2026/1713

13.7.2026

ROZHODNUTÍ RADY (SZBP) 2026/1713

ze dne 13. července 2026,

kterým se mění rozhodnutí (SZBP) 2019/797 o omezujících opatřeních proti kybernetickým útokům ohrožujícím Unii nebo její členské státy

RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o Evropské unii, a zejména na článek 29 této smlouvy,

s ohledem na návrh vysoké představitelky Unie pro zahraniční věci a bezpečnostní politiku,

vzhledem k těmto důvodům:

(1) Dne 17. května 2019 přijala Rada rozhodnutí (SZBP) 2019/797 ([1]).

(2) V rámci soustavných, individualizovaných a koordinovaných opatření Unie zaměřených proti aktérům přetrvávajících kybernetických hrozeb by na seznam fyzických a právnických osob, subjektů a orgánů, na něž se vztahují omezující opatření, obsažený v příloze rozhodnutí (SZBP) 2019/797, mělo být zařazeno osm fyzických osob a čtyři subjekty. Tyto osoby a subjekty jsou odpovědné za kybernetické útoky s významným dopadem, které představují vnější hrozbu pro Unii nebo její členské státy, tyto útoky podporují nebo jsou nich zapojeny.

(3) Rozhodnutí (SZBP) 2019/797 by proto mělo být odpovídajícím způsobem změněno,

PŘIJALA TOTO ROZHODNUTÍ:

Článek 1

Příloha rozhodnutí (SZBP) 2019/797 se mění v souladu s přílohou tohoto rozhodnutí.

Článek 2

Toto rozhodnutí vstupuje v platnost dnem vyhlášení v *Úředním věstníku Evropské unie*.

V Bruselu dne 13. července 2026.

Za Radu

předsedkyně

K. KALLAS

([1]) Rozhodnutí Rady (SZBP) 2019/797 ze dne 17. května 2019 o omezujících opatřeních proti kybernetickým útokům ohrožujícím Unii nebo její členské státy (Úř. věst. L 129 I, 17.5.2019, s. 13, ELI: http://data.europa.eu/eli/dec/2019/797/oj).

PŘÍLOHA

Příloha rozhodnutí (SZBP) 2019/797 se mění takto:

1) V oddíle „A. Fyzické osoby“ se doplňují nové položky, které znějí:

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
„20.	Vitaly Nikolayevich KOVALEV	Виталий Николаевич КОВАЛЕВ Také znám jako: ‚Bentley‘, ‚Bergen‘, ‚Alex Konor‘, ‚Benny‘, ‚Ben‘, ‚Stern‘ Datum narození: 23.6.1988 Adresa: Serebristy Bulvar 34 (Serebristyy Bul'var); krp 1; flt 528; 197341; Petrohrad, Ruská federace Státní příslušnost: ruská Pohlaví: muž Přidružené subjekty: TrickBot, Wizard Spider, Conti	Vitalij Kovalev (Vitaly Kovalev) je vysoce postavenou figurou malwarových programů ‚Trickbot‘ a ‚Conti‘. Je znám také pod online přezdívkami ‚Bentley‘, ‚Bergen‘, ‚Alex Konor‘, ‚Benny‘, ‚Ben‘ a ‚Stern‘. Malwarové programy ‚Conti‘ a ‚Trickbot‘ byly původně vytvořeny a vyvinuty skupinou ‚Wizard Spider‘. Skupina Wizard Spider vedla ransomwarové kampaně v různých odvětvích, včetně základních služeb, jako je zdravotnictví a bankovnictví, infikovala počítače po celém světě a z jejich malwaru se stala vysoce modulární sada malwaru. Kampaně skupiny Wizard Spider využívající malwary, jako jsou ‚Conti‘ a ‚TrickBot‘, způsobily v Evropské unii značné hospodářské škody. Vitalij Kovalev je tudíž odpovědný za kybernetické útoky s významným dopadem, které představují vnější hrozbu pro Unii nebo její členské státy, a je do těchto útoků zapojen.	13.7.2026

