2026/1713

13.7.2026

ROZHODNUTIE RADY (SZBP) 2026/1713

z 13. júla 2026,

ktorým sa mení rozhodnutie (SZBP) 2019/797 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty

RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o Európskej únii, a najmä na jej článok 29,

so zreteľom na návrh vysokej predstaviteľky Únie pre zahraničné veci a bezpečnostnú politiku,

keďže:

(1) Rada 17. mája 2019 prijala rozhodnutie (SZBP) 2019/797 ([1]).

(2) V rámci trvalých, prispôsobených a koordinovaných opatrení Únie proti pretrvávajúcim aktérom v oblasti kybernetických hrozieb by sa na zoznam fyzických a právnických osôb, subjektov a orgánov, na ktoré sa vzťahujú reštriktívne opatrenia, uvedeného v prílohe k rozhodnutiu (SZBP) 2019/797 malo doplniť osem fyzických osôb a štyri subjekty. Uvedené osoby a subjekty sú zodpovedné za kybernetické útoky so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty, tieto útoky podporujú alebo sa na nich podieľajú.

(3) Rozhodnutie (SZBP) 2019/797 by sa preto malo zodpovedajúcim spôsobom zmeniť,

PRIJALA TOTO ROZHODNUTIE:

Článok 1

Príloha k rozhodnutiu (SZBP) 2019/797 sa mení v súlade s prílohou k tomuto rozhodnutiu.

Článok 2

Toto rozhodnutie nadobúda účinnosť dňom jeho uverejnenia v *Úradnom vestníku Európskej únie*.

V Bruseli 13. júla 2026

Za Radu
predsedníčka
K. KALLAS

([1]) Rozhodnutie Rady (SZBP) 2019/797 zo 17. mája 2019 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty (Ú. v. EÚ L 129 I, 17.5.2019, s. 13, ELI: http://data.europa.eu/eli/dec/2019/797/oj).

PRÍLOHA

Príloha k rozhodnutiu (SZBP) 2019/797 sa mení takto:

1. V časti „A. Fyzické osoby“ sa dopĺňajú tieto záznamy:

	Meno	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia na zoznam
„20.	Vitaly Nikolayevich KOVALEV	Виталий Николаевич КОВАЛЕВ alias: ‚Bentley‘, ‚Bergen‘, ‚Alex Konor‘, ‚Benny‘, ‚Ben‘, ‚Stern‘ Dátum narodenia: 23.6.1988 Adresa: Serebristy Bulvar 34 (Serebristyy Bul'var); krp 1; flt 528; 197341; St Petersburg, Russian Federation Štátna príslušnosť: ruská Pohlavie: muž Subjekty, s ktorými je spojený: TrickBot, Wizard Spider, Conti	Vitalij Kovalev (Vitaly Kovalev) je vplyvnou osobnosťou spojenou s malvérovými programami Trickbot a Conti. Je známy aj pod online prezývkami ‚Bentley‘, ‚Bergen‘, ‚Alex Konor‘, ‚Benny‘, ‚Ben‘ a ‚Stern‘. Programy Conti a TrickBot vytvorila a vyvinula skupina Wizard Spider. Skupina Wizard Spider viedla ransomvérové kampane v rôznych odvetviach vrátane základných služieb, ako je zdravotníctvo a bankovníctvo, nakazila počítače na celom svete a jej malvér sa rozvinul do vysoko modulárneho malvérového balíka. Kampane skupiny Wizard Spider s použitím malvéru, ako je Conti a TrickBot, spôsobili v Európskej únii značné hospodárske škody. Vitalij Kovalev sa je preto zodpovedný za kybernetické útoky so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty, a podieľa sa na nich.	13.7.2026

	Meno	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia na zoznam
21.	Alexander Alexandrovich VOLOSOVIK	Александр Александрович ВОЛОСОВИК Dátum narodenia: 30.1.1983 Miesto narodenia: ZSSR Štátna príslušnosť: ruská Číslo cestovného pasu: 762988138 Pohlavie: muž Subjekty, s ktorými je spojený: Yalishanda, LARVA-34, podzemniyl, Ohyeahhellno, Stas_vl, downlow	Alexander Volosovik je vlastníkom spoločnosti Media Land LLC. Spoločnosť Bullet Proof Hosting service Media Land LLC od roku 2016 uľahčuje širokú škálu malvérových útokov proti Únii aj na celom svete tým, že ponúka hostingové služby, ktoré skrývajú totožnosť používateľov a sú odolné proti zásahom orgánov presadzovania práva. Spoločnosť Media Land LLC umožnila rozsiahle ransomvérové operácie, prevzatie riadenia a kontroly a phishingové operácie zamerané na kritickú infraštruktúru a základné služby v členských štátoch, čo viedlo k značným finančným stratám. Spoločnosť Media Land LLC podporila okrem iného operácie skupín LockBit, EvilCorp a BlackBasta. Spoločnosť Media Land LLC sa preto podieľa na kybernetických útokoch so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu a jej členské štáty. Alexander Volosovik je ako vlastník spoločnosti Media Land LLC zodpovedný za tieto kybernetické útoky a podieľa sa na nich. Je tiež spojený so spoločnosťou Media Land LLC.	13.7.2026

