2026/1078

12.5.2026

REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2026/1078 AL CONSILIULUI

din 11 mai 2026

privind punerea în aplicare a Regulamentului (UE) 2019/796 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 funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) 2019/796 al Consiliului din 17 mai 2019 privind măsuri restrictive împotriva atacurilor cibernetice care reprezintă o amenințare la adresa Uniunii sau a statelor sale membre ([1]), în special articolul 13,

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

întrucât:

(1) La 17 mai 2019, Consiliul a adoptat Regulamentul (UE) 2019/796.

(2) Consiliul a reexaminat lista persoanelor fizice și juridice, a entităților și a organismelor din anexa I la Regulamentul (UE) 2019/796. Pe baza respectivei reexaminări, ar trebui să fie actualizate motivele pentru includerea a patru persoane și a unei entități pe lista persoanelor fizice și juridice, a entităților și a organismelor cărora li se aplică măsuri restrictive.

(3) Prin urmare, anexa I la Regulamentul (UE) 2019/796 ar trebui să fie modificată în consecință,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Anexa I la Regulamentul (UE) 2019/796 se modifică în conformitate cu anexa la prezentul regulament.

Articolul 2

Prezentul regulament intră în vigoare în ziua următoare datei publicării în *Jurnalul Oficial al Uniunii Europene*.

Prezentul regulament este obligatoriu în toate elementele sale și se aplică direct în toate statele membre.

Adoptat la Bruxelles, 11 mai 2026.

Pentru Consiliu

Președintele

K. KALLAS

([1]) JO L 129 I, 17.5.2019, p. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj.

ANEXĂ

Anexa I la Regulamentul (UE) 2019/796 se modifică după cum urmează:

1. În secțiunea „A. Persoane fizice”, rubricile 1, 2, 13 și 14 se înlocuiesc cu următoarele rubrici corespunzătoare:

	Nume	Informații de identificare	Motive	Data includerii pe listă
„1.	GAO Qiang	Data nașterii: 4 octombrie 1983 Locul nașterii: provincia Shandong, China Adresa: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Cetățenia: chineză Sexul: masculin	Gao Qiang are legături cu actorul generic «APT10» («Advanced Persistent Threat 10») (*alias* «Red Apollo», «CVNX», «Stone Panda», «MenuPass» și «Potassium») și a fost 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, precum 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. Gao Qiang este asociat cu infrastructura de comandă și control a APT10. În plus, Huaying Haitai, o societate utilizată de APT10 și desemnată pentru că a oferit sprijin și a facilitat «Operation Cloud Hopper», l-a avut drept angajat pe Gao Qiang. Gao Qiang este asociat și cu Zhang Shilong, care are legături cu APT10 și care a fost, de asemenea, angajat al Huaying Haitai.	30.7.2020

	Nume	Informații de identificare	Motive	Data includerii pe listă
2.	ZHANG Shilong	Data nașterii: 10 septembrie 1981 Locul nașterii: China Adresa: Hedong, Yuyang Road No 121, Tianjin, China Cetățenia: chineză Sexul: masculin	Zhang Shilong are legături cu actorul generic «APT10» («Advanced Persistent Threat 10») (*alias* «Red Apollo», «CVNX», «Stone Panda», «MenuPass» și «Potassium») și a fost 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, precum 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. Zhang Shilong este asociat cu APT10, inclusiv prin programele malware pe care le-a dezvoltat și testat în legătură cu atacurile cibernetice desfășurate de APT10. În plus, Huaying Haitai, o societate utilizată de APT10 și desemnată pentru că a oferit sprijin și a facilitat «Operation Cloud Hopper», l-a avut drept angajat pe Zhang Shilong. Zhang Shilong este asociat cu Gao Qiang, care are legături cu APT10 și care a fost, de asemenea, angajat al Huaying Haitai.	30.7.2020

