2024/1778

24.6.2024

ROZPORZĄDZENIE WYKONAWCZE RADY (UE) 2024/1778

z dnia 24 czerwca 2024 r.

wykonujące rozporządzenie (UE) 2019/796 w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim

RADA UNII EUROPEJSKIEJ,

uwzględniając Traktat o funkcjonowaniu Unii Europejskiej,

uwzględniając rozporządzenie Rady (UE) 2019/796 z dnia 17 maja 2019 r. w sprawie środków ograniczających w celu zwalczania cyberataków zagrażających Unii lub jej państwom członkowskim ([1]), w szczególności jego art. 13 ust. 1,

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

a także mając na uwadze, co następuje:

(1) 17 maja 2019 r. Rada przyjęła rozporządzenie (UE) 2019/796.

(2) Ukierunkowane środki ograniczające w celu zwalczania cyberataków wywołujących znaczące skutki, które to ataki stanowią zewnętrzne zagrożenie dla Unii lub jej państw członkowskich, należą do środków przewidzianych w unijnych ramach wspólnej reakcji dyplomatycznej na szkodliwe działania w cyberprzestrzeni (zestaw narzędzi dla dyplomacji cyfrowej) i są jednym z niezbędnych instrumentów zapobiegania takim działaniom, powstrzymywania ich, zniechęcania do nich i reagowania na nie.

(3) Rośnie liczba, częstotliwość i stopień wyrafinowania szkodliwych działań w cyberprzestrzeni skierowanych przeciwko infrastrukturze krytycznej lub usługom kluczowym, prowadzonych m.in. za pomocą oprogramowania szantażującego i oprogramowania niszczącego dane (wiperware), obejmujących też ataki wymierzone w łańcuchy dostaw i akty cyberszpiegostwa, w tym kradzieże własności intelektualnej. Ze względu na swój zakłócający i destrukcyjny wpływ działania te stanowią systemowe zagrożenie dla bezpieczeństwa, gospodarki, demokracji i całego społeczeństwa Unii.

(4) Cyberoperacje, które umożliwiły niczym niesprowokowaną i nieuzasadnioną wojnę napastniczą Rosji przeciwko Ukrainie i które jej towarzyszą, wpływają na stabilność i bezpieczeństwo na świecie, stanowią poważne ryzyko eskalacji i przyczyniają się do znacznego już wzrostu szkodliwych działań w cyberprzestrzeni, który w ostatnich latach wykraczał poza kontekst konfliktów zbrojnych. Dodatkowymi bodźcami do wprowadzenia środków ograniczających na mocy rozporządzenia (UE) 2019/796 są rosnące zagrożenia w cyberprzestrzeni i ogólnie złożony krajobraz zagrożeń dla cyberbezpieczeństwa, w tym oczywiste ryzyko szybkiego rozprzestrzeniania się cyberincydentów z jednego państwa członkowskiego na inne oraz z państw trzecich na Unię.

(5) W ramach konsekwentnych, ukierunkowanych i skoordynowanych działań Unii przeciwko podmiotom stale powodującym zagrożenia w cyberprzestrzeni w wykazie osób fizycznych i prawnych, podmiotów i organów podlegających środkom ograniczającym zawartym w załączniku I do rozporządzenia (UE) 2019/796 należy zamieścić sześć osób fizycznych. Osoby te są odpowiedzialne za lub zaangażowane w cyberataki wywołujące znaczące skutki i stanowiące zewnętrzne zagrożenie dla Unii lub jej państw członkowskich.

(6) Należy zatem odpowiednio zmienić załącznik I do rozporządzenia (UE) 2019/796,

PRZYJMUJE NINIEJSZE ROZPORZĄDZENIE:

Artykuł 1

W załączniku I do rozporządzenia (UE) 2019/796 wprowadza się zmiany zgodnie z załącznikiem do niniejszego rozporządzenia.

([1]) Dz.U. L 129 I z 17.5.2019, s. 1.

Artykuł 2

Niniejsze rozporządzenie wchodzi w życie z dniem opublikowania go w *Dzienniku Urzędowym Unii Europejskiej*.

Niniejsze rozporządzenie wiąże w całości i jest bezpośrednio stosowane we wszystkich państwach członkowskich.

Sporządzono w Luksemburgu dnia 24 czerwca 2024 r.

W imieniu Rady

Przewodniczący

J. BORRELL FONTELLES

ZAŁĄCZNIK

W sekcji „A. Osoby fizyczne” w załączniku I do rozporządzenia (UE) 2019/796 dodaje się wpisy w brzmieniu:

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
„9.	Ruslan Aleksandrovich PERETYATKO	Руслан Александрович ПЕРЕТЯТЬКО Data urodzenia: 3.8.1985 Obywatelstwo: rosyjskie Płeć: mężczyzna	Ruslan Peretyatko brał udział w cyberatakach wywołujących znaczące skutki i stanowiących zewnętrzne zagrożenie dla Unii lub jej państw członkowskich. Ruslan Peretyatko należy do »grupy Callisto« złożonej z rosyjskich oficerów wywiadu wojskowego prowadzących cyberoperacje przeciwko państwom członkowskim UE i państwom trzecim. Grupa Callisto (inne nazwy: »Seaborgium«, »Star Blizzard«, »ColdRiver«, »TA446«) rozpoczęła wieloletnie kampanie phishingowe wykorzystywane do kradzieży informacji uwierzytelniających i danych. Ponadto grupa Callisto jest odpowiedzialna za kampanie wymierzone w osoby fizyczne i w krytyczne funkcje państwa, w tym w dziedzinie obronności i stosunków zewnętrznych. Ruslan Peretyatko jest zatem zaangażowany w cyberataki wywołujące znaczące skutki i stanowiące zewnętrzne zagrożenie dla Unii lub jej państw członkowskich.	24.6.2024
10.	Andrey Stanislavovich KORINETS	Андрей Станиславович КОРИНЕЦ Data urodzenia: 18.5.1987 Miejsce urodzenia: Syktywkar, Rosja Obywatelstwo: rosyjskie Płeć: mężczyzna	Andrey Stanislavovich Korinets brał udział w cyberatakach wywołujących znaczące skutki i stanowiących zewnętrzne zagrożenie dla Unii lub jej państw członkowskich. Jest on oficerem »Centrum 18« Federalnej Służby Bezpieczeństwa (FSB) Federacji Rosyjskiej. Należy do »grupy Callisto« złożonej z rosyjskich oficerów wywiadu wojskowego prowadzących cyberoperacje przeciwko państwom członkowskim UE i państwom trzecim. Grupa Callisto (inne nazwy: »Seaborgium«, »Star Blizzard«, »ColdRiver«, »TA446«) rozpoczęła wieloletnie kampanie phishingowe wykorzystywane do kradzieży informacji uwierzytelniających i danych. Ponadto grupa Callisto jest odpowiedzialna za kampanie wymierzone w osoby fizyczne i w krytyczne funkcje państwa, w tym w dziedzinie obronności i stosunków zewnętrznych. Andrey Stanislavovich Korinets jest zatem zaangażowany w cyberataki wywołujące znaczące skutki i stanowiące zewnętrzne zagrożenie dla Unii lub jej państw członkowskich.	24.6.2024

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
11.	Oleksandr SKLIANKO	Александр СКЛЯНКО (pisownia rosyjska) Олександр СКЛЯНКО (pisownia ukraińska) Data urodzenia: 5.8.1973 Paszport: EC 867868, wydany dnia 27.11.1998 (Ukraina) Płeć: mężczyzna	Oleksandr Sklianko brał udział w wywołujących znaczące skutki cyberatakach wymierzonych w państwa członkowskie UE oraz w wywołujących znaczące skutki cyberatakach wymierzonych w państwa trzecie. Należy on do grupy hakerskiej »Armageddon« wspieranej przez Federalną Służbę Bezpieczeństwa (FSB) Federacji Rosyjskiej, która przeprowadziła różne cyberataki mające znaczący wpływ na rząd Ukrainy oraz na państwa członkowskie UE i ich urzędników rządowych, w tym za pomocą wiadomości poczty elektronicznej noszących znamiona phishingu i złośliwego oprogramowania. Oleksandr Sklianko jest zatem zaangażowany w wywołujące znaczące skutki cyberataki wymierzone w państwa trzecie oraz w cyberataki wywołujące znaczące skutki i stanowiące zewnętrzne zagrożenie dla Unii lub jej państw członkowskich.	24.6.2024
12.	Mykola CHERNYKH	Николай ЧЕРНЫХ (pisownia rosyjska) Микола ЧЕРНИХ (pisownia ukraińska) Data urodzenia: 12.10.1978 Paszport: EC 922162, wydany dnia 20.01.1999 (Ukraina) Płeć: mężczyzna	Mykola Chernykh brał udział w wywołujących znaczące skutki cyberatakach wymierzonych w państwa członkowskie UE oraz w wywołujących znaczące skutki cyberatakach wymierzonych w państwa trzecie. Należy on do grupy hakerskiej »Armageddon« wspieranej przez Federalną Służbę Bezpieczeństwa (FSB) Federacji Rosyjskiej, która przeprowadziła różne cyberataki mające znaczący wpływ na rząd Ukrainy oraz na państwa członkowskie UE i ich urzędników rządowych, w tym za pomocą wiadomości poczty elektronicznej noszących znamiona phishingu i złośliwego oprogramowania. Jako były pracownik Służby Bezpieczeństwa Ukrainy jest oskarżany w Ukrainie o zdradę i nieupoważnioną ingerencję w działanie elektronicznych maszyn obliczeniowych i systemów zautomatyzowanych. Mykola Chernykh jest zatem zaangażowany w cyberataki wywołujące znaczące skutki i stanowiące zewnętrzne zagrożenie dla Unii lub jej państw członkowskich.	24.6.2024

	Nazwisko i imię	Dane identyfikacyjne	Powody	Data umieszczenia
13.	Mikhail Mikhailovich TSAREV	Михаил Михайлович ЦАРЕВ Data urodzenia: 20.4.1989 Miejsce urodzenia: Sierpuchow, Federacja Rosyjska Obywatelstwo: rosyjskie Adres: Sierpuchow Płeć: mężczyzna	Mikhail Mikhailovich Tsarev brał udział w cyberatakach wywołujących znaczące 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«. Złośliwe oprogramowanie Conti i Trickbot zostało stworzone i opracowane przez Wizard Spider. Wizard Spider przeprowadziła 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 i TrickBot, powodują znaczne szkody gospodarcze w Unii Europejskiej. Mikhail Mikhailovich Tsarev jest zatem zaangażowany w cyberataki wywołujące znaczące 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: 19.5.1982 Miejsce urodzenia: Abakan, Federacja Rosyjska Obywatelstwo: rosyjskie Płeć: mężczyzna	Maksim Sergeevich Galochkin brał udział w cyberatakach wywołujących znaczące 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 opracowaniu 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 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 i »Ryuk« i TrickBot, powodują znaczne szkody gospodarcze w Unii Europejskiej. Maksim Sergeevich Galochkin jest zatem zaangażowany w cyberataki wywołujące znaczące skutki i stanowiące zewnętrzne zagrożenie dla Unii lub jej państw członkowskich.	24.6.2024”.