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
21.	Alexander Alexandrovich VOLOSOVIK	Александр Александрович ВОЛОСОВИК Datum narození: 30.1.1983 Místo narození: SSSR Státní příslušnost: ruská Číslo pasu: 762988138 Pohlaví: muž Přidružené subjekty: Yalishanda, LARVA-34, podzemniyl, Ohyeahhellno, Stas_vl, downlow	Alexandr Volosovik (Alexander Volosovik) je vlastníkem společnosti Media Land LLC. Společnost Media Land LLC jako poskytovatel ‚neprůstřelného hostingu' od roku 2016 usnadňuje širokou škálu malwarových útoků proti Unii i na celém světě tím, že nabízí hostingové služby, které skrývají totožnost uživatelů a odolávají odstraňování obsahu donucovacími orgány. Media Land LLC umožnila rozsáhlé ransomwarové operace, služby skrytých serverů k ovládání malwaru a phishingové operace zaměřené na kritickou infrastrukturu a základní služby v členských státech, což vedlo ke značným finančním ztrátám. Mezi operacemi usnadněnými společností Media Land LLC jsou mimo jiné operace ‚LockBit', ‚EvilCorp' a ‚BlackBasta'. Společnost Media Land LLC je tudíž zapojena do kybernetických útoků s významným dopadem, které představují vnější hrozbu pro Unii nebo její členské státy. Jako vlastník společnosti Media Land LLC je Alexandr Volosovik za tyto kybernetické útoky odpovědný a je do nich zapojen. Je rovněž spojen se společností Media Land LLC.	13.7.2026

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
22.	Denis Olegovich DEGTYARENKO	Денис Олегович ДЕГТЯРЕНКО Také znám jako: ‚Dena‘ Datum narození: 9.10.1989 Místo narození: SSSR Státní příslušnost: ruská Pohlaví: muž Adresa: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburská oblast, Ruská federace	Denis Degtjarenko (Denis Degtyarenko), také znám jako Dena, je ruský hacker, který pracuje pro skupinu CARR (Cyber Army of Russia Reborn). Skupina CARR je odpovědná za kybernetické útoky na služby nezbytné pro zachování základních hospodářských činností a kritických funkcí státu v členských státech, jakož i na infrastrukturu na Ukrajině a v dalších třetích zemích. CARR je podporována hlavním střediskem pro speciální služby (GTsSS) hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GRU). GTsSS nadále provádí kybernetické útoky proti Unii nebo jejím členským státům. Mezi cíle útoků skupiny CARR patří vládní agentury, finanční instituce, média a kritická infrastruktura v členských státech a ve Spojených státech. CARR provedla útoky DDoS na Ukrajině a na vlády a společnosti se sídlem v zemích, které Ukrajinu podporují. Denis Degtjarenko, přední hacker CARR, je tudíž zapojen do kybernetických útoků s významným dopadem, včetně pokusů o kybernetické útoky s potenciálně významným dopadem, které představují vnější hrozbu pro členské státy, jakož i proti třetím státům. Jako člen skupiny CARR je rovněž spojen s GTsST.	13.7.2026

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
23.	Yuliya Vladimirovna PANKRATOVA	Юлия Владимировна ПАНКРАТОВА Také známa jako: ‚YUliYA‘ Datum narození: 6.4.1984 Místo narození: SSSR Státní příslušnost: ruská Pohlaví: žena Adresa: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburská oblast, Ruská federace	Julija Pankratova (Yuliya Pankratova) je ruská hackerka, která pracuje pro skupinu CARR (Cyber Army of Russia Reborn) a později založila skupinu Z-Pentest, pro kterou nadále pracuje. Skupina CARR je odpovědná za kybernetické útoky na služby nezbytné pro zachování základních hospodářských činností a kritických funkcí státu v členských státech, jakož i na infrastrukturu na Ukrajině a v dalších třetích zemích. CARR je podporována hlavním střediskem pro speciální služby (GTsSS) hlavního ředitelství generálního štábu ozbrojených sil Ruské federace (GRU). GTsSS nadále provádí kybernetické útoky proti Unii nebo jejím členským státům. Mezi cíle útoků skupiny CARR patří vládní agentury, finanční instituce, média a kritická infrastruktura v členských státech a ve Spojených státech. CARR provedla útoky DDoS na Ukrajině a na vlády a společnosti se sídlem v zemích, které Ukrajinu podporují. Skupina Z-Pentest je odpovědná za kybernetické útoky s významným dopadem mimo jiné na služby nezbytné pro zachování základních činností v členských státech. Julija Pankratova, přední hackerka skupin CARR a Z-Pentest, je tudíž zapojena do kybernetických útoků s významným dopadem, včetně pokusů o kybernetické útoky s potenciálně významným dopadem, které představují vnější hrozbu pro členské státy, jakož i pro třetí státy. Je rovněž spojena se skupinou Z-Pentest.	13.7.2026

