II

(Nelegislatívne akty)

NARIADENIA

VYKONÁVACIE NARIADENIE RADY (EÚ) 2020/1744

z 20. novembra 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) Rada 30. júla 2020 prijala vykonávacie nariadenie (EÚ) 2020/1125 ([2]), ktorým sa do zoznamu fyzických a právnických osôb, subjektov a orgánov, na ktoré sa vzťahujú reštriktívne opatrenia, uvedeného v prílohe I k nariadeniu (EÚ) 2019/796 doplnilo šesť fyzických osôb a tri subjekty alebo orgány.

(3) Boli doručené aktualizované informácie týkajúce sa dvoch záznamov fyzických osôb.

(4) 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.

Článok 2

Toto nariadenie nadobúda účinnosť dňom nasledujúcim po jeho uverejnení v *Úradnom vestníku Európskej únie*.

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

V Bruseli 20. novembra 2020

Za Radu
predseda
M. ROTH

([1]) Ú. v. EÚ L 129 I, 17.5.2019, s. 1.
([2]) 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 (Ú. v. EÚ L 246, 30.7.2020, s. 4).

PRÍLOHA

V prílohe I k nariadeniu (EÚ) 2019/796 sa pod nadpisom „A. Fyzické osoby“ záznamy 1 a 2 nahrádzajú týmito záznamami:

	Meno a priezvisko	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia do zoznamu
„1.	GAO Qiang	Dátum narodenia: 4. októbra 1983 Miesto narodenia: Provincia Shandong, Čína Adresa: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, Čína 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. „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.	30.7.2020
2.	ZHANG Shilong	Dátum narodenia: 10. septembra 1981 Miesto narodenia: Čína Adresa: Hedong, Yuyang Road No 121, Tianjin, Čína 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“). 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 Gaoa Qianga.	30.7.2020“