	Meno	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia na zoznam
22.	Denis Olegovich DEGTYARENKO	Денис Олегович ДЕГТЯРЕНКО alias: ‚Dena‘ Dátum narodenia: 9.10.1989 Miesto narodenia: ZSSR Štátna príslušnosť: ruská Pohlavie: muž Adresa: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation	Denis Degtjarenko (Denis Degtyarenko) známy tiež ako Dena je ruský hacker, ktorý pracuje pre skupinu CARR (Cyber Army of Russia Reborn). Skupina CARR je zodpovedná za kybernetické útoky proti službám potrebným na zachovanie základných hospodárskych činností a kritických funkcií štátu v členských štátoch, ako aj proti infraštruktúre na Ukrajine a v iných tretích krajinách. Skupina CARR je prepojená s Hlavným strediskom pre špeciálne technológie (GTsST) Hlavného riaditeľstva Generálneho štábu ozbrojených síl Ruskej federácie (GRU). GTsST naďalej aktívne vykonáva kybernetické útoky proti Únii alebo jej členským štátom. Medzi ciele skupiny CARR patria vládne agentúry, finančné inštitúcie, médiá a kritická infraštruktúra v členských štátoch a Spojených štátoch. Skupina CARR uskutočnila distribuované útoky na vyradenie služby (DDoS) na Ukrajine a proti vládam a spoločnostiam nachádzajúcim sa v krajinách, ktoré podporujú Ukrajinu. Denis Degtjarenko, hlavný hacker skupiny CARR, sa preto podieľa na kybernetických útokoch so závažným vplyvom vrátane pokusov o kybernetické útoky s potenciálne závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre členské štáty, ako aj na kybernetických útokoch na tretie štáty. Ako člen skupiny CARR je tiež spojený s GTsST.	13.7.2026

	Meno	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia na zoznam
23.	Yuliya Vladimirovna PANKRATOVA	Юлия Владимировна ПАНКРАТОВА alias: ‚YUliYA‘ Dátum narodenia: 6.4.1984 Miesto narodenia: ZSSR Štátna príslušnosť: ruská Pohlavie: žena Adresa: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation	Julija Pankratová (Yuliya Pankratova) je ruská hackerka, ktorá pracovala pre skupinu CARR (Cyber Army of Russia Reborn) a potom založila skupinu Z-Pentest, pre ktorú naďalej pracuje. Skupina CARR je zodpovedná za kybernetické útoky proti službám potrebným na zachovanie základných hospodárskych činností a kritických funkcií štátu v členských štátoch, ako aj proti infraštruktúre na Ukrajine a v iných tretích krajinách. Skupina CARR je prepojená s Hlavným strediskom pre špeciálne technológie (GTsST) Hlavného riaditeľstva Generálneho štábu ozbrojených síl Ruskej federácie (GRU). GTsST naďalej aktívne vykonáva kybernetické útoky proti Únii alebo jej členským štátom. Medzi ciele skupiny CARR patria vládne agentúry, finančné inštitúcie, médiá a kritická infraštruktúra v členských štátoch a Spojených štátoch. Skupina CARR uskutočnila distribuované útoky na vyradenie služby (DDoS) na Ukrajine a proti vládam a spoločnostiam nachádzajúcim sa v krajinách, ktoré podporujú Ukrajinu. Skupina Z-Pentest je zodpovedná za kybernetické útoky so závažným vplyvom okrem iného na služby potrebné na zachovanie základných činností v členských štátoch. Julija Pankratová, popredná hackerka skupín CARR a Z-Pentest, sa preto podieľa na kybernetických útokoch so závažným vplyvom vrátane pokusov o kybernetické útoky s potenciálne závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre členské štáty, ako aj na kybernetických útokoch na tretie štáty. Je tiež spojená so skupinou Z-Pentest.	13.7.2026