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
24.	Maksim Evgenevich VORONIN	Максим Евгеньевич ВОРОНИН Také znám jako: ‚Daugn0‘ Státní příslušnost: údajně ruská Pohlaví: muž	Maxim Voronin (Maksim Voronin), také znám jako Daugn0, se podílí na vývoji, distribuci a prodeji malwaru platformy ‚LummaC2‘ zaměřeného na krádeže dat (také znám jako ‚Lumma Infostealer‘ a ‚Lumma Stealer‘). ‚LummaC2‘ je platforma malwarových služeb (Malware-as-a-Service, MaaS), která se používá ke krádežím citlivých dat z internetových prohlížečů, kryptopeněženek nebo systémových informací, k nasazení dalšího malwaru na infikovaných zařízeních, ke krádežím kryptoměn a ke špionážním kampaním. Kybernetické útoky s použitím malwaru platformy ‚LummaC2‘ jsou využívány také finančně motivovanými aktéry kybernetických hrozeb, jako jsou Storm-113, Storm-1607, Storm-1674, Octo Tempest a další. Malware platformy ‚LummaC2‘ byl použit ke kybernetickým útokům na kritické funkce a služby státu nezbytné pro zachování základních sociálních a hospodářských činností členských států. V letech 2024 a 2025 patřila platforma ‚LummaC2‘ mezi celosvětově nejpoužívanější nástroje pro krádeže dat. Maxim Voronin jako vývojář, distributor a prodejce malwaru platformy ‚LummaC2‘ je tudíž zapojen do kybernetických útoků s významným dopadem, které představují vnější hrozbu pro členské státy, a tyto útoky usnadňuje.	13.7.2026

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
25.	Maksim Aleksandrovich GORDIENKO také znám jako Maxim Alexandrovich GORDIENKO	Максим Александрович ГОРДИЕНКО Také znám jako: ‚Lummaseller‘ Státní příslušnost: údajně ruská pohlaví: muž	Maxim Gordijenko (Maksim Gordienko), také znám jako Lummaseller, se podílí na vývoji a distribuci malwaru platformy ‚LummaC2‘ zaměřeného na krádeže dat (také známé jako ‚Lumma Infostealer‘ a ‚Lumma Stealer‘). ‚LummaC2‘ je platforma malwarových služeb (Malware-as-a-Service, MaaS), která se používá ke krádežím citlivých dat z internetových prohlížečů, kryptopeněženek nebo systémových informací, k nasazení dalšího malwaru na infikovaných zařízeních, ke krádežím kryptoměn a ke špionážním kampaním. Kybernetické útoky s použitím malwaru platformy ‚LummaC2‘ jsou využívány také finančně motivovanými aktéry kybernetických hrozeb, jako jsou Storm-113, Storm-1607, Storm-1674, Octo Tempest a další. Malware platformy ‚LummaC2‘ byl použit ke kybernetickým útokům na kritické funkce a služby státu nezbytné pro zachování základních sociálních a hospodářských činností členských států. V letech 2024 a 2025 patřila platforma ‚LummaC2‘ mezi celosvětově nejpoužívanější nástroje pro krádeže dat. Maxim Gordijenko jako vývojář, distributor a prodejce malwaru platformy ‚LummaC2‘ je tudíž zapojen do kybernetických útoků s významným dopadem, které představují vnější hrozbu pro členské státy, a tyto útoky usnadňuje.	13.7.2026

