2024/1778

24.6.2024

# VYKONÁVACIE NARIADENIE RADY (EÚ) 2024/1778

## z 24. júna 2024,

## ktorým sa vykonáva nariadenie (EÚ) 2019/796 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty

RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o fungovaní Európskej únie,

so zreteľom na nariadenie Rady (EÚ) 2019/796 zo 17. mája 2019 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty ([1]), a najmä na jeho článok 13 ods. 1,

so zreteľom na návrh vysokého predstaviteľa Únie pre zahraničné veci a bezpečnostnú politiku,

keďže:

(1) Rada 17. mája 2019 prijala nariadenie (EÚ) 2019/796.

(2) Cielené reštriktívne opatrenia proti kybernetickým útokom so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty, patria medzi opatrenia zahrnuté do rámca pre spoločnú diplomatickú reakciu Únie na škodlivé kybernetické činnosti (súboru nástrojov kybernetickej diplomacie) a sú kľúčovým nástrojom na predchádzanie takýmto činnostiam, odrádzanie od nich a reakciu na ne.

(3) Škodlivé kybernetické činnosti proti kritickej infraštruktúre alebo základným službám, a to aj prostredníctvom ransomvéru a malvéru typu wiper, zacielenie na dodávateľské reťazce a kybernetická špionáž vrátane krádeží duševného vlastníctva sú čoraz početnejšie, častejšie a sofistikovanejšie. Tieto činnosti so svojimi rušivými a deštruktívnymi účinkami predstavujú systémovú hrozbu pre bezpečnosť, hospodárstvo, demokraciu a spoločnosť Únie ako celok.

(4) Využívanie kybernetických operácií, ktoré umožňujú a sprevádzajú nevyprovokovanú a neodôvodnenú útočnú vojnu Ruska proti Ukrajine, ovplyvňuje globálnu stabilitu a bezpečnosť, predstavuje významné riziko eskalácie a prispieva k už aj tak výraznému nárastu škodlivých kybernetických činností mimo kontextu ozbrojeného konfliktu v posledných rokoch. Rastúce kyberneticko-bezpečnostné riziká a celkovo zložité prostredie kybernetických hrozieb s jasným rizikom rýchleho presahu kybernetických incidentov z jedného členského štátu do iných a z tretích krajín do Únie si ďalej vyžadujú reštriktívne opatrenia podľa nariadenia (EÚ) 2019/796.

(5) 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 I k nariadeniu (EÚ) 2019/796 malo zaradiť šesť fyzických osôb. Uvedené osoby sú zodpovedné za kybernetické útoky so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty, alebo sa na nich podieľali.

(6) Príloha I k nariadeniu (EÚ) 2019/796 by sa preto mala zodpovedajúcim spôsobom zmeniť,

PRIJALA TOTO NARIADENIE:

*Článok 1*

Príloha I k nariadeniu (EÚ) 2019/796 sa mení tak, ako sa uvádza v prílohe k tomuto nariadeniu.

([1]) Ú. v. EÚ L 129 I, 17.5.2019, s. 1.

*Článok 2*

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

Toto nariadenie je záväzné v celom rozsahu a priamo uplatniteľné vo všetkých členských štátoch.

V Luxemburgu 24. júna 2024

*Za Radu*

*predseda*

J. BORRELL FONTELLES

*PRÍLOHA*

V prílohe I k nariadeniu (EÚ) 2019/796 sa do oddielu „A. Fyzické osoby“ dopĺňajú tieto záznamy:

| | Meno a priezvisko | Informácie o totožnosti | Odôvodnenie | Dátum zaradenia na zoznam |
|---|---|---|---|---|
| „9. | Ruslan Aleksandrovich PERETYATKO | Руслан Александрович ПЕРЕТЯТЬКО<br>Dátum narodenia: 3.8.1985<br>Štátna príslušnosť: ruská<br>Pohlavie: muž | Ruslan PERETYATKO sa zúčastnil na kybernetických útokoch so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty.<br>Ruslan PERETYATKO je súčasťou ‚skupiny Callisto‘ ruských vojenských spravodajských dôstojníkov vykonávajúcich kybernetické operácie proti členským štátom EÚ a tretím štátom.<br>Callisto Group (alias ‚Seaborgium‘, ‚Star Blizzard‘, ‚ColdRiver‘, ‚TA446‘) spustila viacročné phishingové kampane používané na krádež prihlasovacích údajov a údajov účtu. Okrem toho je skupina Callisto zodpovedná za kampane zamerané na jednotlivcov a kritické funkcie štátu, a to aj v oblasti obrany a vonkajších vzťahov.<br>Ruslan PERETYATKO sa preto podieľa na kybernetických útokoch so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty. | 24.6.2024 |
| 10. | Andrey Stanislavovich KORINETS | Андрей Станиславович КОРИНЕЦ<br>Dátum narodenia: 18.5.1987<br>Miesto narodenia: mesto Syktyvkar, Rusko<br>Štátna príslušnosť: ruská<br>Pohlavie: muž | Andrey Stanislavovich KORINETS sa zúčastnil na kybernetických útokoch so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty.<br>Andrey Stanislavovich KORINETS je dôstojníkom ‚Center 18‘ Federálnej bezpečnostnej služby (FSB) Ruskej federácie. Andrey Stanislavovich KORINETS je súčasťou ‚skupiny Callisto‘ ruských vojenských spravodajských dôstojníkov vykonávajúcich kybernetické operácie proti členským štátom EÚ a tretím štátom.<br>Callisto Group (alias ‚Seaborgium‘, ‚Star Blizzard‘, ‚ColdRiver‘, ‚TA446‘) spustila viacročné phishingové kampane používané na krádež prihlasovacích údajov a údajov účtu. Okrem toho je skupina Callisto zodpovedná za kampane zamerané na jednotlivcov a kritické funkcie štátu, a to aj v oblasti obrany a vonkajších vzťahov.<br>Andrey Stanislavovich KORINETS sa preto podieľa na kybernetických útokoch so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty. | 24.6.2024 |

| | Meno a priezvisko | Informácie o totožnosti | Odôvodnenie | Dátum zaradenia na zoznam |
|---|---|---|---|---|
| 11. | Oleksandr SKLIANKO | Александр СКЛЯНКО (ruský pravopis)<br>Олександр СКЛЯНКО (ukrajinský pravopis)<br>Dátum narodenia: 5.8.1973<br>Cestovný pas: EC 867868, vydaný 27. 11. 1998 (Ukrajina)<br>Pohlavie: muž | Oleksandr SKLIANKO sa zúčastnil na kybernetických útokoch so závažným vplyvom na členské štáty EÚ, ako aj na kybernetických útokoch so závažným vplyvom na tretie štáty.<br>Oleksandr SKLIANKO je súčasťou hackerskej skupiny Armageddon podporovanej Federálnou bezpečnostnou službou (FSB) Ruskej federácie, ktorá vykonala rôzne kybernetické útoky s významným vplyvom na vládu Ukrajiny a na členské štáty EÚ a ich vládnych úradníkov, a to aj prostredníctvom phishingových e-mailov a malvérových kampaní.<br>Oleksandr SKLIANKO sa preto podieľa na kybernetických útokoch so závažným vplyvom na tretie štáty, ako aj na kybernetických útokoch so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty. | 24.6.2024 |
| 12. | Mykola CHERNYKH | Николай ЧЕРНЫХ (ruský pravopis)<br>Микола ЧЕРНИХ (ukrajinský pravopis)<br>Dátum narodenia: 12.10.1978<br>Cestovný pas: EC 922162, vydaný 20. 1. 1999 (Ukrajina)<br>Pohlavie: muž | Mykola CHERNYKH sa zúčastnil na kybernetických útokoch so závažným vplyvom na členské štáty EÚ, ako aj na kybernetických útokoch so závažným vplyvom na tretie štáty.<br>Mykola CHERNYKH je súčasťou hackerskej skupiny ‚Armageddon' podporovanej Federálnou bezpečnostnou službou (FSB) Ruskej federácie, ktorá vykonala rôzne kybernetické útoky s významným vplyvom na vládu Ukrajiny a na členské štáty EÚ a ich štátnych úradníkov, a to aj prostredníctvom phishingových e-mailov a malvérových kampaní.<br>Ako bývalý zamestnanec bezpečnostnej služby Ukrajiny je na Ukrajine obvinený z vlastizrady a neoprávneného zasahovania do prevádzky elektronických výpočtových strojov a automatizovaných systémov.<br>Mykola CHERNYKH sa preto podieľa na kybernetických útokoch so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty. | 24.6.2024 |

