



Bruksela, 5 maja 2026 r.  
(OR. en)

7281/26

LIMITE

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

#### **AKTY USTAWODAWCZE I INNE INSTRUMENTY**

---

Dotyczy: DECYZJA RADY zmieniająca decyzję (WPZiB) 2019/797 w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim

---

**DECYZJA RADY (WPZiB) 2026/...**

**z dnia ...**

**zmieniająca decyzję (WPZiB) 2019/797 w sprawie środków ograniczających  
w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim**

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o Unii Europejskiej, w szczególności jego art. 29,

uwzględniając wniosek Wysokiego Przedstawiciela Unii do Spraw Zagranicznych i Polityki  
Bezpieczeństwa,

a także mając na uwadze, co następuje:

- (1) W dniu 17 maja 2019 r. Rada przyjęła decyzję (WPZiB) 2019/797<sup>1</sup>.
- (2) Decyzję (WPZiB) 2019/797 stosuje się do dnia 18 maja 2028 r.
- (3) Na podstawie przeglądu załącznika do decyzji (WPZiB) 2019/797 należy przedłużyć do dnia 18 maja 2027 r. stosowanie środków określonych w art. 4 i 5 tej decyzji w odniesieniu do osób fizycznych i prawnych, podmiotów i organów wymienionych w tym załączniku. Ponadto należy zaktualizować powody umieszczenia czterech osób i jednego podmiotu w wykazie osób fizycznych i prawnych, podmiotów i organów objętych środkami ograniczającymi.
- (4) Należy zatem odpowiednio zmienić decyzję (WPZiB) 2019/797,

PRZYJMUJE NINIEJSZĄ DECYZJĘ:

---

<sup>1</sup> Decyzja Rady (WPZiB) 2019/797 z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim (Dz.U. L 129 I z 17.5.2019, s. 13, ELI: <http://data.europa.eu/eli/dec/2021/797/oj>).

### *Artykuł 1*

W decyzji (WPZiB) 2019/797 wprowadza się następujące zmiany:

- 1) art. 10 otrzymuje brzmienie:

*„Artykuł 10*

Niniejszą decyzję stosuje się do dnia 18 maja 2028 r. Jest ona poddawana stałemu przeglądowi. Środki określone w art. 4 i 5 stosuje się do osób fizycznych i prawnych, podmiotów i organów wymienionych w załączniku do dnia 18 maja 2027 r.”;

- 2) w załączniku wprowadza się zmiany określone w załączniku do niniejszej decyzji.

### *Artykuł 2*

Niniejsza decyzja wchodzi w życie następnego dnia po jej opublikowaniu w *Dzienniku Urzędowym Unii Europejskiej*.

Sporządzono w ...

*W imieniu Rady*

*Przewodniczący/Przewodnicząca*

**ZAŁĄCZNIK**

W załączniku do decyzji (WPZiB) 2019/797 wprowadza się następujące zmiany:

1) w części „A. Osoby fizyczne” wpisy 1, 2, 13 i 14 otrzymują brzmienie:

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
„1.	GAO Qiang	Data urodzenia: 4 października 1983 r. Miejsce urodzenia: provincia Szantung, Chiny Adres: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Obywatelstwo: chińskie Płeć: mężczyzna	<p>Gao Qiang jest powiązany z podmiotem nadrzędnym APT10 („Advanced Persistent Threat 10”) (alias „Red Apollo”, „CVNX”, „Stone Panda”, „MenuPass” i „Potassium”) i był zaangażowany w „Operation Cloud Hopper”, serię cyberataków wywołujących poważne skutki, przeprowadzanych spoza Unii i stanowiących zewnętrzne zagrożenie dla Unii lub jej państw członkowskich, oraz cyberataków wywołujących poważne skutki dla państw trzecich.</p> <p>Cyberataki „Operation Cloud Hopper” były skierowane przeciwko systemom informacyjnym przedsiębiorstw wielonarodowych na sześciu kontynentach, w tym przedsiębiorstw mających siedzibę w Unii, oraz skutkowały nieuprawnionym dostępem do danych wrażliwych pod względem handlowym, powodując znaczne straty gospodarcze.</p> <p>Gao Qiang jest powiązany z infrastrukturą sterowania i kontroli APT10. Ponadto Gao Qiang był zatrudniony przez Huaying Haitai, spółkę wykorzystywaną przez APT10 i umieszczoną w wykazie w związku ze wspieraniem i ułatwianiem „Operation Cloud Hopper”. Ma również powiązania z Zhangiem Shilongiem, który jest powiązany z APT10 i był również zatrudniony przez Huaying Haitai.</p>	30.7.2020

