VYKONÁVACIE NARIADENIE RADY (EÚ) 2020/1125

z 30. júla 2020,

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, sú jedným z opatrení zahrnutých do rámca pre spoločnú diplomatickú reakciu EÚ na škodlivé kybernetické činnosti (súboru nástrojov kybernetickej diplomacie) a kľúčovým nástrojom na odrádzanie od páchania takýchto činností a reagovania na ne. Reštriktívne opatrenia sa môžu uplatňovať aj v reakcii na kybernetické útoky so závažným vplyvom na tretie štáty alebo medzinárodné organizácie, ak sa to považuje za potrebné na dosiahnutie cieľov spoločnej zahraničnej a bezpečnostnej politiky stanovených v príslušných ustanoveniach článku 21 Zmluvy o Európskej únii.

(3) Rada 16. apríla 2018 prijala závery, v ktorých dôrazne odsúdila zlomyseľné zneužitie informačných a komunikačných technológií vrátane útokov verejne označovaných ako „WannaCry“ a „NotPetya“, ktoré spôsobili značné škody a hospodárske strany v Únii aj mimo nej. Predseda Európskej rady a predseda Európskej komisie a vysoký predstaviteľ Únie pre zahraničné veci a bezpečnostnú politiku (ďalej len „vysoký predstaviteľ“) vyjadrili 4. októbra 2018 v spoločnom vyhlásení vážne obavy z pokusu o kybernetický útok s cieľom narušiť integritu Organizácie pre zákaz chemických zbraní (OPCW) v Holandsku – agresívneho aktu, ktorý bol prejavom pohŕdania vážnym účelom OPCW. Okrem toho vysoký predstaviteľ vo vyhlásení v mene Únie z 12. apríla 2019 vyzval aktérov, aby prestali so zlomyseľnými kybernetickými aktivitami, ktoré narúšajú integritu, bezpečnosť a hospodársku konkurencieschopnosť Únie vrátane rastúceho počtu krádeží duševného vlastníctva umožnených počítačom. Takéto krádeže umožnené počítačom zahŕňajú činy spáchané aktérom verejne označovaným ako „APT10“ („Advanced Persistent Threat 10“).

(4) V tejto súvislosti a s cieľom predchádzať pretrvávajúcemu a čoraz intenzívnejšiemu zlomyseľnému správaniu v kybernetickom priestore, odrádzať od neho a reagovať naň by sa malo na zoznam fyzických a právnických osôb, subjektov a orgánov, na ktoré sa vzťahujú reštriktívne opatrenia, uvedený v prílohe I k nariadeniu (EÚ) 2019/796, zaradiť šesť fyzických osôb a tri subjekty alebo orgány. Uvedené osoby a subjekty alebo orgány sú zodpovedné za kybernetické útoky alebo pokusy o kybernetické útoky vrátane pokusu o kybernetický útok na OPCW a kybernetických útokov verejne označovaných ako „WannaCry“ a „NotPetya“, ako aj „Operation Cloud Hopper“, alebo im poskytli podporu, boli do nich zapojené alebo ich uľahčili.

(5) Nariadenie (EÚ) 2019/796 by sa preto malo zodpovedajúcim spôsobom zmeniť,

PRIJALA TOTO NARIADENIE:

Článok 1

Príloha I k nariadeniu (EÚ) 2019/796 sa mení v súlade s prílohou 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 Bruseli 30. júla 2020

Za Radu
predseda
M. ROTH

PRÍLOHA

Do zoznamu fyzických a právnických osôb, subjektov a orgánov uvedeného v prílohe I k nariadeniu (EÚ) 2019/796 sa dopĺňajú tieto osoby a subjekty alebo orgány:

