Consiglio
dell'Unione europea

Bruxelles, 13 maggio 2024
(OR. en)

8502/24

LIMITE

CORLX 356
CFSP/PESC 512
RELEX 467
CYBER 110
JAI 572
FIN 341

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) 2024/… 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 129 I del 17.5.2019, pag. 1.

considerando quanto segue:

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

(2) Alla luce dei persistenti e crescenti comportamenti dolosi nel ciberspazio, compresi i comportamenti diretti contro Stati terzi, è opportuno aggiornare i motivi dell'inserimento di sei persone e due entità nell'elenco delle persone fisiche e giuridiche, delle entità e degli organismi soggetti a misure restrittive che figura nell'allegato I del regolamento (UE) 2019/796.

(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 …,

Per il Consiglio
Il presidente

ALLEGATO

L’allegato I del regolamento (UE) 2019/796 ("Elenco delle persone fisiche e giuridiche, delle entità e degli organismi di cui all’articolo 3") è così modificato:

1) nell’elenco dal titolo "A. Persone fisiche", le voci da 3 a 8 sono sostituite dalle seguenti:

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
"3.	Alexey Valeryevich MININ	Алексей Валерьевич МИНИН Data di nascita: 27.5.1972 Luogo di nascita: oblast di Perm, RSFS russa (ora Federazione russa) N. di passaporto: 120017582 Rilasciato da: ministero degli Affari esteri della Federazione russa Validità: dal 17.4.2017 al 17.4.2022 Luogo: Mosca, Federazione russa Cittadinanza: russa Sesso: maschile	Alexey Minin ha partecipato a un tentativo di attacco informatico con effetti potenzialmente significativi contro l'Organizzazione per la proibizione delle armi chimiche (OPCW) nei Paesi Bassi e ad attacchi informatici con effetti significativi contro Stati terzi. In qualità di agente di supporto dell'intelligence della direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU), Alexey Minin faceva parte di una squadra di quattro agenti dell'intelligence militare russa che hanno cercato di ottenere un accesso non autorizzato alla rete Wi-Fi dell'OPCW all'Aia (Paesi Bassi) nell'aprile 2018. Il tentativo di attacco informatico era finalizzato a ottenere un accesso abusivo alla rete Wi-Fi dell'OPCW, che, in caso di successo, avrebbe compromesso la sicurezza della rete e i lavori di indagine dell'OPCW in corso. Il Servizio di intelligence e sicurezza militare dei Paesi Bassi (*Militaire Inlichtingen- en Veiligheidsdienst*) ha sventato il tentativo di attacco informatico, impedendo in tal modo gravi danni all'OPCW. Un grand jury nel distretto occidentale della Pennsylvania (Stati Uniti d'America) ha accusato Alexey Minin, in quanto agente della direzione principale dell'intelligence (GRU) russa, di pirateria informatica, frode telematica, furto aggravato d'identità e riciclaggio.	30.7.2020

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
4.	Aleksei Sergeyvich MORENETS	Алексей Сергеевич МОРЕНЕЦ Data di nascita: 31.7.1977 Luogo di nascita: oblast di Murmanskaya, RSFS russa (ora Federazione russa) N. di passaporto: 100135556 Rilasciato da: ministero degli Affari esteri della Federazione russa Validità: dal 17.4.2017 al 17.4.2022 Luogo: Mosca, Federazione russa Cittadinanza: russa Sesso: maschile	Aleksei Morenets ha partecipato a un tentativo di attacco informatico con effetti potenzialmente significativi contro l'Organizzazione per la proibizione delle armi chimiche (OPCW) nei Paesi Bassi e ad attacchi informatici con effetti significativi contro Stati terzi. In qualità di operatore informatico della direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU), Aleksei Morenets faceva parte di una squadra di quattro agenti dell'intelligence militare russa che hanno cercato di ottenere un accesso non autorizzato alla rete Wi-Fi dell'OPCW all'Aia (Paesi Bassi) nell'aprile 2018. Il tentativo di attacco informatico era finalizzato a ottenere un accesso abusivo alla rete Wi-Fi dell'OPCW, che, in caso di successo, avrebbe compromesso la sicurezza della rete e i lavori di indagine dell'OPCW in corso. Il Servizio di intelligence e sicurezza militare dei Paesi Bassi (*Militaire Inlichtingen- en Veiligheidsdienst*) ha sventato il tentativo di attacco informatico, impedendo in tal modo gravi danni all'OPCW. Un grand jury nel distretto occidentale della Pennsylvania (Stati Uniti d'America) ha accusato Aleksei Morenets, in quanto assegnato all'unità militare 26165, di pirateria informatica, frode telematica, furto aggravato d'identità e riciclaggio.	30.7.2020

