Consiglio dell'Unione europea

Bruxelles, 10 marzo 2026
(OR. en)

5136/26

LIMITE

CORLX 12
CFSP/PESC 19
RELEX 11
CYBER 6
JAI 23
FIN 10

ATTI LEGISLATIVI ED ALTRI STRUMENTI

Oggetto:	REGOLAMENTO DI ESECUZIONE DEL CONSIGLIO che attua il regolamento (UE) 2019/796, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri

REGOLAMENTO DI ESECUZIONE (UE) 2026/… DEL CONSIGLIO

del …

che attua il regolamento (UE) 2019/796, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri

IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) 2019/796 del Consiglio, del 17 maggio 2019, concernente misure restrittive contro gli attacchi informatici che minacciano l'Unione o i suoi Stati membri[1], in particolare l'articolo 13, paragrafo 1,

vista la proposta dell'alto rappresentante dell'Unione per gli affari esteri e la politica di sicurezza,

[1] GU L 129I del 17.5.2019, pag. 1, ELI: http://data.europa.eu/eli/reg/2019/796/oj.

considerando quanto segue:

(1) Il 17 maggio 2019 il Consiglio ha adottato il regolamento (UE) 2019/796.

(2) Nel quadro dell'azione dell'Unione duratura, mirata e coordinata contro gli autori di minacce informatiche persistenti, due persone fisiche e tre entità dovrebbero essere inserite nell'elenco delle persone fisiche e giuridiche, delle entità e degli organismi oggetto di misure restrittive di cui all'allegato I del regolamento (UE) 2019/796. Tali persone fisiche ed entità sono responsabili di attacchi informatici o vi sono coinvolte con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.

(3) È pertanto opportuno modificare di conseguenza l'allegato I del regolamento (UE) 2019/796,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

L'allegato I del regolamento (UE) 2019/796 è modificato conformemente all'allegato del presente regolamento.

Articolo 2

Il presente regolamento entra in vigore il giorno della pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a …, il …

Per il Consiglio
Il presidente

ALLEGATO

L'allegato I del regolamento (UE) 2019/796 è così modificato:

1) Le voci seguenti sono aggiunte alla sezione "A. Persone fisiche":

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
"18.	CHEN Cheng	陈诚 (grafia cinese) Pseudonimi: Jesse Chen lengmo l3n6m0 Data di nascita: 20.10.1984 Luogo di nascita: Yancheng, Jiangsu, Cina Cittadinanza: cinese Sesso: maschile	Chen Cheng è un uomo d'affari cinese, cofondatore e uno dei direttori generali (direttore operativo) di Anxun Information Technology Co. Ltd. È anche rappresentante legale della filiale di tale società del Sichuan di tale società. Anxun Information Technology Co. Ltd., nota anche come i-Soon, è una società con sede nella Repubblica popolare cinese che offre servizi di "hacking-for-hire" (hackeraggio su commissione). Anxun Information Technology Co. Ltd. ha preso di mira infrastrutture critiche e funzioni statali essenziali degli Stati membri, ha avuto accesso a informazioni classificate e le ha vendute. Anxun Information Technology Co. Ltd. ha inoltre attaccato governi di vari Stati terzi, costituendo una minaccia per gli obiettivi della politica estera e di sicurezza comune (PESC) dell'Unione, come stabilito nell'articolo 21, paragrafo 2, lettere da a) a c), del trattato sull'Unione europea.. Anxun Information Technology Co. Ltd. trae un importante vantaggio economico dai servizi forniti.	+

+ GU: inserire la data di entrata in vigore del presente regolamento.

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
			Anxun Information Technology Co. Ltd è pertanto responsabile di attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione e i suoi Stati membri e di attacchi informatici con effetti significativi nei confronti di Stati terzi. In tale veste, Chen Cheng è responsabile di attacchi informatici con effetti significativi che costituiscono una minaccia esterna per gli Stati membri, nonché di attacchi informatici con effetti significativi nei confronti di Stati terzi, e vi è coinvolto.	

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
19.	WU Haibo	吴海波 (grafia cinese) Pseudonimi: shutdown shutd0wn Luogo di nascita: Cina Cittadinanza: cinese Sesso: maschile	Wu Haibo è un uomo d'affari cinese, cofondatore e uno dei direttori generali (direttore operativo) di Anxun Information Technology Co. Ltd. È anche rappresentante legale, presidente e direttore generale della filiale di Shanghai ("società madre") di Anxun Information Technology Co. Ltd. Inoltre agisce inoltre in qualità di rappresentante legale della filiale del Sichuan di tale società. Anxun Information Technology Co. Ltd., nota anche come i-Soon, è una società con sede nella Repubblica popolare cinese che offre servizi di "hacking-for-hire" (hackeraggio su commissione). Anxun Information Technology Co. Ltd. ha preso di mira infrastrutture critiche e funzioni statali essenziali degli Stati membri, ha avuto accesso a informazioni classificate e le ha vendute. Anxun Information Technology Co. Ltd ha inoltre attaccato governi di vari Stati terzi, costituendo una minaccia per gli obiettivi della politica estera e di sicurezza comune (PESC) dell'Unione, come stabilito nell'articolo 21, paragrafo 2, lettere da a) a c), del trattato sull'Unione europea.. Anxun Information Technology Co. Ltd trae un importante vantaggio economico dai servizi forniti.	[+]";

[+] GU: inserire la data di entrata in vigore del presente regolamento.