„A. Fyzické osoby

	Meno a priezvisko	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia do zoznamu
1.	GAO Qiang	Miesto narodenia: Provincia Shandong, Čína Adresa: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Štátna príslušnosť: čínska Pohlavie: muž	Gao Qiang je zapojený do série kybernetických útokov „Operation Cloud Hopper“ so závažným vplyvom a s pôvodom mimo Únie, ktorá predstavuje vonkajšiu hrozbu pre Úniu a jej členské štáty a kybernetických útokov so značnými dôsledkami na tretie štáty. „Operation Cloud Hopper“ bola zacielená na informačné systémy nadnárodných spoločností na šiestich kontinentoch vrátane spoločností nachádzajúcich sa v Únii, a získal sa ňou neoprávnený prístup k citlivým obchodným údajom, čo viedlo k značným hospodárskym stratám.	30. 7. 2020
			„Operation Cloud Hopper“ uskutočnil aktér, ktorý je verejne označovaný ako „APT10“ („Advanced Persistent Threat 10“) (alias „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ a „Potassium“). Možno konštatovať prepojenie medzi Gaom Qiangom a APT10 vrátane veliacej a kontrolnej infraštruktúry APT10. Gao Qiang bol okrem toho zamestnaný v spoločnosti Huaying Haitai, čo je subjekt označený za poskytovanie podpory a uľahčenie útoku „Operation Cloud Hopper“. Má tiež prepojenie na Zhanga Shilonga, ktorý je označený v súvislosti s útokom „Operation Cloud Hopper“. Gao Qiang má tak prepojenia na subjekt Huaying Haitai a na Zhanga Shilonga.	
2.	ZHANG Shilong	Adresa: Hedong, Yuyang Road No 121, Tianjin, China Štátna príslušnosť: čínska Pohlavie: muž	Zhang Shilong je zapojený do série kybernetických útokov „Operation Cloud Hopper“ so závažným vplyvom a pôvodom mimo Únie, ktorá predstavuje vonkajšiu hrozbu pre Úniu a jej členské štáty a kybernetických útokov so značnými dôsledkami na tretie štáty. „Operation Cloud Hopper“ bola zacielená na informačné systémy nadnárodných spoločností na šiestich kontinentoch vrátane spoločností nachádzajúcich sa v Únii, a získal sa ňou neoprávnený prístup k citlivým obchodným údajom, čo viedlo k značným hospodárskym stratám. „Operation Cloud Hopper“ uskutočnil aktér, ktorý je verejne označovaný ako „APT10“ („Advanced Persistent Threat 10“) (alias „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ a „Potassium“).	30. 7. 2020
			Možno konštatovať prepojenie medzi Zhangom Shilongom a APT10 vrátane malvéru, ktorý vyvinul a testoval v súvislosti s kybernetickými útokmi, ktoré uskutočnil APT10. Zhang Shilong bol okrem toho zamestnaný v spoločnosti Huaying Haitai, čo je subjekt označený za poskytovanie podpory a uľahčenie útoku „Operation Cloud Hopper“. Má tiež prepojenie na Gaoa Qianga, ktorý je označený v súvislosti s útokom „Operation Cloud Hopper“. Zhang Shilong má tak prepojenia na subjekt Huaying Haitai a na Zhanga Shilonga.	