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
5.	Evgenii Mikhaylovich SEREBRIAKOV	Евгений Михайлович СЕРЕБРЯКОВ Data di nascita: 26.7.1981 Luogo di nascita: Kursk, RSFS russa (ora Federazione russa) N. di passaporto: 100135555 Rilasciato da: ministero degli Affari esteri della Federazione russa Validità: dal 17.4.2017 al 17.4.2022 Luogo: Mosca, Federazione russa Cittadinanza: russa Sesso: maschile	Evgenii Serebriakov ha partecipato a un tentativo di attacco informatico con effetti potenzialmente significativi contro l'Organizzazione per la proibizione delle armi chimiche (OPCW) nei Paesi Bassi e ad attacchi informatici con effetti significativi contro Stati terzi. In qualità di operatore informatico della direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU), Evgenii Serebriakov faceva parte di una squadra di quattro agenti dell'intelligence militare russa che hanno cercato di ottenere un accesso non autorizzato alla rete Wi-Fi dell'OPCW all'Aia (Paesi Bassi) nell'aprile 2018. Il tentativo di attacco informatico era finalizzato a ottenere un accesso abusivo alla rete Wi-Fi dell'OPCW, che, in caso di successo, avrebbe compromesso la sicurezza della rete e i lavori di indagine dell'OPCW in corso. Il Servizio di intelligence e sicurezza militare dei Paesi Bassi (*Militaire Inlichtingen- en Veiligheidsdienst*) ha sventato il tentativo di attacco informatico, impedendo in tal modo gravi danni all'OPCW. Dalla primavera del 2022 Evgenii Serebriakov guida "Sandworm" (alias "Sandworm Team", "BlackEnergy Group", "Voodoo Bear", "Quedagh", "Olympic Destroyer" e "Telebots"), un soggetto e un gruppo di pirateria informatica affiliato all'unità 74455 della direzione principale dell'intelligence russa. Sandworm ha sferrato attacchi informatici contro l'Ucraina, compresi organismi pubblici ucraini, a seguito della guerra di aggressione della Russia contro l'Ucraina.	30.7.2020

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
6.	Oleg Mikhaylovich SOTNIKOV	Олег Михайлович СОТНИКОВ Data di nascita: 24.8.1972 Luogo di nascita: Ulyanovsk, RSFS russa (ora Federazione russa) N. di passaporto: 120018866 Rilasciato da: ministero degli Affari esteri della Federazione russa Validità: dal 17.4.2017 al 17.4.2022 Luogo: Mosca, Federazione russa Cittadinanza: russa Sesso: maschile	Oleg Sotnikov ha partecipato a un tentativo di attacco informatico con effetti potenzialmente significativi contro l'Organizzazione per la proibizione delle armi chimiche (OPCW) nei Paesi Bassi e ad attacchi informatici con effetti significativi contro Stati terzi. In qualità di agente di supporto dell'intelligence della direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU), Oleg Sotnikov faceva parte di una squadra di quattro agenti dell'intelligence militare russa che hanno cercato di ottenere un accesso non autorizzato alla rete Wi-Fi dell'OPCW all'Aia (Paesi Bassi) nell'aprile 2018. Il tentativo di attacco informatico era finalizzato a ottenere un accesso abusivo alla rete Wi-Fi dell'OPCW, che, in caso di successo, avrebbe compromesso la sicurezza della rete e i lavori di indagine dell'OPCW in corso. Il Servizio di intelligence e sicurezza militare dei Paesi Bassi (*Militaire Inlichtingen- en Veiligheidsdienst*) ha sventato il tentativo di attacco informatico, impedendo in tal modo gravi danni all'OPCW. Un grand jury nel distretto occidentale della Pennsylvania ha accusato Oleg Sotnikov, in quanto agente della direzione principale dell'intelligence (GRU) russa, di pirateria informatica, frode telematica, furto aggravato d'identità e riciclaggio.	30.7.2020

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
7.	Dmitry Sergeyevich BADIN	Дмитрий Сергеевич БАДИН Data di nascita: 15.11.1990 Luogo di nascita: Kursk, RSFS russa (ora Federazione russa) Cittadinanza: russa Sesso: maschile	Dmitry Badin ha partecipato a un attacco informatico con effetti significativi contro il parlamento federale tedesco (*Deutscher Bundestag*) e ad attacchi informatici con effetti significativi contro Stati terzi. In qualità di agente dell'intelligence militare dell'85º Centro principale per i servizi speciali (GTsSS), direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU), Dmitry Badin faceva parte di una squadra di agenti dell'intelligence militare russa che ha condotto un attacco informatico contro il parlamento federale tedesco tra aprile e maggio 2015. Tale attacco ha colpito il sistema informatico del parlamento, compromettendone il funzionamento per diversi giorni. È stato sottratto un ingente volume di dati e sono stati violati gli account di posta elettronica di diversi parlamentari, nonché quello dell'ex cancelliera Angela Merkel. Un grand jury nel distretto occidentale della Pennsylvania (Stati Uniti d'America) ha accusato Dmitry Badin, in quanto assegnato all'unità militare 26165, di pirateria informatica, frode telematica, furto aggravato d'identità e riciclaggio.	22.10.2020

