Consiglio dell'Unione europea

Bruxelles, 7 luglio 2026
(OR. en)

8645/26

LIMITE

CORLX 390
CFSP/PESC 586
RELEX 561
CYBER 194
JAI 507
FIN 594

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, otto persone fisiche e quattro entità dovrebbero essere aggiunte all'elenco delle persone fisiche e giuridiche, delle entità e degli organismi soggetti a misure restrittive di cui all'allegato I del regolamento (UE) 2019/796. Tali persone ed entità sono responsabili di attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri, o vi sono coinvolte.

(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 …, …

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
"20.	Vitaly Nikolayevich KOVALEV	Виталий Николаевич КОВАЛЕВ Pseudonimi: "Bentley", "Bergen", "Alex Konor", "Benny", "Ben", "Stern" Data di nascita: 23.6.1988 Indirizzo: Serebristy Bulvar 34 (Serebristyy Bul'var); krp 1; flt 528; 197341; St Petersburg, Russian Federation Cittadinanza: russa Sesso: maschile Entità associate: TrickBot, Wizard Spider, Conti	Vitaly Kovalev è una figura di alto livello nell'ambito dei programmi malware "Trickbot" e "Conti". È conosciuto anche con i soprannomi online "Bentley", "Bergen", "Alex Konor", "Benny", "Ben" e "Stern". Conti e Trickbot sono stati originariamente creati e sviluppati da Wizard Spider. Wizard Spider ha condotto campagne di ransomware in diversi settori, tra cui servizi essenziali quali la sanità e il settore bancario, ha infettato computer in tutto il mondo e i suoi malware sono stati trasformati in una serie di malware altamente modulari. Le campagne di Wizard Spider, che utilizzano malware quali Conti e TrickBot, sono responsabili di rilevanti danni economici nell'Unione europea. Vitaly Kovalev è pertanto responsabile di attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri, e vi è coinvolto.	[+]

[+] GU: inserire la data di pubblicazione del presente regolamento.

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
21.	Alexander Alexandrovich VOLOSOVIK	Александр Александрович ВОЛОСОВИК Data di nascita: 30.1.1983 Luogo di nascita: URSS Cittadinanza: russa N. di passaporto: 762988138 Sesso: maschile Entità associate: Yalishanda, LARVA-34, podzemniyl, Ohyeahhellno, Stas_vl, downlow	Alexander Volosovik è proprietario di Media Land LLC. Dal 2016 Media Land LLC, società di servizi bulletproof hosting, agevola un'ampia gamma di attacchi malware contro l'Unione e a livello mondiale, offrendo servizi di hosting che nascondono le identità degli utenti e resistono alle rimozioni da parte delle autorità di contrasto. Media Land LLC ha consentito operazioni di ransomware su larga scala, servizi di comando e controllo e operazioni di phishing che prendono di mira le infrastrutture critiche e i servizi essenziali negli Stati membri, con conseguenti perdite finanziarie significative. Le operazioni agevolate da Media Land LLC comprendono, tra l'altro, LockBit, EvilCorp e BlackBasta. Media Land LLC è pertanto coinvolta in attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri. In qualità di proprietario di Media Land LLC, Alexander Volosovik è responsabile di tali attacchi informatici e vi è coinvolto. È inoltre associato a Media Land LLC.	+

+ GU: inserire la data di pubblicazione del presente regolamento.

