Rada
Európskej únie

V Bruseli 5. mája 2026
(OR. en)

7281/26

LIMITE

CORLX 271
CFSP/PESC 388
CYBER 113
JAI 338
FIN 406

LEGISLATÍVNE AKTY A INÉ PRÁVNE AKTY

Predmet:	ROZHODNUTIE RADY, ktorým sa mení rozhodnutie (SZBP) 2019/797 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty

ROZHODNUTIE RADY (SZBP) 2026/...

z ...,

ktorým sa mení rozhodnutie (SZBP) 2019/797 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty

RADA EURÓPSKEJ ÚNIE,

so zreteľom na Zmluvu o Európskej únii, a najmä jej článok 29,

so zreteľom na návrh vysokej predstaviteľky Únie pre zahraničné veci a bezpečnostnú politiku,

keďže:

(1) Rada 17. mája 2019 prijala rozhodnutie (SZBP) 2019/797[1].

(2) Rozhodnutie (SZBP) 2019/797 sa uplatňuje do 18. mája 2028.

(3) Na základe preskúmania prílohy k rozhodnutiu (SZBP) 2019/797 by sa uplatňovanie opatrení stanovených v článkoch 4 a 5 uvedeného rozhodnutia vo vzťahu k fyzickým a právnickým osobám, subjektom a orgánom uvedeným v zozname v uvedenej prílohe malo predĺžiť do 18. mája 2027. Okrem toho by sa mali aktualizovať odôvodnenia na zaradenie štyroch osôb a jedného subjektu do zoznamu fyzických a právnických osôb, subjektov a orgánov, na ktoré sa vzťahujú reštriktívne opatrenia.

(4) Rozhodnutie (SZBP) 2019/797 by sa preto malo zodpovedajúcim spôsobom zmeniť,

PRIJALA TOTO ROZHODNUTIE:

[1] Rozhodnutie Rady (SZBP) 2019/797 zo 17. mája 2019 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty (Ú. v. EÚ L 129 I, 17.5.2019, s. 13, ELI: http://data.europa.eu/eli/dec/2019/797/oj).

Článok 1

Rozhodnutie (SZBP) 2019/797 sa mení takto:

1. Článok 10 sa nahrádza takto:

„*Článok 10*

Toto rozhodnutie sa uplatňuje do 18. mája 2028 a pravidelne sa preskúmava. Opatrenia stanovené v článkoch 4 a 5 sa vo vzťahu k fyzickým a právnickým osobám, subjektom a orgánom uvedeným v zozname v prílohe uplatňujú do 18. mája 2027.“

2. Príloha sa mení v súlade s prílohou k tomuto rozhodnutiu.

Článok 2

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

V ...

Za Radu
predseda/predsedníčka

PRÍLOHA

Príloha k rozhodnutiu (SZBP) 2019/797 sa mení takto:

1. Pod nadpisom „A. Fyzické osoby“ sa záznamy 1, 2, 13 a 14 nahrádzajú týmito zodpovedajúcimi záznamami:

	Meno a priezvisko	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia na zoznam
„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 spojený so zastrešujúcim aktérom „APT10“ („Advanced Persistent Threat 10“) (alias „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ a „Potassium“) a 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. Gao Qiang má prepojenie na infraštruktúru velenia a riadenia aktéra APT10. Gao Qiang bol okrem toho zamestnaný v spoločnosti Huaying Haitai, ktorú využíval APT10 a ktorá je označená za poskytovanie podpory a uľahčenie útoku „Operation Cloud Hopper“. Je tiež spojený so Zhangom Shilongom, ktorý je prepojený s APT10 a bol tiež zamestnaný v spoločnosti Huaying Haitai.	30.7.2020

	Meno a priezvisko	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia na zoznam
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 spojený so zastrešujúcim aktérom „APT10“ („Advanced Persistent Threat 10“) (alias „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ a „Potassium“) a 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. Zhang Shilong je prepojený s 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, ktorú využíval APT10 a ktorá je označená za poskytovanie podpory a uľahčenie útoku „Operation Cloud Hopper“. Je spojený s Gaom Qiangom, ktorý je prepojený s APT10 a bol tiež zamestnaný v spoločnosti Huaying Haitai.	30.7.2020

	Meno a priezvisko	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia na zoznam
13.	Mikhail Mikhailovich TSAREV	Михаил Михайлович ЦАРЕВ Dátum narodenia: 20.4.1989 Miesto narodenia: Serpukhov, Ruská federácia Štátna príslušnosť: ruská Adresa: Serpukhov Pohlavie: muž	Mikhail Mikhailovich Tsarev sa zúčastnil na kybernetických útokoch so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty. 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. Skupina Wizard Spider naďalej vyvíja a zintenzívňuje svoju činnosť. 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“, TrickBot alebo Black Basta, sú zodpovedné za značné hospodárske škody v Európskej únii. 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 Dátum narodenia: 19.5.1982 Miesto narodenia: Abakan, Ruská federácia Štátna príslušnosť: ruská Pohlavie: muž	Maksim Galochkin sa zúčastnil na kybernetických útokoch so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty. 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. Skupina Wizard Spider naďalej vyvíja a zintenzívňuje svoju činnosť. 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“, TrickBot alebo Black Basta, sú zodpovedné za značné hospodárske škody v Európskej únii. Maksim Galochkin sa preto podieľa na kybernetických útokoch so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty.	24.6.2024“

2. Pod nadpisom „B. Právnické osoby, subjekty a orgány“ sa záznam 1 nahrádza takto:

	Meno a priezvisko	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia na zoznam
„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 aj medzi spoločnosťou Huaying Haitai a Gaom Qiangom a Zhangom Shilongom.	30.7.2020“