



Brusel 5. května 2026  
(OR. en)

7281/26

LIMITE

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

## PRÁVNÍ PŘEDPISY A JINÉ AKTY

---

Předmět: ROZHODNUTÍ RADY, kterým se mění rozhodnutí (SZBP) 2019/797 o omezujících opatřeních proti kybernetickým útokům ohrožujícím Unii nebo její členské státy

---

**ROZHODNUTÍ RADY (SZBP) 2026/...**

ze dne ...,

**kterým se mění rozhodnutí (SZBP) 2019/797 o omezujících opatřeních  
proti kybernetickým útokům ohrožujícím Unii nebo její členské státy**

RADA EVROPSKÉ UNIE,

s ohledem na Smlouvu o Evropské unii, a zejména na článek 29 této smlouvy,

s ohledem na návrh vysoké představitelky Unie pro zahraniční věci a bezpečnostní politiku,

vzhledem k těmto důvodům:

- (1) Dne 17. května 2019 přijala Rada rozhodnutí (SZBP) 2019/797<sup>1</sup>.
- (2) Rozhodnutí (SZBP) 2019/797 je použitelné do 18. května 2028.
- (3) Na základě přezkumu přílohy rozhodnutí (SZBP) 2019/797 by měla být použitelnost opatření stanovených v člancích 4 a 5 uvedeného rozhodnutí, která se použijí na fyzické a právnické osoby, subjekty a orgány uvedené na seznamu v dané příloze, prodloužena do dne 18. května 2027. Kromě toho by na seznamu fyzických a právnických osob, subjektů a orgánů, na něž se vztahují omezující opatření mělo být aktualizováno odůvodnění u položek týkajících se čtyř osob a jednoho subjektu.
- (4) Rozhodnutí (SZBP) 2019/797 by proto mělo být odpovídajícím způsobem změněno,

PŘIJALA TOTO ROZHODNUTÍ:

---

<sup>1</sup> Rozhodnutí Rady (SZBP) 2019/797 ze dne 17. května 2019 o omezujících opatřeních proti kybernetickým útokům ohrožujícím Unii nebo její členské státy (Úř. věst. L 129I, 17.5.2019, s. 13, ELI: <http://data.europa.eu/eli/dec/2019/797/oj>).

## *Článek 1*

Rozhodnutí (SZBP) 2019/797 se mění takto:

- 1) Článek 10 se nahrazuje tímto:

*„Článek 10*

Toto rozhodnutí se použije do 18. května 2028 a je průběžně přezkoumáváno. Opatření stanovená v člancích 4 a 5 se použijí na fyzické nebo právnické osoby, subjekty a orgány, jež jsou uvedeny v příloze, do 18. května 2027.“

- 2) Příloha se mění v souladu s přílohou tohoto rozhodnutí.

## *Článek 2*

Toto rozhodnutí vstupuje v platnost prvním dnem po vyhlášení v *Úředním věstníku Evropské unie*.

V ... dne

*Za Radu*

*předseda/předsedkyně*

---

**PŘÍLOHA**

Příloha rozhodnutí (SZBP) 2019/797 se mění takto:

1) v části „A. Fyzické osoby“ se položky 1, 2, 13 a 14 nahrazují tímto:

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
„1.	GAO Qiang (KAO Čchiang)	Datum narození: 4. října 1983  Místo narození: provincie Shandong (Šan-tung), Čína  Adresa: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin (Tchien-ťin), Čína  Státní příslušnost: čínská  Pohlaví: muž	<p>Kao Čchiang (Gao Qiang) je spojen se zastřešujícím aktérem „APT10“ („Advanced Persistent Threat 10“) (také znám jako „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ a „Potassium“) a byl zapojen do „operace Cloud Hopper“, což byla série kybernetických útoků s významným dopadem pocházejících ze zemí mimo Unii a představujících vnější hrozbu pro Unii nebo její členské státy a kybernetických útoků s významným dopadem na třetí státy.</p> <p>„Operace Cloud Hopper“ byla namířena na informační systémy nadnárodních společností na šesti světadílech, včetně společností se sídlem v Unii, a v jejím rámci byl získán neoprávněný přístup k údajům citlivým z obchodního hlediska, což mělo za následek významné ekonomické ztráty.</p> <p>Kao Čchiang je spojen s řídicí a kontrolní infrastrukturou aktéra APT10. Kromě toho byl Kao Čchiang zaměstnán u společnosti Huaying Haitai, kterou využívá aktér APT10 a která je označena z důvodu poskytování podpory pro „operaci Cloud Hopper“ a napomáhání k ní. Je rovněž spojen s Čang Š'-lungem (Zhang Shilong), který je spojen s aktérem APT10 a který byl rovněž zaměstnán u společnosti Huaying Haitai.</p>	30.7.2020

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
2.	ZHANG Shilong (ČANG Š'-lung)	<p>Datum narození: 10. září 1981</p> <p>Místo narození: Čína</p> <p>Adresa: Hedong, Yuyang Road No 121, Tianjin (Tchien-ťin), Čína</p> <p>Státní příslušnost: čínská</p> <p>Pohlaví: muž</p>	<p>Čang Š'-lung (Zhang Shilong) je spojen se zastřešujícím aktérem „APT10“ („Advanced Persistent Threat 10“) (také znám jako „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ a „Potassium“) a byl zapojen do „operace Cloud Hopper“, což byla série kybernetických útoků s významným dopadem pocházejících ze zemí mimo Unii a představujících vnější hrozbu pro Unii nebo její členské státy a kybernetických útoků s významným dopadem na třetí státy.</p> <p>„Operace Cloud Hopper“ byla namířena na informační systémy nadnárodních společností na šesti světadílech, včetně společností se sídlem v Unii, a v jejím rámci byl získán neoprávněný přístup k údajům citlivým z obchodního hlediska, což mělo za následek významné ekonomické ztráty.</p> <p>Čang Š'-lung je spojen s aktérem APT10, a to i prostřednictvím malwaru, který v souvislosti s kybernetickými útoky provedenými aktérem APT10 vyvinul a otestoval.</p> <p>Kromě toho byl Čang Š'-lung zaměstnán u společnosti Huaying Haitai, kterou využívá aktér APT10 a která je označena z důvodu poskytování podpory pro „operaci Cloud Hopper“ a napomáhání k ní.</p> <p>Je spojen s Kao Čchiangem (Gao Qiang), který je spojen s aktérem APT10 a který byl rovněž zaměstnán u společnosti Huaying Haitai.</p>	30.7.2020

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
13.	Mikhail Mikhailovich TSAREV	<p>Михаил Михайлович ЦАРЕВ</p> <p>Datum narození: 20.4.1989</p> <p>Místo narození: Serpuchov, Ruská federace</p> <p>Státní příslušnost: Rusko</p> <p>Adresa: Serpuchov</p> <p>Pohlaví: muž</p>	<p>Michail Michajlovič Carev (Mikhail Mikhailovich Tsarev) se zúčastnil kybernetických útoků s významným dopadem, které představují vnější hrozbu pro členské státy EU.</p> <p>Michail Michajlovič Carev, známý také pod online přezdívkami „Mango“, „Alexander Grachev“, „Super Misha“, „Ivanov Mixail“, „Misha Krutysa“ a „Nikita Andreevich Tsarev“ je klíčovým aktérem při šíření malwarových programů Conti a Trickbot a je zapojen do činnosti nepřátelsky působící skupiny „Wizard Spider“ působící z Ruska. Skupina „Wizard Spider“ se nadále rozvíjí a zintenzivňuje svou činnost.</p> <p>Skupina „Wizard Spider“ vytvořila a vyvinula malwarové programy Conti a Trickbot. Vede ransomwarové kampaně v různých odvětvích, včetně základních služeb, jako je zdravotnictví a bankovníctví.</p> <p>Tato skupina infikovala počítače na celém světě a její malware se vyvinul ve vysoce modulární sadu malwaru. Kampaně skupiny „Wizard Spider“, využívající malwary, jako jsou Conti, Ryuk, TrickBot či Black Basta, způsobily v Evropské unii značné hospodářské škody.</p> <p>Michail Michajlovič Carev je tudíž zapojen do kybernetických útoků s významným dopadem, které představují vnější hrozbu pro Unii nebo její členské státy.</p>	24.6.2024