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
22.	Denis Olegovich DEGTYARENKO	Денис Олегович ДЕГТЯРЕНКО Pseudonimo: "Dena" Data di nascita: 9.10.1989 Luogo di nascita: URSS Cittadinanza: russa Sesso: maschile Indirizzo: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation	Denis Degtyarenko, alias Dena, è un hacker russo del CARR (*Cyber Army of Russia Reborn*). Il CARR è stato responsabile di attacchi informatici contro servizi necessari al mantenimento di attività economiche fondamentali e di funzioni statali essenziali negli Stati membri, nonché contro infrastrutture in Ucraina e in altri paesi terzi. È collegato al Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU) (Centro principale per le tecnologie speciali (GTsST), direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU)). Il GTsST continua a condurre attacchi informatici contro l'Unione o i suoi Stati membri. Gli obiettivi del CARR comprendono agenzie governative, istituti finanziari, organi di informazione e infrastrutture critiche negli Stati membri e negli Stati Uniti. Il CARR ha condotto attacchi distribuiti di negazione del servizio (*distributed denial-of-service* – DDoS) in Ucraina e contro governi e imprese situati in paesi che hanno sostenuto l'Ucraina. Denis Degtyarenko, un hacker primario del CARR, è pertanto coinvolto in attacchi informatici con effetti significativi, inclusi i tentati attacchi informatici con effetti potenzialmente significativi, che costituiscono una minaccia esterna per gli Stati membri e contro Stati terzi. In qualità di membro del CARR, è altresì associato al GTsST.	+

+ GU: inserire la data di pubblicazione del presente regolamento.

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
23.	Yuliya Vladimirovna PANKRATOVA	Юлия Владимировна ПАНКРАТОВА Pseudonimo: "YUliYA" Data di nascita: 6.4.1984 Luogo di nascita: URSS Cittadinanza: russa Sesso: femminile Indirizzo: 130 Lenina Avenue, Novy Gorod microdistrict, Orsk, Orenburg Region, Russian Federation	Yuliya Pankratova è un'hacker russa che ha lavorato per il CARR (Cyber Army of Russia Reborn) e fondato Z-Pentest, per il quale continua a lavorare. Il CARR è stato responsabile di attacchi informatici contro servizi necessari al mantenimento di attività economiche fondamentali e di funzioni statali essenziali negli Stati membri, nonché contro infrastrutture in Ucraina e in altri paesi terzi. È collegato al Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU) (Centro principale per le tecnologie speciali (GTsST), direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU)). Il GTsST continua a condurre attacchi informatici contro l'Unione o i suoi Stati membri. Gli obiettivi del CARR comprendono agenzie governative, istituti finanziari, organi di informazione e infrastrutture critiche negli Stati membri e negli Stati Uniti. Il CARR ha condotto attacchi distribuiti di negazione del servizio (*distributed denial-of-service* – DDoS) in Ucraina e contro governi e imprese situati in paesi che hanno sostenuto l'Ucraina.	+

+ GU: inserire la data di pubblicazione del presente regolamento.

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
			Z-Pentest è responsabile di attacchi informatici con effetti significativi contro, tra gli altri, i servizi necessari per il mantenimento di attività fondamentali negli Stati membri. Yuliya Pankratova, un'hacker primaria del CARR e di Z-Pentest, è pertanto coinvolta in attacchi informatici con effetti significativi, inclusi i tentati attacchi informatici con effetti potenzialmente significativi, che costituiscono una minaccia esterna per gli Stati membri, e contro Stati terzi. È inoltre associata a Z-Pentest.	

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
24.	Maksim Evgenevich VORONIN	Максим Евгеньевич ВОРОНИН Pseudonimo: "Daugn0" Cittadinanza: presumibilmente russa Sesso: maschile	Maksim Voronin alias Daugn0 è coinvolto nello sviluppo, nella distribuzione e nella vendita del malware volto a rubare informazioni LummaC2 (alias Lumma Infostealer o Lumma Stealer). LummaC2 è una piattaforma Malware-as-a-Service (MaaS), utilizzata per rubare dati sensibili, credenziali di browser, portafogli di criptovalute o informazioni di sistema, per installare malware aggiuntivi su dispositivi infetti, per il furto di criptovalute e per campagne di spionaggio. Gli attacchi informatici che coinvolgono il malware LummaC2 sono commessi anche da autori di minacce informatiche con motivazioni finanziarie come Storm-113, Storm-1607, Storm-1674, Octo Tempest e altri. Il malware LummaC2 è stato utilizzato per attacchi informatici contro funzioni e servizi statali essenziali necessari per il mantenimento delle attività sociali ed economiche fondamentali degli Stati membri. Nel 2024 e nel 2025 LummaC2 è stato uno degli strumenti più utilizzati per rubare informazioni a livello mondiale. Maksim Voronin, in qualità di sviluppatore, distributore e venditore di LummaC2, è pertanto coinvolto in attacchi informatici con effetti significativi, che costituiscono una minaccia esterna per gli Stati membri, e li agevola.	+

+ GU: inserire la data di pubblicazione del presente regolamento.