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
8.	Igor Olegovich KOSTYUKOV	Игорь Олегович КОСТЮКОВ Data di nascita: 21.2.1961 Cittadinanza: russa Sesso: maschile	Igor Kostyukov è l'attuale capo della direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU), presso cui ha precedentemente svolto le funzioni di primo vice capo. Tra le unità sotto il suo comando vi è l'85º Centro principale per i servizi speciali (GTsSS), (alias "unità militare 26165", alias: "APT28", "Fancy Bear", "Sofacy Group", "Pawn Storm", "Strontium"). In tale veste, Igor Kostyukov è responsabile degli attacchi informatici condotti dal GTsSS, tra cui quelli con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri. In particolare, agenti dell'intelligence militare del GTsSS hanno partecipato all'attacco informatico contro il parlamento federale tedesco (*Deutscher Bundestag*) tra aprile e maggio 2015, nonché al tentativo di attacco informatico finalizzato a ottenere un accesso abusivo alla rete Wi-Fi dell'Organizzazione per la proibizione delle armi chimiche (OPCW) nei Paesi Bassi nell'aprile 2018. L'attacco informatico contro il parlamento federale tedesco ha colpito il sistema informatico del parlamento, compromettendone il funzionamento per diversi giorni. È stato sottratto un ingente volume di dati e sono stati violati gli account di posta elettronica di diversi parlamentari, nonché quello dell'ex cancelliera Angela Merkel."	22.10.2020

2) nell’elenco dal titolo "B. Persone giuridiche, entità e organismi", le voci 3 e 4 sono sostituite dalle seguenti:

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
"3.	Main Centre for Special Technologies (GTsST) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)	Indirizzo: 22 Kirova Street, Moscow, Russian Federation	Il 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)), noto anche come unità 74455, è coinvolto in attacchi informatici con effetti significativi che provengono dall'esterno dell'Unione e costituiscono una minaccia esterna per l'Unione o i suoi Stati membri e in attacchi informatici con effetti significativi nei confronti di Stati terzi, compresi gli attacchi informatici pubblicamente noti come "NotPetya" o "EternalPetya" nel giugno 2017 e gli attacchi informatici diretti a una rete elettrica ucraina nell'inverno del 2015 e del 2016. "NotPetya" o "EternalPetya" ha reso i dati inaccessibili a diverse imprese nell'Unione, in Europa in generale e nel resto del mondo, compromettendo i computer con ransomware e bloccando l'accesso ai dati e causando così, tra l'altro, perdite economiche significative. L'attacco informatico a una rete elettrica ucraina ha fatto sì che parti della stessa rimanessero spente durante l'inverno.	30.7.2020

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
			Il soggetto pubblicamente noto come "Sandworm" (alias "Sandworm Team", "BlackEnergy Group", "Voodoo Bear", "Quedagh", "Olympic Destroyer" e "Telebots"), che è anche all'origine dell'attacco alla rete elettrica ucraina, è responsabile di "NotPetya" o "EternalPetya". Sandworm ha sferrato attacchi informatici contro l'Ucraina, comprese agenzie governative ucraine e infrastrutture critiche ucraine, a seguito della guerra di aggressione della Russia nei confronti dell'Ucraina. Tali attacchi informatici comprendono campagne di phishing mirato (spear phishing), attacchi malware e ransomware. Il Centro principale per le tecnologie speciali, direzione principale dello Stato maggiore delle forze armate della Federazione russa, ha un ruolo attivo nelle attività informatiche intraprese da Sandworm e può essere collegato a Sandworm.	

	Nome	Informazioni identificative	Motivi	Data di inserimento nell'elenco
4.	85th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU)	Indirizzo: Komsomol'skiy Prospekt, 20, Moscow, 119146, Russian Federation	L'85th Main Centre for Special Services (GTsSS) of the Main Directorate of the General Staff of the Armed Forces of the Russian Federation (GU/GRU) (85º Centro principale per i servizi speciali (GTsSS), direzione principale dello Stato maggiore delle forze armate della Federazione russa (GU/GRU)), (alias "unità militare 26165", alias: "APT28", "Fancy Bear", "Sofacy Group", "Pawn Storm" e "Strontium"), è coinvolto in attacchi informatici con effetti significativi che costituiscono una minaccia esterna per l'Unione o i suoi Stati membri e in attacchi informatici con effetti significativi nei confronti di Stati terzi. In particolare, agenti dell'intelligence militare del GTsSS hanno partecipato all'attacco informatico ai danni del parlamento federale tedesco (*Deutscher Bundestag*) tra aprile e maggio 2015, nonché al tentativo di attacco informatico finalizzato a ottenere un accesso abusivo alla rete Wi-Fi dell'Organizzazione per la proibizione delle armi chimiche (OPCW) nei Paesi Bassi nell'aprile 2018. L'attacco informatico ai danni del parlamento federale tedesco ha colpito il sistema informatico del parlamento, compromettendone il funzionamento per diversi giorni. È stato sottratto un ingente volume di dati e sono stati violati gli account di posta elettronica di diversi parlamentari, nonché quello dell'ex cancelliera Angela Merkel. A seguito della guerra di aggressione della Russia nei confronti dell'Ucraina, il GTsSS ha sferrato attacchi informatici (attacchi di phishing mirato e attacchi basati su malware) contro l'Ucraina.	22.10.2020"