Consiglio dell'Unione europea

Bruxelles, 5 maggio 2026
(OR. en)

7283/26

LIMITE

CORLX 273
CFSP/PESC 390
RELEX 352
CYBER 115
JAI 340
FIN 408

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,

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

[1] GU L 129 I 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) Il Consiglio ha riesaminato l'elenco delle persone fisiche e giuridiche, delle entità e degli organismi che figura nell'allegato I del regolamento (UE) 2019/796. Sulla base di tale riesame, le motivazioni per includere quattro persone e a un'entità nell'elenco delle persone fisiche e giuridiche, delle entità e degli organismi oggetto di misure restrittive dovrebbero essere aggiornate.

(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 successivo alla 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) alla rubrica "A. Persone fisiche", le voci 1, 2, 13 e 14 sono sostituite dalle voci seguenti:

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
"1.	GAO Qiang	Data di nascita: 4 ottobre 1983 Luogo di nascita: provincia di Shandong, Cina Indirizzo: Room 1102, Guanfu Mansion, 46 Xinkai Road, Hedong District, Tianjin, China Cittadinanza: cinese Sesso: maschile	Gao Qiang è collegato al soggetto ombrello "APT10" ("Advanced Persistent Threat 10") (alias "Red Apollo", "CVNX", "Stone Panda", "MenuPass" e "Potassium") ed è stato coinvolto nella campagna "Operation Cloud Hopper", una serie di attacchi informatici con effetti significativi, che proviene dall'esterno dell'Unione e costituisce una minaccia esterna per l'Unione o i suoi Stati membri, e di attacchi informatici con effetti significativi nei confronti di Stati terzi. La campagna "Operation Cloud Hopper" ha preso di mira i sistemi di informazione di imprese multinazionali in sei continenti, tra cui imprese situate nell'Unione, e ha ottenuto l'accesso non autorizzato a dati sensibili sotto il profilo commerciale, causando perdite economiche significative. Gao Qiang è associato all'infrastruttura di comando e controllo di APT10. Inoltre, Huaying Haitai, una società utilizzata da APT10 e designata per il fatto di fornire sostegno e agevolare la campagna "Operation Cloud Hopper", ha impiegato Gao Qiang. È altresì associato a Zhang Shilong, a sua volta collegato ad APT10 e anch'egli in precedenza impiegato presso Huaying Haitai.	30.7.2020

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
2.	ZHANG Shilong	Data di nascita: 10 settembre 1981 Luogo di nascita: Cina Indirizzo: Hedong, Yuyang Road No 121, Tianjin, China Cittadinanza: cinese Sesso: maschile	Zhang Shilong è collegato al soggetto ombrello "APT10" ("Advanced Persistent Threat 10") (alias "Red Apollo", "CVNX", "Stone Panda", "MenuPass" e "Potassium") ed è stato coinvolto nella campagna "Operation Cloud Hopper", una serie di attacchi informatici con effetti significativi, che proviene dall'esterno dell'Unione e costituisce una minaccia esterna per l'Unione o i suoi Stati membri, e di attacchi informatici con effetti significativi nei confronti di Stati terzi. La campagna "Operation Cloud Hopper" ha preso di mira i sistemi di informazione di imprese multinazionali in sei continenti, tra cui imprese situate nell'Unione, e ha ottenuto l'accesso non autorizzato a dati sensibili sotto il profilo commerciale, causando perdite economiche significative. Zhang Shilong è associato ad APT10, anche attraverso il malware che ha sviluppato e testato in relazione agli attacchi informatici condotti da APT10. Inoltre, Huaying Haitai, una società utilizzata da APT10 e designata per il fatto di fornire sostegno e agevolare la campagna "Operation Cloud Hopper", ha impiegato Zhang Shilong. È associato a Gao Qiang, a sua volta collegato ad APT10 e anch'egli in precedenza impiegato presso Huaying Haitai.	30.7.2020