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
26.	Evgeniy Viktorovich BASHEV	Евгений Викторович БАШЕВ Datum narození: 25.1.1980 Místo narození: SSSR Státní příslušnost: ruská Pohlaví: muž Přidružené osoby: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin Přidružené subjekty: Jednotka GRU 29155, ‚Impuls' LLC	Jevgenij Bašev (Evgeniy Bashev) je členem jednotky 29155 ruské vojenské zpravodajské služby GRU. V rámci této jednotky podporuje a usnadňuje kybernetické útoky s významným dopadem na členské státy, mimo jiné ovládáním serveru ‚Aegon', který se používá pro hackerské operace. Zejména poskytuje technickou a materiální podporu kybernetickým útokům jednotky GRU 29155 prostřednictvím své společnosti ‚Impulse' LLC, která usnadňovala provozní krytí, infrastrukturu a platby, a spravovala technická aktiva používaná ke kybernetickým útokům, mimo jiné servery. Rovněž koordinoval spolupráci mezi strukturami GRU a externími sítěmi hackerů. Kybernetické útoky, které zprostředkoval, byly zaměřeny na systémy kritických funkcí a služeb státu nezbytných pro zachování základních sociálních nebo hospodářských činností v členských státech, zejména v odvětví dopravy. Prostřednictvím kampaně ‚WhisperGate' se jednotka GRU 29155 rovněž zaměřila na kritickou infrastrukturu Ukrajiny. Jevgenij Bašev tudíž poskytuje technickou a materiální podporu kybernetickým útokům s významným dopadem, a to i pokusům o útoky s potenciálně významným dopadem, které představují vnější hrozbu pro členské státy, jakož i kybernetickým útokům s významným dopadem proti třetí zemi, nebo je do nich jinak zapojen. Jako vlastník a generální ředitel je spojen se společností ‚Impulse'. Jako člen jednotky 29155 GRU je rovněž spojen s tímto subjektem.	13.7.2026

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

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
27.	Roman Alexandrovich PUNTUS	Роман Александрович ПУНТУС Místo narození: Ruská federace Státní příslušnost: ruská Pohlaví: muž Přidružené osoby: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin, Evgeniy Viktorovich Bashev Přidružené subjekty: Jednotka GRU 29155	Roman Puntus je členem jednotky 29155 ruské vojenské zpravodajské služby GRU. V rámci této jednotky zastává vedoucí úlohu při organizaci a koordinaci kybernetických útoků s významným dopadem na členské státy. Rovněž podporuje rozvoj interních kybernetických kapacit jednotky, včetně náboru pracovníků, jako jsou hackeři a programátoři, a dohledu nad nimi. Zřízením krycí společnosti ‚Aegeon-Impulse' usnadňoval logistické a finanční aspekty kybernetických operací. Koordinoval kybernetické útoky této jednotky zaměřené na systémy kritických funkcí a služeb státu nezbytných pro zachování základních sociálních nebo hospodářských činností v členských státech, zejména v odvětví dopravy. Prostřednictvím kampaně ‚WhisperGate' se jednotka GRU 29155 rovněž zaměřila na kritickou infrastrukturu Ukrajiny. Roman Puntus je tudíž odpovědný za kybernetické útoky s významným dopadem, a to i za pokusy o útoky s potenciálně významným dopadem, které představují vnější hrozbu pro členské státy, jakož i za kybernetické útoky s významným dopadem proti třetí zemi, nebo je do nich jinak zapojen. Jako člen jednotky 29155 GRU je rovněž spojen s tímto subjektem.	13.7.2026“

2) V oddíle „B. Právnické osoby, subjekty a orgány“ se doplňují nové položky, které znějí:

	Název	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
„8.	Media Land LLC	Adresa: Tsvetnochnaya st., 16 Litera P, Room 27 Moskovskaya Zastava Municipal District Petrohrad, 196006, Ruská federace Druh subjektu: společnost s ručením omezeným Místo registrace: Petrohrad Datum registrace: 19.10.2015 Registrační číslo: 1152536009900 Hlavní místo obchodní činnosti: Petrohrad, Ruská federace Přidružený subjekt: ML.Cloud	Společnost Media Land LLC jako poskytovatel ‚neprůstřelného hostingu‘ od roku 2016 usnadňuje širokou škálu malwarových útoků proti členským státům i na celém světě tím, že nabízí hostingové služby, které skrývají totožnost uživatelů a odolávají odstraňování obsahu donucovacími orgány, což vede k významným finančním ztrátám. Media Land LLC umožnila rozsáhlé ransomwarové operace, služby skrytých serverů k ovládání malwaru a phishingové operace zaměřené na kritickou infrastrukturu a základní služby členských států. Mezi operacemi usnadněnými společností Media Land LLC jsou mimo jiné operace ‚LockBit‘, ‚EvilCorp‘ a ‚BlackBasta‘. Společnost Media Land LLC je tudíž zapojena do kybernetických útoků s významným dopadem, které představují vnější hrozbu pro členské státy.	13.7.2026

