2024/1778

24.6.2024

PROVÁDĚCÍ NAŘÍZENÍ RADY (EU) 2024/1778

ze dne 24. června 2024,

kterým se provádí nařízení (EU) 2019/796 o omezujících opatřeních proti kybernetickým útokům ohrožujícím Unii nebo její členské státy

RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o fungování Evropské unie,

s ohledem na nařízení Rady (EU) 2019/796 ze dne 17. května 2019 o omezujících opatřeních proti kybernetickým útokům ohrožujícím Unii nebo její členské státy ([1]), a zejména na čl. 13 odst. 1 uvedeného nařízení,

s ohledem na návrh vysokého představitele Unie pro zahraniční věci a bezpečnostní politiku,

vzhledem k těmto důvodům:

(1) Dne 17. května 2019 přijala Rada nařízení (EU) 2019/796.

(2) Cílená omezující opatření proti kybernetickým útokům s významným dopadem, které představují vnější hrozbu pro Unii nebo její členské státy, patří mezi opatření, která jsou součástí rámce Unie pro společnou diplomatickou reakci na nepřátelské činnosti v kyberprostoru (soubor nástrojů pro diplomacii v oblasti kybernetiky), a jsou klíčovým nástrojem pro prevenci, odstrašování a odrazování od těchto činností a reakci na ně.

(3) Zvyšuje se množství, četnost výskytu i propracovanost nepřátelských činností v kyberprostoru namířených proti kritické infrastruktuře nebo základním službám, a to i činností využívajících ransomwaru a malwarových stíracích programů, jakož i činností zacílených na dodavatelské řetězce a zaměřených na kybernetickou špionáž včetně krádeží duševního vlastnictví. Vzhledem ke svým rušivým a ničivým účinkům představují tyto činnosti systémovou hrozbu pro bezpečnost, ekonomiku, demokracii i společnost Unie jako celek.

(4) Využívání kybernetických operací, které umožnily a doprovázely nevyprovokovanou a neodůvodněnou válečnou agresi Ruska proti Ukrajině, ovlivňuje globální stabilitu a bezpečnost, představuje významné riziko eskalace a přispívá k již tak významnému nárůstu nepřátelských činností v kyberprostoru v posledních letech mimo rámec ozbrojeného konfliktu. Rostoucí kybernetická bezpečnostní rizika a celkově složité prostředí kybernetických hrozeb s jasným rizikem rychlého přelévání kybernetických incidentů z jednoho členského státu do druhého i ze třetích zemí do Unie jsou dále důvodem pro omezující opatření podle nařízení (EU) 2019/796.

(5) 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 I nařízení (EU) 2019/796, mělo být zařazeno šest fyzických osob. Tyto osoby jsou odpovědné za kybernetické útoky s významným dopadem, které představují vnější hrozbu pro Unii nebo její členské státy, nebo byly do těchto útoků zapojeny.

(6) Příloha I nařízení (EU) 2019/796 by proto měla být odpovídajícím způsobem změněna,

PŘIJALA TOTO NAŘÍZENÍ:

Článek 1

Příloha I nařízení (EU) 2019/796 se mění v souladu s přílohou tohoto nařízení.

([1]) Úř. věst. L 129 I, 17.5.2019, s. 1.

Článek 2

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

Toto nařízení je závazné v celém rozsahu a přímo použitelné ve všech členských státech.

V Lucemburku dne 24. června 2024.