	Meno	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia na zoznam
24.	Maksim Evgenevich VORONIN	Максим Евгеньевич ВОРОНИН alias: ‚Daugn0‘ Štátna príslušnosť: údajne ruská Pohlavie: muž	Maksim Voronin, známy tiež ako Daugn0, sa podieľa na vývoji, distribúcii a predaji malvéru LummaC2 (známeho tiež ako Lumma Infostealer, Lumma Stealer), ktorý kradne informácie. LummaC2 je platforma MaaS (mobilita ako služba), ktorá sa používa na krádež citlivých údajov, prihlasovacích údajov uložených v prehliadačoch, kryptopeňaženiek alebo systémových informácií, na nasadenie doplnkového malvéru do infikovaných zariadení, na krádež kryptomien a na špionážne kampane. Kybernetické útoky pomocou malvéru LummaC2 využívajú aj finančne motivovaní aktéri kybernetických hrozieb, ako sú Storm-113, Storm-1607, Storm-1674, Octo Tempest a iní. Malvér LummaC2 sa používa na kybernetické útoky proti kritickým funkciám a službám štátu potrebným na zachovanie základných sociálnych a hospodárskych činností členských štátov. V rokoch 2024 a 2025 bol malvér LummaC2 jedným z najpoužívanejších nástrojov na krádež informácií na celom svete. Maksim Voronin je ako vývojár, distribútor a predajca malvéru LummaC2 sa preto podieľa na kybernetických útokoch so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre členské štáty, a uľahčuje ich.	13.7.2026

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

	Meno	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia na zoznam
25.	Maksim Aleksandrovich GORDIENKO alias Maxim Alexandrovich GORDIENKO	Максим Александрович ГОРДИЕНКО alias ‚Lummaseller‘ Štátna príslušnosť: údajne ruská Pohlavie: muž	Maksim Gordienko sa podieľa na vývoji a distribúcii malvéru LummaC2 (známeho tiež ako Lumma Infostealer, Lumma Stealer), ktorý kradne informácie. LummaC2 je platforma MaaS (mobilita ako služba), ktorá sa používa na krádež citlivých údajov, prihlasovacích údajov uložených v prehliadačoch, kryptopeňaženiek alebo systémových informácií, na nasadenie doplnkového malvéru do infikovaných zariadení, na krádež kryptomien a na špionážne kampane. Kybernetické útoky pomocou malvéru LummaC2 využívajú aj finančne motivovaní aktéri kybernetických hrozieb, ako sú Storm-113, Storm-1607, Storm-1674, Octo Tempest a iní. Malvér LummaC2 sa používa na kybernetické útoky proti kritickým funkciám a službám štátu potrebným na zachovanie základných sociálnych a hospodárskych činností členských štátov. V rokoch 2024 a 2025 bol malvér LummaC2 jedným z najpoužívanejších nástrojov na krádež informácií na celom svete. Maksim Gordienko je ako vývojár, distribútor a predajca malvéru LummaC2 sa preto podieľa na kybernetických útokoch so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre členské štáty, a uľahčuje ich.	13.7.2026

	Meno	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia na zoznam
26.	Evgeniy Viktorovich BASHEV	Евгений Викторович БАШЕВ Dátum narodenia: 25.1.1980 Miesto narodenia: ZSSR Štátna príslušnosť: ruská Pohlavie: muž Osoby, s ktorými je spojený: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin Subjekty, s ktorými je spojený: GRU Unit 29155, Impuls LLC	Jevgenij Bašev (Evgeniy Bashev) je členom jednotky 29155 ruskej vojenskej spravodajskej služby GRU. V rámci tejto jednotky podporuje a uľahčuje kybernetické útoky so závažným vplyvom na členské štáty, okrem iného prostredníctvom kontroly servera Aegon, ktorý sa používa na hackerské operácie. Poskytuje najmä technickú a materiálnu podporu kybernetickým útokom jednotky GRU 29155 prostredníctvom svojej spoločnosti Impuls LLC, ktorá uľahčuje operačné krytie, infraštruktúru a platby a spravuje technické aktíva vrátane serverov, ktoré sa používajú na kybernetické útoky. Taktiež koordinoval spoluprácu medzi štruktúrami GRU a externými hackerskými sieťami. Kybernetické útoky, ktoré uľahčoval, sa zameriavali na systémy a služby kritických štátnych orgánov potrebné na zachovanie základných sociálnych alebo hospodárskych činností v členských štátoch, najmä v odvetví dopravy. V rámci kampane WhisperGate sa jednotka GRU 29155 zamerala aj na kritickú infraštruktúru Ukrajiny. Jevgenij Bašev preto poskytuje technickú a materiálnu podporu kybernetickým útokom so závažným vplyvom vrátane pokusov o kybernetické útoky s potenciálne závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre členské štáty, ako aj kybernetickým útokom so závažným vplyvom na tretiu krajinu, alebo sa na týchto útokoch inak podieľa. Ako vlastník a generálny riaditeľ je spojený so spoločnosťou Impuls LLC. Ako člen jednotky GRU 29155 je spojený aj s týmto subjektom.	13.7.2026