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
2.	ZHANG Shilong	<p>Data urodzenia: 10 września 1981 r.</p> <p>Miejsce urodzenia: Chiny</p> <p>Adres: Hedong, Yuyang Road No 121, Tianjin, China</p> <p>Obywatelstwo: chińskie</p> <p>Płeć: mężczyzna</p>	<p>Zhang Shilong jest powiązany z podmiotem nadrzędnym APT10 („Advanced Persistent Threat 10”) (alias „Red Apollo”, „CVNX”, „Stone Panda”, „MenuPass” i „Potassium”) i był zaangażowany w „Operation Cloud Hopper”, serię cyberataków wywołujących poważne skutki, przeprowadzanych spoza Unii i stanowiących zewnętrzne zagrożenie dla Unii lub jej państw członkowskich, oraz cyberataków wywołujących poważne skutki dla państw trzecich.</p> <p>Cyberataki „Operation Cloud Hopper” były skierowane przeciwko systemom informacyjnym przedsiębiorstw wielonarodowych na sześciu kontynentach, w tym przedsiębiorstw mających siedzibę w Unii, oraz skutkowały nieuprawnionym dostępem do danych wrażliwych pod względem handlowym, powodując znaczne straty gospodarcze.</p> <p>Zhang Shilong ma powiązania z APT10, w tym przez złośliwe oprogramowanie, które opracował i testował w związku z cyberatakami przeprowadzonymi przez APT10.</p> <p>Ponadto Zhang Shilong był zatrudniony przez Huaying Haitai, spółkę wykorzystywaną przez APT10 i umieszczoną w wykazie w związku ze wspieraniem i ułatwianiem „Operation Cloud Hopper”.</p> <p>Ma powiązania z Gao Qiangiem, który jest powiązany z APT10 i był również zatrudniony przez Huaying Haitai.</p>	30.7.2020

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
13.	Mikhail Mikhailovich TSAREV	<p>Михаил Михайлович ЦАРЕВ</p> <p>Data urodzenia: 20 kwietnia 1989 r.</p> <p>Miejsce urodzenia: Sierpuchow, Federacja Rosyjska</p> <p>Obywatelstwo: rosyjskie</p> <p>Adres: Sierpuchow</p> <p>Płeć: mężczyzna</p>	<p>Michaił Carew brał udział w cyberatakach wywołujących poważne skutki i stanowiących zewnętrzne zagrożenie dla państw członkowskich UE.</p> <p>Znany również pod internetowymi pseudonimami „Mango”, „Alexander Grachev”, „Super Misha”, „Ivanov Mixail”, „Misha Krutysha” i „Nikita Andreevich Tsarev” odgrywał kluczową rolę przy wprowadzeniu złośliwego oprogramowania Conti i Trickbot oraz jest związany z umiejscowioną w Rosji grupą cyberprzestępczą Wizard Spider. Wizard Spider rozwija się i intensyfikuje działania.</p> <p>Złośliwe oprogramowanie Conti i Trickbot zostało stworzone i opracowane przez Wizard Spider. Wizard Spider prowadziła kampanie z użyciem oprogramowania szantażującego w różnych sektorach, w tym usług kluczowych, takich jak opieka zdrowotna i bankowość.</p> <p>Grupa infekowała komputery na całym świecie, a ich złośliwe oprogramowanie zostało przekształcone w modułowy pakiet złośliwego oprogramowania. Kampanie Wizard Spider wykorzystujące złośliwe oprogramowanie, takie jak Conti, Ryuk, TrickBot lub Black Basta, powodują znaczne szkody gospodarcze w Unii Europejskiej.</p> <p>Michaił Carew jest zatem zaangażowany w cyberataki wywołujące poważne skutki i stanowiące zewnętrzne zagrożenie dla Unii lub jej państw członkowskich.</p>	24.6.2024