Za Radu

předseda

J. BORRELL FONTELLES

PŘÍLOHA

V oddíle „A. Fyzické osoby“ přílohy I nařízení (EU) 2019/796 se doplňují nové položky, které znějí:

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
„9.	Ruslan Aleksandrovich PERETYATKO	Руслан Александрович ПЕРЕТЯТЬКО Datum narození: 3.8.1985 Státní příslušnost: ruské Pohlaví: muž	Ruslan Peretjatko (Ruslan Peretyatko) se zúčastnil kybernetických útoků s významným dopadem, které představují vnější hrozbu pro Unii nebo její členské státy. Ruslan Peretjatko je členem ‚Callisto Group‘, skupiny ruských vojenských zpravodajských důstojníků provádějících kybernetické operace proti členským státům EU a třetím státům. Callisto Group (také známa jako ‚Seaborgium‘, ‚Star Blizzard‘, ‚ColdRiver‘, ‚TA446‘) zahájila několikaleté phishingové kampaně využívané ke krádeži dat a přihlašovacích údajů k účtům. Callisto Group je dále odpovědná za kampaně zaměřené na jednotlivce a kritické funkce státu, a to i v oblasti obrany a vnějších vztahů. Ruslan Peretjatko je tudíž zapojen do kybernetických útoků s významným dopadem, které představují vnější hrozbu pro Unii nebo její členské státy.	24.6.2024
10.	Andrey Stanislavovich KORINETS	Андрей Станиславович КОРИНЕЦ Datum narození: 18.5.1987 Místo narození: Město Syktyvkar, Rusko Státní příslušnost: ruské Pohlaví: muž	Andrej Stanislavovič Koriněc (Andrey Stanislavovich Korinets) se zúčastnil kybernetických útoků s významným dopadem, které představují vnější hrozbu pro Unii nebo její členské státy. Andrej Stanislavovič Koriněc je důstojníkem útvaru ‚Center 18‘ v rámci Federální bezpečnostní služby (FSB) Ruské federace. Andrej Stanislavovič Koriněc je členem ‚Callisto Group‘, skupiny ruských vojenských zpravodajských důstojníků provádějících kybernetické operace proti členským státům EU a třetím státům. Callisto Group (také známa jako ‚Seaborgium‘, ‚Star Blizzard‘, ‚ColdRiver‘, ‚TA446‘) zahájila několikaleté phishingové kampaně využívané ke krádežím dat a přihlašovacích údajů k účtům. Callisto Group je dále odpovědná za kampaně zaměřené na jednotlivce a kritické funkce státu, a to i v oblasti obrany a vnějších vztahů. Andrej Stanislavovič Koriněc je tudíž zapojen do kybernetických útoků s významným dopadem, které představují vnější hrozbu pro Unii nebo její členské státy.	24.6.2024

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
11.	Oleksandr SKLIANKO	Александр СКЛЯНКО (v ruštině) Олександр СКЛЯНКО (v ukrajinštině) Datum narození: 5.8.1973 Pas č.: EC 867868, vydaný 27.11.1998 (Ukrajina) Pohlaví: muž	Oleksandr Skljanko (Oleksandr Sklianko) se účastnil kybernetických útoků s významným dopadem na členské státy EU, jakož i kybernetických útoků s významným dopadem na třetí země. Oleksandr Skljanko je členem hackerské skupiny Armageddon, podporované Federální bezpečnostní službou Ruské federace (FSB), která provedla různé kybernetické útoky s významným dopadem na vládu Ukrajiny a na členské státy EU a jejich vládní úředníky, mimo jiné prostřednictvím phishingových e-mailů a malwarových kampaní. Oleksandr Skljanko je tudíž zapojen do kybernetických útoků s významným dopadem na třetí země, jakož i do kybernetických útoků s významným dopadem, které představují vnější hrozbu pro Unii nebo její členské státy.	24.6.2024
12.	Mykola CHERNYKH	Николай ЧЕРНЫХ (v ruštině) Микола ЧЕРНИХ (v ukrajinštině) Datum narození: 12.10.1978 Pas č.: EC 922162, vydaný 20.1.1999 (Ukrajina) Pohlaví: muž	Mykola Černych (Mykola Chernykh) se účastnil kybernetických útoků s významným dopadem na členské státy EU, jakož i kybernetických útoků s významným dopadem na třetí země. Mykola Černych je členem hackerské skupiny Armageddon, podporované Federální bezpečnostní službou (FSB) Ruské federace, která provedla různé kybernetické útoky s významným dopadem na vládu Ukrajiny a na členské státy EU a jejich vládní úředníky, mimo jiné prostřednictvím phishingových e-mailů a malwarových kampaní. Jako bývalý příslušník Bezpečnostní služby Ukrajiny je na Ukrajině obviněn z vlastizrady a neoprávněných zásahů do provozu elektronických výpočetních strojů a automatizovaných systémů. Mykola Černych je tudíž zapojen do kybernetických útoků s významným dopadem, které představují vnější hrozbu pro Unii nebo její členské státy.	24.6.2024