	Jméno	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
14.	Maksim Sergeevich GALOCHKIN	<p>Максим Сергеевич ГАЛОЧКИН</p> <p>Datum narození: 19.5.1982</p> <p>Místo narození: Abakan, Ruská federace</p> <p>Státní příslušnost: Rusko</p> <p>Pohlaví: muž</p>	<p>Maxim Galočkin (Maksim Galochkin) se zúčastnil kybernetických útoků s významným dopadem, které představují vnější hrozbu pro členské státy EU.</p> <p>Maxim Galočkin je znám také pod online přezdívkami „Benalen“, „Bentley“, „Volhvb“, „volhvb“, „manuel“, „Max17“ a „Crypt“. Galočkin je klíčovým aktérem při šíření malwarových programů Conti a Trickbot a je zapojen do činnosti nepřátelsky působící skupiny „Wizard Spider“ působící z Ruska. Vede skupinu testerů pověřených vývojem testů pro malwarový program TrickBot, který vytvořila a nasadila nepřátelsky působící skupina „Wizard Spider“, dohledem nad těmito testy a jejich prováděním. Skupina „Wizard Spider“ se nadále rozvíjí a zintenzivňuje svou činnost.</p> <p>Wizard Spider vede ransomwarové kampaně v různých odvětvích, včetně základních služeb, jako je zdravotnictví a bankovníctví. Tato skupina infikovala počítače na celém světě a její malware se vyvinul ve vysoce modulární sadu malwaru. Kampaně skupiny „Wizard Spider“, využívající malwary, jako jsou Conti, Ryuk, TrickBot či Black Basta, způsobily v Evropské unii značné hospodářské škody.</p> <p>Maxim Galočkin je tudíž zapojen do kybernetických útoků s významným dopadem, které představují vnější hrozbu pro Unii nebo její členské státy.</p>	24.6.2024“

2) v části „B. Právnícké osoby, subjekty a orgány“ se položka 1 nahrazuje tímto:

	Název	Identifikační údaje	Odůvodnění	Datum zařazení na seznam
„1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	<p>Také známa jako: Haitai Technology Development Co. Ltd</p> <p>Místo: Tchien-ťin, Čína</p>	<p>Společnost Huaying Haitai poskytovala finanční, technickou nebo materiální podporu pro „operaci Cloud Hopper“, což byla série kybernetických útoků s významným dopadem pocházejících ze zemí mimo Unii a představujících vnější hrozbu pro Unii nebo její členské státy a kybernetických útoků s významným dopadem na třetí státy, a k této operaci napomáhala.</p> <p>„Operace Cloud Hopper“ byla namířena na informační systémy nadnárodních společností na šesti světadílech, včetně společností se sídlem v Unii, a v jejím rámci byl získán neoprávněný přístup k údajům citlivým z obchodního hlediska, což mělo za následek významné ekonomické ztráty.</p> <p>„Operaci Cloud Hopper“ provedl aktér veřejně známý jako „APT10“ („Advanced Persistent Threat 10“) (také znám jako „Red Apollo“, „CVNX“, „Stone Panda“, „MenuPass“ a „Potassium“).</p> <p>Společnost Huaying Haitai může být s aktérem APT10 spojena. Kromě toho společnost Huaying Haitai zaměstnávala Kao Čchianga (Gao Qiang) a Čang Š’-lunga (Zhang Shilong), kteří jsou oba v souvislosti s „operací Cloud Hopper“ označeni. Společnost Huaying Haitai je tudíž také spojena s Kao Čchiangem a Čang Š’-lungem.</p>	30.7.2020“.