	Meno	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia na zoznam
27.	Roman Alexandrovich PUNTUS	Роман Александрович ПУНТУС Miesto narodenia: Ruská federácia Štátna príslušnosť: ruská Pohlavie: muž Osoby, s ktorými je spojený: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin, Evgeniy Viktorovich Bashev Subjekty, s ktorými je spojený: GRU Unit 29155	Roman Puntus je členom jednotky 29155 ruskej vojenskej spravodajskej služby GRU. V rámci tejto jednotky zohráva vedúcu úlohu pri organizácii a koordinácii kybernetických útokov so závažným vplyvom na členské štáty. Podporuje aj rozvoj interných kybernetických spôsobilostí tejto jednotky, čo zahŕňa aj nábor pracovníkov, ako sú hackeri a programátori, a dohľad nad nimi. Zriadením krycej spoločnosti Aegeon-Impulse uľahčil logistické a finančné aspekty kybernetických operácií. Koordinoval kybernetické útoky uvedenej jednotky, ktoré sa zameriavali na systémy a služby kritických štátnych orgánov potrebné na zachovanie základných sociálnych alebo hospodárskych činností v členských štátoch, najmä v odvetví dopravy. V rámci kampane WhisperGate sa jednotka GRU 29155 zamerala aj na kritickú infraštruktúru Ukrajiny. Roman Puntus nesie zodpovednosť za kybernetické útoky so závažným vplyvom vrátane pokusov o kybernetické útoky s potenciálne závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre členské štáty, ako aj za kybernetické útoky so závažným vplyvom na tretiu krajinu, alebo sa na týchto útokoch inak podieľa. Ako člen jednotky GRU 29155 je spojený aj s týmto subjektom.	13.7.2026“.

2. V časti „B. Právnické osoby, subjekty a orgány“ sa dopĺňajú tieto záznamy:

	Názov	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia na zoznam
„8.	Media Land LLC	Adresa: Tsvetnochnaya st., 16 Litera P, Room 27, Moskovskaya Zastava Municipal District St Petersburg, 196006, Russian Federation Druh subjektu: spoločnosť s ručením obmedzeným Miesto registrácie: Petrohrad Dátum registrácie: 19.10.2015 Registračné číslo: 1152536009900 Hlavné miesto podnikateľskej činnosti: Petrohrad, Ruská federácia Subjekt, s ktorým je spojený: ML.Cloud	Spoločnosť Bullet Proof Hosting service Media Land LLC od roku 2016 uľahčuje širokú škálu malvérových útokov proti členským štátom a na celom svete tým, že ponúka hostingové služby, ktoré skrývajú totožnosť používateľov a sú odolné proti zásahom orgánov presadzovania práva, čo spôsobuje značné finančné straty. Spoločnosť Media Land LLC umožnila rozsiahle ransomvérové operácie, prevzatie riadenia a kontroly a phishingové operácie zamerané na kritickú infraštruktúru a základné služby v členských štátoch. Spoločnosť Media Land LLC podporila okrem iného operácie skupín LockBit, EvilCorp a BlackBasta. Spoločnosť Media Land LLC sa preto podieľa na kybernetických útokoch so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre členské štáty.	13.7.2026