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
13.	Mikhail Mikhailovich TSAREV	Михаил Михайлович ЦАРЕВ Data di nascita: 20.4.1989 Luogo di nascita: Serpukhov, Federazione russa Cittadinanza: russa Indirizzo: Serpukhov Sesso: maschile	Mikhail Mikhailovich Tsarev ha preso parte ad attacchi informatici con effetti significativi che costituiscono una minaccia esterna per gli Stati membri dell'UE. Mikhail Mikhailovich Tsarev, noto anche con i soprannomi online "Mango", "Alexander Grachev", "Super Misha", "Ivanov Mixail", "Misha Krutysha" e "Nikita Andreevich Tsarev", svolge un ruolo chiave nell'impiego di programmi malware "Conti" e "Trickbot" ed è coinvolto nel gruppo di minaccia "Wizard Spider"con sede in Russia. Wizard Spider continua a evolversi e a intensificare le sue operazioni. I programmi malware Conti e Trickbot sono stati creati e sviluppati da Wizard Spider. Wizard Spider ha condotto campagne di ransomware in diversi settori, tra cui servizi essenziali come la sanità e il settore bancario. Il gruppo ha infettato computer in tutto il mondo e i suoi malware sono stati sviluppati in una serie di malware altamente modulari.Le campagne di Wizard Spider, che utilizzano malware quali Conti, "Ryuk" TrickBot o Black Basta, sono responsabili di rilevanti danni economici nell'Unione europea. Pertanto, Mikhail Mikhailovich Tsarev è coinvolto in attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.	24.6.2024

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
14.	Maksim Sergeevich GALOCHKIN	Максим Сергеевич ГАЛОЧКИН Data di nascita: 19.5.1982 Luogo di nascita: Abakan, Federazione russa Cittadinanza: russa Sesso: maschile	Maksim Galochkin ha preso parte ad attacchi informatici con effetti significativi che costituiscono una minaccia esterna per gli Stati membri dell'UE. Maksim Galochkin è noto anche con i soprannomi online "Benalen", "Bentley", "Volhvb", "volhvb", "manuel", "Max17" e "Crypt". Galochkin svolge un ruolo chiave nell'impiego di programmi malware "TrickBot" e "Conti" ed è coinvolto nel gruppo di minaccia "Wizard Spider" con sede in Russia. Ha guidato un gruppo di tester, con responsabilità per lo sviluppo, la supervisione e l'attuazione di test per il programma malware TrickBot, creato e impiegato da Wizard Spider. Wizard Spider continua a evolversi e a intensificare le sue operazioni. Wizard Spider ha condotto campagne di ransomware in diversi settori, tra cui servizi essenziali come la sanità e il settore bancario. Il gruppo ha infettato computer in tutto il mondo e i suoi malware sono stati sviluppati in una serie di malware altamente modulari. Le campagne di Wizard Spider, che utilizzano malware quali Conti, "Ryuk" TrickBot o Black Basta, sono responsabili di rilevanti danni economici nell'Unione europea. Pertanto, Maksim Galochkin è coinvolto in attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri.	24.6.2024";

2) alla rubrica "B. Persone giuridiche, entità e organismi", la voce 1 è sostituita dalla seguente:

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
"1.	Tianjin Huaying Haitai Science and Technology Development Co. Ltd (Huaying Haitai)	Alias: Haitai Technology Development Co. Ltd Ubicazione: Tianjin, China	Huaying Haitai ha fornito sostegno finanziario, tecnico o materiale e ha agevolato la campagna "Operation Cloud Hopper", una serie di attacchi informatici con effetti significativi, che proviene dall'esterno dell'Unione e costituisce una minaccia esterna per l'Unione o i suoi Stati membri, e di attacchi informatici con effetti significativi nei confronti di Stati terzi. La campagna "Operation Cloud Hopper" ha preso di mira i sistemi di informazione di imprese multinazionali in sei continenti, tra cui imprese situate nell'Unione, e ha ottenuto l'accesso non autorizzato a dati sensibili sotto il profilo commerciale, causando perdite economiche significative. Il soggetto noto pubblicamente come "APT10" ("Advanced Persistent Threat 10") (alias "Red Apollo", "CVNX", "Stone Panda", "MenuPass" e "Potassium") ha condotto la campagna "Operation Cloud Hopper". Huaying Haitai può essere collegata ad APT10. Inoltre, Huaying Haitai impiegava Gao Qiang e Zhang Shilong, entrambi designati in relazione alla campagna "Operation Cloud Hopper". Pertanto, Huaying Haitai è altresì associata a Gao Qiang e a Zhang Shilong.	30.7.2020".