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
25.	Maksim Aleksandrovich GORDIENKO alias Maxim Alexandrovich GORDIENKO	Максим Александрович ГОРДИЕНКО Pseudonimo: "Lummaseller" Cittadinanza: presumibilmente russa Sesso: maschile	Maksim Gordienko alias Lummaseller è coinvolto nello sviluppo e nella distribuzione del malware volto a rubare informazioni LummaC2 (alias Lumma Infostealer o Lumma Stealer). LummaC2 è una piattaforma Malware-as-a-Service (MaaS), utilizzata per rubare dati sensibili, credenziali di browser, portafogli di criptovalute o informazioni di sistema, per installare malware aggiuntivi su dispositivi infetti, per il furto di criptovalute e per campagne di spionaggio. Gli attacchi informatici che coinvolgono il malware LummaC2 sono commessi anche da autori di minacce informatiche con motivazioni finanziarie come Storm-113, Storm-1607, Storm-1674, Octo Tempest e altri. Il malware LummaC2 è stato utilizzato per attacchi informatici contro funzioni e servizi statali essenziali necessari per il mantenimento delle attività sociali ed economiche fondamentali degli Stati membri. Nel 2024 e nel 2025 LummaC2 è stato uno degli strumenti più utilizzati per rubare informazioni a livello mondiale. Maksim Gordienko, in qualità di sviluppatore, distributore e venditore di LummaC2, è pertanto coinvolto in attacchi informatici con effetti significativi, che costituiscono una minaccia esterna per gli Stati membri, e li agevola.	+

+ GU: inserire la data di pubblicazione del presente regolamento.

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
26.	Evgeniy Viktorovich BASHEV	Евгений Викторович БАШЕВ Data di nascita: 25.1.1980 Luogo di nascita: URSS Cittadinanza: russa Sesso: maschile Persone associate: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin Entità associate: GRU Unit 29155, "Impuls" LLC	Evgeniy Bashev è membro dell'agenzia di intelligence militare russa GRU, unità 29155. All'interno dell'unità sostiene e agevola attacchi informatici con effetti significativi contro gli Stati membri, tra l'altro attraverso il controllo del server "Aegon", utilizzato per le operazioni di pirateria informatica. In particolare, fornisce sostegno tecnico e materiale agli attacchi informatici dell'unità 29155 del GRU tramite la sua società "Impuls" LLC, che ha agevolato la copertura operativa, le infrastrutture e i pagamenti, e ha gestito le risorse tecniche, compresi i server, utilizzate per gli attacchi informatici. Ha inoltre coordinato la cooperazione tra le strutture del GRU e le reti di hacker esterne. Gli attacchi informatici che ha agevolato hanno preso di mira funzioni, sistemi e servizi statali essenziali necessari per il mantenimento di attività sociali o economiche fondamentali negli Stati membri, in particolare nel settore dei trasporti. Con la campagna WhisperGate, l'unità 29155 del GRU ha preso di mira anche le infrastrutture critiche dell'Ucraina.	+

+ GU: inserire la data di pubblicazione del presente regolamento.

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
			Pertanto, Evgeniy Bashev fornisce sostegno tecnico e materiale per attacchi informatici con effetti significativi, inclusi tentati attacchi informatici con effetti potenzialmente significativi, che costituiscono una minaccia esterna per gli Stati membri, nonché per attacchi informatici con effetti significativi nei confronti di un paese terzo, o vi è altrimenti coinvolto. In qualità di proprietario e direttore generale, è associato alla società "Impuls" LLC. In qualità di membro dell'unità 29155 del GRU, è altresì associato a tale entità.	

