DECIZIA (PESC) 2020/1748 A CONSILIULUI

din 20 noiembrie 2020

de modificare a Deciziei (PESC) 2019/797 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre

CONSILIUL UNIUNII EUROPENE,

având în vedere Tratatul privind Uniunea Europeană, în special articolul 29,

având în vedere propunerea Înaltului Reprezentant al Uniunii pentru afaceri externe și politica de securitate,

întrucât:

(1) La 17 mai 2019, Consiliul a adoptat Decizia (PESC) 2019/797 ([1]).

(2) La 30 iulie 2020, Consiliul a adoptat Decizia (PESC) 2020/1127 ([2]), prin care șase persoane fizice și trei entități sau organisme au fost adăugate pe lista persoanelor fizice și juridice, a entităților și a organismelor cărora li se aplică măsuri restrictive, prevăzută în anexa la Decizia (PESC) 2019/797.

(3) S-au primit informații actualizate privind două rubrici ale unor persoane fizice.

(4) Prin urmare, Decizia (PESC) 2019/797 ar trebui modificată în consecință,

ADOPTĂ PREZENTA DECIZIE:

Articolul 1

Anexa la Decizia (PESC) 2019/797 se modifică în conformitate cu anexa la prezenta decizie.

Articolul 2

Prezenta decizie intră în vigoare în ziua următoare datei publicării în *Jurnalul Oficial al Uniunii Europene*.

Adoptată la Bruxelles, 20 noiembrie 2020.

Pentru Consiliu
Președintele
M. ROTH

([1]) Decizia (PESC) 2019/797 a Consiliului din 17 mai 2019 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre (JO L 129I, 17.5.2019, p. 13).

([2]) Decizia (PESC) 2020/1127 a Consiliului din 30 iulie 2020 de modificare a Deciziei (PESC) 2019/797 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre (JO L 246, 30.7.2020, p. 12).

ANEXĂ

În anexa la Decizia (PESC) 2019/797, la secțiunea „A. Persoane fizice”, rubricile 1 și 2 se înlocuiesc cu următorul text:

	Nume	Informații de identificare	Motive	Data includerii pe listă
„1.	GAO Qiang	Data nașterii: 4 octombrie 1983 Locul nașterii: Shandong Province, China Adresă: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Cetățenie: chineză Sexul: masculin	Gao Qiang este implicat în «Operation Cloud Hopper», o serie de atacuri cibernetice având efecte importante, a căror origine se situează în afara Uniunii și care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre, și în atacuri cibernetice având efecte importante asupra unor state terțe. «Operation Cloud Hopper» a vizat sistemele de informații ale unor întreprinderi multinaționale de pe șase continente, inclusiv ale unor întreprinderi situate în Uniune, și a dobândit acces neautorizat la date sensibile din punct de vedere comercial, ceea ce a provocat pierderi economice importante. Actorul cunoscut în mod public sub numele de «APT10» («Advanced Persistent Threat 10») (*alias*: «Red. Apollo», «CVNX», «Stone Panda», «MenuPass» și «Potassium») a efectuat «Operation Cloud Hopper». Se poate stabili o legătură între Gao Qiang și APT10, inclusiv prin asocierea acestuia cu infrastructura de comandă și control a APT10. În plus, Huaying Haitai, entitate desemnată pentru că a oferit sprijin și a facilitat «Operation Cloud Hopper», l-a avut drept angajat pe Gao Qiang. Acesta are legături cu Zhang Shilong, desemnat la rândul său în legătură cu «Operation Cloud Hopper». Prin urmare, Gao Qiang este asociat atât cu Huaying Haitai, cât și cu Zhang Shilong.	30.7.2020
2.	ZHANG Shilong	Data nașterii: 10 septembrie 1981 Locul nașterii: China Adresă: Hedong, Yuyang Road No 121, Tianjin, China Cetățenie: chineză Sexul: masculin	Zhang Shilong este implicat în «Operation Cloud Hopper», o serie de atacuri cibernetice având efecte importante, a căror origine se situează în afara Uniunii și care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre, și în atacuri cibernetice având efecte importante asupra unor state terțe. «Operation Cloud Hopper» a vizat sistemele de informații ale unor întreprinderi multinaționale de pe șase continente, inclusiv ale unor întreprinderi situate în Uniune, și a dobândit acces neautorizat la date sensibile din punct de vedere comercial, ceea ce a provocat pierderi economice importante. Actorul cunoscut în mod public sub numele de «APT10» («Advanced Persistent Threat 10») (*alias*: «Red. Apollo», «CVNX», «Stone Panda», «MenuPass» și «Potassium») a efectuat «Operation Cloud Hopper». Se poate stabili o legătură între Zhang Shilong și APT10, inclusiv prin programele malware pe care acesta le-a dezvoltat și testat în legătură cu atacurile cibernetice desfășurate de APT10. În plus, Huaying Haitai, entitate desemnată pentru că a oferit sprijin și a facilitat «Operation Cloud Hopper», l-a avut drept angajat pe Zhang Shilong. Acesta are legături cu Gao Qiang, desemnat la rândul său în legătură cu «Operation Cloud Hopper». Prin urmare, Zhang Shilong este asociat atât cu Huaying Haitai, cât și cu Gao Qiang.	30.7.2020”