3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Dátum narodenia: 27. mája 1972 Miesto narodenia: Permská oblasť, RSFSR (v súčasnosti Ruská federácia) Č. cestovného pasu: 120017582 Vydaný: Ministerstvom zahraničných vecí Ruskej federácie Platnosť: od 17. apríla 2017 do 17. apríla 2022 Miesto: Moskva, Ruská federácia Štátna príslušnosť: ruská Pohlavie: muž	Alexey Minin sa zúčastnil na pokuse o kybernetický útok s potenciálne závažným vplyvom proti Organizácii pre zákaz chemických zbraní (OPCW) v Holandsku. Ako príslušník Hlavného riaditeľstva Generálneho štábu ozbrojených síl Ruskej federácie (GU/GRU) zodpovedný za podporu osobného získavania spravodajských informácií bol Alexey Minin členom tímu štyroch príslušníkov ruskej vojenskej spravodajskej služby, ktorí sa v apríli 2018 pokúsili o neoprávnený prístup do siete wifi OPCW v holandskom Haagu. Pokus o kybernetický útok bol zameraný na hacknutie siete wifi OPCW, ktorý by v prípade úspechu ohrozil bezpečnosť siete a prebiehajúce vyšetrovanie OPCW. Holandská obranná spravodajská a bezpečnostná služba (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) pokus o kybernetický útok narušila, a tak zabránila spôsobeniu závažnej ujmy OPCW.	30. 7. 2020
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Dátum narodenia: 31. júla 1977 Miesto narodenia: Murmanská oblasť, RSFSR (v súčasnosti Ruská federácia) Č. cestovného pasu: 100135556 Vydaný: Ministerstvom zahraničných vecí Ruskej federácie Platnosť: od 17. apríla 2017 do 17. apríla 2022 Miesto: Moskva, Ruská federácia Štátna príslušnosť: ruská Pohlavie: muž	Alexei Morenets sa zúčastnil na pokuse o kybernetický útok s potenciálne závažným vplyvom proti Organizácii pre zákaz chemických zbraní (OPCW) v Holandsku. Ako kybernetický operátor Hlavného riaditeľstva Generálneho štábu ozbrojených síl Ruskej federácie (GU/GRU) bol Aleksei Morenets členom tímu štyroch príslušníkov ruskej vojenskej spravodajskej služby, ktorí sa v apríli 2018 pokúsili o neoprávnený prístup do siete wifi OPCW v holandskom Haagu. Pokus o kybernetický útok bol zameraný na hacknutie siete wifi OPCW, ktorý by v prípade úspechu ohrozil bezpečnosť siete a prebiehajúce vyšetrovanie OPCW. Holandská obranná spravodajská a bezpečnostná služba (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) pokus o kybernetický útok narušila, a tak zabránila spôsobeniu závažnej ujmy OPCW.	30. 7. 2020
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Dátum narodenia: 26. júla 1981 Miesto narodenia: Kursk, RSFSR (v súčasnosti Ruská federácia) Č. cestovného pasu: 100135555 Vydaný: Ministerstvom zahraničných vecí Ruskej federáciePlatnosť: od 17. apríla 2017 do 17. apríla 2022 Miesto: Moskva, Ruská federácia Štátna príslušnosť: ruská Pohlavie: muž	Evgenii Serebriakov sa zúčastnil na pokuse o kybernetický útok s potenciálne závažným vplyvom proti Organizácii pre zákaz chemických zbraní (OPCW) v Holandsku. Ako kybernetický operátor Hlavného riaditeľstva Generálneho štábu ozbrojených síl Ruskej federácie (GU/GRU) bol Evgenii Serebriakov členom tímu štyroch príslušníkov ruskej vojenskej spravodajskej služby, ktorí sa v apríli 2018 pokúsili o neoprávnený prístup do siete wifi OPCW v holandskom Haagu. Pokus o kybernetický útok bol zameraný na hacknutie siete wifi OPCW, ktorý by v prípade úspechu ohrozil bezpečnosť siete a prebiehajúce vyšetrovanie OPCW. Holandská obranná spravodajská a bezpečnostná služba (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) pokus o kybernetický útok narušila, a tak zabránila spôsobeniu závažnej ujmy OPCW.	30. 7. 2020

6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Dátum narodenia: 24. augusta 1972 Miesto narodenia: Ulianovsk, RSFSR (v súčasnosti Ruská federácia) Č. cestovného pasu: 120018866 Vydaný: Ministerstvom zahraničných vecí Ruskej federáciePlatnosť: od 17. apríla 2017 do 17 apríla 2022 Miesto: Moskva, Ruská federácia Štátna príslušnosť: ruská Pohlavie: muž	Oleg Sotnikov sa zúčastnil na pokuse o kybernetický útok s potenciálne závažným vplyvom proti Organizácii pre zákaz chemických zbraní (OPCW) v Holandsku. Ako príslušník Hlavného riaditeľstva Generálneho štábu ozbrojených síl Ruskej federácie (GU/GRU) zodpovedný za podporu osobného získavania spravodajských informácií bol Oleg Sotnikov členom tímu štyroch príslušníkov ruskej vojenskej spravodajskej služby, ktorí sa v apríli 2018 pokúsili o neoprávnený prístup do siete wifi OPCW v holandskom Haagu. Pokus o kybernetický útok bol zameraný na hacknutie siete wifi OPCW, ktorý by v prípade úspechu ohrozil bezpečnosť siete a prebiehajúce vyšetrovanie OPCW. Holandská obranná spravodajská a bezpečnostná služba (Militaire Inlichtingen- en Veiligheidsdienst – MIVD) pokus o kybernetický útok narušila, a tak zabránila spôsobeniu závažnej ujmy OPCW.	30. 7. 2020