	Nume	Informații de identificare	Motive	Data includerii pe listă
13.	Mikhail Mikhailovich TSAREV	Михаил Михайлович ЦАРЕВ Data nașterii: 20.4.1989 Locul nașterii: Serpuhov, Federația Rusă Cetățenia: rusă Adresa: Serpuhov Sexul: masculin	Mikhail Mikhailovich Tsarev a participat la atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa statelor membre ale UE. Mikhail Mikhailovich Tsarev, cunoscut și sub pseudonimele online «Mango», «Alexander Grachev», «Super Misha», «Ivanov Mixail», «Misha Krutysha» și «Nikita Andreevich Tsarev», este un actor-cheie în răspândirea programelor malware «Conti» și «Trickbot» și este implicat în grupul ostil «Wizard Spider» din Rusia. Wizard Spider continuă să evolueze și să își intensifice operațiunile. Programele malware Conti și Trickbot au fost create și dezvoltate de Wizard Spider. Wizard Spider a desfășurat campanii de tip ransomware în diverse sectoare, inclusiv servicii esențiale cum ar fi sănătatea și serviciile bancare. Grupul a infectat computere în întreaga lume, iar programele sale malware au fost dezvoltate într-un ansamblu de programe malware foarte modular. Campaniile desfășurate de Wizard Spider, prin utilizarea de programe malware cum ar fi Conti, TrickBot «Ryuk» sau Black Basta, sunt responsabile pentru daune economice substanțiale în Uniunea Europeană. Prin urmare, Mikhail Mikhailovich Tsarev este implicat în atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre.	24.6.2024

ELI: http://data.europa.eu/eli/reg_impl/2026/1078/oj

	Nume	Informații de identificare	Motive	Data includerii pe listă
14.	Maksim Sergeevich GALOCHKIN	Максим Сергеевич ГАЛОЧКИН Data nașterii: 19.5.1982 Locul nașterii: Abakan, Federația Rusă Cetățenia: rusă Sexul: masculin	Maksim Galochkin a participat la atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa statelor membre ale UE. Maksim Galochkin este cunoscut și sub pseudonimele online «Benalen», «Bentley», «Volhvb», «volhvb», «manuel», «Max17» și «Crypt». Galochkin este un actor-cheie în răspândirea programelor malware «Conti» și «Trickbot» și este implicat în grupul ostil «Wizard Spider» din Rusia. El a condus un grup de testeri, având responsabilități legate de dezvoltarea, controlul și aplicarea testelor pentru programul malware TrickBot, creat și implementat de Wizard Spider. Wizard Spider continuă să evolueze și să își intensifice operațiunile. Wizard Spider a desfășurat campanii de tip ransomware în diverse sectoare, inclusiv servicii esențiale cum ar fi sănătatea și serviciile bancare. Grupul a infectat computere în întreaga lume, iar programele sale malware au fost dezvoltate într-un ansamblu de programe malware foarte modular. Campaniile desfășurate de Wizard Spider, prin utilizarea de programe malware cum ar fi Conti, TrickBot «Ryuk» sau Black Basta, sunt responsabile pentru daune economice substanțiale în Uniunea Europeană. Prin urmare, Maksim Galochkin este implicat în atacuri cibernetice cu un efect semnificativ care constituie o amenințare externă la adresa Uniunii sau a statelor sale membre.	24.6.2024”

2. În secțiunea „B. Persoane juridice, entități și organisme”, rubrica 1 se înlocuiește cu următorul text:

	Nume	Informații de identificare	Motive	Data includerii pe listă
„1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Compania de dezvoltare științifică și tehnologică Huaying Haitai SRL din Tianjin) (Huaying Haitai)	*alias*: Haitai Technology Development Co. Ltd Localitate: Tianjin, China	Huaying Haitai a sprijinit financiar, tehnic sau material și a facilitat «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, precum și 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 desfășurat «Operation Cloud Hopper». Poate fi stabilită o legătură între Huaying Haitai și APT10. În plus, Gao Qiang și Zhang Shilong, ambii desemnați în legătură cu «Operation Cloud Hopper», au fost angajați ai Huaying Haitai. Prin urmare, Huaying Haitai este, de asemenea, asociată cu Gao Qiang și Zhang Shilong.	30.7.2020”