Povezani subjekti: Jedinica 29155 GRU-a	‚Impuls' LLC rusko je društvo u vlasništvu Evgeniya Viktorovicha Basheva, člana jedinice 29155 ruske vojne obavještajne agencije GRU. Poduzeće pruža tehničku i materijalnu potporu za kibernetičke napade i pokušaje kibernetičkih napada koje je izvela jedinica 29155 GRU-a. Društvo ‚Impuls' LLC osobito služi kao operativni posrednik koji omogućuje aktivnosti povezane s hakiranjem putem društva koje formalno nije povezano s ruskom državom. Olakšalo je operativno pokriće i plaćanja te pružilo infrastrukturu za kibernetičke napade te je bilo povezano s tehničkom imovinom, među ostalim poslužiteljima koji se upotrebljavaju za potporu aktivnostima hakiranja. Konkretno, društvo ‚Impuls' LLC omogućilo je suradnju između struktura GRU-a i vanjskih hakerskih mreža. Kibernetičke operacije koje olakšava društvo ‚Impuls' LLC usmjerene su na ključne državne funkcije i službe nužne za održavanje ključnih društvenih i gospodarskih aktivnosti u državama članicama, posebno u prometnom sektoru. U okviru kampanje sa softverom WhisperGate jedinica 29155 GRU-a bila je usmjerena i na ključnu infrastrukturu Ukrajine. Stoga društvo ‚Impuls' LLC pruža tehničku i materijalnu potporu za kibernetičke napade za znatnim učinkom ili je na drugi način uključeno u takve kibernetičke napade, koji predstavljaju vanjsku prijetnju državama članicama, kao i za kibernetičke napade sa znatnim učinkom protiv treće zemlje.	13.7.2026.

ELI: http://data.europa.eu/eli/dec/2026/1713/oj

	Ime	Identifikacijski podaci	Obrazloženje	Datum uvrštenja na popis
11.	Z-Pentest	također poznat kao: ‚Z-Pentest Alliance', ‚Z-Alliance' Glavno sjedište: Ruska Federacija Povezane osobe: Yuliya Pankratova Povezani subjekti: Cyber Army of Russia Reborn / CARR Račun na društvenoj mreži X.com: ZPentest (suspendiran račun) Račun na platformi Telegram: Zpentestalliance	Z-Pentest je proruska skupina za hakerski aktivizam koja se sastoji od članova skupina CARR (Cyber Army of Russia Reborn) i NoName057 i koja je usmjerena na ključnu infrastrukturu u cijelom svijetu, osobito energetski i vodni sektor. Konkretno, skupina je u prosincu 2024. napala dansko poduzeće za vodoopskrbu. Stoga je skupina Z-Pentest odgovorna za kibernetičke napade sa znatnim učinkom koji predstavljaju vanjsku prijetnju državama članicama.	13.7.2026.”