| | Meno a priezvisko | Informácie o totožnosti | Odôvodnenie | Dátum zaradenia na zoznam |
|---|---|---|---|---|
| 13. | Mikhail Mikhailovich TSAREV | Михаил Михайлович ЦАРЕВ<br>Dátum narodenia: 20.4.1989<br>Miesto narodenia: Serpukhov, Ruská federácia<br>Štátna príslušnosť: ruská<br>Adresa: Serpukhov<br>Pohlavie: muž | Mikhail Mikhailovich TSAREV sa zúčastnil na kybernetických útokoch so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty.<br>Mikhail Mikhailovich TSAREV, známy aj pod prezývkami ‚Mango', ‚Alexander Grachev', ‚Super Misha', ‚Ivanov Mixail', ‚Misha Krutysha' a ‚Nikita Andreevich Tsarev', je kľúčovým hráčom pri nasadení malvérových programov Conti a Trickbot a je zapojený do skupiny hrozieb ‚Wizard Spider' so sídlom v Rusku.<br>Malvérové programy Conti a TrickBot vytvorila a vyvinula skupina hrozieb ‚Wizard Spider'. Skupina Wizard Spider viedla ransomvérové kampane v rôznych odvetviach, vrátane základných služieb, ako je zdravotníctvo a bankovníctvo. Skupina napadla počítače po celom svete a ich malvér sa rozvinul do vysoko modulárneho malvérového balíka. Kampane skupiny Wizard Spider s použitím malvéru, ako sú Conti, ‚Ryuk' a TrickBot, sú zodpovedné za značné hospodárske škody v Európskej únii.<br>Mikhail Mikhailovich TSAREV sa preto podieľa na kybernetických útokoch so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty. | 24.6.2024 |

| | Meno a priezvisko | Informácie o totožnosti | Odôvodnenie | Dátum zaradenia na zoznam |
|---|---|---|---|---|
| 14. | Maksim Sergeevich GALOCHKIN | Максим Сергеевич ГАЛОЧКИН<br>Dátum narodenia: 19.5.1982<br>Miesto narodenia: Abakan, Ruská federácia<br>Štátna príslušnosť: ruská<br>Pohlavie: muž | Maksim GALOCHKIN sa zúčastnil na kybernetických útokoch so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty.<br>Maksim Galochkin je známy aj pod online prezývkami ‚Benalen', ‚Bentley', ‚Volhvb', ‚volhvb', ‚manuel', ‚Max17' a ‚Crypt'. Galochkin je kľúčovým hráčom pri nasadení malvérových programov Conti a TrickBot a je zapojený do skupiny hrozieb ‚Wizard Spider' so sídlom v Rusku. Viedol skupinu testerov so zodpovednosťou za vývoj, dohľad a vykonávanie testov pre malvérový program TrickBot, ktorý vytvorila a nasadila skupina Wizard Spider.<br>Skupina Wizard Spider viedla ransomvérové kampane v rôznych odvetviach, vrátane základných služieb, ako je zdravotníctvo a bankovníctvo. Skupina napadla počítače po celom svete a ich malvér sa rozvinul do vysoko modulárneho malvérového balíka. Kampane skupiny Wizard Spider s použitím malvéru, ako sú Conti, ‚Ryuk' a TrickBot, sú zodpovedné za značné hospodárske škody v Európskej únii.<br>Maksim Galochkin sa preto podieľa na kybernetických útokoch so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty. | 24.6.2024“ |





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