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
13.	Mikhail Mikhailovich TSAREV	Михаил Михайлович ЦАРЕВ Datum narození: 20.4.1989 Místo narození: Serpuchov, Ruská federace Státní příslušnost: ruské Adresa: Serpuchov Pohlaví: muž	Michail Michajlovič Carev (Mikhail Mikhailovich Tsarev) se zúčastnil kybernetických útoků s významným dopadem, které představují vnější hrozbu pro členské státy EU. Michail Michajlovič Carev, známý také pod online přezdívkami ‚Mango', ‚Alexander Grachev', ‚Super Misha', ‚Ivanov Mixail', ‚Misha Krutysha' a ‚Nikita Andreevich Tsarev' je klíčovým aktérem při šíření malwarových programů Conti a Trickbot a je zapojen do činnosti nepřátelsky působící skupiny ‚Wizard Spider' působící z Ruska. Malwarové programy Conti a Trickbot byly vytvořeny a vyvinuty nepřátelsky působící skupina ‚Wizard Spider'. Wizard Spider vede ransomwarové kampaně v různých odvětvích, včetně základních služeb, jako je zdravotnictví a bankovnictví. Tato skupina infikovala počítače na celém světě a její malware se vyvinul ve vysoce modulární sadu malwaru. Kampaně skupiny Wizard Spider využívající malwary, jako jsou Conti, Ryuk a TrickBot,, způsobily v EU závažné hospodářské škody. Michail Michajlovič Carev je tudíž zapojen do kybernetických útoků s významným dopadem, které představují vnější hrozbu pro Unii nebo její členské státy.	24.6.2024

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
14.	Maksim Sergeevich GALOCHKIN	Максим Сергеевич ГАЛОЧКИН Datum narození: 19.5.1982 Místo narození: Abakan, Ruská federace Státní příslušnost: ruské Pohlaví: muž	Maxim Galočkin (Maxim Galochkin) se zúčastnil kybernetických útoků s významným dopadem, které představují vnější hrozbu pro členské státy EU. Maxim Galočkin je znám také pod online přezdívkami ‚Benalen', ‚Bentley', ‚Volhvb', ‚volhvb', ‚manuel', ‚Max17' a ‚Crypt'. Galočkin je klíčovým aktérem při šíření malwarových programů Conti a Trickbot a je zapojen do činnosti nepřátelsky působící skupiny ‚Wizard Spider' působící z Ruska. Vede skupinu testerů pověřených vývojem testů pro malwarový program TrickBot, který vytvořila a nasadila nepřátelsky působící skupina ‚Wizard Spider', dohledem nad těmito testy a jejich prováděním. Wizard Spider vede ransomwarové kampaně v různých odvětvích, včetně základních služeb, jako je zdravotnictví a bankovnictví. Tato skupina infikovala počítače na celém světě a její malware se vyvinul ve vysoce modulární sadu malwaru. Kampaně skupiny Wizard Spider využívající malwary, jako jsou Conti, Ryuk a TrickBot,způsobily v EU značné hospodářské škody. Maxim Galočkin je tudíž zapojen do kybernetických útoků s významným dopadem, které představují vnější hrozbu pro Unii nebo její členské státy.	24.6.2024“

ELI: http://data.europa.eu/eli/reg_impl/2024/1778/oj