B. Právnické osoby, subjekty a orgány

	Meno a priezvisko	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia do zoznamu
1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	alias: Haitai Technology Development Co. Ltd Miesto: Tianjin, Čína	Spoločnosť Huaying Haitai poskytla finančnú, technickú a materiálnu podporu pre sériu kybernetických útokov „Operation Cloud Hopper“ so závažným vplyvom a pôvodom mimo Únie, ktorá predstavuje vonkajšiu hrozbu pre Úniu a jej členské štáty a kybernetických útokov so značnými dôsledkami na tretie štáty, a uľahčila ju. „Operation Cloud Hopper“ bola zacielená na informačné systémy nadnárodných spoločností na šiestich kontinentoch vrátane spoločností nachádzajúcich sa v Únii, a získal sa ňou neoprávnený prístup k citlivým obchodným údajom, čo viedlo k značným hospodárskym stratám. „Operation Cloud Hopper“ uskutočnil aktér, ktorý je verejne označovaný ako „APT10“ („Advanced Persistent Threat 10“) (alias „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ a „Potassium“). Možno konštatovať prepojenie medzi spoločnosť Huaying Haitai a APT10. Okrem toho spoločnosť Huaying Haitai zamestnávala Gaoa Qianga a Zhanga Shilonga, ktorí sú označení v súvislosti s útokom „Operation Cloud Hopper“. Existuje teda väzba medzi spoločnosťou Huaying Haitai a Gaom Qiangom a Zhangom Shilongom.	30. 7. 2020
2.	Chosun Expo	alias: Chosen Expo; Korea Export Joint Venture Miesto: KĽDR	Spoločnosť Chosun Expo poskytla finančnú, technickú a materiálnu podporu pre viaceré kybernetické útoky so závažným vplyvom a pôvodom mimo Únie, ktoré predstavujú vonkajšiu hrozbu pre Úniu a jej členské štáty a kybernetické útoky, ktoré majú značné dôsledky na tretie štáty, vrátane kybernetických útokov označovaných ako „WannaCry“ a kybernetických útokov proti poľskému orgánu finančného dohľadu a spoločnosti Sony Pictures Entertainment, ako aj kybernetickej krádeže z Bangladesh Bank a pokusu o kybernetickú krádež z Vietnam Tien Phong Bank, a uľahčila tieto útoky.	30. 7. 2020

			Pri útoku „WannaCry“ boli pomocou ransomvéru a blokovania prístupu k údajom narušené informačné systémy po celom svete. Zasiahnuté boli informačné systémy spoločností v Únii vrátane informačných systémov súvisiacich so službami potrebnými na zachovanie základných služieb a hospodárskej činnosti v členských štátoch. Útok „WannaCry“ uskutočnil aktér verejne označovaný ako „APT38“ („Advanced Persistent Threat 38“) alebo „Lazarus Group“. Možno konštatovať prepojenie medzi spoločnosťou Chosun Expo a APT38/Lazarus Group, a to vrátane účtov použitých na kybernetické útoky.	
3.	Hlavné stredisko pre špeciálne technológie (GTsST) Hlavného riaditeľstva Generálneho štábu ozbrojených síl Ruskej federácie (GU/GRU)	Adresa: 22 Kirova Street, Moscow, Russian Federation	Hlavné stredisko pre špeciálne technológie (GTsST) Hlavného riaditeľstva Generálneho štábu ozbrojených síl Ruskej federácie (GU/GRU), označované tiež ako 74455 podľa svojho poštového smerovacieho čísla, je zodpovedné za kybernetické útoky so závažným vplyvom a pôvodom mimo Únie, ktoré predstavujú vonkajšiu hrozbu pre Úniu a jej členské štáty a kybernetické útoky, ktoré majú značné dôsledky na tretie štáty, a to vrátane kybernetických útokov s názvom „NotPetya“ alebo „EternalPetya“ v júni 2017 a kybernetických útokov zameraných na ukrajinskú energetickú sieť v zime 2015 a 2016. Útoky „NotPetya“ a „EternalPetya“ spôsobili neprístupnosť údajov vo viacerých spoločnostiach v Únii, inde v Európe a vo svete prostredníctvom ransomvéru a zablokovania prístupu k údajom, čo viedlo k značným hospodárskym stratám. Kybernetické útoky na ukrajinskú energetickú sieť viedli k čiastočným výpadkom siete počas zimy.	30. 7. 2020“
			Útok „NotPetya“ alebo „EternalPetya“ uskutočnil aktér, ktorý je verejne označovaný ako „Sandworm“ (alias „Sandworm Team“, „BlackEnergy Group“, „Voodoo Bear“, „Quedagh“, „Olympic Destroyer“ a „Telebots“) a stojí aj za útokom na ukrajinskú energetickú sieť. Hlavné stredisko pre špeciálne technológie Hlavného riaditeľstva Generálneho štábu ozbrojených síl Ruskej federácie zohráva aktívnu úlohu pri kybernetických aktivitách subjektu Sandworm a možno konštatovať prepojenie naň.	