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
27.	Roman Alexandrovich PUNTUS	Роман Александрович ПУНТУС Luogo di nascita: Federazione russa Cittadinanza: russa Sesso: maschile Persone associate: Denis Igorevich Denisenko, Yuriy Fedorovich Denisov, Dmitriy Yuryevich Goloshubov, Nikolay Alexandrovich Korchagin, Evgeniy Viktorovich Bashev Entità associate: GRU Unit 29155	Roman Puntus è membro dell'agenzia di intelligence militare russa GRU, unità 29155. All'interno dell'unità, svolge un ruolo guida nell'organizzazione e nel coordinamento degli attacchi informatici con effetti significativi contro gli Stati membri. Sostiene inoltre lo sviluppo della capacità informatica interna dell'unità, comprese l'assunzione di membri del personale come hacker e programmatori e la loro supervisione. Con l'istituzione della società di copertura "Aegeon-Impulse", ha agevolato gli aspetti logistici e finanziari delle operazioni informatiche. Sotto il suo coordinamento, l'unità ha condotto attacchi informatici contro funzioni, sistemi e servizi statali essenziali necessari per il mantenimento di attività sociali o economiche fondamentali negli Stati membri, in particolare nel settore dei trasporti. Con la campagna WhisperGate, l'unità 29155 del GRU ha preso di mira anche le infrastrutture critiche dell'Ucraina.	[+]"

[+] GU: inserire la data di pubblicazione del presente regolamento.

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
			Roman Puntus è pertanto responsabile di attacchi informatici con effetti significativi, inclusi tentati attacchi informatici con effetti potenzialmente significativi, che costituiscono una minaccia esterna per gli Stati membri, nonché di attacchi informatici con effetti significativi nei confronti di un paese terzo, o vi è altrimenti coinvolto. In qualità di membro dell'unità 29155 del GRU, è altresì associato a tale entità.	

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

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
"8.	Media Land LLC	Indirizzo: Tsvetnochnaya st., 16 Litera P, Room 27, Moskovskaya Zastava Municipal District St Petersburg, 196006, Russian Federation Tipo di entità: società a responsabilità limitata Luogo di registrazione: St Petersburg Data di registrazione: 19.10.2015 Numero di registrazione: 1152536009900 Sede principale: St Petersburg, Russian Federation Entità associata: ML.Cloud	Dal 2016 Media Land LLC, società di servizi bulletproof hosting, agevola un'ampia gamma di attacchi malware contro gli Stati membri e a livello mondiale, offrendo servizi di hosting che nascondono le identità degli utenti e resistono alle rimozioni da parte delle autorità di contrasto con conseguenti perdite finanziarie significative. Media Land LLC ha consentito operazioni di ransomware su larga scala, servizi di comando e controllo e operazioni di phishing che prendono di mira le infrastrutture critiche e i servizi essenziali tra gli Stati membri. Le operazioni agevolate da Media Land LLC comprendono, tra l'altro, LockBit, EvilCorp e BlackBasta. Media Land LLC è pertanto coinvolta in attacchi informatici con effetti significativi, che costituiscono una minaccia esterna per gli Stati membri.	[+]

[+] GU: inserire la data di pubblicazione del presente regolamento.