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
			Anxun Information Technology Co. Ltd è pertanto responsabile di attacchi informatici con effetti significativi che costituiscono una minaccia esterna per gli Stati membri e di attacchi informatici con effetti significativi nei confronti di Stati terzi. Wu Haibo è stato coinvolto nella direzione e nell'incoraggiamento di tentati attacchi informatici con effetti significativi nei confronti degli Stati membri. In tale veste, è responsabile di attacchi informatici con effetti significativi che costituiscono una minaccia esterna per gli Stati membri, nonché di attacchi informatici con effetti significativi nei confronti di Stati terzi, e vi è coinvolto.	

2) Le voci seguenti sono aggiunte alla sezione "B. Persone giuridiche, entità e organismi":

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
"5.	Integrity Technology Group	永信至诚科技集团股份有限公司 (grafia cinese) Pseudonimo: Beijing Integrity Technology Company Limited, Yongxin Zhicheng Technology Group Company Limited Indirizzo: Fenghao East Road, Room 103, Building 6, No. 9, Beijing Haidian District, China	Integrity Technology Group è un'impresa di cibersicurezza con sede nella Repubblica popolare cinese che ha agevolato attacchi informatici legati alla minaccia mirata e persistente (*Advanced Persistent Threat* – APT) Flax Typhoon. Tale minaccia APT ha utilizzato i prodotti e la tecnologia di Integrity Technology Group per realizzare le sue attività di sfruttamento delle reti informatiche. Da allora, i prodotti di Integrity Technology Group sono utilizzati per compromettere i dispositivi dell'internet delle cose negli Stati membri, nonché in paesi in tutta Europa e nel mondo, e per accedervi. Tra il 2022 e il 2023 Flax Typhoon ha avuto accesso ad almeno 65 600 dispositivi dell'internet delle cose in sei Stati membri utilizzando i prodotti di Integrity Technology. Pertanto, i prodotti e le infrastrutture commerciali di Integrity Technology Group sono stati utilizzati regolarmente per attacchi informatici nei confronti di Stati membri e Stati terzi. Di conseguenza, colpendo i sistemi di informazione relativi alle infrastrutture digitali, Integrity Technology Group fornisce sostegno tecnico e materiale per attacchi informatici con effetti significativi che costituiscono una minaccia esterna per gli Stati membri e gli Stati terzi.	[+]

[+] GU: inserire la data di entrata in vigore del presente regolamento.

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
		Luogo di registrazione: Beijing, China Data di registrazione: 2.9.2010 Codice unificato di credito sociale: 91110108562135265P		

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
6.	Emennet Pasargad	Pseudonimo: Anzu Team, Holy Souls, Aria Sepehr Ayandehsazan, Haywire Kitten Luogo di registrazione: Tehran, Iran Numero di registrazione: 554267 Sede principale: Tehran, Iran	Emennet Pasargad è un attore informatico iraniano (società) che ha preso di mira numerose entità, in particolare negli Stati membri e negli Stati Uniti. Emennet Pasargard, che opera con lo pseudonimo "Anzu Team", ha preso di mira l'infrastruttura digitale in Svezia e ha compromesso un servizio di SMS svedese, con conseguenze per un gran numero di persone. Inoltre, agendo con lo pseudonimo "Holy Souls", l'entità ha compromesso la banca dati degli abbonati della rivista satirica francese Charlie Hebdo mettendola in vendita sul dark web. Emennet Pasargad ha compromesso i cartelloni pubblicitari durante i Giochi olimpici di Parigi diffondendo campagne di disinformazione. Emennet Pasargad ha inoltre tentato di interferire con le elezioni presidenziali statunitensi del 2020, minacciando la democrazia e lo Stato di diritto, ottenendo informazioni riservate sugli elettori statunitensi e un accesso non autorizzato alla rete informatica di una società statunitense che opera nel settore dei media. Emennet Pasargad è pertanto responsabile di attacchi informatici con effetti significativi che costituiscono una minaccia esterna per gli Stati membri e di attacchi informatici con effetti significativi nei confronti di uno Stato terzo.	[+]

[+] GU: inserire la data di entrata in vigore del presente regolamento.

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
7.	Anxun Information Technology Co. Ltd	安洵信息技术有限公司 (grafia cinese) Pseudonimo: i-Soon Indirizzo: Room 1002, Qiangqiang Building, No. 1318 Qixin Road, Minhang District, Shanghai Codice unificato di credito sociale: 91510105332025597A (filiale del Sichuan) Codice unificato di credito sociale: 91310116561906136G (filiale di Shanghai)	Anxun Information Technology Co. Ltd. è una società con sede nella Repubblica popolare cinese che offre servizi di "hacking-for-hire" (hackeraggio su commissione). Ha preso di mira infrastrutture critiche e funzioni statali essenziali degli Stati membri, ha avuto accesso a informazioni classificate e le ha vendute. Anxun Information Technology Co. Ltd. ha inoltre attaccato governi di vari Stati terzi, costituendo una minaccia per gli obiettivi della politica estera e di sicurezza comune (PESC) dell'Unione, come stabilito nell'articolo 21, paragrafo 2, lettere da a) a c), del trattato sull'Unione europea.. Anxun Information Technology Co. Ltd. trae un importante vantaggio economico dai servizi forniti. Anxun Information Technology Co. Ltd. è pertanto responsabile di attacchi informatici con effetti significativi che costituiscono una minaccia esterna per gli Stati membri e di attacchi informatici con effetti significativi nei confronti di Stati terzi.	[+]".

[+] GU: inserire la data di entrata in vigore del presente regolamento.

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
		Sito web: i-soon.net, isoon.net, i-soon.com.cn, isoonren.com, isoon.win Numeri di telefono: +862161119992, +8605645893417, +8613761671735, +864000665915 E-mail: shutdown@163.com, isoon2015@126.com, tao_tingting@i-soon.net, li_ping@i-soon.net		