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

	Názov	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia na zoznam
9.	ML.Cloud	Adresa: Brivibas iela 52, Riga, LV-1011, Latvija; Russian Federation, Kazan, Peterburgskaya st. 52 Miesto registrácie: Riga Osoby, s ktorými je spojená: Alexander Volosovik Ďalšie subjekty, s ktorými je spojená: Media Land LLC	ML.Cloud je sesterskou spoločnosťou spoločnosti Media Land LLC a poskytuje spoločnosti Media Land LLC technickú infraštruktúru. Spoločnosť Bullet Proof Hosting service Media Land LLC od roku 2016 uľahčuje širokú škálu malvérových útokov proti členským štátom a na celom svete tým, že ponúka hostingové služby, ktoré skrývajú totožnosť používateľov a sú odolné proti zásahom orgánov presadzovania práva, čo spôsobuje značné finančné straty. Spoločnosť Media Land LLC umožnila rozsiahle ransomvérové operácie, prevzatie riadenia a kontroly a phishingové operácie zamerané na kritickú infraštruktúru a základné služby v členských štátoch. Spoločnosť Media Land LLC podporila okrem iného operácie skupín LockBit, EvilCorp a BlackBasta. Spoločnosť Media Land LLC sa preto podieľa na kybernetických útokoch, ktoré predstavujú vonkajšiu hrozbu so závažným vplyvom na členské štáty EÚ. Spoločnosť ML.Cloud preto poskytuje technickú podporu kybernetickým útokom so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre členské štáty.	13.7.2026

	Názov	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia na zoznam
10.	Impuls LLC	Общество с ограниченной ответственностью ‚Импульс' Adresa: 344015, Russian Federation, Rostov Region, Rostov-on-Don, ul. Eremenko, d. 56, k. 6, apt. 88 Druh subjektu: spoločnosť s ručením obmedzeným Miesto registrácie: Interdistrict Inspectorate of the Federal Tax Service No. 26 for the Rostov Region, 344019, Rostov-on-Don, ul. Myasnikova, d. 52/32, Russian Federation Dátum registrácie: 27.9.2010 Registračné číslo: INN (ИНН): 6168033776; OGRN (ОГРН): 1106194004850 Hlavné miesto podnikateľskej činnosti: Ruská federácia Osoby, s ktorými je spojená: Evgeniy Bashev Subjekty, s ktorými je spojená: GRU Unit 29155	Impuls LLC je ruská spoločnosť vo vlastníctve Jevgenija Viktoroviča Baševa, člena jednotky 29155 ruskej vojenskej spravodajskej služby GRU. Spoločnosť poskytuje technickú a materiálnu podporu kybernetickým útokom a pokusom o kybernetické útoky, ktoré vykonáva jednotka GRU 29155. Spoločnosť Impuls LLC pôsobí najmä ako operačný sprostredkovateľ, ktorý umožňuje vykonávať činnosti súvisiace s hackerskými útokmi, ktoré je potrebné uskutočniť prostredníctvom spoločnosti formálne neprepojenej s ruským štátom. Uľahčila operačné krytie, infraštruktúru a platby za kybernetické útoky a bola spojená s technickými prostriedkami vrátane serverov používaných na podporu hackerských činností. Spoločnosť Impuls LLC umožnila najmä spoluprácu medzi štruktúrami GRU a externými hackerskými sieťami. Kybernetické operácie uľahčované spoločnosťou Impuls LLC sa zameriavajú na kritické funkcie a služby štátu potrebné na zachovanie základných sociálnych a hospodárskych činností v členských štátoch, najmä v odvetví dopravy. V rámci kampane WhisperGate sa jednotka GRU 29155 zamerala aj na kritickú infraštruktúru Ukrajiny. Spoločnosť Impuls LLC preto poskytuje technickú a materiálnu podporu kybernetickým útokom so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre členské štáty, ako aj kybernetickým útokom so závažným vplyvom na tretiu krajinu, alebo sa na týchto útokoch inak podieľa.	13.7.2026

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

	Názov	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia na zoznam
11.	Z-Pentest	alias: ‚Z-Pentest Alliance', ‚Z-Alliance' Hlavné miesto podnikateľskej činnosti: Ruská federácia Osoby, s ktorými je spojená: Yuliya Pankratova Subjekty, s ktorými je spojená: Cyber Army of Russia Reborn/CARR Účet na X.com: ZPentest (pozastavený) Účet na Telegrame: Zpentestalliance	Z-Pentest je proruská skupina hakerských aktivistov zložená z členov skupín CARR (Cyber Army of Russia Reborn) a NoName057, ktorá sa celosvetovo zameriava na kritickú infraštruktúru, najmä na odvetvie energetiky a vodného hospodárstva. Konkrétne skupina v decembri 2024 zaútočila na dánsku vodárenskú spoločnosť. Skupina Z-Pentest je preto zodpovedná za kybernetické útoky so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre členské štáty.	13.7.2026“.