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
14.	Maksim Sergeevich GALOCHKIN	<p>Максим Сергеевич ГАЛОЧКИН</p> <p>Data urodzenia: 19 maja 1982 r.</p> <p>Miejsce urodzenia: Abakan, Federacja Rosyjska</p> <p>Obywatelstwo: rosyjskie</p> <p>Płeć: męczyzna</p>	<p>Maksim Gałoczkin brał udział w cyberatakach wywołujących poważne skutki i stanowiących zewnętrzne zagrożenie dla państw członkowskich UE.</p> <p>Znany jest również pod internetowymi pseudonimami „Benalen”, „Bentley”, „Volhvb”, „volhvb”, „manuel”, „Max17” i „Crypt”. Odgrywał kluczową rolę przy wprowadzeniu złośliwego oprogramowania Conti i Trickbot oraz jest związany z umiejscowioną w Rosji grupą cyberprzestępczą Wizard Spider. Kierował grupą testerów odpowiedzialnych za opracowanie, nadzorowanie i wdrażanie testów złośliwego oprogramowania TrickBot, stworzonego i wprowadzonego przez Wizard Spider. Wizard Spider rozwija się i intensyfikuje działania.</p> <p>Wizard Spider prowadziła kampanie z użyciem oprogramowania szantażującego w różnych sektorach, w tym usług kluczowych, takich jak opieka zdrowotna i bankowość. Grupa infekowała komputery na całym świecie, a ich złośliwe oprogramowanie zostało przekształcone w modułowy pakiet złośliwego oprogramowania. Kampanie Wizard Spider wykorzystujące złośliwe oprogramowanie, takie jak Conti, Ryuk, TrickBot lub Black Basta, powodują znaczne szkody gospodarcze w Unii Europejskiej.</p> <p>Maksim Gałoczkin jest zatem zaangażowany w cyberataki wywołujące poważne skutki i stanowiące zewnętrzne zagrożenie dla Unii lub jej państw członkowskich.</p>	24.6.2024”.

2) w części „B. Osoby prawne, podmioty i organy” wpis 1 otrzymuje brzmienie:

	Nazwa	Dane identyfikacyjne	Powody	Data umieszczenia
„1.	Tianjin Huaying Haitai Science and Technology Development Co Ltd (Huaying Haitai)	Alias: Haitai Technology Development Co. Ltd Miejsce: Tiencin, Chiny	<p>Huaying Haitai udzielił finansowego, technicznego lub materialnego wsparcia na rzecz „Operation Cloud Hopper”, serii cyberataków wywołujących poważne skutki, pochodzących spoza Unii i stanowiących zewnętrzne zagrożenie dla Unii lub jej państw członkowskich, oraz cyberataków wywołujących poważne skutki dla państw trzecich; ułatwił także te cyberataki.</p> <p>Cyberataki „Operation Cloud Hopper” były skierowane przeciwko systemom informacyjnym przedsiębiorstw wielonarodowych na sześciu kontynentach, w tym przedsiębiorstw mających siedzibę w Unii, oraz skutkowały nieuprawnionym dostępem do danych wrażliwych pod względem handlowym, powodując znaczne straty gospodarcze.</p> <p>Cyberataki „Operation Cloud Hopper” zostały przeprowadzone przez podmiot powszechnie znany jako APT10 („Advanced Persistent Threat 10”) (alias „Red Apollo”, „CVNX”, „Stone Panda”, „MenuPass” i „Potassium”).</p> <p>Huaying Haitai można powiązać z APT10. Ponadto Gao Qiang i Zhang Shilong, obaj umieszczeni w wykazie w związku z „Operation Cloud Hopper”, byli zatrudnieni przez Hujaing Haitai. Huaying Haitai ma zatem także powiązania zarówno z Gao Qiangiem, jak i Zhangiem Shilongiem.</p>	30.7.2020”.