	Název	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
9.	ML.Cloud	Adresa: Brivibas iela 52, Riga, LV-1011, Lotyšsko; Ruská federace, Kazaň, Peterburgskaya st. 52 Místo registrace: Riga Přidružená osoba: Alexander Volosovik Další přidružené subjekty: Media Land LLC	ML.Cloud je sesterská společnost společnosti Media Land LLC, které poskytuje technickou infrastrukturu. Společnost Media Land LLC jako poskytovatel ‚neprůstřelného hostingu' od roku 2016 usnadňuje širokou škálu malwarových útoků proti členským státům i na celém světě tím, že nabízí hostingové služby, které skrývají totožnost uživatelů a odolávají odstraňování obsahu donucovacími orgány, což vede k významným finančním ztrátám. Media Land LLC umožnila rozsáhlé ransomwarové operace, služby skrytých serverů k ovládání malwaru a phishingové operace zaměřené na kritickou infrastrukturu a základní služby členských států. Mezi operacemi usnadněnými společností Media Land LLC jsou mimo jiné operace ‚LockBit', ‚EvilCorp' a ‚BlackBasta'. Společnost Media Land LLC je tudíž zapojena do kybernetických útoků, které pro členské státy představují vnější hrozbu s významným dopadem. Společnost ML.Cloud tudíž poskytuje technickou podporu kybernetickým útokům s významným dopadem, které představují vnější hrozbu pro členské státy.	13.7.2026

	Název	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
10.	‚Impuls' LLC	Общество с ограниченной ответственностью ‚Импульс' Adresa: 344015, Ruská federace, Rostovská oblast, Rostov na Donu, ul. Eremenko, d. 56, k. 6, apt. 88 Druh subjektu: společnost s ručením omezeným Místo registrace: Interdistrict Inspectorate of the Federal Tax Service No. 26 for the Rostov Region, 344019, Rostov na Donu, ul. Myasnikova, d. 52/32, Ruská federace Datum registrace: 27.9.2010 Registrační číslo: INN (ИНН): 6168033776; OGRN (ОГРН): 1106194004850 Hlavní místo obchodní činnosti: Ruská federace Přidružené osoby: Evgeniy Bashev Přidružené subjekty: Jednotka GRU 29155	‚Impuls' LLC je ruská společnost vlastněná Jevgenijem Viktorovičem Baševem, členem jednotky 29155 ruské vojenské zpravodajské služby GRU. Tato společnost poskytuje technickou a materiální podporu kybernetickým útokům a pokusům o tyto útoky, které provádí jednotka GRU 29155. ‚Impuls' LLC slouží zejména jako provozní zprostředkovatel, který umožňuje provádět činnosti související s hackerskými útoky prostřednictvím společnosti formálně bez vazby na ruský stát. Usnadnila provozní krytí, infrastrukturu a platby za kybernetické útoky a byla spojena s technickými prostředky, včetně serverů používaných na podporu hackerských činností. Společnost ‚Impuls' LLC zejména umožnila spolupráci mezi strukturami GRU a externími hackerskými sítěmi. Kybernetické operace zprostředkované společností ‚Impuls' LLC se zaměřují na kritické státní funkce a služby nezbytné pro zachování základních sociálních nebo hospodářských činností v členských státech, zejména v odvětví dopravy. Prostřednictvím kampaně ‚WhisperGate' se jednotka GRU 29155 rovněž zaměřila na kritickou infrastrukturu Ukrajiny. Společnost ‚Impuls' LLC tudíž poskytuje technickou a materiální podporu kybernetickým útokům s významným dopadem, které představují vnější hrozbu pro členské státy, jakož i kybernetickým útokům s významným dopadem proti třetí zemi, nebo je do nich jinak zapojena.	13.7.2026

	Název	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
11.	Z-Pentest	Také známa jako: ‚Z-Pentest Alliance', ‚Z-Alliance' Hlavní místo obchodní činnosti: Ruská federace Přidružené osoby: Yuliya Pankratova Přidružené subjekty: Cyber Army of Russia/CARR Účet na síti X.com: ZPentest (účet zablokován) Účet na síti Telegram: Zpentestalliance	Z-Pentest je proruská aktivistická hackerská skupina složená z členů skupiny CARR (Cyber Army of Russia Reborn) a skupiny NoName057, která se v globálním měřítku zaměřuje na kritickou infrastrukturu, zejména na odvětví energetiky a vodohospodářství. Především tato skupina v prosinci 2024 zaútočila na dánské vodárenské zařízení. Skupina Z-Pentest je tudíž odpovědná za kybernetické útoky s významným dopadem, které představují vnější hrozbu pro členské státy.	13.7.2026“