

V Bruseli 5. mája 2026
(OR. en)

7283/26

LIMITE

CORLX 273
CFSP/PESC 390
RELEX 352
CYBER 115
JAI 340
FIN 408

LEGISLATÍVNE AKTY A INÉ PRÁVNE AKTY

Predmet: VYKONÁVACIE NARIADENIE RADY, ktorým sa vykonáva nariadenie (EÚ) 2019/796 o reštriktívnych opatreniach proti kybernetickým útokom ohrozujúcim Úniu alebo jej členské štáty

VYKONÁVACIE NARIADENIE RADY (EÚ) 2026/...

Z ...,

**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 štáty¹, a najmä na jeho článok 13,

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

¹ Ú. v. EÚ L 129I, 17.5.2019, s. 1, ELI: <http://data.europa.eu/eli/reg/2019/796/oj>.

keďže:

- (1) Rada 17. mája 2019 prijala nariadenie (EÚ) 2019/796.
- (2) Rada preskúmala zoznam fyzických a právnických osôb, subjektov a orgánov v prílohe I k nariadeniu (EÚ) 2019/796. Na základe tohto preskúmania 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.
- (3) 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 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 ...

Za Radu

predseda/predsedička

PRÍLOHA

Príloha I k nariadeniu (EÚ) 2019/796 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	<p>Dátum narodenia: 10. septembra 1981</p> <p>Miesto narodenia: Čína</p> <p>Adresa: Hedong, Yuyang Road No 121, Tianjin, Čína</p> <p>Štátna príslušnosť: čínska</p> <p>Pohlavie: muž</p>	<p>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.</p> <p>„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.</p> <p>Zhang Shilong je prepojený s APT10 vrátane malvéru, ktorý vyvinul a testoval v súvislosti s kybernetickými útokmi, ktoré uskutočnil APT10.</p> <p>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“.</p> <p>Je spojený s Gaom Qiangom, ktorý je prepojený s APT10 a bol tiež zamestnaný v spoločnosti Huaying Haitai.</p>	30.7.2020

	Meno a priezvisko	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia na zoznam
13.	Mikhail Mikhailovich TSAREV	<p>Михаил Михайлович ЦАРЕВ</p> <p>Dátum narodenia: 20.4.1989</p> <p>Miesto narodenia: Serpukhov, Ruská federácia</p> <p>Štátna príslušnosť: ruská</p> <p>Adresa: Serpukhov</p> <p>Pohlavie: muž</p>	<p>Mikhail Mikhailovich Tsarev sa zúčastnil na kybernetických útokoch so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty.</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>Mikhail Mikhailovich Tsarev sa preto podieľa na kybernetických útokoch so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty.</p>	24.6.2024

	Meno a priezvisko	Informácie o totožnosti	Odôvodnenie	Dátum zaradenia na zoznam
14.	Maksim Sergeevich GALOCHKIN	<p>Максим Сергеевич ГАЛОЧКИН</p> <p>Dátum narodenia: 19.5.1982</p> <p>Miesto narodenia: Abakan, Ruská federácia</p> <p>Štátna príslušnosť: ruská</p> <p>Pohlavie: muž</p>	<p>Maksim Galochkin sa zúčastnil na kybernetických útokoch so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty.</p> <p>Maksim Galochkin je známy aj pod online prezývkami „Benalen“, „Bentley“, „Volhvb“, „volhvb“, „manuel“, „Max17“ a „Crypt“.</p> <p>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.</p> <p>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.</p> <p>Maksim Galochkin sa preto podieľa na kybernetických útokoch so závažným vplyvom, ktoré predstavujú vonkajšiu hrozbu pre Úniu alebo jej členské štáty.</p>	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	<p>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.</p> <p>„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.</p> <p>„Operation Cloud Hopper“ uskutočnil aktér, ktorý je verejne označovaný ako „APT10“ („Advanced Persistent Threat 10“) (alias „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ a „Potassium“).</p> <p>Možno konštatovať prepojenie medzi spoločnosťou 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.</p>	30.7.2020“