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
9.	ML.Cloud	Indirizzo: Brivibas iela 52, Riga, LV-1011, Latvija; Russian Federation, Kazan, Peterburgskaya st. 52 Luogo di registrazione: Riga Persona associata: Alexander Volosovik Altre entità associate: Media Land LLC	ML.Cloud è la società consorella di Media Land LLC e fornisce l'infrastruttura tecnica per Media Land LLC. Dal 2016 Media Land LLC, società di servizi bulletproof hosting, agevola un'ampia gamma di attacchi malware contro gli Stati membri e a livello mondiale, offrendo servizi di hosting che nascondono le identità degli utenti e resistono alle rimozioni da parte delle autorità di contrasto con conseguenti perdite finanziarie significative. Media Land LLC ha consentito operazioni di ransomware su larga scala, servizi di comando e controllo e operazioni di phishing che prendono di mira le infrastrutture critiche e i servizi essenziali tra gli Stati membri. Le operazioni agevolate da Media Land LLC comprendono, tra l'altro, LockBit, EvilCorp e BlackBasta. Media Land LLC è pertanto coinvolta in attacchi informatici che costituiscono una minaccia esterna con effetti significativi per gli Stati membri dell'UE. ML.,Cloud fornisce pertanto sostegno tecnico per attacchi informatici con effetti significativi, che costituiscono una minaccia esterna per gli Stati membri.	+

+ GU: inserire la data di pubblicazione del presente regolamento.

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
10.	"Impuls" LLC	Общество с ограниченной ответственностью "Импульс" Indirizzo: 344015, Russian Federation, Rostov Region, Rostov-on-Don, ul. Eremenko, d. 56, k. 6, apt. 88 Tipo di entità: società a responsabilità limitata Luogo di registrazione: Interdistrict Inspectorate of the Federal Tax Service No. 26 for the Rostov Region, 344019, Rostov-on-Don, ul. Myasnikova, d. 52/32, Russian Federation Data di registrazione: 27.9.2010	Impuls" LLC è una società russa di proprietà di Evgeniy Viktorovich Bashev, membro dell'agenzia di intelligence militare russa GRU, unità 29155. La società fornisce sostegno tecnico e materiale per attacchi informatici e tentati attacchi informatici condotti dall'unità 29155 del GRU. In particolare, LLC "Impuls" LLC funge da intermediario operativo in quanto consente lo svolgimento di attività connesse alla pirateria informatica attraverso una società formalmente non collegata allo Stato russo. Ha agevolato la copertura operativa, le infrastrutture e i pagamenti per attacchi informatici ed è stata collegata a risorse tecniche, compresi i server utilizzati a sostegno delle attività di pirateria informatica. In particolare, "Impuls" LLC ha consentito la cooperazione tra le strutture del GRU e le reti di hacker esterne.Le operazioni informatiche agevolate da "Impuls" LLC sono state condotte contro funzioni e servizi statali essenziali necessari per il mantenimento di attività sociali e economiche fondamentali negli Stati membri, in particolare nel settore dei trasporti. Con la campagna WhisperGate, l'unità 29155 del GRU ha preso di mira anche le infrastrutture critiche dell'Ucraina.	+

+ GU: inserire la data di pubblicazione del presente regolamento.

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
		Numero di registrazione: INN (ИНН): 6168033776; OGRN (ОГРН): 1106194004850 Sede principale: Russian Federation Persone associate: Evgeniy Bashev Entità associate: GRU Unit 29155	Pertanto, "Impuls" LLC fornisce sostegno tecnico e materiale per attacchi informatici con effetti significativi, che costituiscono una minaccia esterna per gli Stati membri, nonché per attacchi informatici con effetti significativi nei confronti di un paese terzo, o vi è altrimenti coinvolta.	

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
11.	Z-Pentest	Pseudonimi: "Z-Pentest Alliance", "Z-Alliance" Sede principale: Russian Federation Persone associate: Yuliya Pankratova Entità associate: Cyber Army of Russia/CARR Account X.com: ZPentest (sospeso) Account Telegram: Zpentestalliance	Z-Pentest è un gruppo hacktivista filorusso, composto da membri del CARR (Cyber Army of Russia Reborn) e NoName057, che prende di mira a livello mondiale le infrastrutture critiche, in particolare il settore energetico e quello idrico. In particolare, il gruppo ha attaccato un'azienda di servizi idrici danese nel dicembre 2024. Z-Pentest è pertanto responsabile di attacchi informatici con effetti significativi, che costituiscono una minaccia esterna per gli Stati membri.	[+]".

[+] GU: inserire la data di pubblicazione del presente regolamento.