2026/1079

12.5.2026

DECYZJA RADY (WPZiB) 2026/1079

z dnia 11 maja 2026 r.

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 ([1]).

(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:

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 Brukseli dnia 11 maja 2026 r.

W imieniu Rady

Przewodnicząca

K. KALLAS

([1]) 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/2019/797/oj).

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: prowincja Szantung, Chiny Adres: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Obywatelstwo: chińskie Płeć: mężczyzna	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. 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. 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.	30.7.2020

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
2.	ZHANG Shilong	Data urodzenia: 10 września 1981 r. Miejsce urodzenia: Chiny Adres: Hedong, Yuyang Road No 121, Tianjin, China Obywatelstwo: chińskie Płeć: mężczyzna	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. 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. Zhang Shilong ma powiązania z APT10, w tym przez złośliwe oprogramowanie, które opracował i testował w związku z cyberatakami przeprowadzonymi przez APT10. 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«. Ma powiązania z Gao Qiangiem, który jest powiązany z APT10 i był również zatrudniony przez Huaying Haitai.	30.7.2020

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
13.	Mikhail Mikhailovich TSAREV	Михаил Михайлович ЦАРЕВ Data urodzenia: 20 kwietnia 1989 r. Miejsce urodzenia: Sierpuchow, Federacja Rosyjska Obywatelstwo: rosyjskie Adres: Sierpuchow Płeć: mężczyzna	Michaił Carew brał udział w cyberatakach wywołujących poważne skutki i stanowiących zewnętrzne zagrożenie dla państw członkowskich UE. 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. 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. 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. Michaił Carew jest zatem zaangażowany w cyberataki wywołujące poważne skutki i stanowiące zewnętrzne zagrożenie dla Unii lub jej państw członkowskich.	24.6.2024

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
14.	Maksim Sergeevich GALOCHKIN	Максим Сергеевич ГАЛОЧКИН Data urodzenia: 19 maja 1982 r. Miejsce urodzenia: Abakan, Federacja Rosyjska Obywatelstwo: rosyjskie Płeć: mężczyzna	Maksim Gałoczkin brał udział w cyberatakach wywołujących poważne skutki i stanowiących zewnętrzne zagrożenie dla państw członkowskich UE. 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. 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. Maksim Gałoczkin jest zatem zaangażowany w cyberataki wywołujące poważne skutki i stanowiące zewnętrzne zagrożenie dla Unii lub jej państw członkowskich.	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	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. 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. 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«). 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.	30.7.2020”